Agencja Restrukturyzacji
i Modernizacji Rolnictwa

adres korespondencyjny
Centrala ARiMR
ul. Poleczki 33, 02-822 Warszawa

Specyfikacja Warunków Zamówienia

w postępowaniu o udzielenie zamówienia publicznego
o wartości równej lub przekraczającej progi unijne
prowadzonym w trybie przetargu nieograniczonego

na:

„Świadczenie usługi polegającej na zapewnieniu systemu ochrony przed wyciekiem informacji (DLP) i 300 godzin konsultacji”

numer referencyjny sprawy: DPiZP.2610.30.2020

wszczętym na podstawie ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019 ze. zm.)

Informacje dotyczące prowadzonego postępowania o udzielenie zamówienia publicznego

A. Dane Zamawiającego

1. Zamawiającym jest:

   Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie (adres: Al. Jana Pawła II 70, 00-175 Warszawa); adres do korespondencji: ul. Poleczki 33, 02-822 Warszawa, tel. 22 595 06 11, adres e-mail: zamowieniapubliczne@arimr.gov.pl;

   REGON: 010613083;

   NIP: 526-19-33-940.
2. Adres strony internetowej prowadzonego postępowania o udzielenie zamówienia publicznego (dalej: *„postępowanie”*): https://platformazakupowa.pl/pn/arimr.
3. Niniejsze postępowanie prowadzone jest w trybie przetargu nieograniczonego na podstawie przepisów ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019 ze zm.; dalej: *„ustawa”*).

B. Pozostałe informacje dotyczące prowadzonego postępowania

1. Zmiany i wyjaśnienia treści Specyfikacji Warunków Zamówienia (dalej: *„SWZ”*) oraz inne dokumenty zamówienia bezpośrednio związane z niniejszym postępowaniem będą zamieszczane na stronie internetowej pod adresem https://platformazakupowa.pl/pn/arimr gdzie należy wybrać zakładkę „postępowania”, a następnie przejść na formularz niniejszego postępowania.
2. Postępowanie prowadzone jest w języku polskim. Komunikacja między Zamawiającym a Wykonawcami w niniejszym postępowaniu odbywa się przy użyciu środków komunikacji elektronicznej, tj. Platformy Zakupowej dostępnej pod adresem https://platformazakupowa.pl/pn/arimr (dalej: *„Platforma Zakupowa”*).
3. Poniżej Zamawiający przedstawia wymagania techniczno-organizacyjne związane z udziałem Wykonawców w postępowaniu:
   3.1. Złożenie oferty możliwe jest przez Wykonawców, którzy posiadają konto na Platformie Zakupowej oraz przez Wykonawców nieposiadających konta na Platformie Zakupowej. W celu założenia konta na Platformie Zakupowej należy wybrać zakładkę „Zaloguj się” w kolejnym kroku należy wybrać „Załóż konto”, następnie należy wypełnić formularze i postępować zgodnie z poleceniami wyświetlającymi się na ekranie monitora. W przypadku Wykonawców niezalogowanych w celu złożenia oferty niezbędne jest podanie adresu e-mail (na który wysłane będzie potwierdzenie złożenia oferty), nr NIP oraz nazwy firmy i nr telefonu.
   3.2. Złożenie oferty oraz oświadczenia, o którym mowa w art. 125 ustawy, składanych w trakcie toczącego się postępowania wymaga od Wykonawcy posiadania kwalifikowanego podpisu elektronicznego.
   3.3. Wykonawca składa ofertę, która w przypadku prawidłowego złożenia oferty zostaje automatycznie zaszyfrowana przez system. Nie jest możliwe zapoznanie się z treścią złożonej oferty przed upływem terminu otwarcia ofert.
   3.4. W przypadku przekazywania w postępowaniu dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym podpisem elektronicznym jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku kwalifikowanym podpisem elektronicznym.
4. Zamawiający, zgodnie z § 11 ust. 2 Rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (t.j. Dz. U. z 2020 r. poz. 2452; dalej: *„Rozporządzenie w sprawie środków komunikacji”*), udostępnia informacje na temat specyfikacji połączenia, formatu przesyłanych danych oraz szyfrowania i oznaczania czasu przekazania i odbioru danych umożliwiających pracę na Platformie Zakupowej, tj.:
   4.1. stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
   4.2. komputer klasy PC lub MAC, o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10.4, Linux, lub ich nowsze wersje,
   4.3. zainstalowana dowolna przeglądarka internetowa; w przypadku Internet Explorer minimalnie wersja 10.0.,
   4.4. włączona obsługa JavaScript,
   4.5. zainstalowany program Adobe Acrobat Reader, lub inny obsługujący format plików PDF.
   4.6. Platforma Zakupowa działa według standardu przyjętego w komunikacji sieciowej - kodowanie UTF8,
5. Zamawiający, zgodnie z § 11 ust. 2 Rozporządzenia w sprawie środków komunikacji, określa dopuszczalne formaty przesyłanych danych, tj. plików o wielkości do 150 MB. Zalecany format: PDF.
6. Zamawiający, zgodnie z § 11 ust. 2 Rozporządzenia w sprawie środków komunikacji, określa informacje na temat szyfrowania oraz czasu przekazania i odbioru danych, tj.:
   6.1. Szyfrowanie na Platformie Zakupowej (platformazakupowa.pl) odbywa się za pomocą protokołu TLS 1.3.
   6.2. Plik załączony przez Wykonawcę na Platformie Zakupowej i zapisany nie jest widoczny dla Zamawiającego, gdyż jest w systemie jako zaszyfrowany. Możliwość otworzenia pliku dostępna jest dopiero po odszyfrowaniu przez system, co następuje po upływie terminu otwarcia ofert,
   6.3. Oznaczenie czasu przekazania i odbioru danych przez Platformę Zakupową stanowi przypiętą do oferty elektronicznej datę oraz dokładny czas (hh:mm:ss), znajdujące się w kolumnie dotyczącej danej oferty, w sekcji - "Data złożenia oferty”.
7. Zamawiający określa dopuszczalny format kwalifikowanego podpisu elektronicznego w przypadku:
   7.1. dokumentów sporządzonych w formacie PDF zaleca się podpisanie dokumentu podpisem w formacie PAdES;

7.2. dokumentów sporządzonych w formacie innym niż PDF zaleca się podpisanie dokumentu podpisem w formacie XAdES.

8. Wykonawca przystępując do niniejszego postępowania akceptuje warunki korzystania z Platformy Zakupowej, określone w Regulaminie zamieszczonym na stronie internetowej pod adresem https://platformazakupowa.pl/pn/arimr w zakładce „Regulamin" oraz uznaje go za wiążący.
9. Zamawiający informuje, że instrukcje korzystania z Platformy Zakupowej dotyczące w szczególności logowania, pobrania dokumentacji, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu Platformy Zakupowej znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem https://platformazakupowa.pl/pn/arimr.
10. Korzystanie z Platformy Zakupowej jest bezpłatne. W celu ułatwienia Wykonawcom korzystania z Platformy Zakupowej operator platformy uruchomił Centrum Wsparcia Klienta, które służy pomocą techniczną od 8:00 do 17:00 w dni robocze od poniedziałku do piątku pod numerem telefonu 22 101 02 02 lub e-mai: **cwk@platformazakupowa.pl.**

Rozdział I. Przedmiot zamówienia

I.1. Opis przedmiotu zamówienia

1. Kod Wspólnego Słownika Zamówień (CPV).
   1.1. Główny kod: 79111000-5 [usługi w zakresie doradztwa prawnego]
2. Przedmiotem zamówienia jest zakup przez Agencję Restrukturyzacji i Modernizacji Rolnictwa w Warszawie, zwaną dalej „Zamawiającym", usługi polegającej na zapewnieniu systemu ochrony przed wyciekiem informacji (ang. DLP - Data Loss Protection, dalej „system DLP") i 300 godzin konsultacji.
3. Zamawiający wymaga, by systemem objętych było 12 tys. użytkowników lub 15 tys. urządzeń (komputery, laptopy, urządzenia mobilne) oraz dodatkowo 20 serwerów plików.
4. System musi umożliwiać ochronę przed wyciekiem informacji z systemów informatycznych Zamawiającego.
5. System musi realizować swoje funkcje zarówno na poziomie sieci (Network DLP) oraz stacji końcowej jak komputer, laptop, urządzenie mobilne (Endpoint DLP).
6. Zarządzanie, obsługa incydentów, oraz raportowanie musi być spójne dla ochrony na poziomie sieci i stacji końcowych i odbywać się z pojedynczej webowej konsoli zarządzającej.
7. Dostęp do konsoli zarządzającej powinien odbywać się w bezpiecznym połączeniu https.
8. Ochrona informacji powinna odbywać się w oparciu o reguły bezpieczeństwa informacji odzwierciedlające procesy biznesowe.
9. System musi umożliwiać monitorowanie i ochronę wielu typowych kanałów komunikacyjnych, w szczególności:
   9.1. http oraz https,
   9.2. email,
   9.3. komunikatory internetowe.
10. System musi umożliwiać definiowanie własnych kanałów transmisji, które mają być monitorowane.
11. System w zakresie stacji końcowej musi umożliwiać monitorowanie takich czynności jak kopiowanie informacji na zewnętrzne nośniki danych, nagrywanie płyt, lokalne drukowanie, wklejanie informacji w okna aplikacji.
12. System musi umożliwiać tworzenie polityk uwzględniających takie akcje jak:
    12.1. wysyłanie powiadomień w ramach odnotowanych incydentów, przy czym powiadamiane powinny być następujące osoby:
    - nadawca, czyli osoba, która wysyłała informacje,
    - zwierzchnik nadawcy,
    - właściciel informacji zdefiniowany w polityce,
    - właściciel polityki,
    12.2. blokowanie transmisji naruszających zdefiniowaną politykę,
    12.3. kwarantannę informacji,
    12.4. szyfrowanie informacji,
    12.5. umożliwienie użytkownikowi kontynuowania operacji po zatwierdzeniu komunikatu wyświetlonego przez agenta ochrony informacji na stacji końcowej.
13. System musi umożliwiać łączenie polityk w grupy.
14. System musi umożliwiać budowanie polityk ochrony informacji uwzględniając kontekst w jakim informacja jest używana, czyli musi uwzględniać okoliczności jak:
    14.1. kto wysyła informacje,
    14.2. gdzie informacje są wysyłane,
    14.3. w jaki sposób informacje są wysyłane,
    14.4. co jest wysyłane, czyli właściwa identyfikacja treści.
15. System musi wykorzystywać szeroką gamę mechanizmów identyfikowania treści, m.in.:
    15.1. słowa kluczowe,
    15.2. wyrażenia regularne,
    15.3. tworzenie odcisku palca – fingerprinting,
    15.4. algorytmy Machine Learning,
    15.5. weryfikacja klasyfikacji treści w przypadku, gdy stosowane jest rozwiązanie typu „Data Classification".
16. Algorytm tworzenia odcisku palca powinien działać tak, aby chronić informacje zawarte w pliku (również jego fragmenty), a nie wyłącznie dokument w całości.
17. System powinien również umożliwić tworzenie odcisków palca z zasobów zawartych w bazach danych. Tworzenie takich odcisków powinno odbywać się bez uprzedniego kopiowania informacji do pliku (np. za pomocą ODBC).
18. System musi zawierać predefiniowane reguły ochrony informacji, dotyczące np. numerów krat kredytowych, IBAN, oraz takich identyfikatorów jak PESEL, REGON, NIP, nr Dowodu Osobistego.
19. System musi umożliwiać integrację z usługami katalogowymi (minimum AD DS, lub Azure AD) umożliwiająca m.in.:
    19.1. przypisywanie użytkowników i grup jako autoryzowanych nadawców i odbiorców monitorowanych informacji,
    19.2. przypisanie użytkowników do ról zarządzających takich jak administrator, audytor, manager incydentów,
    19.3. wyświetlanie szczegółów dotyczących użytkownika w ramach incydentu związanego z jego aktywnością, np. powinno być możliwe wyświetlenie informacji o zwierzchniku użytkownika.

20. System musi umożliwiać zautomatyzowane wykrywanie informacji objętych politykami ochrony na serwerach i stacjach końcowych w sieci Zamawiającego (funkcjonalność Discovery). Funkcjonalność ta powinna być również oferowana dla folderów Exchange, Exchange Online, serwera SharePoint, Sharepoint Online.
21. Konsola zarządzająca powinna zawierać ekran przedstawiający podstawowe statystki aktywności z ostatnich 24 godzin jak ilość incydentów względem ważności, najczęściej naruszane kategorie polityk, stacje końcowe, na których wykryto najwięcej naruszeń, etc.
22. Konsola zarządzająca powinna umożliwiać zarządzanie incydentami, m.in. zmianę ich statusu, przekazywanie do innego administratora.
23. System musi umożliwić ziarnistą delegację uprawnień do konfiguracji systemu, polityk, raportów oraz incydentów w oparciu o wbudowane jak również własne role, takie jak administrator, audytor, manager incydentów.
24. System w ramach odnotowanych incydentów musi udostępniać informacje dotyczące reguły, która została naruszona, jak również kopię informacji, która była przesyłana. Wgląd w tak szczegółowe informacje powinien być kontrolowany zgodnie z uprawnieniami administratora.
25. System powinien umożliwiać rozpoznawanie tekstu zawartego w plikach graficznych (OCR) i jego analizę pod względem wrażliwości informacji. Ta funkcjonalność powinna być oferowana co najmniej dla dokumentów graficznych wysyłanych poprzez styk z Internetem (smtp, http, https).
26. Oprogramowanie klienckie (Endpoint) powinno być oferowane w polskiej wersji językowej.
27. System powinien być zaopatrzony we własny moduł analityczny, który umożliwi wskazanie z listy incydentów tych najbardziej istotnych poprzez ich korelacje i grupowanie. System musi zwrócić alert w przypadku zwiększonej ilości zdarzeń mających wspólne źródło np. w jednym konkretnym użytkowniku.
28. System powinien posiadać możliwość rozbudowy o ochronę informacji przechowywanej w aplikacjach oferowanych jako SaaS, w szczególności MS O365 oraz Google for Business.
29. Ochrona informacji w chmurze powinna opierać się o te same mechanizmy stosowane w rozwiązaniu lokalnym włączając Fingerprinting oraz Machine Learning.
30. System musi posiadać funkcjonalność klasyfikowania informacji (w tym plików oraz wiadomości pocztowych email), lub w pełni integrować się z takim rozwiązaniem.

W zakresie klasyfikacji informacji, o której mowa w pkt. 30 powyżej, system powinien posiadać następujące funkcje:

1. Definiowanie dowolnych nazw dla poziomów klasyfikacji (np.: typ, klient, departament, projekt itp.),
2. Definiowanie dowolnych nazw dla klasyfikacji (np.: wewnętrzna – poufna - dane osobowe, kadry – produkcja - księgowość, Projekt X – Projekt Y, itd.).
3. Definiowane klasyfikacji opartej o:
   3.1. listę jednokrotnego wyboru,
   3.2. listę wielokrotnego wyboru (ze zdefiniowaniem minimalnej i maksymalnej liczby zaznaczeń),
   3.3. dowolny ciąg znaków, tzw. „sygnatura/znak sprawy" (z możliwością zdefiniowania szablonu logicznego dla takiego ciągu znaków).
4. Tworzenie klasyfikacji wielopoziomowej (minimum 5 poziomów oznaczeń klasyfikacji).
5. Definiowanie automatycznego nadawania klasyfikacji w oparciu o analizę treści informacji.
6. Klasyfikowanie dokumentu w następujących aplikacjach natywnych służących do edycji danego typu dokumentu (z poziomu aplikacji, a nie klasyfikowanie z poziomu plików):
   6.1. MS Word,
   6.2. MS Excel,
   6.3. MS PowerPoint,
   6.4. MS Visio,
   6.5. MS Project.
7. Wyświetlanie informacji o nadanej klasyfikacji, podczas edycji dokumentu w aplikacji natywnej.
8. Wyświetlanie przycisków klasyfikacji na wstążce aplikacji w postaci zarówno kolorowych pól (kolory zdefiniowane dla danego poziomu klasyfikacji), jak również w postaci dowolnie zdefiniowanych grafik/ikonek.
9. Dynamiczne wyświetlanie poziomów klasyfikacji tzn. możliwość wyboru podkategorii pojawia się dopiero po wybraniu przez użytkownika tej kategorii, dla której można/należy wybrać podkategorię.
10. Możliwość klasyfikowania plików (nie tylko MS Office, ale i innych plików kompatybilnych z technologią XMP, np. PDF, ZIP, itd.), plików tekstowych, obrazów itp.
11. Klasyfikowanie pliku/dokumentu z użyciem menu kontekstowego systemu operacyjnego (bez potrzeby jego otwierania).
12. Masowe nadanie klasyfikacji plikom/dokumentom poprzez:
    12.1. wskazanie folderu (z lub bez podfolderów) z plikami/dokumentami do oznaczenia,
    12.2. zdefiniowanie filtrów oznaczania (np. wszystkie pliki, których nazwa lub rozszerzenie zawiera wskazany wyróżnik),
    12.3. możliwe klasyfikowanie poprzez narzędzie z interfejsem okienkowym i poprzez polecenia konsoli tekstowej.
13. Wymuszanie na użytkowniku dokonania klasyfikacji, jeśli użytkownik tego nie zrobi:
    13.1. w wiadomości email MS Outlook,
    13.2. w dokumentach edytowalnych (w odniesieniu do aplikacji natywnej służącej do edycji danego dokumentu).
14. Wyświetlanie podpowiedzi/ostrzeżeń dotyczących wymogów klasyfikacji dla użytkownika lub innych informacji w zależności od podejmowanych działań przez użytkownika odnośnie informacji sklasyfikowanej na danym poziomie.

15. Wymuszanie na użytkowniku podania uzasadnienia dla wykonywanego działania odnośnie informacji sklasyfikowanej na danym poziomie.
16. Automatyczne wstawianie (dla wybranego poziomu klasyfikacji i w odniesieniu do aplikacji natywnej służącej do edycji danego dokumentu):
    16.1. stopek/nagłówków (także grafiki),
    16.2. znaków wodnych (także grafiki),
    16.3. prefiksów,
    16.4. osoby klasyfikującej,
    16.5. daty nadania klasyfikacji.
17. Wymuszanie szyfrowania poczty elektronicznej.
18. Dokonanie zmiany lub uniemożliwienie zmiany klasyfikacji dokumentu lub dokonanie zmiany wyłącznie w jednym kierunku (np. tylko podwyższenie poziomu klasyfikacji) przez użytkowników/ autora dokumentu.
19. Informacja o klasyfikacji dokumentu zapisywana jest w metadanych dokumentu.
20. Poziom klasyfikacji maila jest zapisywany w nagłówku wiadomości mail (X-Header).
21. We wszystkich aplikacjach natywnych służących do edycji danego typu dokumentu interfejs związany z klasyfikacją informacji jest taki sam.
22. Możliwe jest opcjonalne rozbudowanie systemu o automatyczne i działające na bieżąco klasyfikowanie maili przychodzących do organizacji (na poziomie serwera Exchange).
23. Możliwe jest opcjonalne rozbudowanie systemu o komponenty dla serwera Sharepoint 2013 i wyższych, aby Sharepoint mógł odczytywać i interpretować nadane poziomy klasyfikacji.
24. Możliwe jest opcjonalne rozbudowanie systemu o komponent na urządzenia mobilne, który pozwoli na klasyfikowanie maili na urządzeniu mobilnym (Android, iOS).
25. Dla uruchomienia klasyfikacji i dystrybucji polityk system nie wymaga serwera bazy danych lub innych rozwiązań serwerowych.
26. Publikacja polityk do użytkowników może być realizowana przez współdzielony katalog (network share), lokalną usługę dystrybucji oprogramowania, lub serwis chmurowy.
27. Reguły dla klienta pocztowego odnośnie możliwości przesyłania maili o wskazanych poziomach klasyfikacji są definiowane w oparciu o nazwy domen pocztowych oraz w oparciu o grupy użytkowników (AD DS lub Azure AD).
28. Możliwe jest zdefiniowanie kilku zestawów polityk (o zróżnicowanym poziomie restrykcji) i ich odpowiedni przydział do wskazanych osób zgodnie z pozycją w strukturach zarządczych w organizacji.
29. Możliwa jest automatyczna instalacja oprogramowania na stacjach użytkowników z wykorzystaniem narzędzi do automatycznej zdalnej instalacji.
30. System umożliwia pracę użytkownikowi (klasyfikowanie dokumentów, działanie polityk) także w przypadku gdy komputer użytkownika nie ma połączenia z siecią organizacji.
31. System zapisuje (loguje) wszystkie zdarzenia związane z klasyfikowaniem informacji, działaniem zdefiniowanych reguł/polityk.
32. Interfejs użytkownika końcowego w języku polskim (wszystkie nazwy, komunikaty, przyciski, opisy, itd.). Możliwe jest dostosowanie treści do terminologii i konwencji przyjętej w organizacji.
33. Informacja o poziomie klasyfikacji dokumentu, nadanej za pośrednictwem systemu klasyfikacji, może być wykorzystana przy tworzeniu polityk.
34. System integruje się z rozwiązaniami DLP Discovery (system Discovery po zidentyfikowaniu dokumentu zawierającego informacje spełniające zadane kryteria może automatycznie nadać klasyfikację wg poziomów zdefiniowanych w systemie klasyfikacji).
35. Do instalacji/działania systemu nie są wymagane żadne elementy/komponenty producentów trzecich (np. bazy danych).
36. System musi pracować w systemie wysokiej dostępności (High Availability).
37. Zamawiający wymaga, aby wykonanie przedmiotu zamówienia nastąpiło na warunkach i zasadach określonych projektowanych postanowieniach umowy wraz z załącznikami, stanowiącym Załącznik nr 7 do SWZ.

I.2. Opis części zamówienia

1. Zamawiający nie dopuszcza składania przez Wykonawcę ofert częściowych w rozumieniu art. 7 pkt 15) ustawy.
2. Zamawiający wskazuje powody niedokonania podziału zamówienia na części, ponieważ system DLP stanowi jednorodną całość, zatem podział na części mógłby spowodować nadmierne trudności techniczne w trakcie realizacji umowy, w szczególności poprzez rozmycie odpowiedzialności za prawidłowe działanie oprogramowania i w konsekwencji przenoszenie odpowiedzialności pomiędzy wykonawcami poszczególnych części zamówienia (dotyczy to szczególnie odpowiedzialności za poprawność wdrożenia systemu oraz świadczenie usługi wsparcie i asysty technicznej).
   Ponadto koniecznym byłoby skoordynowanie działań różnych wykonawców realizujących poszczególne części zamówienia, zaś w przypadku jakichkolwiek utrudnień we współpracy z różnymi wykonawcami mogłaby zagrozić właściwemu wykonaniu zamówienia i doprowadzić do odmiennych i niekompatybilnych działań naprawczych. W przypadku przedmiotowego zamówienia, podział na części, bez względu na przyjęte kryterium podziału, zwiększa realne ryzyko niezłożenia ofert na wszystkie części zamówienia. Brak rozstrzygnięcia jakiejkolwiek części zamówienia jest nie do zaakceptowania z uwagi na konieczność zabezpieczenia realizacji istotnych potrzeb Zamawiającego.

I.3. Powierzenie Podwykonawcy wykonania części zamówienia

1. Zamawiający dopuszcza powierzenie Podwykonawcom wykonania części zamówienia.

2. Wykonawca zobowiązany jest do wskazania w ofercie części zamówienia, której wykonanie zamierza powierzyć Podwykonawcy oraz do podania firm Podwykonawców, jeżeli są już znani.

I.4. Pozostałe istotne elementy związane z przedmiotem zamówienia

1. Zamawiający nie przewiduje udzielenie zamówień, o których mowa w art. 214 ust. 1 pkt 7) ustawy.
2. Zamawiający nie dopuszcza składania ofert wariantowych w rozumieniu ustawy.
3. Zamawiający nie przewiduje zawarcia umowy ramowej, jak również nie przewiduje przeprowadzenia aukcji elektronicznej.
4. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
5. Wszelkie rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).

Rozdział II. Termin wykonania zamówienia

Zamawiający wymaga realizacji zamówienia w następujących terminach:

1. wdrożenia systemu DLP w terminie nie przekraczającym 90 Dni Roboczych od dnia zawarcia Umowy,
2. przekazania do akceptacji Projektu Technicznego wraz z harmonogramem realizacji w terminie do 21 Dni Roboczych od daty zawarcia Umowy,
3. korzystania z Usługi Asysty Technicznej w okresie 36 miesięcy od dnia podpisania bez zastrzeżeń Protokołu Wdrożenia.

** Definicje „wdrożenia", „Dni Roboczych", „Projektu Technicznego, „Usługi Asysty Technicznej" zostały opisane w §1 projektowanych postanowień umowy wraz z załącznikami, stanowiących Załącznik nr 7 do SWZ.*

Rozdział III. Podstawy wykluczenia oraz warunki udziału w postępowaniu, jednolity europejski dokument zamówienia

1. O zamówienie objęte niniejszym postępowaniem mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu z postępowania na podstawie przesłanek wskazanych w Rozdz. III.1. SWZ oraz spełniają warunki udziału w postępowaniu opisane w Rozdz. III.2 SWZ.
2. Wykonawca jest zobowiązany wykazać, że spełnia warunki udziału w postępowaniu i nie podlega wykluczeniu z postępowania. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia brak podstaw wykluczenia, o których mowa w Rozdz. III.1 SWZ musi wykazać każdy Wykonawca z osobna.
3. Zamawiający informuje, że zgodnie z procedurą wskazaną w art. 139 ust. 1 ustawy, najpierw dokona badania i oceny ofert, a następnie dokona kwalifikacji podmiotowej Wykonawcy, którego oferta została najwyżej oceniona (na podstawie kryteriów oceny ofert określonych w SWZ) w zakresie braku podstaw wykluczenia oraz spełniania warunków udziału w postępowaniu.

III.1. Podstawy wykluczenia

1. Z postępowania, na podstawie art. 108 ust. 1 ustawy, Zamawiający wykluczy Wykonawcę:
   1.1. będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
      1.1.1. udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
      1.1.2. handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
      1.1.3. o którym mowa w art. 228-230a, art. 250a Kodeksu karnego lub w art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie,
      1.1.4. finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
      1.1.5. o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
      1.1.6. powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej,
      1.1.7. przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,
      1.1.8. o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej

   – lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;
   1.2. jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1.1.;
   1.3. wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że Wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
   1.4. wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
   1.5. jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty,

oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;

1.6. jeżeli, w przypadkach, o których mowa w art. 85 ust. 1 ustawy, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego Wykonawcy lub podmiotu, który należy z Wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.

2. Z postępowania, na podstawie art. 109 ust. 1 pkt 4) ustawy, Zamawiający wykluczy Wykonawcę:

2.1. w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury.

III.2. Warunki udziału w postępowaniu

1. O niniejsze zamówienie mogą ubiegać się Wykonawcy spełniający warunki udziału w postępowaniu w zakresie:

1.1. **Zdolności technicznej lub zawodowej.** Zamawiający uzna, że Wykonawca spełnia warunek udziału we wskazanym zakresie, jeżeli Wykonawca wykaże, że:

1.1.1. wykonał, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, **1 usługę polegającą na zapewnieniu ochrony przed wyciekiem informacji (system DLP) obejmujący nie mniej niż 5 000 użytkowników lub urządzeń, o wartości nie mniejszej niż 2 000 000,00 zł brutto (słownie: dwa miliony złotych 00/100) dla każdej umowy.**

UWAGA 1

Jeżeli wartość usługi wskazanej w wykazie jest podana w walucie innej niż PLN, Wykonawca zobowiązany jest, na potrzeby niniejszego postępowania, dokonać przeliczenia jej wartości na PLN wg średniego kursu NBP (www.nbp.pl tabela A – tabela kursów średnich walut obcych) z dnia zakończenia usługi o zakresie jak wyżej wraz z podaniem kursu oraz daty jego obowiązywania (zgodnie z tabelą A – tabela kursów średnich walut obcych) wg których dokonano przeliczenia; w przypadku usług nadal realizowanych - wg tabeli kursów średnich walut obcych z dnia rozpoczęcia realizacji danej usługi.

1.1.2. dysponuje co najmniej następującymi osobami, które zostaną skierowane przez Wykonawcę do realizacji zamówienia, legitymującymi się odpowiednimi kwalifikacjami zawodowymi i doświadczeniem niezbędnym do wykonania zamówienia:

1.1.2.1. jednym inżynierem, który posiadaja wiedzę, doświadczenie i potwierdzone kwalifikacje specjalistyczne potwierdzone certyfikatem wystawionym przez producenta potwierdzającymi stopień kwalifikacji na poziomie inżyniera lub wyższym oraz brały udział w roli inżyniera we wdrożeniu co najmniej 2 systemów ochrony przed wyciekiem danych, w ciągu ostatnich 3 lat przed upływem terminu składania ofert, przy czym okres pełnienia roli inżyniera nie może być krótszy niż 6 miesięcy,

1.1.2.2. jednym analitykiem, który posiada wiedzę, doświadczenie i potwierdzone kompetencje udziałem w roli analityka w co najmniej 2 projektach polegających na budowie i wdrożeniu systemu ochrony przed wyciekiem informacji, w ciągu ostatnich 3 lat przed upływem terminu składania ofert, przy czym okres pełnienia roli analityka nie może być krótszy niż 6 miesięcy,

1.1.2.3. jednym inżynierem bezpieczeństwa informacji, który posiada wiedzę, doświadczenie z zakresu bezpieczeństwa informacji i potwierdzone kompetencje we wdrożeniu co najmniej 2 systemów informatycznych, w ciągu ostatnich 3 lat przed upływem terminu składania ofert, przy czym czas pełnienia roli inżyniera bezpieczeństwa informacji nie może być krótszy niż 6 miesięcy.

UWAGA 2

Zamawiający wyraża zgodę na łączenie roli inżyniera i inżyniera bezpieczeństwa informacji.

1.1.3. posiada certyfikat w zakresie zarządzania bezpieczeństwem informacji ISO/IEC 27001 lub równoważny, wystawiony przez jednostkę akredytowaną do certyfikacji systemu zarządzania ISO/IEC 27001 i opatrzonego znakiem akredytacji.

UWAGA 3

W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z Wykonawców, którzy wykonają usługi, do realizacji których te zdolności są wymagane. W takiej sytuacji Wykonawca składa wraz z ofertą oświadczenie w zakresie wskazania, które usługi wykonają poszczególni Wykonawcy (członkowie konsorcjum). Wzór oświadczenia stanowi Załącznik nr 4 do SWZ.

2. Ocena spełniania ww. warunków dokonana zostanie w oparciu o informacje zawarte we właściwych dokumentach wyszczególnionych w Rozdz. IV niniejszej SWZ. Z treści złożonych dokumentów musi wynikać jednoznacznie, iż ww. warunki Wykonawca spełnił.

Rozdział IV. Zawartość ofert, wykaz podmiotowych środków dowodowych

1. W zakresie nieuregulowanym postanowieniami SWZ zastosowanie mają przepisy rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od Wykonawcy (Dz. U. z 2020 r. poz. 2415, dalej: „*Rozporządzenie w sprawie rodzajów podmiotowych środków dowodowych*").

2. Jeżeli Wykonawca nie złożył oświadczenia, o którym mowa w art. 125 ust. 1 ustawy, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu lub są one niekompletne lub zawierają błędy, Zamawiający wzywa Wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w terminie przez siebie wskazanym, chyba że:
   2.1. oferta Wykonawcy podlega odrzuceniu bez względu na ich złożenie, uzupełnienie lub poprawienie lub
   2.2. zachodzą przesłanki unieważnienia postępowania.

IV.1. Zawartość ofert

1. Ofertę należy złożyć pod rygorem nieważności w formie elektronicznej, podpisaną kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Wykonawca składa ofertę na Formularzu Ofertowym wg Załącznika nr 1 do SWZ **za pośrednictwem Platformy Zakupowej**.
2. Wykonawca obowiązany jest złożyć wraz z ofertą następujące dokumenty:
   2.1. Odpis lub informację z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru, w celu potwierdzenia, że osoba działająca w imieniu Wykonawcy jest umocowana do jego reprezentowania.
   2.2. Pełnomocnictwo lub inny dokument potwierdzający umocowanie osoby działającej w imieniu Wykonawcy do jego reprezentowania, jeżeli oferta nie została podpisana przez osoby upoważnione do tych czynności dokumentem rejestracyjnym, o którym mowa w pkt. 2.1.
   2.3. Dowód wniesienia wadium. Jeżeli Wykonawca wnosi wadium w formie gwarancji lub poręczenia Wykonawca przekazuje Zamawiającemu oryginał gwarancji lub poręczenia, w postaci elektronicznej. W przypadku wniesienia wadium w innej formie niż pieniądz, powinno ono obowiązywać przez cały okres związania ofertą.
   2.4. Zobowiązanie podmiotów udostępniających zasoby do oddania Wykonawcy do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie będzie dysponował niezbędnymi zasobami, jeżeli Wykonawca powołuje się na zasoby innych podmiotów. Zobowiązanie winno być podpisane przez osobę upoważnioną do reprezentacji podmiotu udostępniającego zasoby. Zapisy pkt 2.1. i 2.2. oraz Rozdz. IV.5 SWZ stosuje się odpowiednio.
   2.5. Aktualne na dzień składania ofert oświadczenie w formie jednolitego europejskiego dokumentu zamówienia (dalej: „*JEDZ*") sporządzone zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji (UE) 2016/7 z dnia 5 stycznia 2016 r. ustanawiającym standardowy formularz jednolitego europejskiego dokumentu zamówienia (Dz. Urz. UE L 3 z 06.01.2016, str. 16). Dokument JEDZ należy złożyć pod rygorem nieważności w formie elektronicznej. Dokument JEDZ musi być opatrzony kwalifikowanym podpisem elektronicznym.
   2.6. Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia w zakresie wskazania, które usługi wykonają poszczególni Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (członkowie konsorcjum). Wzór oświadczenia stanowi Załącznik nr 4 do SWZ.

IV.2 Oświadczenie w formie Jednolitego Europejskiego Dokumentu Zamówienia

1. Wykonawca wypełnia JEDZ, tworząc dokument w postaci elektronicznej. Wykonawca może korzystać z narzędzia ESPD lub innych dostępnych narzędzi lub oprogramowania, które umożliwiają wypełnienie JEDZ i utworzenie dokumentu w postaci elektronicznej.
   1.1. Zamawiający udostępnia Wykonawcom plik, w formacie XML, wygenerowany z narzędzia ESPD, który stanowi Załącznik nr 8 do SWZ.
   1.2. Zamawiający informuje, że pod adresem: https://espd.uzp.gov.pl Urząd Zamówień Publicznych udostępnił nieodpłatne narzędzie umożliwiające zamawiającym i wykonawcom utworzenie, wypełnienie i ponowne wykorzystanie standardowego formularza JEDZ (JEDZ/ESPD) w wersji elektronicznej (eESPD).
2. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców oświadczenia JEDZ, o którym mowa w Rozdz. IV.1. pkt 2.5. SWZ, składa każdy z Wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
3. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia także oświadczenia JEDZ, o którym mowa w Rozdz. IV.1. pkt 2.5. SWZ podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby.
4. Środkiem komunikacji elektronicznej, służącym złożeniu JEDZ przez Wykonawcę, jest Platforma Zakupowa.
5. Dokument elektroniczny JEDZ należy złożyć w formacie PDF.
6. Obowiązek złożenia JEDZ w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym w sposób określony powyżej dotyczy również JEDZ składanego na wezwanie w trybie art. 128 ust. 1 ustawy.

IV.3. Wykaz podmiotowych środków dowodowych

Zamawiający przed wyborem najkorzystniejszej oferty wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia za pośrednictwem Platformy Zakupowej, w wyznaczonym terminie, nie krótszym niż 10 dni od dnia wezwania, aktualnych na dzień złożenia podmiotowych środków dowodowych, w formie elektronicznej podpisanych kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności, w poniższym zakresie:

1. braku podstaw wykluczenia Wykonawcy z postępowania o udzielenie zamówienia:
   1.1. informacji z Krajowego Rejestru Karnego w zakresie:
      1.1.1. art. 108 ust. 1 pkt 1 i 2 ustawy,

1.1.2. art. 108 ust. 1 pkt 4 ustawy, dotyczącej orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka karnego,

- sporządzonej nie wcześniej niż 6 miesięcy przed jej złożeniem;

1.2. odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;

1.3. oświadczenia Wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy, w zakresie podstaw wykluczenia z postępowania wskazanych przez zamawiającego, o których mowa w:

1.3.1. art. 108 ust. 1 pkt 3 ustawy,

1.3.2. art. 108 ust. 1 pkt 4 ustawy, dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego,

1.3.3. art. 108 ust. 1 pkt 5 ustawy, dotyczących zawarcia z innymi Wykonawcami porozumienia mającego na celu zakłócenie konkurencji,

1.3.4. art. 108 ust. 1 pkt 6 ustawy

- sporządzone według wzoru, który stanowi Załącznik nr 2 do SWZ.

1.4. oświadczenia Wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r. poz. 1076 i 1086), z innym Wykonawcą, który złożył odrębną ofertę, ofertę częściową, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej. Wzór oświadczenia stanowi Załącznik nr 3 do SWZ;

2. potwierdzenia spełniania warunków udziału w postępowaniu dotyczących zdolności zawodowej:

2.1. wykazu usług wykonanych, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy lub usługi zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te dostawy lub usługi zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy lub usługi zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli Wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów - oświadczenie Wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy. Wzór oświadczenia stanowi Załącznik nr 5 do SWZ;

2.2. wykazu osób, skierowanych przez Wykonawcę do realizacji zamówienia publicznego, w szczególności odpowiedzialnych za świadczenie usług, kontrolę jakości lub kierowanie robotami budowlanymi, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami. Wzór oświadczenia stanowi Załącznik nr 6 do SWZ.

IV.4. Podmiotowe środki dowodowe składane przez Wykonawców mających siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej

1. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast

1.1. informacji z Krajowego Rejestru Karnego, o której mowa w Rozdz. IV.3 pkt 1.1. SWZ – składa informację z odpowiedniego rejestru, takiego jak rejestr sądowy, albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, w zakresie, o którym mowa w Rozdz. IV.3 pkt 1.1. SWZ.

2. Dokument, o którym mowa w pkt 1.1., powinien być wystawiony nie wcześniej niż 6 miesięcy przed ich złożeniem.

3. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w pkt. 1, lub gdy dokumenty te nie odnoszą się do wszystkich przypadków, o których mowa w art. 108 ust. 1 pkt 1, 2 i 4, ustawy, zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy. Postanowienie pkt. 2 stosuje się.

IV.5. Zasady i warunki korzystania przez Wykonawcę ze zdolności lub sytuacji innych podmiotów

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.

2. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających **zasoby, składa, wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby** do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.

3. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w pkt 2, potwierdza, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
   1.1. zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
   1.2. sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
   1.3. czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje usługi, których wskazane zdolności dotyczą.
4. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają usługi, do realizacji których te zdolności są wymagane.
5. Zamawiający żąda od Wykonawcy, który polega na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 118 ustawy, przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych w Rozdz. IV.3 pkt 1.1. – 1.4. SWZ. Postanowienia Rozdz. IV.3. SWZ stosuje się odpowiednio.

IV.6. Klauzule informacyjne w zakresie danych osobowych

W związku z treścią z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2.), dalej: „RODO" Zamawiający informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w toku postępowania jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, al. Jana Pawła II 70, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazanych w pkt 1.
3. Pani/Pana dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu przeprowadzenia niniejszego postępowania o udzielenie zamówienia publicznego.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
   4.1. osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 2 ustawy,
   4.2. organy kontrolne,
   4.3. osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2020 poz. 2176),
   4.4. podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa.
5. Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do przeprowadzenia niniejszego postępowania. Ponadto, zgodnie z art. 78 ust. 1 ustawy przechowywane będą przez okres 4 lat od dnia zakończenia niniejszego postępowania. Okres przechowywania danych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora. Ponadto, okres przechowywania danych może zostać przedłużony na okres 5 lat, na potrzeby archiwizacji.
6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych.
7. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
8. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego, a konsekwencje niepodania określonych danych wynikają z ustawy.

Rozdział V. Informacje o sposobie porozumiewania się zamawiającego z Wykonawcami oraz przekazywania oświadczeń lub dokumentów, a także wskazanie osób uprawnionych do komunikowania się z Wykonawcami

1. Komunikacja między Zamawiającym, a Wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują wyłącznie za pośrednictwem Platformy Zakupowej, z zachowaniem formy albo postaci elektronicznej, w zależności od rodzaju przekazywanego dokumentu – stosownie do obowiązujących w tym zakresie przepisów prawa. Za datę wpływu oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się ich datę wczytania do Platformy Zakupowej.
2. Postępowanie prowadzone jest pod numerem referencyjnym sprawy: **DPiZP.2610.30.2021**, Wykonawcy powinni we wszelkich kontaktach z Zamawiającym powoływać się na wskazany numer referencyjny.
3. Wykonawcy powinni kierować do Zamawiającego wszelką korespondencję z zachowaniem zasad opisanych w pkt 1, za pośrednictwem Platformy Zakupowej.
4. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SWZ. Wniosek należy przesłać za pośrednictwem Platformy Zakupowej.

5. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 6 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego nie później niż na 14 dni przed upływem terminu składania ofert. Treść pytań (bez ujawnienia źródła zapytania) wraz z wyjaśnieniami bądź informacje o dokonaniu zmiany treści SWZ, Zamawiający przekaże (opublikuje) Wykonawcom za pośrednictwem Platformy Zakupowej.
6. Jeżeli wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego po upływie terminu, o którym mowa w pkt 5 Zamawiający nie ma obowiązku udzielania wyjaśnień treści SWZ.
7. W uzasadnionym przypadku Zamawiający może przed terminem składania ofert zmienić treść dokumentów składających się na niniejszą SWZ.
8. Zamawiający nie zamierza zwoływać zebrania Wykonawców.
9. Osobami uprawnionymi ze strony Zamawiającego do kontaktów z Wykonawcami są:
   9.1. Pani Katarzyna Mazur, tel.: +48 22 595 00 63 w godz. 9.00 – 15.00.
   9.2. Pani Kinga Henzel, tel.: +48 22 595 00 66 w godz. 9.00 – 15.00.

Rozdział VI. Wymagania dotyczące wadium

1. Wykonawca zobowiązany jest wnieść wadium w wysokości 50 000,00 (słownie: pięćdziesiąt tysięcy złotych zero groszy).
2. Wadium może być wniesione w:
   2.1. pieniądzu;
   2.2. gwarancjach bankowych;
   2.3. gwarancjach ubezpieczeniowych;
   2.4. poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2020 r. poz. 299).
3. Wadium w formie pieniądza należy wnieść przelewem na rachunek bankowy Zamawiającego prowadzony w Banku Gospodarstwa Krajowego III Oddział w Warszawie numer rachunku – 45 1130 1062 8000 0000 0002 8175, z dopiskiem na przelewie: „wadium w postępowaniu na „Świadczenie usługi polegającej na zapewnieniu systemu ochrony przed wyciekiem informacji (DLP) i 300 godzin konsultacji na 36 miesięcy".
4. W przypadku wnoszenia wadium w innej formie niż pieniądzu Wykonawca wnosi w formie elektronicznej poprzez wczytanie na Platformie Zakupowej. Wadium powinno być oznaczone w następujący sposób: WADIUM – numer referencyjny sprawy, nazwa postępowania lub w inny sposób umożliwiający identyfikację postępowania, którego dotyczy.
5. Dokument wadialny (gwarancja lub poręczenie) musi wyraźnie wskazywać na wszystkie okoliczności jego utraty określone w art. 98 ust. 6 ustawy.
6. Z treści gwarancji/poręczenia powinno wynikać bezwarunkowe, na każde pisemne żądanie zgłoszone przez Zamawiającego, zobowiązanie Gwaranta do wypłaty Zamawiającemu pełnej kwoty wadium w okolicznościach określonych w art. 98 ust. 6 ustawy.
7. Oferta Wykonawcy, który nie wniósł wadium lub wniósł w sposób nieprawidłowy lub nie utrzymywał wadium nieprzerwanie do upływu terminu związania ofertą lub złożył wniosek o zwrot wadium w przypadku, o którym mowa w art. 98 ust. 2 pkt 3 ustawy zostanie odrzucona.
8. W przypadku wniesienia wadium i niezłożenia oferty, Wykonawca jest zobowiązany złożyć do Zamawiającego wniosek o zwrot wadium.

Rozdział VII. Termin związania ofertą

Wykonawcy pozostają związani złożoną ofertą do dnia 9 sierpnia 2021 r. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

Rozdział VIII Opis sposobu przygotowywania ofert

VIII.1. Przygotowanie ofert

1. Ofertę należy złożyć pod rygorem nieważności w formie elektronicznej. Ofertę należy podpisać kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Wykonawca składa ofertę na Formularzu Ofertowym (wg Załącznika nr 1 do SWZ).
2. Treść złożonej oferty musi być zgodna z warunkami zamówienia. Wykonawca ma prawo złożyć tylko jedną ofertę. Oferta powinna być sporządzona w języku polskim, w formie elektronicznej pod rygorem nieważności. Ofertę należy podpisać kwalifikowanym podpisem elektronicznym. Ofertę należy złożyć wyłącznie za pośrednictwem Platformy Zakupowej.
3. Oferta powinna zawierać jedną, jednoznacznie opisaną propozycję.
4. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.
5. Zamawiający informuje, iż zgodnie z art. 74 ust. 1 i 2 ustawy oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu niezwłocznie po otwarciu ofert, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeśli Wykonawca nie później niż w terminie składania ofert zastrzegł, że nie mogą one być udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji określonych w art. 222 ust. 5 ustawy, tj. nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania Wykonawców, których oferty zostały otwarte, cenach lub kosztach zawartych w ofertach.

   Uwaga:

   Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010 ze zm.), które Wykonawca zamierza zastrzec jako tajemnicę

przedsiębiorstwa, muszą zostać odpowiednio oznaczone a następnie załączone na Platformie Zakupowej w osobnym pliku w miejscu właściwym dla Informacji stanowiących tajemnicę przedsiębiorstwa.

6. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia, w takim przypadku:
   6.1. oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia musi być podpisana w taki sposób, by prawnie zobowiązywała wszystkich Wykonawców występujących wspólnie,
   6.2. każdy z Wykonawców wspólnie ubiegających się o udzielenie zamówienia musi udokumentować, że nie podlega wykluczeniu z postępowania na podstawie przesłanek określonych w Rozdz. III.1. SWZ.
   6.3. zgodnie z art. 58 ust. 2 ustawy muszą ustanowić pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
   6.4. wszelka korespondencja oraz rozliczenia dokonywane będą wyłącznie z pełnomocnikiem,
   6.5. przed podpisaniem umowy przedłożą pełnomocnictwo do zawarcia umowy w sprawie zamówienia publicznego, jeżeli pełnomocnictwo takie nie zostało dołączone do oferty.
   6.6. w odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z Wykonawców, którzy wykonają usługi, do realizacji których te zdolności są wymagane.

VIII.2. Forma dokumentów składanych w postępowaniu

1. Wszystkie dokumenty wchodzące w skład oferty oraz składane w trakcie postępowania należy złożyć na Platformie Zakupowej w postaci elektronicznej, podpisane kwalifikowanym podpisem elektronicznym, wystawionym przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne – podpis elektroniczny spełniający wymogi bezpieczeństwa określone w ustawie z dnia 5 września 2016 r. – o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2020 r. poz. 1173 ze zm.).
2. Dokumenty i oświadczenia wchodzące w skład oferty oraz składane w trakcie postępowania, sporządzone w językach obcych muszą być złożone wraz z tłumaczeniami na język polski.
3. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, w tym dokumenty, o których mowa w art. 94 ust. 2 ustawy, lub dokumenty potwierdzające umocowanie do reprezentowania odpowiednio Wykonawcy, Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, podmiotu udostępniającego zasoby na zasadach określonych w art. 118 ustawy lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach, zwane dalej „*dokumentami potwierdzającymi umocowanie do reprezentowania*", zostały wystawione przez upoważnione podmioty inne niż Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, zwane dalej „*upoważnionymi podmiotami*", jako dokument elektroniczny, przekazuje się ten dokument.
4. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, w tym dokumenty, o których mowa w art. 94 ust. 2 ustawy, lub dokumenty potwierdzające umocowanie do reprezentowania, zostały wystawione przez upoważnione podmioty jako dokument w postaci papierowej, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
5. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt. 4, dokonuje w przypadku:
   5.1. podmiotowych środków dowodowych oraz dokumentów potwierdzających umocowanie do reprezentowania – odpowiednio Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych lub dokumentów potwierdzających umocowanie do reprezentowania, które każdego z nich dotyczą;
   5.2. przedmiotowych środków dowodowych – odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia;
   5.3. innych dokumentów, w tym dokumentów, o których mowa w art. 94 ust. 2 ustawy – odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia, w zakresie dokumentów, które każdego z nich dotyczą.
6. Podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, dokumenty, o których mowa w art. 94 ust. 2 ustawy, niewystawione przez upoważnione podmioty, oraz pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym.
7. W przypadku gdy podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, dokumenty, o których mowa w art. 94 ust. 2 ustawy, niewystawione przez upoważnione podmioty lub pełnomocnictwo, zostały sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
8. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt. 7, dokonuje w przypadku:
   8.1. podmiotowych środków dowodowych – odpowiednio Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych, które każdego z nich dotyczą;

8.2. przedmiotowego środka dowodowego, dokumentu, o którym mowa w art. 94 ust. 2 ustawy, oświadczenia, o którym mowa w art. 117 ust. 4 ustawy, lub zobowiązania podmiotu udostępniającego zasoby – odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia;

8.3. pełnomocnictwa – mocodawca.

9. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt. 4 i 7, może dokonać również notariusz.
10. Przez cyfrowe odwzorowanie, o którym mowa w pkt. 2, 5 oraz pkt. 7-9, należy rozumieć dokument elektroniczny będący kopią elektroniczną treści zapisanej w postaci papierowej, umożliwiający zapoznanie się z tą treścią i jej zrozumienie, bez konieczności bezpośredniego dostępu do oryginału.
11. W przypadku przekazywania w postępowaniu dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym podpisem elektronicznym jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku kwalifikowanym podpisem elektronicznym.

Rozdział IX. Sposób oraz termin składania i otwarcia ofert, warunki zmiany albo wycofania oferty

IX.1. Sposób oraz termin składania ofert i otwarcia ofert

1. Ofertę pod rygorem nieważności należy złożyć w formie elektronicznej. Ofertę musi zostać podpisana kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Ofertę należy złożyć na Platformie Zakupowej udostępnionej przez Zamawiającego na stronie internetowej: https://platformazakupowa.pl/pn/arimr.
2. Termin składania ofert upływa w dniu **12 maja 2021 r. o godzinie 10:30**
3. Otwarcie ofert odbędzie się w dniu **12 maja 2021 r. o godzinie 12:00.**
4. Zamawiający nie bierze odpowiedzialności za nieprawidłowe złożenie oferty wynikające z niezastosowania się przez Wykonawcę do wymagań niniejszej SWZ.

IX.2. Warunki zmiany i wycofania złożonej oferty

1. Wykonawca posiadający konto na Platformie Zakupowej, za jej pośrednictwem może przed upływem terminu składania ofert samodzielnie zmienić lub wycofać ofertę.
2. Wykonawca nie posiadający konta na Platformie Zakupowej, za jej pośrednictwem może przed upływem terminu składania ofert samodzielnie zmienić ofertę. Wykonawca niezalogowany nie może samodzielnie wycofać oferty. W celu wycofania oferty należy skontaktować się z Centrum Wsparcia Klienta uruchomione przez Operatorem Platformy Zakupowej, które służy pomocą techniczną od 7:00 do 17:00 od poniedziałku do piątku pod numerem telefonu 22 101 02 02 lub e-mail: cwk@platformazakupowa.pl.
3. Na Platformie Zakupowej w zakładce „Instrukcje dla Wykonawców" opisana jest szczegółowa procedura zmiany i wycofania oferty.
4. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty (załączników).

Rozdział X. Opis sposobu obliczenia ceny

1. Wykonawca zobowiązany jest do wyliczenia i podania cen jednostkowych netto, ceny ofertowej netto, należnego podatku od towarów i usług VAT oraz ceny ofertowej brutto, w sposób określony w Formularzu Ofertowym stanowiącym Załącznik nr 1 do SWZ.
2. Ceny określone w Formularzu Ofertowym powinny zawierać wszystkie koszty związane z wykonaniem przedmiotu zamówienia. Podane ceny nie podlegają zmianom przez okres obowiązywania umowy, z zastrzeżeniem postanowień Rozdz. XIV pkt 4 niniejszej SWZ.
3. Ceny określone w formularzu ofertowym muszą być podane i wyliczone w zaokrągleniu do dwóch miejsc po przecinku (wg zasady zaokrąglenia: poniżej 5 należy końcówkę pominąć, powyżej i równe 5 należy zaokrąglić w górę).
4. Wszystkie ceny podane w Formularzu Ofertowym powinny być wyrażone w złotych polskich.
5. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający dla celów zastosowania kryterium ceny lub kosztu doliczy do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć. Wykonawca, składając ofertę, obowiązany jest do poinformowania Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku, wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.

Rozdział XI. Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem wag tych kryteriów i sposobu oceny ofert

1. Przy wyborze oferty najkorzystniejszej Zamawiający będzie się kierował poniższymi kryteriami:

1.1. kryterium **cena (P_C)** – waga **60%** (**60,00 pkt**), wg poniższego wzoru:

$$P_C = \frac{C_{min.}}{C_b} \text{ x 60,00 pkt,}$$

gdzie:

P_C – ilość punktów oferty badanej w kryterium cena

$C_{min.}$ – cena najniższa spośród ważnych ofert

C_b – cena oferty badanej.

1.2. kryterium **dodatkowe godziny konsultacji (P_k)** – waga **40%** (**40,00 pkt**), zgodnie z poniższą tabelą:

Lp.	Dodatkowe godziny konsultacji	Ilość punktów
1.	0 godzin dodatkowych	0 pkt
2.	25 godzin dodatkowych	10 pkt
3.	50 godzin dodatkowych	20 pkt
4.	75 godzin dodatkowych	30 pkt
5.	100 godzin dodatkowych	40 pkt

Uwaga:

a) *Zamawiający może przyzna ć maksymalnie 40 pkt.*
b) *Ilość dodatkowych godzin konsultacji wskazana przez Wykonawcę w Formularzu Ofertowy, zostanie wpisana w § 2 ust. 1 pkt. 4b) projektowanych postanowień umowy stanowiących Załącznik nr 7 do SWZ.*
c) *W przypadku braku wskazania ilości dodatkowych godzin konsultacji w Formularzu Ofertowym, Zamawiający uzna, że Wykonawca zaoferował 0 (zero) dodatkowych godzin konsultacji.*
d) *W przypadku, gdy Wykonawca zaoferowania więcej niż 100 dodatkowych godzin konsultacji, ilość ta zostawanie wpisana w § 2 ust. 1 pkt. 4b) projektowanych postanowień umowy stanowiących Załącznik nr 7 do SWZ, natomiast do celów oceny ofert Zamawiający uzna, że Wykonawca zaoferował 100 dodatkowych godzin konsultacji i Wykonawca otrzyma 40 pkt.*

2. Za najkorzystniejszą zostanie uznana oferta, która uzyska największą całkowitą liczbę punktów obliczoną z dokładnością do dwóch miejsc po przecinku, wg wzoru:

   $P = P_C + P_k$, *gdzie:*

   P_C - *całkowita ilość punktów oferty w kryterium* ***cena,***

   P_k- *całkowita ilość punktów oferty w kryterium* ***dodatkowe godziny konsultacji****.*

Rozdział XII. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. Zamawiający powiadomi wybranego Wykonawcę o miejscu i terminie podpisania umowy.
2. Wykonawca będzie zobowiązany do niezwłocznego podania Zamawiającemu danych niezbędnych do sporządzenia umowy lub przekazania dokumentów, które okażą się konieczne do zawarcia umowy.

Rozdział XIII. Wymagania dotyczące zabezpieczenia należytego wykonania umowy

1. Zamawiający żąda od Wykonawcy z którym zostanie podpisana umowa wniesienia zabezpieczenia należytego wykonania umowy w wysokości 5% ceny całkowitej podanej w ofercie.
2. Zabezpieczenie należytego wykonania umowy może być wniesione w następujących formach:
   2.1. pieniądzu,
   2.2. poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym,
   2.3. gwarancjach bankowych,
   2.4. gwarancjach ubezpieczeniowych,
   2.5. poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.
3. W przypadku wniesienia zabezpieczenia w formie pieniężnej Zamawiający przechowuje je na oprocentowanym rachunku bankowym.
4. Zabezpieczenie wnoszone w formie gwarancji bankowej, ubezpieczeniowej, poręczenia bankowego lub poręczenia spółdzielczej kasy oszczędnościowo-kredytowej, poręczenia udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości, ma być wystawione przez bank, ubezpieczyciela lub poręczyciela. Bank, ubezpieczyciel, poręczyciel zapłaci, na rzecz Zamawiającego w terminie 30 dni od pisemnego żądania kwotę zabezpieczenia, na pierwsze wezwanie Zamawiającego, bez odwołania, bez warunku, niezależnie od kwestionowania czy zastrzeżeń Wykonawcy i bez dochodzenia czy wezwanie Zamawiającego jest uzasadnione czy nie.
5. W przypadku, gdy zabezpieczenie, o którym mowa w niniejszym Rozdz. SWZ będzie wnoszone w formie innej niż pieniądz, Zamawiający zastrzega sobie prawo do akceptacji projektu ww. dokumentów.
6. Zabezpieczenia w innej formie niż pieniądz, Wykonawca złoży u Zamawiającego w Kancelarii Głównej, mieszczącej się w Warszawie przy ul. Poleczki 33, z adnotacją „dla Departamentu Informatyki" a przypadku zabezpieczenia wnoszonego w postaci elektronicznej należy przekazać na adres e-mail uzyskany od Zamawiającego przed podpisaniem umowy.
7. Zabezpieczenie należytego wykonania umowy służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania umowy.
8. Zabezpieczenie należytego wykonania Umowy zostanie zwrócone w terminach i na zasadach określonych we wzorze umowy.

Rozdział XIV. Informacje dotyczące umowy w sprawie zamówienia publicznego

1. Zawarcie umowy nastąpi wg treść projektowanych postanowień umowy w sprawie zamówienia publicznego, stanowiących Załącznik nr 7 do niniejszej SWZ.
2. Postanowienia ustalone projektowanych postanowieniach umowy nie podlegają negocjacjom.
3. Przyjęcie niniejszych projektowanych postanowień umowy stanowi jeden z istotnych warunków przyjęcia oferty.

4. Zamawiający dopuszcza zmiany postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy. Warunki zmian zostały opisane przez Zamawiającego w projektowanych postanowieniach umowy wraz z załącznikami, stanowiących Załącznik nr 7 do SWZ.

Rozdział XV. Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy w toku postępowania o udzielenie zamówienia publicznego

1. Wykonawcom, którzy mają lub mieli interes w uzyskaniu danego zamówienia oraz ponieśli lub mogą ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy przysługują środki ochrony prawnej określone w dziale IX ustawy.
2. Odwołanie przysługuje na:
   2.1. niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
   2.2. zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której zamawiający był obowiązany na podstawie ustawy.
3. Odwołanie winno zawierać informacje określone w art. 516 ust. 1 ustawy, w szczególności wskazanie czynności lub zaniechania czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy.
4. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej. Pisma w postępowaniu odwoławczym wnosi się w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej, z tym że odwołanie i przystąpienie do postępowania odwoławczego, wniesione w postaci elektronicznej, wymagają opatrzenia podpisem zaufanym.
5. Odwołujący przekazuje Zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, że Zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przekazanie odpowiednio odwołania albo jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
6. Odwołanie wnosi się w terminie:
   6.1 10 (dziesięciu) dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przesłane przy użyciu środków komunikacji elektronicznej;
   6.2 15 (piętnastu) dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przekazana w inny sposób niż określony w pkt. 6.1.;
7. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie lub wobec treści dokumentów zamówienia wnosi się w terminie:
   7.1. 10 (dziesięciu) dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia dokumentów zamówienia na stronie internetowej.
8. Odwołanie w przypadkach innych niż określone w pkt. 6 i 7 wnosi się w terminie:
   8.1. 10 (dziesięciu) dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.

Załączniki do SWZ:

1. Załącznik nr 1 - Wzór Formularza Ofertowego
2. Załącznik nr 2 - Wzór w Oświadczenie o braku podstaw wykluczenia
3. Załącznik nr 3 - Wzór Oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej
4. Załącznik nr 4 - Oświadczenie o podziale obowiązków w trakcie realizacji zamówienia
5. Załącznik nr 5 - Wzór Oświadczenia – Wykaz usług
6. Załącznik nr 6 - Wzór Oświadczenia – Wykaz osób
7. Załącznik nr 7 - projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do umowy w sprawie zamówienia publicznego
8. Załącznik nr 8 - ESPD – plik, w formacie XML, wygenerowany z narzędzia ESPD – do przygotowania formularza jednolitego europejskiego dokumentu zamówienia (JEDZ)

Zatwierdzam SWZ wraz z załącznikami: Warszawa,……2021 r.

Signature Not Verified
Dokument podpisany przez Dariusz Olkiewicz; ARiMR
Data: 2021.04.02 13:26:34 CEST

Załącznik nr 1 do SWZ – wzór Formularza Ofertowego

Formularz Ofertowy
DPiZP.2610.30.2021

Ja(my) niżej podpisany(-i) ……

Działając w imieniu i na rzecz

……

……

…

W odpowiedzi na ogłoszone postępowanie prowadzone w trybie przetargu nieograniczonego na „Świadczenie usługi polegającej na zapewnieniu systemu ochrony przed wyciekiem informacji (DLP) i 300 godzin konsultacji na 36 miesięcy", zgodnie z wymaganiami określonymi w specyfikacji warunków zamówienia i projektowanych postanowieniach umowy wraz z załącznikami, oferuję(-emy) system ochrony przed wyciekiem informacji (system DLP) spełniający poniższe parametry minimalne:

Tabela 1 Wymagane minimalne parametry systemu DLP

Lp.	Wymagane minimalne parametry systemu DLP	Oferowany parametr
1.	Systemem objętych będzie 12 tys. użytkowników lub 15 tys. urządzeń (komputery, laptopy, urządzenia mobilne) oraz dodatkowo 20 serwerów plików.	TAK/NIE*
2.	System umożliwia ochronę przed wyciekiem informacji z systemów informatycznych Zamawiającego.	TAK/NIE*
3.	System realizuje swoje funkcje zarówno na poziomie sieci (Network DLP) oraz stacji końcowej jak komputer, laptop, urządzenie mobilne (Endpoint DLP).	TAK/NIE*
4.	Zarządzanie, obsługa incydentów oraz raportowanie jest spójne dla ochrony na poziomie sieci i stacji końcowych i odbywa się z pojedynczej webowej konsoli zarządzającej.	TAK/NIE*
5.	Dostęp do konsoli zarządzającej odbywa się w bezpiecznym połączeniu https.	TAK/NIE*
6.	Ochrona informacji odbywa się w oparciu o reguły bezpieczeństwa informacji odzwierciedlające procesy biznesowe.	TAK/NIE*
7.	System umożliwia monitorowanie i ochronę wielu typowych kanałów komunikacyjnych, w szczególności:	
7.1.	http oraz https,	TAK/NIE*
7.2.	email,	TAK/NIE*
7.3.	komunikatory internetowe.	TAK/NIE*
8.	System umożliwia definiowanie własnych kanałów transmisji, które mają być monitorowane.	TAK/NIE*
9.	System w zakresie stacji końcowej umożliwia monitorowanie takich czynności jak kopiowanie informacji na zewnętrzne nośniki danych, nagrywanie płyt, lokalne drukowanie, wklejanie informacji w okna aplikacji.	TAK/NIE*
10.	System umożliwia tworzenie polityk uwzględniających takie akcje jak:	
10.1	wysyłanie powiadomień w ramach odnotowanych incydentów, przy czym powiadamiane powinny być następujące osoby: - nadawca, czyli osoba, która wysyłała informacje, - zwierzchnik nadawcy, - właściciel informacji zdefiniowany w polityce, - właściciel polityki,	TAK/NIE*
10.2	blokowanie transmisji naruszających zdefiniowaną politykę,	TAK/NIE*
10.3	kwarantannę informacji,	TAK/NIE*

Lp.	Wymagane minimalne parametry systemu DLP	Oferowany parametr
10.4	szyfrowanie informacji,	TAK/NIE*
10.5	umożliwienie użytkownikowi kontynuowania operacji po zatwierdzeniu komunikatu wyświetlonego przez agenta ochrony informacji na stacji końcowej.	TAK/NIE*
11.	System umożliwia łączenie polityk w grupy.	TAK/NIE*
12.	System umożliwia budowanie polityk ochrony informacji uwzględniając kontekst w jakim informacja jest używana, czyli musi uwzględniać okoliczności jak:	
12.1	kto wysyła informacje,	TAK/NIE*
12.2	gdzie informacje są wysyłane,	TAK/NIE*
12.3	w jaki sposób informacje są wysyłane,	TAK/NIE*
12.4	co jest wysyłane, czyli właściwa identyfikacja treści.	TAK/NIE*
13.	System wykorzystuje szeroką gamę mechanizmów identyfikowania treści, m.in.:	TAK/NIE*
13.1	słowa kluczowe,	TAK/NIE*
13.2	wyrażenia regularne,	TAK/NIE*
13.3	tworzenie odcisku palca – fingerprinting,	TAK/NIE*
13.4	algorytmy Machine Learning,	TAK/NIE*
13.5	weryfikacja klasyfikacji treści w przypadku, gdy stosowane jest rozwiązanie typu „Data Classification”.	TAK/NIE*
14.	Algorytm tworzenia odcisku palca działa tak, aby chronić informacje zawarte w pliku (również jego fragmenty), a nie wyłącznie dokument w całości.	TAK/NIE*
15.	System umożliwia tworzenie odcisków palca z zasobów zawartych w bazach danych. Tworzenie takich odcisków odbywa się bez uprzedniego kopiowania informacji do pliku (np. za pomocą ODBC).	TAK/NIE*
16.	System zawiera predefiniowane reguły ochrony informacji, dotyczące np. numerów krat kredytowych, IBAN oraz takich identyfikatorów jak PESEL, REGON, NIP, nr Dowodu Osobistego.	TAK/NIE*
17.	System umożliwia integrację z usługami katalogowymi (minimum AD DS, lub Azure AD) umożliwiająca m.in.:	TAK/NIE*
17.1	przypisywanie użytkowników i grup jako autoryzowanych nadawców i odbiorców monitorowanych informacji,	TAK/NIE*
17.2	przypisanie użytkowników do ról zarządzających takich jak administrator, audytor, manager incydentów,	TAK/NIE*
17.3	wyświetlanie szczegółów dotyczących użytkownika w ramach incydentu związanego z jego aktywnością, np. powinno być możliwe wyświetlenie informacji o zwierzchniku użytkownika.	TAK/NIE*
18.	System umożliwia zautomatyzowane wykrywanie informacji objętych politykami ochrony na serwerach i stacjach końcowych w sieci Zamawiającego (funkcjonalność Discovery). Funkcjonalność ta jest również oferowana dla folderów Exchange, Exchange Online, serwera SharePoint, Sharepoint Online.	TAK/NIE*
19.	Konsola zarządzająca zawiera ekran przedstawiający podstawowe statystki aktywności z ostatnich 24 godzin jak ilość incydentów względem ważności, najczęściej naruszane kategorie polityk, stacje końcowe, na których wykryto najwięcej naruszeń, etc.	TAK/NIE*
20.	Konsola zarządzająca umożliwia zarządzanie incydentami, m.in. zmianę ich statusu, przekazywanie do innego administratora.	TAK/NIE*
21.	System umożliwia ziarnistą delegację uprawnień do konfiguracji systemu, polityk, raportów oraz incydentów w oparciu o wbudowane jak również własne role, takie jak administrator, audytor, manager incydentów.	TAK/NIE*
22.	System w ramach odnotowanych incydentów udostępnia informacje dotyczące reguły, która została naruszona, jak również kopię informacji, która była przesyłana. Wgląd w tak szczegółowe informacje jest kontrolowany zgodnie z uprawnieniami administratora.	TAK/NIE*

Lp.	Wymagane minimalne parametry systemu DLP	Oferowany parametr
23.	System umożliwia rozpoznawanie tekstu zawartego w plikach graficznych (OCR) i jego analizę pod względem wrażliwości informacji. Ta funkcjonalność oferowana jest co najmniej dla dokumentów graficznych wysyłanych poprzez styk z Internetem (smtp, http, https).	TAK/NIE*
24.	Oprogramowanie klienckie (Endpoint) oferowane jest w polskiej wersji językowej.	TAK/NIE*
25.	System jest zaopatrzony we własny moduł analityczny, który umożliwi wskazanie z listy incydentów tych najbardziej istotnych poprzez ich korelacje i grupowanie. System zwróci alert w przypadku zwiększonej ilości zdarzeń mających wspólne źródło np. w jednym konkretnym użytkowniku.	TAK/NIE*
26.	System posiada możliwość rozbudowy o ochronę informacji przechowywanej w aplikacjach oferowanych jako SaaS, w szczególności MS O365 oraz Google for Business.	TAK/NIE*
27.	Ochrona informacji w chmurze opiera się o te same mechanizmy stosowane w rozwiązaniu lokalnym włączając Fingerprinting oraz Machine Learning.	TAK/NIE*
28.	System posiada funkcjonalność klasyfikowania informacji (w tym plików oraz wiadomości pocztowych email), lub w pełni integrować się z takim rozwiązaniem.	TAK/NIE*
	W zakresie klasyfikacji informacji, o której mowa w pkt. 28 powyżej, system posiada następujące funkcje:	
1.	Definiowanie dowolnych nazw dla poziomów klasyfikacji (np.: typ, klient, departament, projekt itp.),	TAK/NIE*
2.	Definiowanie dowolnych nazw dla klasyfikacji (np.: wewnętrzna – poufna - dane osobowe, kadry – produkcja - księgowość, Projekt X – Projekt Y, itd.).	TAK/NIE*
3.	Definiowane klasyfikacji opartej o:	
3.1	listę jednokrotnego wyboru,	TAK/NIE*
3.2	listę wielokrotnego wyboru (ze zdefiniowaniem minimalnej i maksymalnej liczby zaznaczeń),	TAK/NIE*
3.3	dowolny ciąg znaków, tzw. „sygnatura/znak sprawy” (z możliwością zdefiniowania szablonu logicznego dla takiego ciągu znaków).	TAK/NIE*
4.	Tworzenie klasyfikacji wielopoziomowej (minimum 5 poziomów oznaczeń klasyfikacji).	TAK/NIE*
5.	Definiowanie automatycznego nadawania klasyfikacji w oparciu o analizę treści informacji.	TAK/NIE*
6.	Klasyfikowanie dokumentu w następujących aplikacjach natywnych służących do edycji danego typu dokumentu (z poziomu aplikacji, a nie klasyfikowanie z poziomu plików):	
6.1	MS Word,	TAK/NIE*
6.2	MS Excel,	TAK/NIE*
6.3	MS PowerPoint,	TAK/NIE*
6.4	MS Visio,	TAK/NIE*
6.5	MS Project.	TAK/NIE*
7.	Wyświetlanie informacji o nadanej klasyfikacji, podczas edycji dokumentu w aplikacji natywnej.	TAK/NIE*
8.	Wyświetlanie przycisków klasyfikacji na wstążce aplikacji w postaci zarówno kolorowych pól (kolory zdefiniowane dla danego poziomu klasyfikacji), jak również w postaci dowolnie zdefiniowanych grafik/ikonek.	TAK/NIE*
9.	Dynamiczne wyświetlanie poziomów klasyfikacji tzn. możliwość wyboru podkategorii pojawia się dopiero po wybraniu przez użytkownika tej kategorii, dla której można/należy wybrać podkategorię.	TAK/NIE*
10.	Możliwość klasyfikowania plików (nie tylko MS Office, ale i innych plików kompatybilnych z technologią XMP, np. PDF, ZIP, itd.), plików tekstowych, obrazów itp.	TAK/NIE*
11.	Klasyfikowanie pliku/dokumentu z użyciem menu kontekstowego systemu operacyjnego (bez potrzeby jego otwierania).	TAK/NIE*

Lp.	Wymagane minimalne parametry systemu DLP	Oferowany parametr
12.	Masowe nadanie klasyfikacji plikom/dokumentom poprzez:	
12.1	wskazanie folderu (z lub bez podfolderów) z plikami/dokumentami do oznaczenia,	TAK/NIE*
12.2	zdefiniowanie filtrów oznaczania (np. wszystkie pliki, których nazwa lub rozszerzenie zawiera wskazany wyróżnik),	TAK/NIE*
12.3	możliwe klasyfikowanie poprzez narzędzie z interfejsem okienkowym i poprzez polecenia konsoli tekstowej.	TAK/NIE*
13.	Wymuszanie na użytkowniku dokonania klasyfikacji, jeśli użytkownik tego nie zrobi:	
13.1	w wiadomości email MS Outlook,	TAK/NIE*
13.2	w dokumentach edytowalnych (w odniesieniu do aplikacji natywnej służącej do edycji danego dokumentu).	TAK/NIE*
14.	Wyświetlanie podpowiedzi/ostrzeżeń dotyczących wymogów klasyfikacji dla użytkownika lub innych informacji w zależności od podejmowanych działań przez użytkownika odnośnie informacji sklasyfikowanej na danym poziomie.	TAK/NIE*
15.	Wymuszanie na użytkowniku podania uzasadnienia dla wykonywanego działania odnośnie informacji sklasyfikowanej na danym poziomie.	TAK/NIE*
16.	Automatyczne wstawianie (dla wybranego poziomu klasyfikacji i w odniesieniu do aplikacji natywnej służącej do edycji danego dokumentu):	
16.1	stopek/nagłówków (także grafiki),	TAK/NIE*
16.2	znaków wodnych (także grafiki),	TAK/NIE*
16.3	prefiksów,	TAK/NIE*
16.4	osoby klasyfikującej,	TAK/NIE*
16.5	daty nadania klasyfikacji.	TAK/NIE*
17.	Wymuszanie szyfrowania poczty elektronicznej.	TAK/NIE*
18.	Dokonanie zmiany lub uniemożliwienie zmiany klasyfikacji dokumentu lub dokonanie zmiany wyłącznie w jednym kierunku (np. tylko podwyższenie poziomu klasyfikacji) przez użytkowników/ autora dokumentu.	TAK/NIE*
19.	Informacja o klasyfikacji dokumentu zapisywana jest w metadanych dokumentu.	TAK/NIE*
20.	Poziom klasyfikacji maila jest zapisywany w nagłówku wiadomości mail (X-Header).	TAK/NIE*
21.	We wszystkich aplikacjach natywnych służących do edycji danego typu dokumentu interfejs związany z klasyfikacją informacji jest taki sam.	TAK/NIE*
22.	Możliwe jest opcjonalne rozbudowanie systemu o automatyczne i działające na bieżąco klasyfikowanie maili przychodzących do organizacji (na poziomie serwera Exchange).	TAK/NIE*
23.	Możliwe jest opcjonalne rozbudowanie systemu o komponenty dla serwera Sharepoint 2013 i wyższych, aby Sharepoint mógł odczytywać i interpretować nadane poziomy klasyfikacji.	TAK/NIE*
24.	Możliwe jest opcjonalne rozbudowanie systemu o komponent na urządzenia mobilne, który pozwoli na klasyfikowanie maili na urządzeniu mobilnym (Android, iOS).	TAK/NIE*
25.	Dla uruchomienia klasyfikacji i dystrybucji polityk system nie wymaga serwera bazy danych lub innych rozwiązań serwerowych.	TAK/NIE*
26.	Publikacja polityk do użytkowników może być realizowana przez współdzielony katalog (network share), lokalną usługę dystrybucji oprogramowania, lub serwis chmurowy.	TAK/NIE*
27.	Reguły dla klienta pocztowego odnośnie możliwości przesyłania maili o wskazanych poziomach klasyfikacji są definiowane w oparciu o nazwy domen pocztowych oraz w oparciu o grupy użytkowników (AD DS lub Azure AD).	TAK/NIE*
28.	Możliwe jest zdefiniowanie kilku zestawów polityk (o zróżnicowanym poziomie restrykcji) i ich odpowiedni przydział do wskazanych osób zgodnie z pozycją w strukturach zarządczych w organizacji.	TAK/NIE*

Lp.	Wymagane minimalne parametry systemu DLP	Oferowany parametr
29.	Możliwa jest automatyczna instalacja oprogramowania na stacjach użytkowników z wykorzystaniem narzędzi do automatycznej zdalnej instalacji.	TAK/NIE*
30.	System umożliwia pracę użytkownikowi (klasyfikowanie dokumentów, działanie polityk) także w przypadku gdy komputer użytkownika nie ma połączenia z siecią organizacji.	TAK/NIE*
31.	System zapisuje (loguje) wszystkie zdarzenia związane z klasyfikowaniem informacji, działaniem zdefiniowanych reguł/polityk.	TAK/NIE*
32.	Interfejs użytkownika końcowego w języku polskim (wszystkie nazwy, komunikaty, przyciski, opisy, itd.). Możliwe jest dostosowanie treści do terminologii i konwencji przyjętej w organizacji.	TAK/NIE*
33.	Informacja o poziomie klasyfikacji dokumentu, nadanej za pośrednictwem systemu klasyfikacji, może być wykorzystana przy tworzeniu polityk.	TAK/NIE*
34.	System integruje się z rozwiązaniami DLP Discovery (system Discovery po zidentyfikowaniu dokumentu zawierającego informacje spełniające zadane kryteria może automatycznie nadać klasyfikację wg poziomów zdefiniowanych w systemie klasyfikacji).	TAK/NIE*
35.	Do instalacji/działania systemu nie są wymagane żadne elementy/komponenty producentów trzecich (np. bazy danych).	TAK/NIE*
36.	System pracuje w systemie wysokiej dostępności (High Availability).	TAK/NIE*

**niepotrzebne skreślić*

za cenę:

Tabela 2

Lp.	Przedmiot	Cena jednostkowa netto (zł)	Jednostka	Cena netto (zł)	Podatek VAT		Cena brutto (zł)
					(%)	(zł)	
[a]	[b]	[c]	[d]	[e]=[c]×[d]	[f]	[g]=[f]×[e]	[h]=[e]+[g]
1	Subskrypcja do korzystania z systemu DLP		36 miesięcy				
2	Wdrożenie systemu DLP		1 wdrożenie				
3	Usługa Asysty Technicznej		36 miesięcy				
4	Usługa Wsparcia		300 godzin				
5	Razem						

Słownie zł cena ofertowa netto: _____

Słownie zł cena ofertowa brutto: _____

Oświadczamy, że:

1. Zapoznaliśmy się z treścią specyfikacji warunków zamówienia (SWZ), w tym projektowanych postanowień umowy i nie wnosimy do nich zastrzeżeń oraz przyjmujemy warunki w nich zawarte.
2. Realizację przedmiotu zamówienia wykonamy w terminach określonych w Rozdz. II SWZ oraz projektowanych postanowieniach umowy.
3. W ramach zaoferowanej ceny oferujemy ……. Dodatkowych godzin konsultacji, o których mowa w § 2 ust. 1 pkt 4b) projektowanych postanowień umowy.

Uwaga:

Zamawiający zastrzega, że dodatkowe godziny konsultacji będą wykorzystane w pierwszej kolejności i bez dodatkowego wynagrodzenia.

4. W cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia.
5. Uważamy się za związanych niniejszą ofertą do terminu określonego w SWZ.
6. Wadium w wysokości **50 000,00 zł** (słownie: pięćdziesiąt tysięcy złotych zero groszy) wnieśliśmy przed upływem terminu składania ofert.
7. Wadium wniesione w formie pieniądza należy zwrócić na rachunek bankowy nr ……prowadzony w banku ……. Oświadczenie o zwolnieniu wadium wniesionego w innej formie niż pieniądz należy przekazać gwarantowi/poręczycielowi na następujący adres e-mail……..
8. Zobowiązujemy się do wniesienia przed podpisaniem umowy zabezpieczenia należytego wykonania umowy w wysokości **5%** *ceny całkowitej podanej w ofercie/maksymalnej wartości nominalnej zobowiązania wynikającego z Umowy*.
9. W przypadku udzielenia nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.
10. Podwykonawcom zamierzamy powierzyć wykonanie następującej(-ych) części zamówienia (należy podać zakres prac oraz nazwę Podwykonawcy, jeśli jest już znany):
    10.1. ……[1]

[1] *w* przypadku *niewypełnienia Zamawiający uzna, że Wykonawca nie zamierza powierzyć wykonania żadnej części zamówienia podwykonawcom.*

UWAGA:

Zamawiający przypomina, że powyższy punkt Formularza Ofertowego należy wypełnić w każdym przypadku, jeśli Wykonawca zamierza powierzyć podwykonawcom wykonanie części zamówienia, a także mając na uwadze treść art. 118 ust. 2 ustawy cyt.: „W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane."

Udział podmiotu trzeciego w realizacji zamówienia w odniesieniu do warunków winien mieć charakter podwykonawstwa, w związku z czym wypełnieniu podlega pkt 9 Formularza Ofertowego.

11. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na poniższy adres e-mail: ……
    Dane kontaktowe: imię i nazwisko ……, nr tel. ……., adres e-mail: ……..
12. Dokumenty wymienione od strony …… do strony …… stanowią tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010 z późn. zm.) i nie mogą być ujawnione pozostałym uczestnikom postępowania.
    UWAGA*:*
    Zamawiający przypomina, że stosownie do treści:
    - *art. 18 ust. 3 ustawy Wykonawca winien nie później niż w terminie składania ofert wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa*
    - *Rozdz. VIII.1. pkt 5 SWZ wszelkie informacje stanowiące tajemnicę przedsiębiorstwa muszą zostać odpowiednio oznaczone a następnie załączone na Platformie Zakupowej w osobnym pliku w miejscu właściwym dla Informacji stanowiących tajemnicę przedsiębiorstwa.*
13. Wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO)[2] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.[3]

[2] *rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2).*

[3] *w przypadku, gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie ma obowiązku składać (w takim przypadku Wykonawca może usunąć treści oświadczenia np. przez jego wykreślenie, przekreślenie, itp.).*

14. Jednocześnie, zgodnie z treścią art. 225 ust. 2 ustawy oświadczam, że wybór niniejszej oferty:
    14.1. **nie będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego[4]
    14.2. **będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, w związku z tym:[4]
        14.2.1. ……[5]

[4] *Niepotrzebne skreślić. W przypadku nieskreślenia (nie wskazania) żadnej z ww. treści oświadczenia i niewypełnienia powyższego pola oznaczonego: „należy wskazać nazwę (rodzaj) towaru/usługi, których dostawa/świadczenie będzie prowadzić do jego powstania oraz ich wartość bez kwoty podatku od towarów i usług" – Zamawiający uzna, że wybór przedmiotowej oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego.*

[5] *W pkt. 13.2.1. należy wskazać: nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego, wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku, stawkę podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.*

15. Zgodnie z Rozdz. IV.1. SWZ do oferty zostają załączone dokumenty:
    15.1. odpis lub informację z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru,
    15.2. pełnomocnictwo lub inny dokument potwierdzający umocowanie osoby działającej w imieniu Wykonawcy do jego reprezentowania, jeżeli oferta nie została podpisana przez osoby upoważnione do tych czynności dokumentem rejestracyjnym, o którym mowa w pkt. 15.1.,
    15.3. dowód wniesienia wadium,
    15.4. zobowiązanie podmiotów udostępniających zasoby do oddania Wykonawcy do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie będzie dysponował niezbędnymi zasobami, jeżeli Wykonawca powołuje się na zasoby innych podmiotów,
    15.5. aktualne na dzień składania ofert oświadczenie w formie jednolitego europejskiego dokumentu zamówienia (JEDZ)
    15.6. oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia w zakresie wskazania, które usługi wykonają poszczególni Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (członkowie konsorcjum).

Świadom odpowiedzialności karnej oświadczam, że załączone do oferty dokumenty opisują stan prawny i faktyczny, aktualny na dzień złożenia oferty (art. 297 k.k.).

Załącznik nr 2 do SWZ – wzór Oświadczenia o braku podstaw wykluczenia

Nazwa Wykonawcy: ……

Adres Wykonawcy: …….

Oświadczenie o braku podstaw wykluczenia

DPIZP.2610.30.2020

Przystępując do udziału w postępowaniu o zamówienie publiczne na „Świadczenie usługi polegającej na zapewnieniu systemu ochrony przed wyciekiem informacji (DLP) i 300 godzin konsultacji na 36 miesięcy" oświadczam(-y), że na dzień złożenia niniejszego oświadczenia aktualne pozostają informacje zawarte w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy, tj. nie podlegam(-y) wykluczeniu na podstawie:

1. art. 108 ust. 1 pkt 3 ustawy,
2. art. 108 ust. 1 pkt 4 ustawy dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego,
3. art. 108 ust. 1 pkt 5 ustawy dotyczących zawarcia z innymi Wykonawcami porozumienia mającego na celu zakłócenie konkurencji,
4. art. 108 ust. 1 pkt 6 ustawy.

Załącznik nr 3 do SWZ – wzór Oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej

Nazwa Wykonawcy: ……

Adres Wykonawcy: …….

Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej
DPIZP.2610.30.2020

Przystępując do udziału w postępowaniu o zamówienie publiczne na „Świadczenie usługi polegającej na zapewnieniu systemu ochrony przed wyciekiem informacji (DLP) i 300 godzin konsultacji na 36 miesięcy" oświadczam(-y), że:

1. **nie należę(-ymy) do grupy kapitałowej** w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r., poz. 1076 ze zm.) **z żadnym z Wykonawców, którzy złożyli odrębną ofertę[1]/ofertę częściową[1] w przedmiotowym postępowaniu** o udzielenie zamówienia publicznego[1].
2. **należę(-ymy) do grupy kapitałowej** w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r., poz. 1076 ze zm.) **z następującymi Wykonawcami, którzy złożyli odrębną ofertę[1]/ofertę częściową[1] w przedmiotowym postępowaniu** o udzielenie zamówienia publicznego[1]:

Lp.	Nazwa podmiotu	Siedziba
1		
(…)		

Jednocześnie na potwierdzenie, że nasza oferta[1]/oferta częściowa[1] została przygotowana niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej składam(-y) następujące informacje i/lub dokumenty:

……
……
……
……
……
……
……
……
……
……

UWAGA:

[1] niepotrzebne skreślić

Załącznik nr 4 do SWZ – wzór Oświadczenia o podziale obowiązków w trakcie realizacji zamówienia

Oświadczenie o podziale obowiązków w trakcie realizacji zamówienia
(dotyczy Wykonawców wspólnie ubiegających się o udzielenie zamówienia)

DPIZP.2610.30.2020

Działając w imieniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia: ……..[1], przystępując do udziału w postępowaniu o zamówienie publiczne na „Świadczenie usługi polegającej na zapewnieniu systemu ochrony przed wyciekiem informacji (DLP) i 300 godzin konsultacji na 36 miesięcy" oświadczam(-y), że wyszczególnione poniżej dostawy/usługi zostaną zrealizowane zgodnie z poniższym:

1. Wykonawca ……..[2] wykona następujące usługi/dostawy w ramach realizacji zamówienia:
   1.1. ……..
   1.2. ……..
   1.3. ……..
2. Wykonawca ……..[2] wykona następujące usługi/dostawy w ramach realizacji zamówienia:
   2.1. ……..
   2.2. ……..
   2.3. ……..
3. Wykonawca ……..[2] wykona następujące usługi/dostawy w ramach realizacji zamówienia:
   3.1. ……..
   3.2. ……..
   3.3. ……..

UWAGA:

[1] należy wpisać firmy wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia

[2] należy wpisać firmy i adresy poszczególnych Wykonawców wspólnie ubiegających się o udzielenie zamówienia

Załącznik nr 5 do SWZ – wzór Oświadczenia – Wykaz usług

[warunek udziału w postępowaniu]

Nazwa Wykonawcy: ……

Adres Wykonawcy: ……..

Oświadczenie – Wykaz usług

DPIZP.2610.30.2020

Przystępując do udziału w postępowaniu o zamówienie publiczne na „Świadczenie usługi polegającej na zapewnieniu systemu ochrony przed wyciekiem informacji (DLP) i 300 godzin konsultacji na 36 miesięcy”**,** składam(-y) wykaz usług wykonanych (wykonywanych) w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, na potwierdzenie spełniania warunku udziału w postępowaniu, o którym mowa w Rozdz. III.2. pkt 1.1.1. SWZ.

Lp.	Przedmiot wykonanych/wykonywanych usług (*wg warunku udziału w postępowaniu*)	Wartość brutto usługi w zł (*w przypadku gdy zakres usługi jest szerszy, należy podać wyłącznie wartość usługi odpowiadającej treści warunku udziału w postępowaniu w badanym zakresie, wg warunku udziału w postępowaniu*)	Podmiot na rzecz którego wykonano usługę *(nazwa i adres)*	Daty wykonania		Dowody	Informacje uzupełniające	
				Od dd-mm-rrrr	Do dd-mm-rrrr		Zasoby innego podmiotu	Nazwa innego podmiotu
1	2	3	4	5	6	7	8	*9*
1								
2								
3								

<u>Uwaga do kol. 7:</u>

1. *Do wykazu należy dołączyć dowody potwierdzające, że powyższe usługi zostały wykonane lub są wykonywane należycie, tj.:*
   - *1.1. referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonywane lub są wykonywane należycie, z tym, że w odniesieniu do nadal wykonywanych usług okresowych lub ciągłych referencje bądź inne dokumenty powinny być wydane nie wcześniej niż 3 m-ce przed upływem terminu składania ofert;*
   - *1.2. oświadczenie Wykonawcy - jeżeli z uzasadnionych przyczyn o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać dokumentów, o którym mowa wyżej w pkt 1.1;*
2. *Należy wpisać nazwę dowodu (dokumentu) potwierdzającego, że usługi zostały wykonane lub są wykonywane należycie (podać numer strony);*

<u>Uwaga do kol. 8:</u>

1. *Zaznaczyć „TAK", tylko w przypadku, gdy Wykonawca polega na zasobach innego podmiotu dla wykazania spełniania warunku udziału;*
2. *Dla wykazania spełniania warunku udziału w postępowaniu, opisanego w Rozdz. III.2. pkt 1.4.SIWZ, Wykonawca może polegać, na zasadach określonych w art. 118 Ustawy. W tym celu Wykonawca składa dokumenty i oświadczenia zgodnie z* zasadami *określonymi w Rozdz. IV.5. SIWZ.*

Załącznik nr 6 do SWZ – wzór Oświadczenia — Wykaz osób

[warunek udziału w postępowaniu]

Nazwa Wykonawcy: ……

Adres Wykonawcy: …….

Oświadczenie – Wykaz osób
skierowanych przez Wykonawcę do realizacji zamówienia publicznego
DPiZP.2610.30.2020

Przystępując do udziału w postępowaniu o zamówienie publiczne na „Świadczenie usługi polegającej na zapewnieniu systemu ochrony przed wyciekiem informacji (DLP) i 300 godzin konsultacji na 36 miesięcy”**,** składam(-y) wykaz osób, które skieruję(-emy) do realizacji niniejszego zamówienia, na potwierdzenie spełniania warunku udziału w postępowaniu, o którym mowa w Rozdz. III.2. pkt 1.1.2 SWZ:

Lp	Imię i Nazwisko	Informacja na temat kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia	Zakres czynności wykonywanych w ramach umowy	Dysponujemy osobą na podstawie art. 22a Prawa zamówień publicznych (informacja o podstawie dysponowania wykazanymi osobami)
1)				tak/nie* **niewłaściwe skreślić*
2)				tak/nie* **niewłaściwe skreślić*
3)				tak/nie* **niewłaściwe skreślić*
4)				tak/nie* **niewłaściwe skreślić*
5)				tak/nie* **niewłaściwe skreślić*

Załącznik nr 7 do SWZ – projektowane postanowienia umowy

Umowa nr …/DI/2021/2610

zawarta w Warszawie, pomiędzy:

Agencją Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie i adresem przy Al. Jana Pawła II nr 70, 00-175 Warszawa, (adres do korespondencji: ARiMR Departament Informatyki ul. Poleczki 33, 02-822 Warszawa), REGON 010613083, zarejestrowanym podatnikiem podatku od towarów i usług, NIP 526-19-33-940, zwaną dalej „**Zamawiającym**" lub „**ARiMR"**, którą reprezentuje:

Pan Dariusz Olkiewicz – Zastępca Prezesa ARiMR, Pełnomocnik;

Pani Barbara Okupniak–Stefańska – Dyrektor Departamentu Księgowości, w ramach zajmowanego stanowiska wykonująca obowiązki Głównego Księgowego, Pełnomocnik;

a

……, zwaną dalej „**Wykonawcą**", którą reprezentuje:

…… – ……;

w wyniku wyboru oferty w postępowaniu o udzielenie zamówienia publicznego przeprowadzonego w trybie przetargu nieograniczonego zgodnie z art. 132 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2019 r. poz.2019 ze zm.) o następującej treści:

§ 1.
Definicje

W niniejszej umowie następujące wyrażenia i określenia będą miały znaczenie zgodnie z podanymi poniżej definicjami, zapisane z wielkiej litery w celu podkreślenia, że jest to pojęcie zdefiniowane:

1) **Aktualizacja** - Updates (zaktualizowanie), Upgrades (ulepszenie), Patches (poprawka) oraz wszelkie nowe wersje DLP i udoskonalenia do wersji bieżących DLP (nowe edycje, wydania uzupełniające, poprawki programistyczne) wraz z ich dokumentacją, wydane przez producenta DLP w okresie korzystania przez Zamawiającego z Usługi Asysty Technicznej zgodnie z Umową;
2) **Dni Robocze** – dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy lub dni wolnych od pracy u Zamawiającego, o których zostanie poinformowany Wykonawca;
3) **Dokumentacja powykonawcza** – wykonany przez Wykonawcę na podstawie zatwierdzonego i odebranego przez Zamawiającego Projektu Technicznego dokument, zawierający w szczególności konfigurację, opis techniczny i zasady działania wdrożonego systemu DLP, w tym instrukcje, wytyczne i zalecenia wymagane do korzystania z Systemu DLP przez jej użytkowników i administratorów;
4) **Lokalizacje** - Centrala ARiMR, ul. Poleczki 33, Warszawa oraz serwerownie: COPD – ul. Poleczki 23 Warszawa oraz ROPD – ul. Jana Pawła II 66 Piaseczno (przy czym Zamawiający zastrzega sobie prawo zmiany Lokalizacji Serwerowni w okresie obowiązywania Umowy);
5) **DLP** – system informatyczny wspomagający ochronę danych przed utratą i wyciekami informacji spełniający wymagania określone w Załączniku nr 1 do Umowy i wdrożony przez Wykonawcę u Zamawiającego;
6) **Projekt Techniczny** – dokumentacja projektowa, wykonana przez Wykonawcę i odebrana przez Zamawiającego, szczegółowo określająca i opisująca wszelkie elementy systemu DLP w szczególności takie jak: zakres i opis wykonywanych prac konfiguracyjnych, parametryzacji i optymalizacji DLP na potrzeby Zamawiającego, zasady instalacji, zastosowane technologie i rozwiązania techniczne, opis obsługiwanych procesów, procedury konfiguracyjne, a także harmonogram testów i procedury testowe DLP u Zamawiającego, zasady archiwizacji i przenoszenia danych do i z systemu;
7) **Strony** – Zamawiający i Wykonawca wymienieni w komparycji Umowy;
8) **Umowa** – niniejsza umowa wraz z załącznikami, regulująca prawa i obowiązki Stron z niej wynikające i związane z jej wykonaniem;
9) **Usługa Asysty Technicznej** - usługa polegająca na świadczeniu serwisu technicznego dla oprogramowania DLP przez wykwalifikowanych inżynierów zapewnionych przez producenta DLP, w tym udzieleniu dostępu do Aktualizacji, z której Zamawiający uprawniony będzie do korzystania zgodnie z warunkami Umowy i ogólnymi warunkami producenta DLP w okresie wskazanym w Umowie;
10) **Usługa Wsparcia** – usługa polegająca na świadczeniu wsparcia w zakresie korzystania z systemu DLP, w tym modelowaniu procesów biznesowych przy użyciu tego narzędzia, poprzez zapewnienie konsultacji technicznych (zarówno deweloperskich, administracyjnych, jak i programistycznych) świadczonych przez osoby wskazane w § 3 ust. 1 pkt. 5, z której Zamawiający uprawniony będzie do korzystania zgodnie z warunkami Umowy w okresie wskazanym w Umowie;
11) **Wdrożenie** – ogół czynności Wykonawcy mających na celu dostosowanie systemu DLP do potrzeb Zamawiającego, w tym modelowanie procesów, integracja z innymi systemami oraz konfiguracja, instalacja i produkcyjne uruchomienie DLP u Zamawiającego zgodnie z warunkami Umowy.

§ 2.

Przedmiot Umowy

1. Wykonawca, na podstawie Umowy, zobowiązany jest do świadczenia usługi polegającej na zapewnieniu systemu DLP, w ramach której:
   1) przeprowadzi Wdrożenie systemu DLP na wskazanej przez Zamawiającego platformie sprzętowo-systemowej w Lokalizacji Zamawiającego, w tym wykona Projekt Techniczny oraz Dokumentację powykonawczą dla DLP zgodnie z warunkami Umowy;
   2) zapewni Zamawiającemu prawo do korzystania z systemu DLP wraz z jego dokumentacją, zgodnie z ich charakterem i przeznaczeniem (subskrypcja obowiązująca przez okres 36 miesięcy od dnia podpisania przez Zamawiającego Protokołu Wdrożenia) na zasadach określonych w Umowie oraz ogólnych warunkach producenta;
   3) zapewni Zamawiającemu prawo korzystania z Usługi Asysty Technicznej producenta DLP na zasadach określonych w Umowie oraz ogólnych warunkach producenta;
   4) zapewni Zamawiającemu świadczenie Usługi Wsparcia, polegającej na zapewnieniu do:
      a) 300 godzin konsultacji technicznych (deweloperskich, administracyjnych, programistycznych) w zakresie związanym z działaniem Systemu DLP, w miarę potrzeb Zamawiającego zgłaszanych zarówno na etapie Wdrożenia jak i w okresie korzystania z systemu DLP;
      b) dodatkowych ……godzin konsultacji technicznych (zgodnie z deklaracją Wykonawcy złożoną w Formularzu Ofertowym) w okresie obowiązywania Umowy, przy czym Zamawiający zastrzega, że dodatkowe godziny konsultacji będą wykorzystane w pierwszej kolejności i bez dodatkowego wynagrodzenia.
2. Usługa Asysty Technicznej będzie zapewniona Zamawiającemu przez okres 36 miesięcy od dnia podpisania przez Zamawiającego bez zastrzeżeń Protokołu Wdrożenia zgodnie z § 4 ust. 13 Umowy.
3. Usługa Wsparcia będzie świadczona przez Wykonawcę zgodnie z bieżącym zapotrzebowaniem Zamawiającego, począwszy od dnia zawarcia umowy do wyczerpania maksymalnej puli godzin konsultacji wskazanej w ust. 1 pkt. 4, nie dłużej jednak niż do upływu okresu obowiązywania Usługi Asysty Technicznej zgodnie z ust. 2.

§ 3.

Wymagania dotyczące wykonania Umowy

1. Wykonawca oświadcza, że:
   1) zarówno DLP jak i jego Aktualizacje wraz dokumentacją, nie są obciążone wadami prawnymi oraz jest uprawniony do zapewnienia licencji (na zasadach subskrypcji) umożliwiającej Zamawiającemu korzystanie z DLP na warunkach określonych w Umowie, a dodatkowo w przypadku, gdy Wykonawca nie jest producentem DLP- oświadcza, że nabył od producenta licencję (na zasadach subskrypcji) umożliwiającą korzystanie z DLP, (z prawem do sublicencji) przez okres, o którym mowa w § 2 ust. 1 pkt. 2 Umowy,
   2) jest uprawniony do wykonywania wszelkich prac programistycznych, optymalizacyjnych, konfiguracyjnych, umożliwiających dostosowanie DLP do potrzeb Zamawiającego zgodnie z warunkami Umowy;
   3) jest uprawniony do zapewnienia Zamawiającemu prawa do korzystania z Usługi Asysty Technicznej i Usługi Wsparcia na zasadach określonych w Umowie,
   4) posiada konieczne doświadczenie i profesjonalne kwalifikacje niezbędne do prawidłowego wykonania Umowy i zobowiązuje się do wykonania Umowy przy zachowaniu należytej staranności określonej w art. 355 § 2 Kodeksu Cywilnego,
   5) dysponuje osobami posiadającymi specjalistyczne kwalifikacje potwierdzone certyfikatami wystawionymi przez producenta potwierdzającymi stopień kwalifikacji na poziomie inżyniera lub wyższym w zakresie świadczonej Usługi Wsparcia. Wykaz osób (zgodny ze złożonym w postępowaniu) stanowi Załącznik nr 4 do Umowy, przy czym po uprzednim pisemnym powiadomieniu i uzyskaniu akceptacji Zamawiającego, Wykonawca może dokonać zmiany osób określonych w Wykazie osób na inne osoby posiadające specjalistyczne kwalifikacje, o których mowa w niniejszym punkcie, potwierdzone odpowiednimi certyfikatami. Zmiana osób, o których mowa w zdaniu poprzedzającym nie wymaga formy aneksu. W przypadku zmiany osób wskazanych w Wykazie osób (Załącznik nr 4 do Umowy) nowa osoba musi posiadać kwalifikacje i doświadczenie nie gorsze od wskazanych w Wykazie osób, które będą uczestniczyć w wykonywaniu zamówienia, złożonym wraz z ofertą,
   6) dostarczone i wykonane w ramach Umowy oprogramowanie jest wolne od oprogramowania szkodliwego i szpiegującego, a także jest zabezpieczone przed nieautoryzowanym dostępem,
2. Wykonawca nie ma prawa, bez zgody Zamawiającego, do korzystania przy wykonywaniu Umowy w jakimkolwiek charakterze z osób zatrudnionych u Zamawiającego, pod rygorem odstąpienia od Umowy przez Zamawiającego z winy Wykonawcy oraz zapłaty kary umownej w wysokości określonej w § 10 ust. 5 Umowy wraz z prawem do żądania od Wykonawcy odszkodowania uzupełniającego na zasadach ogólnych Kodeksu cywilnego, z zastrzeżeniem ust. 3.
3. W przypadku stwierdzenia naruszenia, o których mowa w ust. 2 Zamawiający zastrzega sobie również prawo do każdorazowego naliczenia kary umownej w wysokości określonej w § 10 ust. 1 Umowy, bez skorzystania z uprawnienia do odstąpienia od Umowy.

§ 4.

Wdrożenie systemu DLP

1. Wykonawca zobowiązany jest do przeprowadzenia Wdrożenia systemu DLP w terminie nie przekraczającym 90 Dni Roboczych od dnia zawarcia Umowy.
2. W terminie do 21 Dni Roboczych od daty zawarcia Umowy, Wykonawca przekaże Zamawiającemu do akceptacji Projekt techniczny wraz z harmonogramem realizacji poszczególnych czynności wymaganych na etapie Wdrożenia DLP. Harmonogram powinien umożliwiać przeprowadzenie całości procesu Wdrożenia w terminie wynikającym z ust. 1.
3. Wykonawca uprawniony jest do wnioskowania o przekazanie przez Zamawiającego dokumentów lub informacji niezbędnych do realizacji Projektu Technicznego lub Wdrożenia. W szczególności Wykonawca uprawniony jest do wnioskowania o przeprowadzenie spotkań analitycznych, w celu uszczegółowienia zakresu Projektu Technicznego lub warunków Wdrożenia, o ile jest to obiektywnie wymagane w celu prawidłowej realizacji Projektu Technicznego lub Wdrożenia. Przekazywanie informacji przez Zamawiającego lub prowadzenie spotkań analitycznych pozostaje bez wpływu na terminy wykonania Projektu Technicznego i wykonanie Wdrożenia, z zastrzeżeniem ust. 4.
4. W uzasadnionych przypadkach, gdy brak dokumentacji lub informacji od Zamawiającego uniemożliwia Wykonawcy wykonanie Projektu Technicznego lub w ramach prowadzonych przez Strony uzgodnień analitycznych wyniknie potrzeba wykonania dodatkowych czynności na potrzeby Wdrożenia, Wykonawca uprawniony jest do złożenia wniosku o wydłużenie terminów wskazanych w ust. 1 lub 2, wraz z uzasadnieniem wskazującym rzeczywisty wpływ zaistniałych okoliczności na możliwość terminowej realizacji zadań umownych. Zamawiający po analizie wniosku Wykonawcy może przesunąć termin realizacji zobowiązania, o którym mowa w ust. 1 lub ust. 2, przy czym przesunięcie takie nie będzie dłuższe niż 30 Dni Roboczych.
5. Zamawiający w terminie do 10 Dni Roboczych od daty otrzymania Projektu Technicznego od Wykonawcy, dokona jego weryfikacji i zgłosi ewentualne zastrzeżenia.
6. Wykonawca zobowiązany jest do uwzględnienia zastrzeżeń Zamawiającego zgłoszonych do Projektu Technicznego i do przekazania poprawionych dokumentów w terminie 3 Dni Roboczych od daty otrzymania zastrzeżeń. Na wniosek Wykonawcy zgłoszenie i omówienie zastrzeżeń Zamawiającego może mieć miejsce w trakcie spotkania uzgodnieniowego, po którym uwagi Zamawiającego zostaną sporządzone w formie notatki.
7. Akceptacja przez Zamawiającego Protokołu Technicznego nastąpi poprzez podpisanie Protokołu Odbioru, sporządzonego zgodnie z Załącznikiem nr 2 do Umowy.
8. W terminach wynikających z harmonogramu stanowiącego element Projektu Technicznego Wykonawca dokona poszczególnych czynności wchodzących w zakres Wdrożenia, w tym w szczególności:
   1) skonfiguruje, przeprowadzi parametryzację i dostosuje DLP do potrzeb Zamawiającego zgodnie z Projektem Technicznym,
   2) zamodeluje procesy biznesowe w DLP uzgodnione z Zamawiającym, na zasadach określonych w Projekcie Technicznym,
   3) zainstaluje DLP na środowisku wskazanym przez Zamawiającego w Lokalizacjach Zamawiającego,
   4) dokona integracji DLP z systemami dziedzinowymi zgodnie z zasadami określonymi w Projekcie Technicznym,
   5) przekaże sporządzoną w języku polskim dokumentację producenta DLP (techniczną, administratora, użytkownika) oraz ogólne warunki licencyjne i warunki korzystania z Usługi Asysty Technicznej producenta,
   6) przekaże sporządzoną w języku polskim Dokumentację powykonawczą, sporządzoną na zasadach określonych w Projekcie Technicznym.
9. W ramach wdrożenia Wykonawca dokona pełnej konfiguracji i sprawdzenia poprawności działania DLP. Wykonawca, przy udziale wyznaczonych pracowników Zamawiającego, przeprowadzi testy wdrożeniowe (zgodnie z zaakceptowanym przez Zamawiającego planem testów), zapewniające możliwość sprawdzenia poprawności działania wszystkich funkcjonalności i wymagań umownych, w tym wynikających z Projektu Technicznego, odnoszących się do systemu DLP.
10. Odbiór dokumentów przekazanych na etapie Wdrożenia nastąpi poprzez podpisanie przez Zamawiającego Protokołu Odbioru, sporządzonego zgodnie z Załącznikiem nr 2 do Umowy.
11. Wykonawca zobowiązuje się do wdrożenia DLP na podstawie zaakceptowanego przez Zamawiającego Projektu Technicznego, na wskazanej przez Zamawiającego platformie sprzętowo-systemowej, w dacie wynikającej z zaakceptowanego przez Zamawiającego haromonogramu stanowiącego element Projektu Technicznego.
12. Prawidłowość przeprowadzenia Wdrożenia poddana będzie weryfikacji przez Zamawiającego, w szczególności poprzez przeprowadzenie testów odbiorowych systemu DLP zgodnie z zasadami opisanymi w Projekcie Technicznym. Harmonogram realizacji prac wdrożeniowych stanowiący element Projektu Technicznego powinien uwzględniać możliwość zgłaszania przez Zamawiającego uwag oraz konieczność ich uwzględnienia przez Wykonawcę, przy dochowaniu terminu wdrożenia systemu DLP określonego w ust. 1.
13. Prawidłowe wykonanie Wdrożenia (w tym prawidłowy wynik testów wdrożeniowych) zostanie potwierdzone podpisanym przez Zamawiającego bez zastrzeżeń Protokołem Wdrożenia, którego wzór stanowi Załącznik nr 3 do Umowy.
14. W przypadku stwierdzenia przez Zamawiającego jakichkolwiek nieprawidłowości w działaniu DLP lub jego poszczególnych funkcjonalności (w szczególności jeżeli DLP nie będzie spełniał któregokolwiek z wymagań określonych w Umowie lub Projekcie Technicznym) lub w wykonaniu którejkolwiek z czynności lub dokumentów zrealizowanych w ramach Wdrożenia - Zamawiający odmówi podpisania Protokołu Wdrożenia, sporządzając protokół zawierający przyczyny odmowy odbioru. Uprawnienie do odmowy odbioru Wdrożenia przysługuje Zamawiającemu niezależnie od ilości i zakresu czynności lub dokumentów wykonanych w ramach Wdrożenia, których dotyczy stwierdzony brak lub nieprawidłowość.

15. W przypadku odmowy odbioru Wdrożenia przez Zamawiającego w sytuacji określonej w ust. 14, Zamawiający wyznaczy termin ponownego przeprowadzenia Wdrożenia, w tym wykonania nieprawidłowo zrealizowanych czynności lub przekazania poprawionych dokumentów wolnych od wad. Procedura czynności odbioru zostanie powtórzona na zasadach określonych w niniejszym paragrafie, przy czym może się ona ograniczać do wadliwie zrealizowanych czynności lub dokumentów w ramach Wdrożenia. Procedura weryfikacji czynności związanych z Wdrożeniem (testowaniem) systemu DLP zostanie powtórzona tylko jeden raz, chyba że Zamawiający postanowi inaczej.
16. W przypadku ponownego stwierdzenia przez Zamawiającego, że Wdrożenie, w tym którykolwiek jego element nie zostały zrealizowane prawidłowo - Zamawiający odmówi podpisania Protokołu Wdrożenia i jednocześnie przekaże Wykonawcy protokół przedstawiający powód kolejnej odmowy odbioru. W takiej sytuacji, jak również w przypadku niedotrzymania przez Wykonawcę wskazanego zgodnie z ust. 14 terminu, Zamawiającemu przysługuje prawo odstąpienia od Umowy z winy Wykonawcy zgodnie z § 11 ust. 2 pkt. 2 Umowy.
17. Wszelkie czynności związane z Wdrożeniem odbywają się na koszt i ryzyko Wykonawcy.

§ 5.
Zakres Usługi Asysty Technicznej oraz Usługi Wsparcia

1. W ramach Usługi Wsparcia świadczonej przez Wykonawcę, w okresie wskazanym w § 2 ust. 3 Umowy, Zamawiający będzie miał prawo do korzystania z konsultacji związanych z działaniem oraz zasadami korzystania z systemu DLP, w tym modelowania procesów biznesowych przy wykorzystaniu tego narzędzia.
2. Konsultacje, o których mowa w ust. 1 dotyczyć mogą wszelkich problemów zgłaszanych przez Zamawiającego odnośnie DLP lub związanych z zasadami działania DLP, jak również na wykonywaniu prac lub udzielaniu wsparcia Zamawiającemu przy bieżących pracach administracyjnych, konfiguracyjnych, analitycznych, raportowych związanych z DLP.
3. Konsultacje będą świadczone w języku polskim, przez osoby wskazane w § 3 ust. 1 pkt. 5 drogą elektroniczną – adres e-mail: ……. lub telefoniczną pod numerem telefonu: ……., lub w siedzibie Zamawiającego w Dni Robocze, w godzinach: 9.00 – 15.00.
4. Konsultacje w ramach Usługi Wsparcia polegać będą w szczególności na udzielaniu Zamawiającemu asysty lub doradztwa przy:
   1) pracach biznesowych na Platformie DLP w tym modelowaniu procesów;
   2) implementacji i automatyzacji procesów biznesowych u Zamawiającego;
   3) realizowanych przez Zamawiającego prac programistycznych;
   4) konfiguracji lub rekonfiguracji oprogramowania DLP;
   5) prowadzeniu analiz dotyczących działania DLP;
   6) współpracy DLP z innymi systemami;
   7) przygotowywania raportów z działania DLP, w tym na potrzeby audytowe;
   8) prowadzeniu prac programistycznych, w tym polegających na wytwarzaniu oprogramowania lub jego dokumentacji, w zakresie dedykowanych potrzeb Zamawiającego związanych z korzystaniem z systemu DLP.
5. Wykonawca będzie przyjmował zgłoszenia Zamawiającego w godz. 7.00 - 15.00 w Dni Robocze pod nr telefonu …….. lub na adres e-mail: ……..Wykonawca zobowiązany jest potwierdzić przyjęcie zgłoszenia drogą elektroniczną na adres e-mail:....., niezwłocznie, jednak nie dłużej niż w ciągu 2 godzin od momentu jego otrzymania. Niepotwierdzenie zgłoszenia w powyższym terminie Zamawiający uznaje za przyjęcie zgłoszenia. Zgłoszenie potrzeby konsultacji złożone do Wykonawcy po godzinie 15.00 powinno zostać obsłużone do godziny 15.00 następnego Dnia Roboczego.
   O każdej zmianie adresu poczty elektronicznej lub numerów telefonów wskazanych powyżej, Wykonawca zobowiązany jest niezwłocznie powiadomić na piśmie Zamawiającego. Zmiana danych, o których mowa w zdaniu poprzedzającym nie wymaga zmiany Umowy w formie pisemnego aneksu.
6. Wykonawca zobowiązany jest do bieżącego rozwiązywania problemów zgłaszanych w trakcie konsultacji, nie później jednak niż w 8 godzin od zgłoszenia problemu przez Zamawiającego. Upoważnieni przedstawiciele Stron mogą uzgodnić inne terminy realizacji konsultacji, przy uwzględnieniu specyfiki zgłaszanego problemu, w tym ustalone w Dniach Roboczych od daty zgłoszenia problemu (w szczególności w przypadku zlecenia pracy polegającej na przygotowaniu dokumentu lub wykonaniu prac programistycznych).
7. Czas poszczególnych konsultacji udzielonych w danym miesiącu Usługi Wsparcia podlega sumowaniu w Protokole świadczenia Usługi Wsparcia. Łączna liczba konsultacji udzielonych w danym miesiącu świadczenia Usługi Wsparcia, po ich zsumowaniu, będzie zaokrąglona do pełnej godziny, zgodnie z zasadą że jeśli zsumowana wartość przekracza pełną godzinę powyżej 20 minut, jest zaokrąglana do kolejnej pełnej godziny.
8. Wykonawca zobowiązany będzie w całym okresie świadczenia Usługi Wsparcia do cyklicznego (co poniedziałek) informowania Zamawiającego o łącznej liczbie wykorzystanego przez pracowników Zamawiającego czasu konsultacji oraz czasu prac programistycznych, wraz z opisem wykonanych zadań w ramach zrealizowanych świadczeń.
9. Wykonanie przez Wykonawcę zobowiązań z tytułu Usługi Wsparcia w każdym kwartale jej świadczenia zostanie potwierdzone przez upoważnionych przedstawicieli Stron Protokołem świadczenia Usługi Wsparcia, którego wzór stanowi Załącznik nr 5 do Umowy. W protokole tym będą wskazane utwory wykonane na rzecz Zamawiającego w danym okresie rozliczeniowym.
10. Wykonawca zobowiązany będzie do zapewnienia Zamawiającemu możliwości korzystania z producenckiej Usługi Asysty Technicznej dla oprogramowania DLP, zgodnie z ogólnymi warunkami producenta oraz warunkami niniejszej Umowy.

11. W ramach Usługi Asysty Technicznej, Zamawiający będzie miał prawo do:
    1) otrzymywania Aktualizacji wraz z dokumentacją Aktualizacji (o ile dla danej Aktualizacji została przez producenta wytworzona); Wykonawca na podstawie Umowy udziela Zamawiającemu licencji (na zasadach subskrypcji) uprawniającej do korzystania przez Zamawiającego z Aktualizacji (w okresie obowiązywania Usługi Asysty Technicznej wskazanym w § 2 ust. 2 Umowy wraz z dokumentacją Aktualizacji, zgodnie z ogólnymi warunkami licencyjnymi producenta, na następujących zasadach:
        a) Wykonawca w ramach udzielonej licencji upoważnia Zamawiającego do instalowania, utrwalania i korzystania z Aktualizacji wraz z jej dokumentacją oraz trwałego lub czasowego zwielokrotnienia Aktualizacji w całości lub części jakimikolwiek środkami i w jakiejkolwiek formie w zakresie, w którym jest to niezbędne dla wprowadzania, wyświetlania, stosowania, przystosowania, przechowywania Aktualizacji dla własnych potrzeb Zamawiającego, zgodnie z jej charakterem i przeznaczeniem oraz warunkami Umowy,
        b) licencja udzielona zgodnie z lit. a może być wykorzystywana wyłącznie dla celów działalności Zamawiającego i nie obejmuje prawa do wprowadzania Aktualizacji do obrotu lub przekazywania ani w części ani w całości osobom trzecim zarówno odpłatnie, jak i nieodpłatnie w żadnej formie prawnej,
        c) w ramach udzielonej licencji Wykonawca upoważnia także Zamawiającego do korzystania z dokumentacji Aktualizacji dostępnej wraz z Aktualizacją, na polach eksploatacji wskazanych w lit. a,
        d) korzystanie z Aktualizacji wraz z ich dokumentacją następuje w ramach wynagrodzenia określonego w § 6 ust. 1 pkt 3 Umowy, bez konieczności ponoszenia przez Zamawiającego jakichkolwiek dodatkowych opłat licencyjnych;
    2) przeniesienia DLP, w tym Aktualizacji na inną platformę systemową, jeżeli potrzeba taka po stronie Zamawiającego zaistnieje, oraz wsparcia technicznego udzielanego przez Wykonawcę w tym zakresie;
    3) korzystania z pomocy telefonicznej i elektronicznej dotyczącej DLP lub Aktualizacji w światowych centrach producenta DLP we wszystkie dni roku, przez 24 godziny pod numer telefonu: ……, e-mail: ……,
    4) dostępu elektronicznego przez 24 godziny na dobę, 7 dni w tygodniu (poprzez serwis internetowy producenta) do informacji na temat subskrybowanych przez Zamawiającego produktów producenta, biuletynów technicznych DLP, list dyskusyjnych, bazy danych problemów technicznych dotyczących DLP rejestrowanych przez pracowników działu Asysty Technicznej producenta.
12. Potwierdzenie uprawnienia do korzystania przez Zamawiającego z Usługi Asysty Technicznej nastąpi poprzez podpisanie przez Strony bez zastrzeżeń Protokołu Wdrożenia, zgodnie z wzorem stanowiącym Załącznik nr 3 do Umowy.

§ 6.
Wynagrodzenie

1. Maksymalne łączne wynagrodzenie z tytułu wykonania Umowy zawiera w sobie wszelkie koszty Wykonawcy związane z realizacją Umowy i nie przekroczy netto …… zł (słownie złotych: ……..) powiększone o należny podatek od towarów i usług (VAT), co daje kwotę wynagrodzenia brutto …….. zł (słownie złotych: ……), w tym:
    1) wynagrodzenie z tytułu korzystania z systemu DLP na zasadach subskrypcji, zgodnie z ogólnymi warunkami producenta DLP wynosi: netto …… zł (słownie złotych: ……..) powiększone o należny podatek od towarów i usług (VAT), co daje kwotę wynagrodzenia brutto ……zł (słownie złotych: ……),
    2) wynagrodzenie z tytułu Wdrożenia Systemu DLP wynosi: netto …… zł (słownie złotych: ……..) powiększone o należny podatek od towarów i usług (VAT), co daje kwotę wynagrodzenia brutto ……zł (słownie złotych: ……),
    3) wynagrodzenie z tytułu korzystania z Usługi Asysty Technicznej w okresie wskazanym w § 2 ust. 2 Umowy wynosi netto …… zł (słownie złotych: ……..) powiększone o należny podatek od towarów i usług (VAT), co daje kwotę wynagrodzenia brutto …….. zł (słownie złotych:……),
    4) łączne wynagrodzenie z tytułu świadczenia Usługi Wsparcia w okresie wskazanym w § 2 ust. 3 Umowy wyniesie nie więcej niż netto …….. zł (słownie złotych: ……) powiększone o należny podatek od towarów i usług (VAT), co daje kwotę wynagrodzenia brutto …… zł (słownie złotych: ……).
2. Wynagrodzenie jednostkowe z tytułu jednej godziny świadczenia Usługi Wsparcia wynosi netto: …… zł (słownie złotych: ……..), powiększone o należny podatek od towarów i usług (VAT), co daje kwotę wynagrodzenia brutto …….. (słownie złotych: ……..).
3. Wynagrodzenie Wykonawcy z tytułu realizacji Usługi Wsparcia w danym kwartale zostanie ustalone jako iloczyn faktycznie udzielonych godzin konsultacji wynikających z Protokołu Świadczenia Usługi Wsparcia oraz stawki jednostkowej brutto za jedną godzinę świadczenia Usługi Wsparcia wskazanej w ust. 2. Wynagrodzenie kwartalne ustalone według powyższych zasad każdorazowo pomniejsza łączną kwotę wynagrodzenia wskazaną w ust. 1 pkt 4 Umowy.
4. W wynagrodzeniu, o którym mowa w ust. 1 pkt 1 zawierają się wszelkie koszty z tytułu udzielenia Zamawiającemu licencji uprawniającej do korzystania z systemu DLP (wraz z dokumentacją) zgodnie z warunkami Umowy, jak również z Aktualizacji wraz z ich dokumentacją pozyskanych przez Zamawiającego w trakcie świadczenia Usługi Asysty Technicznej.
5. W wynagrodzeniu, o którym mowa w ust. 1 pkt 2 zawierają się wszelkie koszty z tytułu realizacji wszelkich czynności w ramach Wdrożenia, w tym wynagrodzenie z tytułu przeniesienia na Zamawiającego autorskich praw majątkowych do utworów wykonanych w ramach Wdrożenia (w tym do Projektu Technicznego i Dokumentacji powykonawczej).

6. W wynagrodzeniu, o którym mowa w ust. 1 pkt 4 zawierają się wszelkie koszty z tytułu realizacji wszelkich czynności w ramach Usługi Wsparcia, w tym wynagrodzenie z tytułu przeniesienia na Zamawiającego autorskich praw majątkowych do utworów powstałych w ramach Usługi Wsparcia.
7. Wykonawca oświadcza i gwarantuje, że warunki korzystania z systemu DLP oraz Usługi Asysty Technicznej nie wymagają ponoszenia dodatkowych opłat na rzecz Wykonawcy lub jakiejkolwiek osoby trzeciej, zaś wynagrodzenie wskazane w ust. 1 obejmuje całość wynagrodzenia za wykonanie przez Wykonawcę obowiązków wynikających z Umowy. Zamawiający nie będzie zobowiązany do nabywania żadnych usług ani uprawnień innych niż wyraźnie zdefiniowanych Umową, w szczególności zobowiązanie Wykonawcy oznacza, że nie jest konieczne nabycie przez Zamawiającego żadnych dodatkowych licencji ani uprawnień poza opisanymi Umową i objętymi łącznym maksymalnym wynagrodzeniem za wykonanie Umowy wskazanym w ust. 1.
8. Wykonawca przyjmuje do wiadomości, że wynagrodzenie określone w ust. 1 pkt 4 ma charakter maksymalny, a Zamawiający zastrzega sobie prawo do skorzystania ze świadczeń w zakresie Usług Wsparcia w liczbie mniejszej niż wynikałaby z kwoty wskazanej w ust. 1 pkt 4, zaś Wykonawcy w takim przypadku nie będzie przysługiwać jakiekolwiek roszczenie wobec Zamawiającego z tego tytułu. Wykonawcy przysługuje wynagrodzenie odpowiadające wyłącznie faktycznej liczbie zrealizowanych na rzecz Zamawiającego konsultacji w ramach poszczególnych okresów rozliczeniowych Usługi Wsparcia, obliczone zgodnie z ust. 3.
9. Zapłata wynagrodzenia, o którym mowa w ust. 1 pkt 1-3 nastąpi w terminie 28 dni od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT, w trzech równych częściach, przy czym Wykonawca uprawniony jest wystawić fakturę obejmującą pierwszą cześć wynagrodzenia w dniu podpisania bez zastrzeżeń Protokołu Wdrożenia, o którym mowa w § 4 ust. 13 Umowy, fakturę obejmującą drugą cześć wynagrodzenia – po upływie roku od wystawienia pierwszej faktury, jednak nie później niż 30.11.2022 r. oraz fakturę obejmującą trzecią część wynagrodzenia po upływie roku od wystawienia drugiej faktury, jednak nie później niż 30.11.2023 r. Zapłata wynagrodzenia za świadczenie Usługi Wsparcia w danym kwartale będzie następowała w terminie 28 dni od daty otrzymania przez Zamawiającego poszczególnych faktur VAT. Podstawą do wystawienia przez Wykonawcę faktur VAT z tytułu wynagrodzenia określonego w ust. 1 pkt. 4 będzie podpisany bez zastrzeżeń przez Zamawiającego Protokół świadczenia Usługi Wsparcia, o którym mowa w § 5 ust. 9 Umowy.
10. Błędnie wystawiona faktura VAT lub brak któregokolwiek z protokołów, o którym mowa w ust. 9 spowoduje naliczenie ponownego 28 dniowego terminu płatności, od daty dostarczenia prawidłowo wystawionej faktury lub właściwego dokumentu stanowiącego podstawę do zapłaty.
11. Wykonawca jest uprawniony do wystawiania faktur VAT i posiada numer NIP: ……..
12. Zapłata wynagrodzenia będzie dokonywana przelewem na rachunek bankowy Wykonawcy wskazany na fakturze. Za termin wykonania płatności uznaje się dzień obciążenia rachunku bankowego Zamawiającego.
13. W przypadku niezgodności, w dniu realizacji płatności, numeru rachunku bankowego wskazanego przez Wykonawcę na fakturze z numerem rachunku bankowego zamieszczonym w wykazie podmiotów, o których mowa w art. 96b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2020 r., poz. 106 ze zm.), Strony ustalają, że realizacja płatności nastąpi w trybie art. 108a ww. ustawy.
14. Jeżeli w trakcie realizacji Umowy nastąpi zmiana:
    1) stawki podatku od towarów i usług oraz podatku akcyzowego,
    2) wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej ustalonych na podstawie ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę,
    3) zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub ubezpieczenie zdrowotne,
    4) zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych (Dz. U. poz. 2215 oraz z 2019 r. poz. 1074 i 1572)

    a zmiany te będą miały wpływ na koszty wykonania Umowy – zastosowanie mają zasady wprowadzania zmian wysokości wynagrodzenia należnego Wykonawcy określone w ust. 16-22 poniżej.
15. Zmiana wysokości wynagrodzenia wymaga zmiany Umowy w drodze aneksu.
16. Wykonawca najpóźniej w terminie 30 dni od dnia wejścia w życie przepisów wprowadzających zmiany o których mowa w ust. 14 uprawniony jest do wystąpienia do Zamawiającego z pisemnym wnioskiem o dokonanie zmiany Umowy w zakresie wysokości wynagrodzenia wraz z jej uzasadnieniem oraz dokumentami niezbędnymi do oceny przez Zamawiającego, czy zmiany, o których mowa w ust. 14 mają wpływ na koszty wykonania Umowy przez Wykonawcę oraz w jakim stopniu zmiany tych kosztów uzasadniają zmianę wysokości wynagrodzenia Wykonawcy określonego w Umowie, a w szczególności:
    1) szczegółową kalkulację proponowanej zmienionej wysokości wynagrodzenia Wykonawcy oraz wykazanie adekwatności propozycji do zmiany wysokości kosztów wykonania Umowy przez Wykonawcę.
    2) przyjęte przez Wykonawcę zasady kalkulacji wysokości kosztów wykonania Umowy oraz założenia co do wysokości dotychczasowych oraz przyszłych kosztów wykonania Umowy, wraz z dokumentami potwierdzającymi prawidłowość przyjętych założeń - takimi jak np. umowy o pracę, dokumenty potwierdzające zgłoszenie pracowników do ubezpieczeń.
17. W terminie 30 dni od otrzymania wniosku o którym mowa w ust. 16, Zamawiający może zwrócić się do Wykonawcy o jego uzupełnienie lub przekazanie dodatkowych wyjaśnień lub dokumentów (np. zażądać: oryginałów do wglądu, przekazania kopii dokumentów potwierdzonych za zgodność z oryginałami).

18. Zamawiający w terminie 30 dni od dnia otrzymania kompletnego wniosku zajmie w stosunku do niego pisemne stanowisko. Za dzień przekazania stanowiska uznaje się dzień jego wysłania na adres właściwy dla doręczeń pism dla Wykonawcy.
19. Zamawiający najpóźniej w terminie 30 dni od dnia wejścia w życie przepisów wprowadzających zmiany, o których mowa w ust. 14 może przekazać Wykonawcy pisemny wniosek o dokonanie zmiany Umowy. Wniosek powinien zawierać co najmniej propozycję zmiany Umowy w zakresie wysokości wynagrodzenia oraz powołanie zmian przepisów.
20. Przed przekazaniem wniosku, o którym mowa w ust. 19, Zamawiający może zwrócić się do Wykonawcy o złożenie wyjaśnień lub dokumentów (oryginałów do wglądu lub kopii potwierdzonych za zgodność z oryginałem) niezbędnych do oceny przez Zamawiającego, czy zmiany, o których mowa w ust. 16, mają wpływ na koszty wykonania Umowy przez Wykonawcę oraz w jakim stopniu zmiany tych kosztów uzasadniają zmianę wysokości wynagrodzenia. Rodzaj i zakres tych informacji określi Zamawiający. Postanowienia ust. 17-18 stosuje się odpowiednio, z tym, że Wykonawca jest zobowiązany w każdym przypadku do zajęcia pisemnego stanowiska w terminie 30 dni od dnia otrzymania wniosku od Zamawiającego.
21. W przypadku niewykonania lub nienależytego wykonania przez Wykonawcę zobowiązania określonego w ust. 20 w terminie określonym w ust. 20, Wykonawca zapłaci na rzecz Zamawiającego karę umowną w wysokości 300,00 zł za każdy rozpoczęty dzień kalendarzowy zwłoki. Jeżeli w terminie określonym w ust. 20 Wykonawca nie przedłoży wyjaśnień lub dokumentów, o których mowa w ust. 20 lub przedłożone przez Wykonawcę wyjaśnienia lub dokumenty będą niewystarczające do dokonania przez Zamawiającego oceny, o której mowa w ust. 16 - Zamawiający wyznaczy Wykonawcy dodatkowy termin, nie dłuższy niż 10 dni, na dostarczenie lub uzupełnienie wyjaśnień lub dokumentów. W przypadku bezskutecznego upływu terminu wyznaczonego zgodnie ze zdaniem drugim, Zamawiający uprawniony będzie do wypowiedzenia Umowy z zachowaniem miesięcznego terminu wypowiedzenia.
22. Jeżeli w trakcie procedury opisanej w ust. 16-21 zostanie wykazane, że zmiany, o których mowa w ust. 14 uzasadniają zmianę wysokości wynagrodzenia, Strony uzgodnią treść aneksu do Umowy oraz podpiszą aneks, z zachowaniem zasady zmiany wysokości wynagrodzenia w kwocie odpowiadającej zmianie kosztów wykonania Umowy wywołanych przyczynami określonymi w ust. 14.
23. Zasady zmiany wynagrodzenia określone w ust. 15 – 22 powyżej mają odpowiednie zastosowanie do zmiany wysokości wynagrodzenia w przypadku zmiany średniorocznego wskaźnika cen towarów i usług konsumpcyjnych ogółem ogłaszanego w komunikacie Prezesa Głównego Urzędu Statystycznego na podstawie przepisów ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (dalej „wskaźnik"), z zastrzeżeniem następujących zasad:
    1) zmiana wynagrodzenia jest możliwa, gdy wskaźnik w stosunku do roku poprzedniego będzie wyższy niż 101,5 albo będzie niższy niż 98,5 (tj. wzrost poziomu cen o 1,5% albo spadek poziomu cen o 1,5%);
    2) zmiana wynagrodzenia obowiązuje w stosunku do wynagrodzenia, które stanie się należne dopiero po dniu podpisania aneksu do Umowy (w formie pisemnej pod rygorem nieważności), tym samym zmiana nie dotyczy wynagrodzenia ustalonego (wystawienie faktury) lub rozliczonego przed dokonaniem zmiany Umowy;
    3) zmiana wynagrodzenia możliwa jest najwcześniej po upływie 12 miesięcy od zawarcia Umowy (tzn., jeżeli Umowa została zawarta w październiku 2021 roku, to pierwsza zmiana będzie możliwa po publikacji wskaźnika w 2023 roku), chyba że data zawarcia Umowy przypada 180 dni od daty złożenia oferty przez Wykonawcę, wówczas:
        a) zmiana wynagrodzenia możliwa jest po upływie 12 miesięcy od dnia otwarcia oferty Wykonawcy,
        b) wartość zmiany wskaźnika zostanie ustalona nie względem roku poprzedniego, a względem roku, w którym doszło do otwarcia oferty Wykonawcy;
    4) z zastrzeżeniem limitu ustalonego w pkt 5, w przypadku zmiany wskaźnika, każdorazowa wartość zmiany wynagrodzenia jednostkowe z tytułu jednej godziny świadczenia Usługi Wsparcia, określonego w ust. 2 będzie ustalana w następujący sposób:
        a) jeśli zmiana wskaźnika będzie na poziomie powyżej 101,5 do 103 (wzrost poziomu cen od 1,5% do 3%) - wynagrodzenie z tytułu jednej godziny świadczenia Usługi Wsparcia określone w ust. 2 wzrośnie o 1% względem wynagrodzenia, które w chwili zmiany wynika z Umowy, a jeśli zmiana wskaźnika będzie na poziomie poniżej 98,5 do 97 (spadek poziomu cen od 1,5% do 3%) - wynagrodzenie z tytułu jednej godziny świadczenia Usługi Wsparcia określone w ust. 2 zmaleje o 1% względem wynagrodzenia, które w chwili zmiany wynika z Umowy,
        b) jeśli zmiana wskaźnika będzie na poziomie powyżej 103 do 105 (wzrost poziomu cen od 3 % do 5 %) - wynagrodzenie z tytułu jednej godziny świadczenia Usługi Wsparcia określone w ust. 2 wzrośnie o 2 % względem wynagrodzenia, które w chwili zmiany wynika z Umowy, a jeśli zmiana wskaźnika będzie na poziomie poniżej 97 do 95 (spadek poziomu cen od 3% do 5%) - wynagrodzenie z tytułu jednej godziny świadczenia Usługi Wsparcia określone w ust. 2 zmaleje o 2% względem wynagrodzenia, które w chwili zmiany wynika z Umowy,
        c) jeśli zmiana wskaźnika będzie na poziomie powyżej 105 (wzrost poziomu cen ponad 5%) - wynagrodzenie z tytułu jednej godziny świadczenia Usługi Wsparcia określone w ust. 2 zmieni się o 3,5% względem wynagrodzenia, które w chwili zmiany wynika z Umowy, a jeśli zmiana wskaźnika będzie na poziomie poniżej 5 (spadek poziomu cen o ponad 5%) - wynagrodzenie z tytułu jednej godziny świadczenia Usługi Wsparcia określone w ust. 2 zmaleje o 3,5% względem wynagrodzenia, które w chwili zmiany wynika z Umowy;
    5) zmiany wskaźnika skutkować mogą w całym okresie obowiązywania Umowy zmianą ceny z tytułu jednej godziny świadczenia Usługi Wsparcia, określonej w ust. 2 łącznie nie więcej niż o 10 % w stosunku do wartości wskazanej w ofercie;
    6) zmiany wynagrodzenia zgodnie z zasadami określonymi w niniejszym ustępie są możliwe do wysokości nieprzekraczającej łącznie 5% wartości wynagrodzenia określonego w ust. 1 Umowy;
    7) uprawnienie do wnioskowania o waloryzację wynagrodzenia zastrzeżone jest dla obu Stron umowy.

24. Wykonawca, którego wynagrodzenie zostało zmienione w związku ze wskaźnika, o którym mowa w ust. 23, zobowiązany jest do zmiany wynagrodzenia przysługującego podwykonawcy, z którym zawarł umowę, w zakresie odpowiadającym zmianom cen materiałów lub kosztów dotyczących zobowiązania podwykonawcy.

§ 7.

Prawo do korzystania z DLP, przeniesienie autorskich praw do utworów wykonanych przez Wykonawcę w ramach realizacji Umowy i odpowiedzialność za wady prawne

1. Wykonawca zapewnia, że korzystanie przez Zamawiającego z rezultatów prac przekazanych Zamawiającemu w ramach Umowy, stanowiących utwory w rozumieniu przepisów ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz. U. z 2019 r., poz. 1231 ze zm.), nie będzie naruszało praw osób trzecich, w szczególności praw autorskich oraz praw własności przemysłowej. Wykonawca zapewnia, że osoby uprawnione z tytułu osobistych praw autorskich do utworów powstałych w wyniku realizacji Umowy nie będą wykonywać takich praw w stosunku do Zamawiającego. Na podstawie Umowy Wykonawca udziela licencji (na zasadzie subskrypcji) oraz przeniesie na Zamawiającego autorskie prawa majątkowe w zakresie i w sposób opisany poniżej. Przeniesienie autorskich praw majątkowych następuje z chwilą wydania Zamawiającemu przez Wykonawcę utworu wykonanego na podstawie Umowy.
2. Zamawiający, w ramach wynagrodzenia, o którym mowa w § 6 ust. 1 pkt 1 Umowy nabędzie prawo upoważniające do korzystania na zasadzie subskrypcji w okresie wskazanym w § 2 ust. 1 pkt 2 Umowy, z dostarczonej przez Wykonawcę systemu DLP wraz z jej dokumentacją (w tym Aktualizacji i ich dokumentacji). Prawo do korzystania (subskrypcja) obowiązuje przez okres 36 miesięcy od daty podpisania przez Zamawiającego bez zastrzeżeń Protokołu Wdrożenia.
3. W ramach prawa, o którym mowa w ust. 2, Zamawiający jest upoważniony do instalowania, utrwalania i korzystania z systemu DLP oraz jej dokumentacji, w tym trwałego lub czasowego zwielokrotnienia DLP lub dokumentacji w całości lub części jakimikolwiek środkami i w jakiejkolwiek formie w zakresie, w którym jest to niezbędne dla wprowadzania, wyświetlania, stosowania, przystosowania, przechowywania DLP oraz jego dokumentacji dla własnych potrzeb Zamawiającego, zgodnie z ich: charakterem i przeznaczeniem oraz warunkami Umowy i ogólnymi warunkami licencyjnymi producenta DLP.
4. Wykonawca oświadcza, że warunki licencyjne dostarczonego DLP wraz z dokumentacją są zgodne z warunkami Umowy oraz ponosi wobec Zamawiającego odpowiedzialność, jeżeli jakakolwiek osoba trzecia zgłosi wobec Zamawiającego zarzut, że korzystanie przez Zamawiającego z DLP lub jego dokumentacji zgodnie z Umową narusza ogólne warunki licencyjne producenta.
5. Jeżeli w wyniku realizacji Wdrożenia, Usługi Asysty Technicznej lub Usługi Wsparcia powstanie utwór w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych majątkowe prawa autorskie do utworu zostają na podstawie niniejszej Umowy przeniesione na Zamawiającego w zakresie i w sposób opisany poniżej.
6. Na podstawie Umowy, z chwilą powstania jakiegokolwiek utworu w wyniku realizacji którejkolwiek z czynności w ramach Wdrożenia (w tym Projektu Technicznego i Dokumentacji powykonawczej), Usługi Asysty Technicznej lub Usługi Wsparcia Wykonawca przenosi na Zamawiającego autorskie prawa majątkowe do powstałego utworu, na polach eksploatacji wskazanych w ust. 7 i 8, w ramach wynagrodzenia, ustalonego zgodnie z § 6 ust. 1 Umowy.
7. Przeniesienie autorskich praw majątkowych do utworów, o których mowa w niniejszym paragrafie, innych niż programy komputerowe, obejmuje następujące pola eksploatacji:
   1) w zakresie utrwalania i zwielokrotniania utworu – wytwarzanie każdą techniką egzemplarzy utworów, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;
   2) w zakresie obrotu oryginałem oraz egzemplarzami, na których utwory utrwalono – wprowadzanie do obrotu, użyczanie oraz najem oryginału oraz egzemplarzy;
   3) w zakresie rozpowszechniania utworów w sposób inny niż określony w pkt 2 – publiczne wykonanie, wystawienie, wyświetlanie, odtwarzanie oraz nadawanie i reemitowanie, a także publiczne udostępnianie utworów w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i w czasie przez siebie wybranym;
   4) dowolne przetwarzanie utworów, w tym łączenie z innymi utworami;
   5) tłumaczenie, przystosowanie, zmiany układu lub jakiekolwiek inne zmiany w utworze;
   6) zezwalanie na wykonywanie zależnych praw autorskich poprzez rozporządzanie i korzystanie na wszystkich polach eksploatacji wymienionych w pkt 1-5.
8. Przeniesienie autorskich praw majątkowych do utworów, o których mowa w niniejszym paragrafie, będących programami komputerowymi, obejmuje następujące pola eksploatacji:
   1) trwałe i czasowe zwielokrotnianie utworów w całości lub części, jakimikolwiek środkami i w jakiejkolwiek formie, w tym do wprowadzania, wyświetlania, stosowania, przekazywania i przechowywania, m.in. do systemu informatycznego, pamięci komputerów, sieci komputerowych;
   2) tłumaczenie, przystosowanie, zmiany układu lub jakiekolwiek inne zmiany w programie komputerowym, w tym łączenie w jeden system z innymi programami, z zachowaniem praw osoby, która tych zmian dokonała;
   3) rozpowszechnianie, w tym użyczanie, najem, dzierżawa, upoważnienie innych osób do wykorzystywania w całości lub części programu komputerowego lub jego kopii;
   4) modyfikacje kodu źródłowego;
   5) zezwalanie na wykonywanie zależnych praw autorskich poprzez rozporządzanie i korzystanie na wszystkich polach eksploatacji wymienionych w pkt 1-4.

9. Z chwilą przekazania utworu będącego programem komputerowym Wykonawca każdorazowo przekaże Zamawiającemu kody źródłowe wraz z dokumentacją projektową, skrypty konfiguracyjne lub inne skrypty (np. budujące aplikację, instalacyjne, zasilające inicjalnie).
10. Z chwilą przekazania Zamawiającemu poszczególnych utworów wykonanych w ramach realizacji poszczególnych Usług, Zamawiający nabywa własność nośników, na których utwory te utrwalono, w ramach wynagrodzenia ustalonego zgodnie z § 6 ust. 1 Umowy.
11. W przypadku wystąpienia osób trzecich wobec Zamawiającego z roszczeniami opartymi na twierdzeniu, iż używane przez Zamawiającego: systemu DLP lub jakikolwiek inny utwór, z którego Zamawiający będzie korzystał na podstawie Umowy naruszają jakiekolwiek prawa, o których mowa w ust. 1, Zamawiającemu przysługują wszystkie niżej wymienione uprawnienia, które ma prawo zrealizować według swojego wyboru (łącznie lub osobno):
    1) prawo odstąpienia od Umowy, przy czym Wykonawcy nie przysługuje w takim wypadku zwrot jakichkolwiek kosztów, odszkodowań itp.,
    2) prawo żądania zapłaty przez Wykonawcę kary umownej w wysokości określonej w § 10 ust. 5 Umowy oraz prawo żądania odszkodowania uzupełniającego na zasadach ogólnych Kodeksu cywilnego.
12. W przypadku wytoczenia przeciwko Zamawiającemu powództwa opartego na twierdzeniu opisanym w ust. 11 Wykonawca zobowiązuje się zapewnić Zamawiającemu na swój koszt ochronę sądową oraz ponieść konsekwencje zapadłego wyroku sądowego tj. Wykonawca pokryje wszelkie opłaty, koszty, odszkodowania lub zadośćuczynienia, które będzie musiał zapłacić Zamawiający, jeżeli zapewnienie, o którym mowa w ust. 1, ust. 4 lub § 3 ust. 1 pkt 1 Umowy nie okaże się prawdziwe.

§ 8.

Zabezpieczenie należytego wykonania Umowy (dalej: „**ZNWU**")

1. Wykonawca złożył u Zamawiającego ZNWU w wysokości …… zł (słownie złotych: ……..) w jednej z form, o których mowa w art. 450 ustawy Prawo zamówień publicznych, co stanowi … % wynagrodzenia brutto, o którym mowa w § 6 ust. 1 Umowy.
2. ZNWU dotyczy wykonania Umowy.
3. ZNWU zostanie zwolnione (zwrócone) w terminie 30 dni od daty wykonania Umowy i uznania jej przez Zamawiającego za należycie wykonaną.
4. W przypadku zmiany formy ZNWU w trakcie wykonywania Umowy stosuje się postanowienia ust. 5-10.
5. ZNWU w formie pieniężnej Wykonawca wpłaca przelewem na rachunek bankowy wskazany przez Zamawiającego.
6. ZNWU wnoszone w formie gwarancji bankowej lub ubezpieczeniowej może być wystawione przez bank albo ubezpieczyciela. Bank lub ubezpieczyciel zapłaci, na rzecz Zamawiającego w terminie 30 dni od pisemnego żądania kwotę …….. (słownie złotych: ……), na pierwsze wezwanie Zamawiającego, bez odwołania, bez warunku, niezależnie od kwestionowania czy zastrzeżeń Wykonawcy i bez dochodzenia czy wezwanie Zamawiającego jest uzasadnione czy nie.
7. ZNWU wnoszone w formie poręczenia ma być wystawione przez bank, spółdzielczą kasę oszczędnościowo-kredytową lub podmiot, o którym mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości, który poręczy należyte wykonanie umowy do wysokości ……. (słownie złotych: ……..).
8. W przypadku, gdy ZNWU będzie wnoszone w formie: poręczenia, bankowej lub ubezpieczeniowej gwarancji, Zamawiający zastrzega sobie prawo do akceptacji projektu tych dokumentów.
9. ZNWU wniesione w formie pieniężnej podlega zwrotowi wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszty prowadzenia rachunku bankowego oraz prowizji bankowej za przelew pieniędzy na rachunek Wykonawcy.
10. ZNWU w formie innej niż pieniężna Wykonawca złoży u Zamawiającego w Kancelarii Głównej, Warszawa ul. Poleczki 33, z dopiskiem „Dla Departamentu Informatyki".

§ 9.

Poufność, bezpieczeństwo informacji i zasady przetwarzania danych osobowych

1. Wszelkie wiadomości, w których posiadanie wszedł Wykonawca przy zawieraniu i wykonywaniu Umowy jest on zobowiązany zachować w poufności. Wykonawca zobowiązuje się nie ujawniać ich osobom trzecim, wyjąwszy przypadki prawem przewidziane.
2. Wykonawca zobowiązuje się do pisemnego zobowiązania osób realizujących Umowę do zachowania w poufności wiadomości, o których mowa w ust. 1.
3. Wykonawca zobowiązany jest do:
    1) przestrzegania regulacji wewnętrznych Zamawiającego dotyczących bezpieczeństwa informacji oraz bezpieczeństwa systemów informatycznych, w szczególności wskazanych w ust. 4;
    2) przestrzegania zasad użytkowania infrastruktury IT, w tym sprzętu informatycznego oraz oprogramowania wdrożonego u Zamawiającego, w szczególności zobowiązuje się, że wdrożony system DLP nie zakłóci w żaden sposób pracy funkcjonujących u Zamawiającego aplikacji;
    3) przestrzegania obowiązujących u Zamawiającego przepisów, w szczególności w zakresie ochrony informacji wrażliwych, w tym danych osobowych oraz innych informacji prawnie chronionych;

4) nieujawniania osobom trzecim informacji uzyskanych w trakcie i po wykonywaniu Umowy bez zgody Zamawiającego.

4. Wykonawca zobowiązuje się do wykonania Umowy w sposób spełniający wymogi bezpieczeństwa informacji, których treść jest określona w poniższych załącznikach do Zarządzenia Prezesa ARiMR nr 78/2019 z dnia 3 czerwca 2019 r. w sprawie wprowadzenia polityki bezpieczeństwa w ARiMR, stanowiących Załącznik nr 8 do Umowy:
   1) „Regulamin użytkownika" - załącznik nr 5;
   2) „Regulamin zarządzania incydentami" – załącznik nr 8;
   3) „Regulamin eksploatacji systemów teleinformatycznych" - załącznik nr 12;
   4) „Regulamin ochrony danych osobowych" - załącznik nr 14.
5. Wykonawca może korzystać ze świadczeń osób trzecich jako swoich podwykonawców, przy czym ponosi pełną odpowiedzialność za wykonywanie zobowiązań przez podwykonawcę, jak za własne działania lub zaniechania.
6. Wykonawca zobowiązuje się do przeszkolenia pracowników i osób trzecich, realizujących objęte Umową zadania, w zakresie zachowania zasad bezpieczeństwa informacji określonych w dokumentach stanowiących Załącznik nr 6 do Umowy oraz zasad przetwarzania danych osobowych określonych w przepisach o ochronie danych osobowych.
7. Wykonawca zobowiązuje się do przestrzegania przy wykonywaniu Umowy przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE.L. 2016.119.1 ze zm.) oraz przepisów krajowych wydanych w związku z ogólnym rozporządzeniem o ochronie danych, zwanym dalej także: „RODO".
8. Wykonawca pisemnie zobowiąże pracowników i osoby trzecie realizujące zobowiązania określone w Umowie do przestrzegania przepisów, o których mowa w ust. 7.
9. Wykonawca oświadcza, że zapoznał się z klauzulami informacyjnymi w zakresie przetwarzania danych osobowych, stanowiącymi Załącznik nr 7 do Umowy.
10. Wykonawca zobowiązuje się do złożenia oświadczenia o wypełnieniu obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane bezpośrednio lub pośrednio pozyskał w celu zawarcia oraz wykonania Umowy zgodnie z wzorem oświadczenia stanowiącym Załącznik nr 7A do Umowy.
11. Powierzenie przetwarzania danych osobowych niezbędnych do realizacji Umowy, następuje na podstawie odrębnej umowy, stanowiącej Załącznik nr 8 do Umowy. Dane osobowe z zasobów Zamawiającego mogą być przekazane podwykonawcy Wykonawcy jedynie na podstawie umowy powierzenia przetwarzania danych osobowych, której wzór zawiera Załącznik nr 8A do Umowy.
12. Przed przystąpieniem do realizacji Umowy Wykonawca dostarczy Zamawiającemu wykaz podwykonawców, z którymi będą zawarte umowy powierzenia przetwarzania danych osobowych.
13. W przypadku, gdy na skutek nieprawidłowości w przetwarzaniu danych osobowych przez podwykonawcę zostanie mu naliczona przez Zamawiającego kara umowna lub Zamawiający będzie dochodzić od podwykonawcy odszkodowania uzupełniającego na zasadach ogólnych Kodeksu cywilnego na podstawie odrębnej umowy zawartej zgodnie z Załącznikiem nr 8A do Umowy – Zamawiający zastrzega sobie prawo do potrącenia naliczonej podwykonawcy kary umownej lub odszkodowania z wynagrodzenia należnego Wykonawcy lub do skorzystania ze złożonego przez Wykonawcę zabezpieczenia należytego wykonania Umowy na co Wykonawca niniejszym wyraża zgodę.

§ 10.
Kary umowne

1. Wykonawca zobowiązany jest do zapłaty na rzecz Zamawiającego kary umownej w wysokości 10 000,00 zł za każdy stwierdzony przypadek naruszenia zakazu, o którym mowa w § 3 ust. 2 Umowy.
2. Za każdy rozpoczęty dzień kalendarzowy zwłoki w stosunku do któregokolwiek z terminów wynikających z § 4 ust. 1 2,4,6 lub 15 Umowy, Zamawiającemu przysługuje kara umowna w wysokości 0,05 % kwoty łącznego wynagrodzenia brutto, o którym mowa w § 6 ust. 1 Umowy.
3. Jeżeli zwłoka, o której mowa w ust. 2 wyniesie 14 dni, Zamawiający może, bez wyznaczenia dodatkowego terminu, odstąpić od Umowy (w terminie 30 dni od wystąpienia przesłanki umożliwiającej mu odstąpienie od Umowy) oraz zażądać kary umownej w wysokości 20% kwoty łącznego wynagrodzenia brutto określonego w § 6 ust. 1 Umowy, z zachowaniem prawa do naliczenia kary umownej zgodnie z ust. 2 do dnia odstąpienia przez Zamawiającego od Umowy.
4. W przypadku, gdy Wykonawca nie dotrzyma terminu udzielenia konsultacji w ramach Usługi Wsparcia wynikającego z § 5 ust. 6 Umowy – Zamawiający wyznaczy Wykonawcy dodatkowy, nieprzekraczalny termin na rozwiązanie problemu zgłoszonego w trakcie konsultacji lub udostępnienie specjalisty. Po bezskutecznym upływie tego terminu Zamawiający ma prawo naliczać karę umowną w wysokości 200,00 zł za każdą rozpoczętą godzinę zwłoki w stosunku do terminu wyznaczonego przez Zamawiającego. Jeżeli zwłoka przekroczy 48 godzin Zamawiający po bezskutecznym upływie tego terminu ma prawo naliczać karę umowną wskazaną w zdaniu poprzedzającym w podwójnej wysokości, do dnia udzielenia konsultacji lub rozpoczęcia uzgodnionych zadań włącznie.
5. W przypadku odstąpienia od Umowy lub wypowiedzenia Umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy, Zamawiającemu przysługuje kara umowna w wysokości 20% kwoty wynagrodzenia brutto, o którym mowa w § 6 ust. 1 Umowy.

6. W przypadku braku zapłaty lub nieterminowej zapłaty wynagrodzenia należnego podwykonawcom z tytułu zmiany wysokości wynagrodzenia, odpowiadającego zmianie wskaźnika, o którym mowa w § 6 ust. 24, Zamawiającemu przysługiwać będzie od Wykonawcy kara umowna w wysokości 1 000,00 zł za każdy stwierdzony przypadek.
7. Łączna wysokość kar umownych ze wszystkich tytułów wynikających z Umowy, zastrzeżonych na rzecz Zamawiającego jest ograniczona w stosunku do Wykonawcy do 100 % łącznej wartości Umowy brutto wynikającej z § 6 ust. 1 Umowy.
8. Jeżeli na skutek niewykonania bądź nienależytego wykonania Umowy powstanie szkoda przewyższająca zastrzeżoną w Umowie karę umowną, Zamawiającemu oprócz tej kary przysługuje prawo do dochodzenia odszkodowania uzupełniającego. Jeżeli szkoda powstanie z przyczyn innych niż te, ze względu, na które zastrzeżono karę umowną, Zamawiającemu przysługuje prawo do dochodzenia odszkodowania na zasadach ogólnych określonych w Kodeksie cywilnym.
9. Kary umowne płatne są w terminie 14 dni od daty otrzymania wezwania, przy czym Zamawiający zastrzega sobie prawo do skorzystania z zabezpieczenia należytego wykonania Umowy lub potrącenia kary z wynagrodzenia za wykonanie Umowy, do czego Wykonawca upoważnia Zamawiającego.

§ 11.

Odstąpienie od Umowy i wypowiedzenie Umowy

1. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy, lub dalsze wykonywanie umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, Zamawiający może odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach. W takim wypadku Wykonawca może żądać jedynie wynagrodzenia należnego z tytułu wykonania części Umowy.
2. Zamawiający uprawniony jest do odstąpienia od Umowy z przyczyn leżących po stronie Wykonawcy:
   1) w sytuacji określonej w § 3 ust. 2 Umowy (naruszenie zakazu korzystania z pracowników Zamawiającego),
   2) w sytuacji określonej w § 4 ust. 16 Umowy (stwierdzenie nieprawidłowości na etapie Wdrożenia DLP),
   3) w sytuacji określonej w § 7 ust.11 Umowy (wystąpienie wad prawnych),
   4) w sytuacji określonej w §10 ust. 3 Umowy (niedotrzymanie któregokolwiek z terminów na etapie Wdrożenia DLP),

   z zachowaniem prawa do kary umownej określonej w § 10 ust. 5 Umowy.
3. Zamawiający uprawiony jest do skorzystania z przewidzianego w Umowie prawa do odstąpienia od Umowy w terminie 30 dni od wystąpienia przesłanki do odstąpienia.
4. Zamawiający uprawiony jest do wypowiedzenia Umowy ze skutkiem natychmiastowym w przypadku:
   1) realizowania Umowy w sposób sprzeczny z przepisami prawa;
   2) naruszenia przez Wykonawcę zasad bezpieczeństwa opisanych w załączonych regulaminach stanowiących załączniki do zarządzenia Prezesa ARiMR nr 78/2019 z dnia 3 czerwca 2019 w sprawie wprowadzenia polityki bezpieczeństwa informacji w ARiMR (Załącznik nr 8 do Umowy) lub zasad poufności;
   3) otwarcia likwidacji, złożenia wniosku o upadłość, wydania sądowego nakazu zajęcia majątku Wykonawcy lub członka konsorcjum Wykonawcy, z którym została zawarta Umowa;
   4) innego istotnego naruszenia przez Wykonawcę warunków Umowy, jeżeli Wykonawca nie zaprzestanie lub nie naprawi naruszenia po upływie 14 dni od dnia wezwania przez Zamawiającego.

§ 12.

Postanowienia końcowe

1. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
2. Zamawiający przewiduje możliwość dokonania zmiany - w uzgodnieniu z Wykonawcą – terminów przekazania Projektu Technicznego lub Wdrożenia jeżeli jest ona wynikiem bieżących potrzeb Zamawiającego w szczególności:
   1) braku możliwości zapewnienia odpowiedniej ilości personelu po stronie Zamawiającego do współpracy przy realizacji Umowy lub uczestnictwa w procesie odbioru i weryfikacji Wdrożenia w terminach wynikających z zatwierdzonego harmonogramu,
   2) konieczności przeorganizowania prac weryfikacyjnych na etapie Wdrożenia, w tym procesu testowania DLP w celu optymalizacji przebiegu procesu odbiorowego,
   3) wystąpienia innych nieprzewidzianych okoliczności, mających wpływ na przebieg procesu Wdrożenia.

   Zmiany takie nie mogą prowadzić do przesunięcia terminu przekazania Projektu Technicznego lub terminu Wdrożenia o okres dłuższy niż 30 Dni Roboczych.
3. Wszelkie zawiadomienia i oświadczenia woli wymienione w Umowie, niezależnie od nazwy pod którą występują, dla swojej skuteczności Strony muszą przekazać na piśmie osobiście za potwierdzeniem odbioru lub pocztą poleconą za zwrotnym poświadczeniem ich odbioru, chyba że Umowa przewiduje inaczej i będą uważane za skutecznie doręczone w dniu ich odbioru. Ustala się następujące dane adresowe:
   1) Zamawiający – Agencja Restrukturyzacji i Modernizacji Rolnictwa, Departament Informatyki,
      ul. Poleczki 33, 02-822 Warszawa
   2) Wykonawca – ……

   Zawiadomienia, zapytania, informacje niewymienione w postanowieniach Umowy mogą być doręczane osobiście, przesyłane kurierem, listem lub za pośrednictwem poczty elektronicznej, pod warunkiem niezwłocznego potwierdzenia ich otrzymania

przez odbiorcę. Zawiadomienia będą wysyłane na adresy podane przez Strony. Każda ze Stron zobowiązana jest do niezwłocznego informowania drugiej Strony o każdej zmianie miejsca siedziby, adresu, adresu poczty elektronicznej. Zmiana adresów nie wymaga zachowania formy pisemnego aneksu do Umowy. Jeżeli Strona nie powiadomiła o zmianie miejsca siedziby, adresu, adresu poczty elektronicznej, zawiadomienia wysłane na ostatni znany adres, adres poczty elektronicznej, Strony uznają za doręczone.

4. Wszelkie spory powstałe w związku z realizacją Umowy Strony poddadzą pod rozstrzygnięcie sądu powszechnego, miejscowo właściwego ze względu na siedzibę Zamawiającego.
5. Wykonawca nie może bez zgody Zamawiającego przenieść praw wynikających z Umowy na osoby trzecie (przelew).
6. Osobami upoważnionymi przez Strony do podpisywania protokołów określonych w Umowie oraz do rozpatrywania bieżących spraw związanych z wykonaniem Umowy, przy zachowaniu określonych w niej warunków, w tym terminów, są:
   po stronie Zamawiającego: _____; tel. _____; e-mail: _____;
   po stronie Wykonawcy: _____; tel. _____; e-mail: _____;
   Zmiana ww. osób nie stanowi zmiany Umowy wymagającej formy pisemnego aneksu.
7. W sprawach nieuregulowanych Umową zastosowanie mają w szczególności przepisy Kodeksu Cywilnego, ustawy z dnia 11 września 2019 Prawo zamówień publicznych oraz ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.
8. Następujące Załączniki stanowią integralną część Umowy:
   1) Załącznik nr 1 - Specyfikacja systemu DLP;
   2) Załącznik nr 2 - Protokół odbioru – wzór;
   3) Załącznik nr 3 - Protokół Wdrożenia– wzór;
   4) Załącznik nr 4 –Wykaz osób;
   5) Załącznik nr 5 - Protokół świadczenia Usługi Wsparcia – wzór;
   6) Załącznik nr 6 – Załączniki nr 5, 8,12 oraz 14 z Zarządzenia nr 78/2019 Prezesa ARiMR;
   7) Załącznik nr 7 – Klauzule informacyjne w zakresie przetwarzania danych osobowych;
   8) Załącznik nr 7A –Oświadczenie o wypełnieniu obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO – wzór;
   9) Załącznik 8 – umowa powierzenia przetwarzania danych osobowych z Wykonawcą – wzór;
   10) Załącznik 8A – umowa powierzenia przetwarzania danych osobowych z Podwykonawcą – wzór.
9. Umowę sporządzono w postaci elektronicznej i opatrzono kwalifikowanymi podpisami elektronicznymi przez upoważnionych przedstawicieli Stron.

Wykonawca	**Zamawiający**
……	……

Załącznik nr 1 do Umowy

SPECYFIKACJA SYSTEMU DLP

System ochrony przeciw wyciekom poufnych danych (ang. DLP–Data Loss Protection)

1. Zamawiający wymaga, by systemem objętych było 12 tys. użytkowników lub 15 tys. urządzeń (komputery, laptopy, urządzenia mobilne) oraz dodatkowo 20 serwerów plików.
2. System musi umożliwiać ochronę przed wyciekiem informacji z systemów informatycznych Zamawiającego.
3. System musi realizować swoje funkcje zarówno na poziomie sieci (Network DLP) oraz stacji końcowej jak komputer, laptop, urządzenie mobilne (Endpoint DLP).
4. Zarządzanie, obsługa incydentów oraz raportowanie musi być spójne dla ochrony na poziomie sieci i stacji końcowych i odbywać się z pojedynczej webowej konsoli zarządzającej.
5. Dostęp do konsoli zarządzającej powinien odbywać się w bezpiecznym połączeniu https.
6. Ochrona informacji powinna odbywać się w oparciu o reguły bezpieczeństwa informacji odzwierciedlające procesy biznesowe.
7. System musi umożliwiać monitorowanie i ochronę wielu typowych kanałów komunikacyjnych, w szczególności:
   a) http oraz https,
   b) email,
   c) komunikatory internetowe
8. System musi umożliwiać definiowanie własnych kanałów transmisji, które mają być monitorowane.
9. System w zakresie stacji końcowej musi umożliwiać monitorowanie takich czynności jak kopiowanie informacji na zewnętrzne nośniki danych, nagrywanie płyt, lokalne drukowanie, wklejanie informacji w okna aplikacji.
10. System musi umożliwiać tworzenie polityk uwzględniających takie akcje jak:
    a) wysyłanie powiadomień w ramach odnotowanych incydentów, przy czym powiadamiane powinny być następujące osoby:
       - nadawca, czyli osoba, która wysyłała informacje,
       - zwierzchnik nadawcy,
       - właściciel informacji zdefiniowany w polityce,
       - właściciel polityki
    b) blokowanie transmisji naruszających zdefiniowaną politykę,
    c) kwarantannę informacji,
    d) szyfrowanie informacji,
    e) umożliwienie użytkownikowi kontynuowania operacji po zatwierdzeniu komunikatu wyświetlonego przez agenta ochrony informacji na stacji końcowej.
11. System musi umożliwiać łączenie polityk w grupy.
12. System musi umożliwiać budowanie polityk ochrony informacji uwzględniając kontekst w jakim informacja jest używana, czyli musi uwzględniać okoliczności jak:
    a) kto wysyła informacje,
    b) gdzie informacje są wysyłane,
    c) w jaki sposób informacje są wysyłane,
    d) co jest wysyłane, czyli właściwa identyfikacja treści.
13. System musi wykorzystywać szeroką gamę mechanizmów identyfikowania treści, m.in.:
    a) słowa kluczowe,
    b) wyrażenia regularne,
    c) tworzenie odcisku palca – fingerprinting,
    d) algorytmy Machine Learning
    e) weryfikacja klasyfikacji treści w przypadku, gdy stosowane jest rozwiązanie typu „Data Classification”
14. Algorytm tworzenia odcisku palca powinien działać tak, aby chronić informacje zawarte w pliku (również jego fragmenty), a nie wyłącznie dokument w całości.
15. System powinien również umożliwić tworzenie odcisków palca z zasobów zawartych w bazach danych. Tworzenie takich odcisków powinno odbywać się bez uprzedniego kopiowania informacji do pliku (np. za pomocą ODBC).

16. System musi zawierać predefiniowane reguły ochrony informacji, dotyczące np. numerów krat kredytowych, IBAN oraz takich identyfikatorów jak PESEL, REGON, NIP, nr Dowodu Osobistego.
17. System musi umożliwiać integrację z usługami katalogowymi (minimum AD DS, lub Azure AD) umożliwiająca m.in.:
    a) przypisywanie użytkowników i grup jako autoryzowanych nadawców i odbiorców monitorowanych informacji,
    b) przypisanie użytkowników do ról zarządzających takich jak administrator, audytor, manager incydentów,
    c) wyświetlanie szczegółów dotyczących użytkownika w ramach incydentu związanego z jego aktywnością, np. powinno być możliwe wyświetlenie informacji o zwierzchniku użytkownika.
18. System musi umożliwiać zautomatyzowane wykrywanie informacji objętych politykami ochrony na serwerach i stacjach końcowych w sieci Zamawiającego (funkcjonalność Discovery). Funkcjonalność ta powinna być również oferowana dla folderów Exchange, Exchange Online, serwera SharePoint, Sharepoint Online.
19. Konsola zarządzająca powinna zawierać ekran przedstawiający podstawowe statystki aktywności z ostatnich 24 godzin jak ilość incydentów względem ważności, najczęściej naruszane kategorie polityk, stacje końcowe, na których wykryto najwięcej naruszeń, etc.
20. Konsola zarządzająca powinna umożliwiać zarządzanie incydentami, m.in. zmianę ich statusu, przekazywanie do innego administratora.
21. System musi umożliwić ziarnistą delegację uprawnień do konfiguracji systemu, polityk, raportów oraz incydentów w oparciu o wbudowane jak również własne role, takie jak administrator, audytor, manager incydentów.
22. System w ramach odnotowanych incydentów musi udostępniać informacje dotyczące reguły, która została naruszona, jak również kopię informacji, która była przesyłana. Wgląd w tak szczegółowe informacje powinien być kontrolowany zgodnie z uprawnieniami administratora.
23. System powinien umożliwiać rozpoznawanie tekstu zawartego w plikach graficznych (OCR) i jego analizę pod względem wrażliwości informacji. Ta funkcjonalność powinna być oferowana co najmniej dla dokumentów graficznych wysyłanych poprzez styk z Internetem (smtp, http, https).
24. Oprogramowanie klienckie (Endpoint) powinno być oferowane w polskiej wersji językowej.
25. System powinien być zaopatrzony we własny moduł analityczny, który umożliwi wskazanie z listy incydentów tych najbardziej istotnych poprzez ich korelacje i grupowanie. System musi zwrócić alert w przypadku zwiększonej ilości zdarzeń mających wspólne źródło np. w jednym konkretnym użytkowniku.
26. System powinien posiadać możliwość rozbudowy o ochronę informacji przechowywanej w aplikacjach oferowanych jako SaaS, w szczególności MS O365 oraz Google for Business.
27. Ochrona informacji w chmurze powinna opierać się o te same mechanizmy stosowane w rozwiązaniu lokalnym włączając Fingerprinting oraz Machine Learning.
28. System musi posiadać funkcjonalność klasyfikowania informacji (w tym plików oraz wiadomości pocztowych email), lub w pełni integrować się z takim rozwiązaniem.

W zakresie klasyfikacji informacji o której mowa w ust. 28 wyżej, system powinien posiadać następujące funkcje:

1. Definiowanie dowolnych nazw dla poziomów klasyfikacji (np.: typ, klient, departament, projekt itp.),
2. Definiowanie dowolnych nazw dla klasyfikacji (np.: wewnętrzna – poufna - dane osobowe, kadry – produkcja - księgowość, Projekt X – Projekt Y, itd.).
3. Definiowane klasyfikacji opartej o:
    a) listę jednokrotnego wyboru,
    b) listę wielokrotnego wyboru (ze zdefiniowaniem minimalnej i maksymalnej liczby zaznaczeń),
    c) dowolny ciąg znaków, tzw. „sygnatura/znak sprawy” (z możliwością zdefiniowania szablonu logicznego dla takiego ciągu znaków).
4. Tworzenie klasyfikacji wielopoziomowej (minimum 5 poziomów oznaczeń klasyfikacji).
5. Definiowanie automatycznego nadawania klasyfikacji w oparciu o analizę treści informacji.
6. Klasyfikowanie dokumentu w następujących aplikacjach natywnych służących do edycji danego typu dokumentu (z poziomu aplikacji, a nie klasyfikowanie z poziomu plików):
    a) MS Word,
    b) MS Excel,
    c) MS PowerPoint,
    d) MS Visio,
    e) MS Project.
7. Wyświetlanie informacji o nadanej klasyfikacji, podczas edycji dokumentu w aplikacji natywnej.
8. Wyświetlanie przycisków klasyfikacji na wstążce aplikacji w postaci zarówno kolorowych pól (kolory zdefiniowane dla danego poziomu klasyfikacji), jak również w postaci dowolnie zdefiniowanych grafik/ikonek.

9. Dynamiczne wyświetlanie poziomów klasyfikacji tzn. możliwość wyboru podkategorii pojawia się dopiero po wybraniu przez użytkownika tej kategorii, dla której można/należy wybrać podkategorię.
10. Możliwość klasyfikowania plików (nie tylko MS Office, ale i innych plików kompatybilnych z technologią XMP, np. PDF, ZIP, itd…), plików tekstowych, obrazów itp.
11. Klasyfikowanie pliku/dokumentu z użyciem menu kontekstowego systemu operacyjnego (bez potrzeby jego otwierania).
12. Masowe nadanie klasyfikacji plikom/dokumentom poprzez:
    a) wskazanie folderu (z lub bez podfolderów) z plikami/dokumentami do oznaczenia,
    b) zdefiniowanie filtrów oznaczania (np. wszystkie pliki, których nazwa lub rozszerzenie zawiera wskazany wyróżnik),
    c) możliwe klasyfikowanie poprzez narzędzie z interfejsem okienkowym i poprzez polecenia konsoli tekstowej.
13. Wymuszanie na użytkowniku dokonania klasyfikacji, jeśli użytkownik tego nie zrobi:
    a) w wiadomości email MS Outlook,
    b) w dokumentach edytowalnych (w odniesieniu do aplikacji natywnej służącej do edycji danego dokumentu).
14. Wyświetlanie podpowiedzi/ostrzeżeń dotyczących wymogów klasyfikacji dla użytkownika lub innych informacji w zależności od podejmowanych działań przez użytkownika odnośnie informacji sklasyfikowanej na danym poziomie.
15. Wymuszanie na użytkowniku podania uzasadnienia dla wykonywanego działania odnośnie informacji sklasyfikowanej na danym poziomie.
16. Automatyczne wstawianie (dla wybranego poziomu klasyfikacji i w odniesieniu do aplikacji natywnej służącej do edycji danego dokumentu):
    a) stopek/nagłówków (także grafiki),
    b) znaków wodnych (także grafiki),
    c) prefiksów,
    d) osoby klasyfikującej,
    e) daty nadania klasyfikacji.
17. Wymuszanie szyfrowania poczty elektronicznej.
18. Dokonanie zmiany lub uniemożliwienie zmiany klasyfikacji dokumentu lub dokonanie zmiany wyłącznie w jednym kierunku (np. tylko podwyższenie poziomu klasyfikacji) przez użytkowników/ autora dokumentu.
19. Informacja o klasyfikacji dokumentu zapisywana jest w metadanych dokumentu.
20. Poziom klasyfikacji maila jest zapisywany w nagłówku wiadomości mail (X-Header).
21. We wszystkich aplikacjach natywnych służących do edycji danego typu dokumentu interfejs związany z klasyfikacją informacji jest taki sam.
22. Możliwe jest opcjonalne rozbudowanie systemu o automatyczne i działające na bieżąco klasyfikowanie maili przychodzących do organizacji (na poziomie serwera Exchange).
23. Możliwe jest opcjonalne rozbudowanie systemu o komponenty dla serwera Sharepoint 2013 i wyższych, aby Sharepoint mógł odczytywać i interpretować nadane poziomy klasyfikacji.
24. Możliwe jest opcjonalne rozbudowanie systemu o komponent na urządzenia mobilne, który pozwoli na klasyfikowanie maili na urządzeniu mobilnym (Android, iOS).
25. Dla uruchomienia klasyfikacji i dystrybucji polityk system nie wymaga serwera bazy danych lub innych rozwiązań serwerowych.
26. Publikacja polityk do użytkowników może być realizowana przez współdzielony katalog (network share), lokalną usługę dystrybucji oprogramowania, lub serwis chmurowy.
27. Reguły dla klienta pocztowego odnośnie możliwości przesyłania maili o wskazanych poziomach klasyfikacji są definiowane w oparciu o nazwy domen pocztowych oraz w oparciu o grupy użytkowników (AD DS lub Azure AD).
28. Możliwe jest zdefiniowanie kilku zestawów polityk (o zróżnicowanym poziomie restrykcji) i ich odpowiedni przydział do wskazanych osób zgodnie z pozycją w strukturach zarządczych w organizacji.
29. Możliwa jest automatyczna instalacja oprogramowania na stacjach użytkowników z wykorzystaniem narzędzi do automatycznej zdalnej instalacji.
30. System umożliwia pracę użytkownikowi (klasyfikowanie dokumentów, działanie polityk) także w przypadku gdy komputer użytkownika nie ma połączenia z siecią organizacji.
31. System zapisuje (loguje) wszystkie zdarzenia związane z klasyfikowaniem informacji, działaniem zdefiniowanych reguł/polityk.
32. Interfejs użytkownika końcowego w języku polskim (wszystkie nazwy, komunikaty, przyciski, opisy, itd.). Możliwe jest dostosowanie treści do terminologii i konwencji przyjętej w organizacji.
33. Informacja o poziomie klasyfikacji dokumentu, nadanej za pośrednictwem systemu klasyfikacji, może być wykorzystana przy tworzeniu polityk.

34. System integruje się z rozwiązaniami DLP Discovery (system Discovery po zidentyfikowaniu dokumentu zawierającego informacje spełniające zadane kryteria może automatycznie nadać klasyfikację wg poziomów zdefiniowanych w systemie klasyfikacji).
35. Do instalacji/działania systemu nie są wymagane żadne elementy/komponenty producentów trzecich (np. bazy danych).
36. System musi pracować w systemie wysokiej dostępności (High Availability).

Załącznik nr 2 do Umowy

Protokołu odbioru– wzór

zgodnie z Umową nr ……. zawartą w dniu ..... r. pomiędzy:
Agencją Restrukturyzacji i Modernizacji Rolnictwa („**Zamawiającym**") a
…… („**Wykonawcą**"),
Zamawiający potwierdza, że Wykonawca wykonał i dostarczył Projekt Techniczny/Dokumentację powykonawczą:

Lp.	Nazwa dokumentu	Ilość (szt.)	Numer seryjny / Uwagi
1			
2			

Upoważnieni przedstawiciele Zamawiającego i Wykonawcy złożonymi pod niniejszym protokołem podpisami zgodnie oświadczają, że:
1. Dostarczone dokumenty zostały wykonane zgodnie z warunkami Umowy.
2. Wykonawca potwierdza uzyskanie praw do korzystania/przeniesienie autorskich praw majątkowych do przekazanych dokumentów zgodnie z warunkami Umowy.

Uwagi i zastrzeżenia:

Zamawiający (*upoważniony przedstawiciel*)			**Wykonawca** (*upoważniony przedstawiciel*)
.....			.....
.....			.....

....., dnia ..... 20__ roku

Załącznik nr 3 do Umowy

Protokołu Wdrożenia - wzór

Zgodnie z Umową …… zawartą w dniu ..... 20… r. pomiędzy ARiMR (**Zamawiającym**) a …… (**Wykonawcą**), Strony potwierdzają dokonanie Wdrożenia systemu DLP zgodnie z warunkami Umowy.

W ramach wdrożenia systemu DLP:

- Testy wdrożeniowe systemu DLP przebiegły pozytywnie,
- Wykonawca zamodelował procesy biznesowe zgodnie z warunkami Umowy,
- Wykonawca dokonał pełnej konfiguracji i sprawdzenia poprawności działania systemu DLP,
- Wykonawca przekazał sporządzoną w języku polskim dokumentację producenta DLP oraz ogólne warunki licencyjne (na zasadach subskrypcji) i warunki korzystania z asysty technicznej producenta
- Wykonawca przekazał Dokumentację powykonawczą, sporządzoną na zasadach określonych w Projekcie Technicznym.
- ……,
- …….

Wykonawca potwierdza prawo licencyjne do korzystania przez Zamawiającego z systemu DLP (na zasadzie subskrypcji) oraz prawo do korzystania z producenckiej Usługi Asysty Technicznej, zgodnie w warunkami Umowy.

Wykonawca	**Zamawiający**
(osoby upoważnione)	*(osoby upoważnione)*
……	……
……	……

Załącznik nr 4 do Umowy

Wykaz osób

Załącznik nr 5 do Umowy

Protokół świadczenia Usługi Wsparcia - wzór

Zgodnie z Umową ……zawartą w dniu ..... 20…. r. pomiędzy ARiMR (Zamawiającym) a …… (Wykonawcą) Zamawiający *potwierdza należyte wykonanie/zgłasza uwagi do wykonania*[1] świadczonych w ramach realizacji Umowy czynności z zakresu Usługi Wsparcia, w okresie od dnia…….do dnia……..
W trakcie wymienionego okresu świadczenia Usługi Wsparcia udzielono … godzin konsultacji.
W trakcie wymienionego okresu świadczenia Usługi Wsparcia Wykonawca zrealizował na rzecz Zamawiającego następujące prace, mające charakter utworu w rozumieniu przepisów ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz. U. z 2019 r., poz. 1231 ze zm.):

- .....
- .....
- .....
- .....
- .....,

które zostały przez Zamawiającego odebrane bez zastrzeżeń i do których Zamawiający pozyskał autorskie prawa majątkowe zgodnie z warunkami Umowy
W trakcie wymienionego okresu świadczenia Usługi Wsparcia wystąpiły n/w zdarzenia:

- .....
- .....
- .....
- .....
- .....
- .....

Ze strony Wykonawcy: **Ze strony Zamawiającego:**

[1] Niepotrzebne skreślić

Załącznik nr 6 do Umowy
Załącznik nr 5 do Polityki bezpieczeństwa informacji w ARiMR

REGULAMIN UŻYTKOWNIKA

Spis treści:

1.
Definicje

Użyte w regulaminie określenia oznaczają:

1. dane uwierzytelniające – informacje wprowadzane do systemu, potwierdzające tożsamość użytkownika (np. hasła dostępu, kody zawarte w sprzętowych tokenach kryptograficznych);
2. hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie teleinformatycznym;
3. konto – część systemu teleinformatycznego (dane, oprogramowanie, zasoby sieciowe), które są powiązane z identyfikatorem użytkownika;
4. spam – niepożądaną przesyłkę poczty elektronicznej kierowaną do niezdefiniowanego adresata;
5. uwierzytelnianie - działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby/podmiotu;
6. urządzenie przenośne – urządzenie mobilne takie jak laptop, notebook, netbook, palmtop, tablet, telefon komórkowy, smartfon, MDA/PDA, pendrive, odtwarzacz mp3/4, aparat cyfrowy, czytnik kart pamięci, urządzenie do nawigacji GPS itp.

§ 2.
Szkolenia dla użytkowników systemów teleinformatycznych

1. Szkolenia użytkowników systemów teleinformatycznych mają na celu uzyskanie przez nich optymalnego poziomu wiedzy i umiejętności, które pozwolą właściwie użytkować i chronić systemy teleinformatyczne.
2. Warunkiem uzyskania podstawowego dostępu do systemu teleinformatycznego Agencji (konto domenowe i konto pocztowe) przez pracownika jest odbycie szkolenia wstępnego przeprowadzanego przez bezpośredniego przełożonego potwierdzone podpisem pracownika na wniosku o przyznanie dostępu, którego wzór zawarto w Książce Procedur KP-611-101-ARiMR – „Obsługa kont użytkowników systemów informatycznych ARiMR".
3. Warunkiem uzyskania dostępu do zaawansowanych funkcjonalności systemów teleinformatycznych Agencji jest odbycie szkoleń i zdanie egzaminów zgodnych z wymaganiami stawianymi przez Właścicieli Zasobów teleinformatycznych.
4. Szkolenia i egzaminy sprawdzające powinny być okresowo powtarzane (częstotliwość takich szkoleń określają Właściciele Zasobów teleinformatycznych) ze szczególnym uwzględnieniem:
    1) zmian dokonywanych w systemach teleinformatycznych, mających wpływ na sposób korzystania z tych systemów przez użytkowników,
    2) zmian przepisów prawa oraz uregulowań wewnętrznych,
    3) wystąpienia przypadków naruszenia bezpieczeństwa, słabości systemu lub zidentyfikowanych błędów systemów teleinformatycznych.

5. Okresowo (nie rzadziej niż raz na rok) przeprowadza się szkolenia doskonalące z zakresu bezpieczeństwa informacji. Szkolenia te obejmują zagadnienia ujęte w niniejszym Regulaminie, a w szczególności dotyczą:
    1) zapoznania z obowiązującymi regulacjami prawnymi dotyczącymi ochrony informacji, w tym z obowiązującą w Agencji polityką bezpieczeństwa informacji oraz polityką systemu zarządzania bezpieczeństwem informacji,
    2) przygotowania użytkowników do właściwego korzystania z powierzonych zasobów (instrukcje użytkowania sprzętu, systemów operacyjnych, aplikacji, itp.),
    3) sposobu postępowania w przypadku zdarzenia związanego z naruszeniem bezpieczeństwa informacji,
    4) sposobów postępowania w sytuacjach awaryjnych i kryzysowych.
6. Szkolenia doskonalące w zakresie obowiązujących w Agencji regulaminów związanych z bezpieczeństwem informacji mogą być przeprowadzane w zależności od zakresu obowiązków danego użytkownika przez:
    1) Administratora Systemu,
    2) Inspektora Bezpieczeństwa Informacji,
    3) Administratora Zabezpieczeń Fizycznych,
    4) Właściciela Procesu / Właściciela Zasobu,
    5) Bezpośredniego przełożonego.
7. Szkolenia doskonalące powinny kończyć się testem sprawdzającym zrozumienie przekazanych informacji adekwatnym do poziomu i zakresu prowadzonego szkolenia.
8. Uczestnictwo w szkoleniu każdy użytkownik potwierdza podpisem na liście obecności, z wyjątkiem szkoleń, które odbywają się w formie e-learning.
9. Szkolenia i egzaminy związane z użytkowaniem systemów teleinformatycznych są odnotowywane w Systemie e-szkoleń ARiMR.
10. Nieprzystąpienie do szkolenia, o którym mowa w § 2 ust. 5 lub niezaliczenie testu, o którym mowa w § 2 ust. 7, w terminie podstawowym i dodatkowym skutkuje blokadą dostępu do systemu teleinformatycznego Agencji na wniosek dyrektora komórki właściwej ds. bezpieczeństwa informacji.
11. Przywrócenie dostępu do systemu teleinformatycznego następuje na wniosek przełożonego użytkownika, zgodnie z procedurą zawartą w KP-611-101-ARiMR, po wcześniejszym odbyciu dodatkowego szkolenia doskonalącego i pozytywnym zaliczeniu testu.

§ 3.

Używanie autoryzowanych środków do przetwarzania informacji

1. Środki do przetwarzania informacji wykorzystywane w Agencji są przeznaczone wyłącznie do wykonywania zadań służbowych.
2. Każdy środek do przetwarzania informacji podlega inwentaryzacji i autoryzacji (dopuszczenie do pracy w systemie teleinformatycznym Agencji) zgodnie z zasadami określonymi w odrębnych dokumentach Agencji.
3. Wykorzystywanie środków do przetwarzania informacji, będących własnością Agencji, w celach niezwiązanych z powierzonymi obowiązkami wymaga uzgodnienia z bezpośrednim przełożonym i, jeżeli zachodzi taka potrzeba wynikająca z zakresu ewentualnego wykorzystania urządzeń, z Administratorem Systemu.
4. Zabrania się podłączania do sieci teleinformatycznej jakichkolwiek urządzeń nie posiadających autoryzacji.
5. Użytkownicy mogą korzystać ze stacji roboczych wyłącznie na stanowiskach im przydzielonych. Korzystanie z innego stanowiska komputerowego dopuszczalne jest jedynie za zgodą i na polecenie bezpośredniego przełożonego lub w przypadkach opisanych w Planach Zapewnienia Ciągłości Działania Agencji.
6. Użytkownik ponosi odpowiedzialność za powierzony sprzęt i oprogramowanie oraz sposób jego eksploatacji.
7. W przypadku korzystania ze stacji roboczej przez kilku użytkowników, kierownik komórki bądź jednostki organizacyjnej wyznacza osobę odpowiedzialną za sprzęt, określając jednocześnie uprawnienia i obowiązki wszystkich współużytkowników tego
sprzętu.
8. Użytkowników obowiązuje zakaz testowania lub podejmowania prób poznania metod zabezpieczenia systemów teleinformatycznych.
9. Użytkownicy nie mogą samodzielnie dokonywać jakiejkolwiek zmiany konfiguracji systemu teleinformatycznego.
10. Nośniki uszkodzone, wycofywane z eksploatacji lub przekazywane do ponownego użycia użytkownik przekazuje Administratorowi Systemu odpowiedzialnemu za przeprowadzenie zniszczenia lub trwałego skasowania danych, korzystając z następujących procedur:
    1) programowego kasowania danych na dyskach twardych – zamieszczonej w Książce Procedur KP-611-204-ARiMR,
    2) niszczenia zawartości komputerowych nośników magnetycznych – zamieszczonej w Książce Procedur KP-611-204-ARiMR,
    3) niszczenia nośników optycznych – zamieszczonej w Książce Procedur KP-611-186-ARiMR.
11. Postanowienia ust. 10 nie ograniczają ani nie wykluczają stosowania obowiązujących w Agencji zasad dotyczących gospodarowania środkami trwałymi oraz wyposażeniem.

§ 4.

Wynoszenie mienia i korzystanie z urządzeń przenośnych

1. Komputery przenośne podlegają szczególnej ochronie polegającej na zabezpieczaniu dostępu do komputera hasłem (hasło na BIOS). Ich używanie poza strefą administracyjną musi mieć uzasadnienie w realizowanych przez użytkownika zadaniach.
2. Wynoszenie sprzętu komputerowego poza Agencję, w tym sposób programowego zabezpieczenia komputerów przenośnych, reguluje procedura wydawania zezwoleń na wynoszenie sprzętu komputerowego z ARiMR zawarta w Książce Procedur KP-611-206-ARiMR.
3. Na użytkowniku urządzenia przenośnego spoczywa obowiązek jego ochrony, w szczególności zabrania się pozostawiania bez opieki tego typu urządzenia w samochodach, przedziałach wagonów, salach konferencyjnych oraz innych miejscach, gdzie użytkownik nie ma możliwości sprawowania nad nimi skutecznego nadzoru.
4. Wszelkie informacje wrażliwe nie mogą być przechowywane w urządzeniach przenośnych, które pracują poza Agencją, jeśli pozostają w postaci niezaszyfrowanej.
5. Każdy użytkownik, któremu powierzono urządzenie przenośne, przed rozpoczęciem użytkowania go poza strefą administracyjną Agencji, obowiązany jest do wystąpienia do Administratora Systemu z wnioskiem o zapewnienie środków techniczno-organizacyjnych gwarantujących poufność i integralność przetwarzanych informacji. Do środków tych zalicza się zabezpieczenia kryptograficzne określone w Polityce kryptografii oraz ochronę antywirusową.
6. W przypadku utraty powierzonego urządzenia przenośnego używanego poza Agencją użytkownik niezwłocznie powiadamia o tym fakcie Help Desk ARiMR oraz bezpośredniego przełożonego, a w przypadku kradzieży niezwłocznie zgłasza ten fakt na policję. Ponadto o kradzieży informuje osobę wydającą zgodę na wyniesienie sprzętu.

§ 5.

Korzystanie z systemów teleinformatycznych Agencji oraz Internetu

1. Przydzielanie uprawnień do korzystania z systemów teleinformatycznych realizowane jest w oparciu o następujące zasady:
   1) „minimalnych przywilejów" – każdy pracownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków,
   2) „wiedzy koniecznej" – pracownicy posiadają wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań,
   3) „domniemanej odmowy" – wszystkie działania, które nie są jawnie dozwolone są zabronione.
2. Każdy użytkownik otrzymuje prawa dostępu wyłącznie w zakresie niezbędnym do realizowania powierzonych zadań na danym stanowisku pracy.
3. Prawa dostępu są przydzielone po nadaniu użytkownikowi identyfikatora i hasła dostępu lub innych danych uwierzytelniających użytkownika.
4. Każdy użytkownik ma w systemie unikalny identyfikator.
5. Przed uzyskaniem dostępu do systemów teleinformatycznych Agencji użytkownik jest informowany przez bezpośredniego przełożonego o zakresie przyznawanych mu uprawnień.
6. Użytkownik ponosi odpowiedzialność za wszelkie czynności wykonane z użyciem jego identyfikatora i hasła.
7. Jeżeli w trakcie korzystania z zasobów systemu teleinformatycznego użytkownik stwierdzi, że posiadane uprawnienia wykraczają poza przyznane, zobowiązany jest niezwłocznie zgłosić ten fakt do Help Desk ARiMR. Nie dokonanie zgłoszenia tego faktu może zostać potraktowane jako celowe i świadome naruszenie praw dostępu.
8. Po stwierdzeniu posiadania większych uprawnień zabronione jest ich testowanie i wykorzystywanie.
9. W przypadku dłuższej nieobecności na stanowisku pracy użytkownik obowiązany jest zakończyć aktywne sesje i wylogować się. Ponadto, użytkownik każdorazowo w przypadku oddalenia się od stacji roboczej obowiązany jest zablokować system.
10. Na użytkowniku spoczywa obowiązek zabezpieczenia opracowywanych bądź tworzonych przez siebie danych przed utratą. Również wszelkie dane źródłowe, na których użytkownik wykonuje operacje, winny być zabezpieczone przed utratą i nieautoryzowanym użyciem bądź modyfikacją.
11. Użytkownik ma następujące możliwości zabezpieczenia danych (plików) przed utratą:
    1) umieszczenie danych na serwerze plików (fileserver) – jest to zalecana forma zabezpieczenia danych,
    2) sporządzenie kopii zapasowej na wymiennym nośniku komputerowym,
    3) sporządzenie wydruków z wyniku pracy nad przetwarzanymi danymi.
12. Niedopuszczalne jest umieszczanie na serwerze plików danych niezwiązanych z wykonywanymi obowiązkami służbowymi.
13. W przypadku potrzeby zabezpieczenia plików o dużych rozmiarach należy skorzystać z procedury nagrywania danych na nośnikach optycznych zawartej w Książce Procedur KP-611-186-ARiMR - „Postępowanie z optycznymi nośnikami danych".
14. Zabronione jest:
    1) umożliwianie dostępu do systemów teleinformatycznych osobom nieupoważnionym,
    2) rejestrowanie się w systemie teleinformatycznym na identyfikatorze innego użytkownika,
    3) korzystanie z konta innego użytkownika, chyba że część lub całość zasobów związanych z tym kontem są udostępniane zgodnie z zasadami obowiązującymi w Agencji,

4) przenoszenie informacji uzyskanych w związku z wykonywanymi zadaniami służbowymi na prywatne nośniki informacji, w szczególności pamięci typu pendrive i inne pamięci zewnętrzne,
5) dokonywanie prób sprawdzania, testowania i omijania zabezpieczeń systemów teleinformatycznych wewnętrznych jak również zewnętrznych, nie należących do Agencji,
6) udzielanie informacji o zasadach ochrony systemów teleinformatycznych Agencji, w tym o identyfikatorach używanych w tych systemach,
7) samowolne modyfikowanie ustawień związanych z bezpieczeństwem w systemach teleinformatycznych,
8) świadome niszczenie danych mających znaczenie archiwalne gromadzonych w systemach teleinformatycznych,
9) świadome wprowadzanie błędnych danych do systemów teleinformatycznych,
10) udostępnianie danych osobom nieupoważnionym,
11) włączanie urządzeń elektrycznych do wydzielonej instalacji elektrycznej przeznaczonej dla systemów teleinformatycznych,
12) przeglądanie stron internetowych o treściach pornograficznych, erotycznych, rasistowskich, użytkowanych przez grupy przestępcze i terrorystyczne,
13) pobieranie z Internetu, kopiowanie, instalowanie, przechowywanie lub rozpowszechnianie nieautoryzowanego przez Komitet oprogramowania i danych,
14) korzystanie z list i forów dyskusyjnych, gier internetowych oraz innych usług, nie mających związku z wykonywaną pracą.

§ 6.

Korzystanie z poczty elektronicznej i innych elektronicznych systemów komunikacyjnych

1. Wszyscy pracownicy Agencji mają dostęp do wewnętrznej poczty elektronicznej.
2. Agencyjna poczta służy wyłącznie do celów służbowych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów teleinformatycznych Agencji podlega rejestrowaniu i filtrowaniu, o którym mowa w ust. 3.
3. Użytkownicy są świadomi, że wiadomości elektroniczne niezwiązane z działalnością Agencji, a zawierające słowa bądź temat uznane za niedozwolone, zgodnie z zasadami filtrowania komunikacji niepożądanej obowiązującymi w Agencji, będą zatrzymywane i następnie usuwane z systemu pocztowego.
4. Zalecanym formatem przesyłanych wiadomości jest „zwykły tekst". O ile nie jest to konieczne, nie należy tworzyć wiadomości w formacie HTML.
5. Użytkownicy obowiązani są do okresowego porządkowania i usuwania wiadomości zbędnych z folderów programu pocztowego tak, aby nie dopuścić do jego zablokowania z powodu przekroczenia dopuszczalnej pojemności skrzynki.
6. Zabronione jest:
   1) rozsyłanie z komputerów Agencji oraz przyznanych użytkownikom kont poczty wiadomości, których treść nie jest związana z wykonywaną pracą, wyjątek stanowią komunikaty niestandardowe rozsyłane zgodnie z „Zasadami świadczenia przez Departament Informatyki usługi dystrybucji komunikatów do dużych grup odbiorców",
   2) wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu),
   3) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Agencji,
   4) odbieranie przesyłek z nieznanych źródeł,
   5) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.,
   6) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych,
   7) ukrywanie lub dokonywanie zmian tożsamości nadawcy,
   8) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika,
   9) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją Administratorowi systemu poczty elektronicznej na adres e-mail: spam@arimr.gov.pl,
   10) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy,
   11) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Agencji lub do poszukiwania dodatkowego zatrudnienia.

§ 7.

Ochrona haseł i kluczy kryptograficznych

1. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
2. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego przechowywanie.
3. Każdy użytkownik posiadający dostęp do systemów teleinformatycznych Agencji zobowiązany jest do:
   1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystywanych do pracy w systemie teleinformatycznym Agencji,
   2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia,

3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez Administratora Systemu,
4) poinformowania Administratora Systemu oraz Inspektora Bezpieczeństwa Informacji o podejrzeniu lub rzeczywistym ujawnieniu hasła,
5) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych,
6) zmiany wykorzystywanych haseł w regularnych odstępach czasu.

4. Zabronione jest:
   1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób,
   2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.,
   3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach,
   4) udostępnianie haseł innym użytkownikom,
   5) przeprowadzanie prób łamania haseł,
   6) wpisywanie haseł „na stałe" (np. w skryptach logowania).
5. W zależności od funkcjonujących w Agencji systemów operacyjnych i aplikacji zasady określone w ust. 3 pkt 3, 5 i 6 oraz ust. 4 pkt 2 i 3 mogą być wymuszane ustawieniami systemu teleinformatycznego wprowadzanymi przez Administratora Systemu na podstawie zasad określonych w odrębnych dokumentach Agencji.
6. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania z uwzględnieniem wymagań określonych w Polityce kryptografii, w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.
7. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić Administratorowi Systemu oraz Inspektorowi Bezpieczeństwa Informacji.

§ 8.

Zgodność oprogramowania z prawami autorskimi

1. Użytkownicy nie mogą instalować oraz uruchamiać żadnych aplikacji, które nie zostały wcześniej formalnie dopuszczone do użytkowania.
2. Użytkownikowi nie wolno:
   1) uruchamiać jakiegokolwiek innego oprogramowania niż to, które zostało mu przydzielone na danej stacji roboczej,
   2) pobierać z sieci, kopiować, przechowywać lub rozprowadzać oprogramowania, utworów muzycznych i wideo oraz innych plików, których używanie może powodować naruszenie praw do własności intelektualnej,
   3) kopiować i rozprowadzać bez upoważnienia oprogramowania stworzonego w Agencji lub na potrzeby Agencji,
   4) samodzielnie usuwać oprogramowania, którego używa.
3. Każdy plik znajdujący się:
   1) na wymiennym nośniku komputerowym,
   2) otrzymany za pomocą poczty elektronicznej lub pobrany z Internetu,

   podlega sprawdzeniu za pomocą oprogramowania antywirusowego zainstalowanego na komputerze przypisanym do użytkownika.
4. W przypadku wykrycia jakichkolwiek plików lub oprogramowania innego niż to, które znajduje się w spisie, Administrator Systemu ma prawo do natychmiastowego ich skasowania bez uzgodnienia z użytkownikiem.
5. O przypadkach używania nieautoryzowanego oprogramowania Administrator Systemu informuje Inspektora Bezpieczeństwa Informacji.
6. Użytkownik ponosi finansowe i prawne konsekwencje posiadania nielegalnego oprogramowania w przypisanym mu komputerze, jeśli nie dopełnił obowiązków wskazanych w niniejszym Regulaminie.

§ 9.

Korzystanie z urządzeń komunikacji głosowej, faksowej i wizyjnej

1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji wrażliwych, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.
2. Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
3. Zabronione jest wykorzystywanie domyślnych („fabrycznych") haseł dla ww. urządzeń.
4. Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających informacje wrażliwe jest zabronione.
5. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających informacje wrażliwe.

§ 10.

Zasady „czystego biurka i czystego ekranu"

1. Palenie, jedzenie oraz picie na stanowiskach komputerowych oraz w pomieszczeniach, w których znajdują się środki przetwarzania informacji (pomieszczenia serwerowni i węzłów teletechnicznych) jest zabronione.
2. W celu ograniczenia ryzyka nieuprawnionego dostępu, utraty lub uszkodzenia informacji w czasie godzin pracy i poza nimi użytkownik jest zobowiązany:
   1) przechowywać dokumenty papierowe i wymienne nośniki komputerowe w odpowiednio zabezpieczonych meblach biurowych,
   2) nie pozostawiać komputerów bez nadzoru w stanie aktywnej sesji dostępu do sieci,
   3) po zakończeniu pracy wylogować się z systemu i wyłączyć komputer, niedopuszczalne jest zakończenie pracy bez wykonania pełnej i poprawnej procedury zamknięcia lub przez wyłączenie napięcia zasilającego,
   4) po zakończeniu pracy uporządkować swoje stanowisko pracy, uniemożliwiając dostęp osób nieupoważnionych do dokumentów zawierających informacje wrażliwe,
   5) przestrzegać zasady niepozostawiania otwartych i niezabezpieczonych drzwi i/lub okien podczas nieobecności w pomieszczeniu,
   6) używać wygaszaczy ekranu zabezpieczonych hasłem,
   7) zabezpieczać nieużywany w danym momencie komputer przed nieupoważnionym dostępem, włączając blokadę systemową; ponowny dostęp do komputera następuje po podaniu hasła,
   8) ustawiać monitory komputerów w taki sposób, żeby uniemożliwić osobom nieupoważnionym wgląd w zawartość ekranu,
   9) odpowiednio zabezpieczyć miejsca przyjmowania/wysyłania korespondencji papierowej oraz odbioru/wysyłania faksów,
   10) włączać blokadę urządzeń kopiujących, zabezpieczając je w ten sposób przed nieuprawnionym użyciem,
   11) zwracać uwagę i powodować usuwanie pozostawionych oryginałów lub kopii w pobliżu urządzeń kserograficznych,
   12) zwracać szczególną uwagą na pracujące drukarki pozostawione bez nadzoru,
   13) nie pozostawiać wymiennych nośników komputerowych w napędach, bądź ogólnie dostępnych miejscach,
   14) niszczyć niepotrzebne nośniki papierowe w niszczarkach, jak np. dokumenty błędnie wydrukowane, powielone kopie itp. (za wyjątkiem nośników zawierających informacje wrażliwe, których sposób niszczenia regulują odrębne przepisy, w tym przepisy kancelaryjno-archiwalne Agencji w zakresie brakowania dokumentacji niearchiwalnej).
3. W uzasadnionych przypadkach realizacji zadań wymagających nieprzerwanego dostępu do zasobów teleinformatycznych (np. długotrwałe wgrywanie patch'y, pobieranie dużych ilości danych, odbywające się poza godzinami pracy ze względu na przepustowość łącz, wydajność baz danych, itp.) dopuszczalne jest, w porozumieniu z komórką właściwą ds. informatyki, odstąpienie od wymogu podanego w ust. 2 pkt 3.

§ 11.

Zgłaszanie zdarzeń o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania lub słabości systemu teleinformatycznego

1. Przed przystąpieniem do pracy użytkownik obowiązany jest sprawdzić stację roboczą (komputer) i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub próbę naruszenia bezpieczeństwa informacji.
2. Do przypadków mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania lub słabości systemu teleinformatycznego zalicza się:
   1) nieautoryzowany dostęp do danych,
   2) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach (np. wyłamane lub zacinające się zamki, naruszone plomby, nie domykające się bądź wybite okna, itp.),
   3) utratę usługi, urządzenia lub funkcjonalności,
   4) nieautoryzowaną modyfikację lub zniszczenie danych,
   5) udostępnienie informacji wrażliwych osobom nieupoważnionym,
   6) pozyskiwanie oprogramowania z nielegalnych źródeł,
   7) pojawianie się nietypowych komunikatów na ekranie,
   8) niemożność zalogowania się do systemu teleinformatycznego,
   9) spowolnienie pracy oprogramowania,
   10) niestabilna praca systemu teleinformatycznego,
   11) brak reakcji systemu na działania użytkownika,
   12) ponowny start lub zawieszanie się komputera,
   13) ograniczenie funkcjonalności oprogramowania.
3. Za naruszenie zasad ochrony informacji wrażliwych uważa się w szczególności:
   1) nieupoważniony dostęp, modyfikację, kopiowanie, udostępnienie lub zniszczenie /usunięcie informacji wrażliwych, zarówno w systemie teleinformatycznym, jak i na nośnikach papierowych i elektronicznych,

2) udostępnianie informacji wrażliwych nieuprawnionym podmiotom,
3) nieautoryzowany dostęp do danych przez połączenie sieciowe,
4) niedopełnienie obowiązku ochrony informacji wrażliwych przez umożliwienie dostępu do danych (np. pozostawienie kopii danych, nie zablokowanie dostępu do systemu, brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach, gdzie przetwarza się informacje wrażliwe),
5) stworzenie niezabezpieczonego kanału dystrybucji informacji wrażliwych,
6) nielegalne bądź nieświadome ujawnienie informacji wrażliwych,
7) pozyskiwanie informacji wrażliwych z nielegalnych źródeł,
8) przetwarzanie informacji wrażliwych niezgodne z uprawnionym celem i zakresem,
9) niepodjęcie działań zmierzających do eliminacji wirusów komputerowych lub innych programów zagrażających integralności systemu teleinformatycznego,
10) ujawnienie indywidualnych haseł dostępu do informacji wrażliwych w systemie,
11) przesyłanie informacji wrażliwych przez Internet bez zabezpieczenia,
12) przesyłanie dokumentów papierowych i nośników elektronicznych z informacja-mi wrażliwymi bez zabezpieczenia,
13) wykonanie nieuprawnionych kopii informacji wrażliwych,
14) kradzież nośników zawierających informacje wrażliwe lub oprogramowanie,
15) kradzież sprzętu służącego do przetwarzania informacji wrażliwych,
16) spowodowanie utraty informacji wrażliwych w systemie teleinformatycznym, na kopiach bezpieczeństwa i na innych nośnikach,
17) dopuszczenie do braku aktualnych kopii bezpieczeństwa informacji wrażliwych lub brak odpowiednich nośników do sporządzania kopii,
18) niewłaściwe niszczenie nośników z informacjami wrażliwymi pozwalające na ich odczyt,
19) naruszenie zasad ochrony fizycznej pomieszczeń, w których przetwarza się informacje wrażliwe,
20) dopuszczenie do przetwarzania informacji wrażliwych pracowników bez odpowiednich upoważnień,
21) nie przeszkolenie pracowników w zakresie zasad bezpieczeństwa informacji wrażliwych,
22) inne sytuacje wskazujące lub potwierdzające naruszenie bezpieczeństwa informacji wrażliwych w Agencji.

4. Wszelkie działania użytkownika związane z samodzielnym naprawianiem, potwierdzaniem lub testowaniem potencjalnych słabości systemu są zabronione.
5. Dokonywanie zmian w miejscu naruszenia ochrony bez wiedzy i zgody Administratora Systemu lub Inspektora Bezpieczeństwa Informacji lub Administratora Zabezpieczeń Fizycznych (w zależności od rodzaju naruszenia), jest dopuszczalne jedynie w sytuacji, gdy zachodzi konieczność ratowania życia lub zdrowia osób oraz mienia w przypadku ich bezpośredniego zagrożenia.
6. W przypadku zauważenia zdarzenia mogącego świadczyć lub świadczącego o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania, błędów lub awarii systemu użytkownik:
   1) zabezpiecza dostęp do miejsca lub urządzenia w sposób umożliwiający odtworzenie okoliczności naruszenia bezpieczeństwa lub niewłaściwego funkcjonowania oprogramowania,
   2) wstrzymuje pracę na stacji roboczej i odseparowuje komputer od sieci,
   3) niezwłocznie informuje Help Desk ARiMR (w przypadku wystąpienia zdarzenia związanego z systemem teleinformatycznym) lub Administratora Zabezpieczeń Fizycznych (jeżeli zdarzenie dotyczy bezpieczeństwa fizycznego i środowiskowego), a także bezpośredniego przełożonego,
   4) niezależnie od zapisów pkt 3) niezwłocznie informuje Inspektora Ochrony Danych oraz Inspektora Bezpieczeństwa Informacji w przypadku naruszenia zasad ochrony danych osobowych przy czym sposób poinformowania Inspektora Ochrony Danych powinien nastąpić w sposób zapewniających, iż informacja zostanie odebrana w możliwie najkrótszym czasie od jej przekazania,
   5) w przypadku zakwalifikowania przez IBI danego zdarzenia jako incydent, wypełnia w porozumieniu z nim część A raportu o incydencie bezpieczeństwa informacji (wzór raportu określa załącznik nr 3 do Regulaminu zarządzania incydentami).

§ 12.

Postępowanie dyscyplinarne w przypadku naruszenia bezpieczeństwa

1. Nieprzestrzeganie zasad określonych w dokumentach określających politykę bezpieczeństwa informacji stosowanych na danym stanowisku pracy przez użytkownika stanowi naruszenie podstawowych obowiązków pracowniczych i podlega odpowiedzialności dyscyplinarnej określonej w Regulaminie pracy.
2. Każdy przypadek wskazany w ust. 1 jest analizowany przez Inspektora Bezpieczeństwa Informacji, który w porozumieniu z Administratorem Systemu, Administratorem Zabezpieczeń Fizycznych oraz bezpośrednim przełożonym użytkownika, dokonuje kwalifikacji naruszenia. W szczególności umyślne działanie może zostać zakwalifikowane jako ciężkie naruszenie obowiązków pracowniczych.
3. Każdy przypadek naruszenia bezpieczeństwa informacji zgłaszany jest niezwłocznie dyrektorowi komórki właściwej ds. bezpieczeństwa informacji i opisywany zgodnie z Regulaminem zarządzania incydentami.

Załącznik nr 8 do Polityki bezpieczeństwa informacji w ARiMR

REGULAMIN ZARZĄDZANIA INCYDENTAMI

Spis treści:

§ 1.

Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji

1. Wszyscy pracownicy Agencji oraz pracownicy reprezentujący podmiot zewnętrzny, którzy mają dostęp do systemów teleinformatycznych Agencji i zobowiązali się do przestrzegania jej regulacji wewnętrznych związanych z bezpieczeństwem informacji, mają obowiązek zgłaszania wszelkich zdarzeń, które naruszają lub mogą naruszyć przepisy prawa oraz polityki, regulaminy i procedury Agencji dotyczące bezpieczeństwa informacji.
2. Zasady zgłaszania zdarzeń związanych z bezpieczeństwem informacji opisane zostały w Regulaminie użytkownika.
3. Osoba dokonująca zgłoszenia jest informowana przez Inspektora Bezpieczeństwa Informacji/Administratora Zabezpieczeń Fizycznych/Help Desk ARiMR o wyniku obsługi zgłoszenia.
4. Administrator Systemu/Administrator Zabezpieczeń Fizycznych ma obowiązek zareagować na alarm wygenerowany przez moduł automatycznego powiadamiania w systemach wykrywania włamań (systemów teleinformatycznych oraz elektronicznych systemów zabezpieczeń). W razie zidentyfikowania zagrożenia naruszenia bezpieczeństwa ochrony danych osobowych Administrator Systemu/Administrator Zabezpieczeń Fizycznych niezwłocznie informuje Inspektora Ochrony Danych, przy czym sposób poinformowania Inspektora Ochrony Danych powinien nastąpić w sposób zapewniających, iż informacja zostanie odebrana w możliwie najkrótszym czasie od jej przekazania,
5. W przypadku powierzenia obowiązków zarządzania systemami informacyjnymi podmiotom zewnętrznym, powiadamianie Administratora Systemu/Administratora Zabezpieczeń Fizycznych/ Inspektora Bezpieczeństwa Informacji/ Inspektora Ochrony Danych o zdarzeniu odbywa się na zasadach określonych w umowie o świadczeniu usług.
6. W celu zapewnienia prawidłowości i kompletności zgłaszania oraz obsługi zdarzeń związanych z bezpieczeństwem informacji, dyrektor komórki właściwej ds. bezpieczeństwa informacji dokonuje:
   1) comiesięcznych analiz z użyciem raportów tworzonych w ramach realizacji umów z podmiotami zewnętrznymi;
   2) przeglądu zdarzeń z wykorzystaniem, udostępnionych przez komórkę właściwą ds. informatyki, narzędzi monitorujących środowisko teleinformatyczne Agencji w czasie rzeczywistym.

§ 2.

Postępowanie z incydentami

1. Administrator Systemu/Administrator Zabezpieczeń Fizycznych lub pracownik Help Desk ARiMR dokonuje wstępnej identyfikacji zdarzenia i na podstawie dostępnych informacji oraz analizy okoliczności kwalifikuje zdarzenie (lub serię zdarzeń) jako:
   1) zdarzenie nie mające cech naruszenia bezpieczeństwa informacji, np. zaplanowana przerwa technologiczna;
   2) błąd w działaniu elementu systemu teleinformatycznego, infrastruktury teleinformatycznej lub infrastruktury biurowej;
   3) awaria techniczna czasowo blokująca dostępność informacji;
   4) incydent niskiej kategorii - związany z naruszeniem bezpieczeństwa informacji, a szczególnie jej integralności i poufności, nie generujący kar finansowych, jednak powodujący pośrednio lub bezpośrednio utrudnienia w realizacji jakiegokolwiek procesu głównego Agencji;
   5) incydent średniej kategorii – związany z naruszeniem bezpieczeństwa informacji skutkujący pośrednio lub bezpośrednio zatrzymaniem realizacji jakiegokolwiek procesu ustawowego i/lub stratami finansowymi nie przekraczającymi kwoty 137 tys. € oraz możliwością konsekwencji prawnych i/lub utraty wizerunku;
   6) incydent wysokiej kategorii - związany z naruszeniem bezpieczeństwa informacji, którego skutkiem jest destrukcja (zniszczenie, utrata) kluczowych zasobów i przerwanie funkcjonowania procesów Agencji; skutki tego incydentu powodują uruchomienie PZCD i wznowienie funkcjonowania w Zapasowych Miejscach Pracy; incydentem wysokiej kategorii jest również incydent, którego skutki mogą spowodować straty przekraczające kwotę 137 tys. €.
2. Inspektor Ochrony Danych dokonuje analizy danych dotyczących zdarzenia związanego z naruszeniem zasad ochrony danych osobowych. W toku tego procesu może występować o wszelkie informacje oraz opinie do jednostek i komórek organizacyjnych Agencji, które są zobowiązane do przekazania informacji oraz opinii w wyznaczonym przez Inspektora Ochrony Danych terminie.
3. O możliwości zaistnienia przypadku naruszenia bezpieczeństwa informacji mogą świadczyć:
   1) nadmierne, w stosunku do wykonywanych zadań (zakresu upoważnienia), uprawnienia użytkownika do zasobów systemu;
   2) niestabilna praca systemu teleinformatycznego;
   3) korzystanie z zasobów systemu poza godzinami pracy (bez zgody przełożonego);
   4) nowe „podejrzane" (nieznane) konta użytkowników;
   5) wysoka aktywność kont, które długo pozostawały niewykorzystane;
   6) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania;
   7) anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa komputerowego);
   8) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których następuje przetwarzanie informacji w Agencji (uszkodzone zamki, okna, drzwi, naruszone plomby, itp.).

4. O zdarzeniu noszącym znamiona incydentu Administrator Systemu/Administrator Zabezpieczeń Fizycznych/pracownik Help Desk ARiMR powiadamia niezwłocznie Inspektora Bezpieczeństwa Informacji (IBI), który dokonuje ostatecznej jego klasyfikacji.
5. Inspektor Bezpieczeństwa Informacji, we współpracy z Administratorem Systemu oraz, jeśli zachodzi taka potrzeba, z Administratorem Zabezpieczeń Fizycznych, przeprowadza analizę incydentu.
6. Analiza incydentu uwzględnia następujące kryteria:
   1) charakter incydentu i jego znaczenie związane z naruszeniem bezpieczeństwa fizycznego lub teleinformatycznego;
   2) miejsce wystąpienia incydentu - identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja, serwer, stacja robocza itp.);
   3) liczba jednostek/komórek organizacyjnych Agencji, zakres zasobów dotkniętych incydentem;
   4) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania z incydentem związanym z bezpieczeństwem informacji;
   5) możliwości rozszerzania się incydentu i sposoby jego ograniczania;
   6) szacowany poziom szkód finansowych;
   7) rodzaj ujawnionej informacji (jeśli ma zastosowanie – np. dane osobowe);
   8) szacunkowy czas, po którym skutki incydentu zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa informacji;
   9) skutki organizacyjne i prawne (wstępny szacunek).
7. W przypadku, gdy incydent ma skutki przekładające się na możliwość zakłócenia działalności ustawowej bądź statutowej Agencji, dyrektor komórki właściwej ds. bezpieczeństwa informacji informuje niezwłocznie Prezesa Agencji.
8. W przypadku, gdy zasięg i szacunkowy czas trwania powoduje zakwalifikowanie incydentu jako incydentu wysokiej kategorii, dyrektor komórki właściwej ds. bezpieczeństwa informacji powiadamia niezwłocznie Prezesa Agencji.
9. W przypadku, gdy zasięg incydentu wykracza poza system teleinformatyczny Agencji, Administrator Systemu, w porozumieniu z dyrektorem komórki właściwej ds. bezpieczeństwa informacji i z zastrzeżeniem posiadania stosownej umowy o poufności z właściwymi podmiotami zewnętrznymi, może przekazać do podmiotu zewnętrznego informacje o incydencie zawierające:
   1) typ zdarzenia;
   2) informacje o odległym systemie, który może być źródłem naruszenia, w tym nazwy serwerów, adresy IP, identyfikatory użytkowników;
   3) wszystkie zapisy z rejestrów zdarzeń w określonym przedziale czasowym;
   4) inne informacje określone w umowie z podmiotem zewnętrznym.
10. W przypadku, gdy rodzaj i zasięg incydentu, zidentyfikowany na którymkolwiek z etapów postępowania, uzasadnia potrzebę powiadomienia organów ścigania, to decyzję o sposobie i terminie powiadomienia podejmuje Prezes Agencji.

§ 3.

Postępowania Inspektora Ochrony Danych w toku obsługi incydentów

1. Inspektor Ochrony Danych dokonuje analizy danych dotyczących zdarzenia związanego z naruszeniem zasad ochrony danych osobowych. W toku tego procesu może występować o wszelkie informacje oraz opinie do jednostek i komórek organizacyjnych Agencji, które są zobowiązane do niezwłocznego przekazania informacji oraz opinii.
2. W wyniku analizy Inspektor Ochrony Danych stwierdza czy jest prawdopodobne, że stwierdzony incydent skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych oraz szacuje ryzyko z tym związane.
3. W przypadku stwierdzenia wysokiego ryzyka naruszenia praw i wolności osób fizycznych Inspektor Ochrony Danych informuje o tym Prezesa ARiMR.
4. Inspektor Ochrony Danych odpowiada za dokonanie czynności zgłoszenia stwierdzonego incydentu naruszenia ochrony danych osobowych, w którym wystąpiło wysokie ryzyko naruszania praw i wolności osób fizycznych, do Urzędu Ochrony Danych Osobowych.
5. Inspektor Ochrony Danych pełni nadzór nad właściwym dokonaniem procesu poinformowania właścicieli danych osobowych, których dotyczy incydent, przez odpowiednie jednostki, komórki organizacyjne Agencji. Informacje z pełnionego nadzoru przekazuje Prezesowi ARiMR oraz Komitetowi Sterowania Bezpieczeństwem Informacji.
6. Inspektor Ochrony Danych prowadzi Rejestr incydentów naruszeń ochrony danych osobowych, o których mowa w ust. 3.

§ 4.

Ograniczanie skutków incydentu

1. Administrator Systemu/Administrator Zabezpieczeń Fizycznych prowadzi bieżącą dokumentację incydentu. Dokumentacja ta w szczególności obejmuje:
   1) wszystkie zdarzenia zachodzące w systemie informacyjnym (zapisy systemowych dzienników audytu zdarzeń i dzienników audytu, lub zapisy z elektronicznych systemów zabezpieczeń);
   2) wszystkie podejmowane działania (opatrzone datą i czasem);
   3) wszystkie przeprowadzone rozmowy (osoba rozmówcy, data i czas zdarzenia, treść rozmowy).

2. Dokumentacja incydentu podlega rygorom ochrony przez tworzenie autoryzowanych kopii tych elementów systemu, które mają zastosowanie przy postępowaniu z incydentem tzn. rejestry urządzeń, systemów operacyjnych i aplikacji, kopie zapasowe, pliki konfiguracyjne i systemowe (zgodnie z rygorami tworzenia materiału dowodowego), bezpieczne przechowywanie tych kopii, przyjęcia dokumentacji oraz jej wszystkich części.
3. Administrator Systemu/Administrator Zabezpieczeń Fizycznych przeprowadza działania zmierzające do ograniczenia skutków incydentu i zidentyfikowania źródła naruszenia bezpieczeństwa. W tym celu może spowodować zablokowanie części systemu lub dostępnych usług.
4. W przypadku, gdy działania opisane w ust. 3 obejmują wyłączenie lub ograniczenie funkcjonowania zasobów niezbędnych do realizowania celów ustawowych bądź statutowych Agencji, Administrator Systemu/Administrator Zabezpieczeń Fizycznych przedstawia decyzję do akceptacji Prezesa Agencji, wraz z rekomendacją dyrektora komórki właściwej ds. bezpieczeństwa informacji.
5. Rekomendacja dyrektora komórki właściwej ds. bezpieczeństwa informacji uwzględnia:
   1) uzależnienie Agencji od systemu teleinformatycznego (jak długo Agencja może funkcjonować przy całkowitym lub częściowym wyłączeniu systemu);
   2) stopień narażenia informacji przetwarzanych w systemach teleinformatycznych Agencji na ujawnienie w przypadku utrzymywania się stanu naruszenia zabezpieczenia;
   3) stopień uświadomienia użytkowników (jaka może być reakcja użytkowników na anormalne zachowanie się systemu – np. niemożność zarejestrowania się, wyłączenie niektórych funkcji, itp.);
   4) konieczność schwytania i ewentualnego ukarania sprawcy (przy założeniu, że istnieją okoliczności umożliwiające takie działanie);
   5) konieczność angażowania zasobów systemu informatycznego (jaka część i jak długo);
   6) aspekt finansowy, organizacyjny i ludzki podejmowanych działań (jak długo działanie ma trwać, w jakim stopniu zakłóca normalne funkcjonowanie Agencji, jakie są tego koszty).
6. Przy ograniczaniu skutków incydentu Administrator Systemu/Administrator Zabezpieczeń Fizycznych, w uzgodnieniu z dyrektorem komórki właściwej ds. bezpieczeństwa informacji, może korzystać z konsultantów zewnętrznych, jeśli Agencja wcześniej zawarła w umowach z tymi podmiotami stosowne zapisy o przekazywaniu i ochronie informacji Agencji.

§ 5.

Odtwarzanie systemu informacyjnego

1. Z zastrzeżeniem ust. 4, Administrator Systemu przystępuje do odtworzenia systemu po zidentyfikowaniu i usunięciu lub zablokowaniu źródła incydentu.
2. W przypadku zaistnienia sytuacji, kiedy nastąpiło uruchomienie Planu Zapewnienia Ciągłości Działania ARiMR, odtwarzanie systemu jest realizowane w oparciu o procedury opisane w tym planie.
3. Odtwarzanie systemu odnosi się do punktu odtworzenia, co do którego Administrator Systemu ma uzasadnioną pewność, że nie zawiera źródła incydentu.
4. Zasoby w postaci oprogramowania oraz danych są odtwarzane z oryginalnych źródeł dystrybucji oprogramowania oraz kopii zapasowych.
5. Prezes Agencji, po zasięgnięciu opinii dyrektora komórki właściwej ds. bezpieczeństwa informacji i Administratora Systemu, może podjąć decyzję o podjęciu przetwarzania mimo braku pewności usunięcia źródła incydentu, jeśli szacowane negatywne skutki braku przetwarzania przewyższają potencjalne ryzyko podjęcia działania.

§ 6.

Działania po zakończeniu incydentu

1. Dyrektor komórki właściwej ds. bezpieczeństwa informacji, przy wsparciu Administratora Systemu, Właścicieli Procesów / Właścicieli Zasobów, Administratora Zabezpieczeń Fizycznych, sporządza raport z incydentu, zgodnie ze wzorem zamieszczonym w załączniku nr 3 do niniejszego regulaminu, oraz przedstawia go Komitetowi.
2. Jeśli zachodzi taka potrzeba, to Administrator Systemu/ Administrator Zabezpieczeń Fizycznych sporządza dodatkowy raport techniczny, stanowiący załącznik do raportu wskazanego w ust. 1 i zawierający co najmniej:
   1) rejestr incydentu, zawierający szczegółowe zapisy chronologiczne dotyczące kolejnych zdarzeń i podejmowanych działań;
   2) opis incydentu w aspekcie technicznym (zakres incydentu, części systemów dotknięte skutkami incydentu, rozmiar bezpośrednich szkód);
   3) kopie dzienników (logów zdarzeń, logów audytu) urządzeń, systemów operacyjnych i aplikacji w części systemów, która była dotknięta skutkami incydentu;
   4) kopię dziennika pracy systemu z okresu trwania incydentu;
   5) informacje o oryginalnych źródłach dystrybucji oprogramowania oraz kopiach zapasowych wykorzystanych do odtworzenia systemu;
   6) zakres informacji technicznych przekazanych Podmiotom zewnętrznym uczestniczącym w działaniach związanych z ograniczaniem skutków incydentu.

3. Dyrektor komórki właściwej ds. bezpieczeństwa informacji przedkłada Prezesowi Agencji rekomendacje w zakresie działań zmierzających do zmniejszenia ryzyka powtórzenia incydentu w przyszłości.

§ 7.

Rejestrowanie informacji o incydentach

1. Dyrektor komórki właściwej ds. bezpieczeństwa informacji prowadzi rejestr incydentów zawierający następujące informacje:
   1) opis incydentu;
   2) datę i godzinę zgłoszenia incydentu;
   3) dane identyfikujące osobę zgłaszającą;
   4) dane osoby przekazującej informację o incydencie;
   5) datę zarejestrowania incydentu;
   6) dane identyfikujące osobę rejestrującą incydent;
   7) informację o zgromadzonych materiałach dowodowych;
   8) informacje dotyczące sposobu postępowania z incydentem.
2. Dyrektor komórki właściwej ds. bezpieczeństwa informacji prowadzi analizy i statystyki incydentów.
3. Dyrektor komórki właściwej ds. bezpieczeństwa informacji zapewnia właściwe wykorzystanie informacji o incydentach związanych z bezpieczeństwem informacji dla celów szkoleniowych i doskonalenia systemu zarządzania bezpieczeństwem informacji.

§ 8.

Gromadzenie materiału dowodowego

1. Na każdym etapie postępowania z incydentem, dyrektor komórki właściwej ds. bezpieczeństwa informacji nadzoruje prawidłowość gromadzenia materiału dowodowego.
2. Każdy element materiału dowodowego – dokument papierowy, dokument elektroniczny, kopia zapasowa bazy danych lub plików systemowych i konfiguracyjnych, obraz dysku, dzienników (logów) zdarzeń, dzienników audytu – jest gromadzony i przechowywany w sposób gwarantujący jego poufność, integralność i kompletność.
3. Każdy element materiału dowodowego jest utrwalany z zachowaniem integralności całego procesu przetwarzania, od utworzenia do ewentualnego przedstawienia jako dowodu w postępowaniu sądowym:
   1) dla dokumentów papierowych - oryginał jest bezpiecznie przechowywany wraz z informacją o źródle, czasie i okolicznościach utrwalenia dokumentu;
   2) dla zapisów utrwalanych na nośnikach komputerowych – sporządzenie kopii zapasowej lub obrazu dysku wraz z udokumentowaniem procesu kopiowania oraz bezpieczne ich przechowanie (np. poza siedzibą Agencji).
4. Zabezpieczenie środków przetwarzania informacji jest przeprowadzane zgodnie z instrukcją zamieszczoną w załączniku nr 1 do niniejszego regulaminu.
5. Protokół ze sporządzenia elementu materiału dowodowego lub zabezpieczenia środków przetwarzania informacji jest sporządzany zgodnie ze wzorem zamieszczonym w załączniku nr 2 do niniejszego regulaminu.
6. Wszelkie działania w systemie teleinformatycznym, związane z postępowaniem z incydentem, mogą być prowadzone wyłącznie z wykorzystaniem kopii zapasowych, obrazów dysków, kopii plików konfiguracyjnych i systemowych, rejestrów systemowych i aplikacji, plików dokumentów, identycznych ze sporządzonymi uprzednio kopiami przechowywanymi jako materiał dowodowy.

Załącznik nr 1 do Regulaminu zarządzania incydentami - Instrukcja zabezpieczania komputerów

1. Odsuń w sposób zdecydowany, ale taktowny całą obsługę od komputerów (mogą później być przydatni). Na czas zabezpieczenia zabroń im korzystania z urządzeń komputerowych i łączności.
2. Jeśli urządzenie jest wyłączone, NIE WŁĄCZAJ GO.
3. Jeśli urządzenie jest włączone, NIE próbuj zamykać programów ani wyłączać komputera. Nie przerywaj drukowania, zabezpiecz, jeśli to możliwe, wykonane wydruki. Zanotuj dokładnie wszystkie wiadomości, jakie pojawiają się na ekranie. Zanotuj wszystkie parametry połączeń komputera:
   1) w przypadku połączenia modemowego, zanotuj numer telefoniczny, adres IP komputera, adresy bramki wychodzącej oraz serwera DNS,
   2) w przypadku połączenia po sieci kablowej, zanotuj typ połączenia, adres IP komputera, adresy bramki wychodzącej oraz serwera DNS,
   3) w przypadku połączenia po sieci bezprzewodowej, zanotuj ustawienia zabezpieczenia sieci adres IP komputera, adresy bramki wychodzącej oraz serwera DNS.
4. Przed zabezpieczeniem zanotuj, w jaki sposób poszczególne części stanowiska są ze sobą połączone. Zrób zdjęcia, wykonaj szkic (plan połączeń z opisem wyposażenia). Oznacz odpowiednio wszystkie przewody i połączenia.
5. Następnie ODŁĄCZ WSZYSTIE KABLE ZEWNĘTRZNE KOMPUTERA. Zanotuj czas odłączenia kabli.
6. Zabezpiecz jednostkę centralną (komputer) oraz inne urządzenia z zainstalowaną na stałe pamięcią masową w wytrzymałych mechanicznie workach foliowych. ZAPLOMBUJ WOREK I WYPEŁNIJ METRYCZKĘ. Metryczka powinna zawierać typ, numer seryjny urządzenia i numer inwentarzowy nadany przez Agencję albo opis jego indywidualnych cech. Wpisz do PROTOKOŁU wykonane czynności (Załącznik nr 2 do Regulaminu zarządzania incydentami).
7. Pakuj ostrożnie okablowanie i sprzęt (klawiatury, monitory, drukarki, plotery, skanery, czytniki kart i pamięci, napędy zewnętrzne itp.).
8. Zabezpiecz wszystkie wymienne nośniki komputerowe: pamięci flash, dyskietki, dyskietki ZIP, JAZZ, taśmy streamera, płyty CD, DVD, MO oraz niezamontowane dyski twarde (także uszkodzone). Grupy nośników pakuj zbiorczo (dyskietki, płyty CD itp.). PAKUJ, NUMERUJ poszczególne paczki, PLOMBUJ I OPISZ W PROTOKOLE. Wpisz do PROTOKOŁU wykonane czynności.
9. Zażądaj od użytkownika spisu oprogramowania zainstalowanego na komputerze, a następnie zgodnie ze spisem - okazania licencji i oryginalnych nośników oprogramowania lub wskazania miejsca przechowywania lub osoby upoważnionej, która zarządza licencjami i oryginalnymi nośnikami oprogramowania. Jeśli użytkownik nie ma spisu oprogramowania, to zażądaj okazania wszystkich posiadanych przez niego licencji i oryginalnych nośników oprogramowania. Oznaczenia licencji i nośników wpisz do protokółu, a następnie zabezpiecz jako materiał porównawczy. Wpisz do protokołu wykonane czynności.
10. Zażądaj od użytkownika przekazania instrukcji programów pisanych na zamówienie lub programów nietypowych (np. FK). Zabezpiecz jako materiał porównawczy i wpisz do protokołu wykonane czynności.
11. Zażądaj od użytkowników i administratora podania parametrów dostępu do BIOS-u, systemu operacyjnego i oprogramowania (kont, haseł, identyfikatorów, itp.), a następnie zabezpiecz je przed osobami postronnymi za pomocą bezpiecznej koperty. Wpisz czynność przejęcia parametrów dostępu do protokołu.
12. Przechowuj zabezpieczone materiały (nośniki i sprzęt) w miejscach suchych i chłodnych z daleka od urządzeń emitujących pole elektromagnetyczne, a bezpieczne koperty w sejfie.

Uwagi końcowe:

a) Sprawdź przed odesłaniem zgodność numerów zabezpieczonych materiałów i dowodów z treścią protokołu (zwróć uwagę na puste pudełka i nośniki pozostawione w napędach komputerowych i innych urządzeniach),
b) Skontaktuj się z odpowiednią komórką organizacyjną Agencji w celu zorganizowania przewozu i badań zabezpieczonych materiałów.

PAMIĘTAJ:

NIE PRÓBUJ SAMODZIELNIE BADAĆ KOMPUTERA, ANI ZAWARTOŚCI NOŚNIKÓW DANYCH.

KAŻDE TWOJE WŁĄCZENIE KOMPUTERA PO ZAKOŃCZENIU ZABEZPIECZENIA WYWOŁUJE POWSTANIE ŚLADÓW WSKAZUJĄCYCH NA NARUSZENIE INTEGRALNOŚCI MATERIAŁU BADAWCZEGO.

Załącznik nr 2 do Regulaminu zarządzania incydentami - Wzór protokołu zabezpieczenia materiału dowodowego

PROTOKÓŁ ZABEZPIECZENIA MATERIAŁU DOWODOWEGO

Wykonano w dniu ..... o godzinie ..... w obecności:

Świadek 1: <imię i nazwisko, stanowisko, komórka organizacyjna Agencji>
Świadek 2: <imię i nazwisko, stanowisko, komórka organizacyjna Agencji>
Świadek 3: <imię i nazwisko, niezależny ekspert>

I. Rodzaj materiału dowodowego

(zaznaczyć właściwe kwadraty i wpisać odpowiednie nazwy i oznaczenia)

Dokument papierowy	☐	*Rodzaj i Nazwa dokumentu:*			
Dokument elektroniczny	☐	*Rodzaj i Nazwa dokumentu:*			
Kopia zapasowa	☐	System operacyjny *Nazwa i wersja systemu:*		Aplikacja *Nazwa i wersja aplikacji:*	☐
		Baza danych *Nazwa i wersja bazy*:	☐	Oznaczenie nośnika	
Obraz dysku	☐	Lokalizacja dysku (adres IP/IPX): ..... Typ i nr seryjny dysku:			
Pliki konfiguracyjne i/lub systemowe	☐	System operacyjny *Nazwa i wersja systemu:*	☐	Aplikacja *Nazwa i wersja aplikacji:*	☐
		Baza danych *Nazwa i wersja bazy*:	☐	Nazwa(y) Pliku(ów)	
Kopie zawartości dzienników (logów) zdarzeń	☐	System operacyjny *Nazwa i wersja systemu:*	☐	Aplikacja *Nazwa i wersja aplikacji:*	☐
		Baza danych *Nazwa i wersja bazy*:	☐	Nazwa(y) Pliku(ów)	
Kopia zawartości skrzynki pocztowej	☐	zewnętrzna	☐	wewnętrzna	☐
		Nazwa skrzynki pocztowej:		*Za okres od:*	

II. Opis czynności

(opisać kolejne czynności z zaznaczeniem Wykonawcy(ów))

III. Wytworzony materiał dowodowy

Wykonano kopie materiału dowodowego w 2 egzemplarzach, którym nadano etykiety:
„....., Egzemplarz nr 1”
„....., Egzemplarz nr 2”
(wprowadzić krótkie oznaczenie zabezpieczonego materiału dowodowego, zgodnie z kategorią wskazaną w pkt. I, datą i godziną wykonania)

IV. Zabezpieczenie materiału dowodowego

(opisać sposób zabezpieczenia jednego z egzemplarzy)
....

…… …… …… …… ……
…… …… …… …… ……

Protokół sporządził: ……

Podpisano:

Świadek 1 . . . . . .
Świadek 2 . . . . . .
Świadek 3 . . . . . .

Załącznik nr 3 do Regulaminu zarządzania incydentami - Wzór raportu z incydentu

Miejscowość, data

RAPORT O INCYDENCIE BEZPIECZEŃSTWA INFORMACJI

A. ZGŁOSZENIE INCYDENTU (wypełnia osoba zgłaszająca zdarzenie/incydent)

DANE OSOBY ZGŁASZAJĄCEJ

Imię i nazwisko……Stanowisko służbowe ……..
Adres ……..
Nr telefonu ……e-mail …….

OPIS INCYDENTU:

……
……
……
……
……
……

Komu zgłoszono: ……..

Data i godzina zgłoszenia: ……

Podpis osoby zgłaszającej ……

B. DZIAŁANIA PO ZAISTNIENIU INCYDENTU

(wypełnia osoba rozpatrująca zgłoszenie incydentu)

DANE OSOBY, KTÓRA PRZYJĘŁA ZGŁOSZENIE INCYDENTU - ADMINISTRATOR SYSTEMU/ ADMINISTRATOR ZABEZPIECZEŃ FIZYCZNYCH/ IBI

Imię i nazwisko…….. Stanowisko ……
Adres ……
Nr telefonu …… e-mail ……

INFORMACJE O INCYDENCIE

Data i czas zajścia incydentu ……
Data i czas wykrycia incydentu ……..
Data i czas zgłoszenia incydentu ……
Czy incydent jest zakończony? TAK ☐ NIE ☐
Jeśli tak, to jak długo trwał (dni/godziny/minuty)? ……
Jeśli nie, należy określić jak długo już trwa? ……
Kogo powiadomiono z KIEROWNICTWA? ……

OPIS WSTĘPNY / PODJĘTE DZIAŁANIA / ZABEZPIECZENIE MATERIAŁU DOWODOWEGO

……
……
……
……

Załączniki (materiał dowodowy):

1. ……..
2. ……..
3. ……..

OPIS ROZWIĄZANIA PROBLEMU / KOSZTY ODTWORZENIA

……
……
……

Imię i Nazwisko …….
Data ……
Podpis ……

C. POSTĘPOWANIE WYJAŚNIAJĄCE/ ZAKOŃCZENIE INCYDENTU
(wypełnia osoba prowadząca postępowanie wyjaśniające – IBI w Centrali/OR)

Data rozpoczęcia postępowania ws. incydentu ……
Data zakończenia incydentu (jeśli jest zakończony) ……
Data zamknięcia skutków incydentu ……
Data zakończenia postępowania ws. incydentu ……
Data przedstawienia incydentu na KSBI ……

USTALENIA – OPIS POSTĘPOWANIA - SPRAWCY INCYDENTU
(w tym opis postępowania dyscyplinarnego, jeśli takie ma miejsce)

……
……
……
……

WNIOSKI I REKOMENDACJE
(w tym zalecenia dotyczące zmian w SZBI)

……
……
……
……
……

WYKAZ DOŁĄCZONYCH DOKUMENTÓW

……
……

DANE OSÓB PROWADZĄCYCH POSTĘPOWANIE WYJAŚNIAJĄCE

Imię i Nazwisko …….
Stanowisko ……..
Data ……..
Podpis ……

Imię i Nazwisko ……
Stanowisko ……
Data ……..
Podpis ……

Załącznik nr 12 do Polityki bezpieczeństwa informacji w ARiMR

REGULAMIN EKSPLOATACJI SYSTEMÓW TELEINFORMATYCZNYCH

Spis treści:

Załącznik nr 4 do Regulaminu eksploatacji systemów teleinformatycznych - Wniosek dotyczący użytkowania programu narzędziowego

§ 1.

Definicje

Użyte w regulaminie określenia oznaczają:

1) blokowanie konta – administracyjne uniemożliwienie korzystania z konta w danym systemie teleinformatycznym;
2) dane uwierzytelniające – informacje wprowadzane do systemu, potwierdzające tożsamość użytkownika (np. hasła dostępu, kody zawarte w sprzętowych tokenach kryptograficznych);
3) hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie teleinformatycznym;
4) integralność systemu - właściwość polegającą na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej (PN-I-13335-1);
5) konto – część systemu teleinformatycznego (dane, oprogramowanie, zasoby sieciowe), które są przypisane do identyfikatora użytkownika;
6) kopia archiwalna – duplikat danych, przechowywanych z uwagi na przepisy prawa lub potrzeby dokumentowania działalności Agencji; kopia archiwalna nie służy do odtworzenia;
7) kopia zapasowa – duplikat danych, przechowywany na wymiennym nośniku komputerowym, służący do odtworzenia systemu, aplikacji, bazy danych lub dokumentu;
8) niezaprzeczalność – możliwość przeprowadzenia dowodu, że działanie lub zdarzenie miało miejsce, tak że nie można temu działaniu lub zdarzeniu później zaprzeczyć;
9) podatność – słabość aktywu lub grupy aktywów, która może być wykorzystana przez jedno lub więcej zagrożeń;
10) profil dostępu – zestaw uprawnień, funkcji i zasobów systemu informatycznego dostępnych poszczególnym użytkownikom systemu;
11) rozliczalność - właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (ISO 7498-2: 1989);
12) spam – niepożądaną przesyłkę poczty elektronicznej kierowaną do niezdefiniowanego adresata;
13) uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
14) zabezpieczenie danych w systemie teleinformatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
15) zmiana – działanie lub ciąg działań mających na celu uzyskanie innego stanu systemu teleinformatycznego (konfiguracji lub funkcjonalności) niż przed podjęciem działania;
16) zmiana infrastruktury/ usługa rutynowa – uzgodnioną i zaakceptowaną wcześniej zmianę konfiguracji urządzeń lub sposobu/ zakresu świadczonych usług;
17) zmiana infrastruktury/ usługa awaryjna - zmianę podejmowaną w trybie nagłym wynikającym z konieczności usunięcia awarii lub błędu w systemie;
18) przywilej – specjalne uprawnienie posiadające wyższe od podstawowych prawa dostępu w systemie lub aplikacji, dostępne jedynie dla wybranych pracowników, w szczególności uprawnienie administracyjne.

Rozdział 1.
Podstawowe zasady eksploatacji systemów teleinformatycznych

§ 2.

Podział obowiązków w eksploatacji

1. Właściciel Procesu/Właściciel Zasobu może powierzyć administrowanie systemem (czynności wykonawcze) Administratorowi Systemu. Właściciel Zasobu sprawuje kontrolę nad działaniami wykonawczymi realizowanymi przez Administratora Systemu.
2. Administrator Systemu ponosi odpowiedzialność za bezpieczeństwo funkcjonowania systemu teleinformatycznego w ramach obowiązków powierzonych mu przez Właściciela Procesu/Właściciela Zasobu.
3. Role zarządcze (Właściciela Procesu/Właściciela Zasobu) i wykonawcze (Administratora Systemu) w zakresie eksploatacji systemów teleinformatycznych mogą być wykonywane przez tą samą komórkę organizacyjną.
4. Nadzór nad bezpieczeństwem informacji w systemach teleinformatycznych obejmującym kontrolę działań decyzyjnych i wykonawczych sprawuje dyrektor komórki właściwej ds. bezpieczeństwa informacji.
5. Obowiązki w zakresie eksploatacji sieci i serwerów są oddzielone od obowiązków w zakresie eksploatacji stacji roboczych poprzez przydzielenie ich różnym osobom (pracownikom Agencji lub pracownikom podmiotów zewnętrznych).
6. Wszystkie krytyczne czynności dotyczące realizacji szczególnie odpowiedzialnych zadań wymagają udziału, co najmniej dwóch osób działających jednocześnie lub wykonujących działania sekwencyjnie (dual control).

§ 3.

Monitorowanie pojemności i wydajności systemów

1. Administrator Systemu jest odpowiedzialny za prognozowanie wymagań dotyczących pojemności oraz wydajności kluczowych elementów systemów teleinformatycznych w celu ograniczenia ryzyka przeciążenia systemu.
2. Wymagania dotyczące pojemności nowych systemów, wynikające z rzeczywistych potrzeb Agencji, są definiowane i zatwierdzane przed dokonaniem zakupu, zaakceptowaniem i wdrożeniem tych systemów, zgodnie z Regulaminem rozwoju aplikacji, stanowiącym załącznik nr 11 do Polityki.
3. Administrator Systemu prowadzi monitorowanie eksploatowanych systemów teleinformatycznych, przez gromadzenie informacji dotyczących krytycznych elementów i parametrów systemów:
   1) infrastruktury sieciowej, w zakresie przepustowości i obciążenia łączy (interfejsów) oraz procesorów urządzeń sieciowych,
   2) serwerów usług wewnętrznych Agencji (serwery plików, wydruków, faksów, itp.), w zakresie obciążenia procesora, zajętości pamięci dyskowej, przyrostu danych w okresie miesiąca,
   3) serwerów aplikacyjnych i baz danych, w zakresie obciążenia procesora, zajętości pamięci dyskowej, przyrostu danych w okresie miesiąca.
4. Raz w roku oraz po wprowadzeniu istotnej zmiany do systemu Administrator Systemu przekazuje Komitetowi informację z monitorowania pojemności i wydajności systemów.
5. W sytuacji, w której analiza pojemności lub wydajności systemów wykazuje wzrost ryzyka niespełnienia celów statutowych Agencji, Administrator Systemu niezwłocznie przekazuje te informacje Przewodniczącemu Komitetu oraz dyrektorowi komórki właściwej ds. bezpieczeństwa informacji.

§ 4.

Ochrona przed szkodliwym oprogramowaniem

1. Stacje robocze i serwery w Agencji są objęte ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory (firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie teleinformatycznym Agencji.
2. Użytkowane poza systemem Agencji wymienne nośniki komputerowe, przed rozpoczęciem pracy z tymi nośnikami w systemach teleinformatycznych Agencji, są sprawdzane za pomocą aktualnego oprogramowania antywirusowego.
3. W systemach Agencji wdrożono scentralizowany system antywirusowy.
4. Aktualizacja baz wirusów odbywa się automatycznie, przynajmniej raz dziennie.
5. Po każdej naprawie i konserwacji urządzenia a przed ponownym włączeniem do systemu teleinformatycznego Agencji zawartość stałych nośników komputerowych jest sprawdzana za pomocą aktualnego oprogramowania antywirusowego zawierającego najnowsze bazy antywirusowe.
6. W przypadku, gdy stacje robocze oraz serwery nie są objęte ochroną w czasie rzeczywistym Administrator Systemu, co najmniej raz w tygodniu dokonuje rutynowej kontroli pod kątem obecności złośliwego oprogramowania, przy czym kontrola może być realizowana w sposób:
   1) automatyczny, zgodnie z harmonogramem zdefiniowanym w scentralizowanym systemie zarządzającym,
   2) automatyczny, zgodnie z harmonogramem zdefiniowanym w każdym systemie teleinformatycznym osobno,
   3) ręczny na żądanie, centralnie lub w każdym systemie teleinformatycznym osobno.
7. Działania Administratora Systemu są dokumentowane stosownymi zapisami w Dzienniku pracy systemu, którego wzór zamieszczono w załączniku nr 3 do niniejszego Regulaminu.

§ 5.

Kontrola licencjonowanego oprogramowania

1. Dla wszystkich systemów i aplikacji użytkowanych w Agencji Administrator Systemu prowadzi spisy licencjonowanego oprogramowania zawierające:
   1) nośniki instalacyjne (i ich kopie, przechowywane w innej lokalizacji),
   2) licencje wraz z okresami ich ważności,
   3) kopie dowodów zakupu licencji,
   4) miejsce zainstalowania,
   5) dane dotyczące użytkownika/Właściciela Procesu/Właściciela Zasobu.
2. Standardowa konfiguracja stacji użytkownika określona jest w Regulaminie standaryzacji stacji roboczych, zatwierdzonym przez Komitet.
3. Za utrzymanie standardu stacji roboczych odpowiada komórka właściwa ds. informatyki.
4. Przeglądy licencjonowanego oprogramowania mogą być przeprowadzane w trybie doraźnym lub w terminie ustalonym w harmonogramie przeglądów, zatwierdzanym przez Prezesa Agencji.
5. Spis licencjonowanego oprogramowania jest sprawdzany przez dyrektora komórki właściwej ds. bezpieczeństwa informacji pod kątem kompletności ewidencji.

6. Okresowo, nie rzadziej niż raz w roku, stacje robocze i udostępnione udziały sieciowe użytkowników są sprawdzane przez Administratora Systemu pod kątem obecności nieautoryzowanego oprogramowania.
7. Przesłanką do podjęcia przeglądu doraźnego jest:
   1) żądanie kierownika komórki organizacyjnej, Właściciela Procesu/Właściciela Zasobu, dyrektora komórki właściwej ds. bezpieczeństwa informacji, Komitetu lub uprawnionych organów ścigania, w związku z informacją o popełnieniu lub podejrzeniu popełnienia czynu niedozwolonego przez pracownika,
   2) otrzymanie zgłoszenia od pracownika o pojawieniu się lub podejrzeniu pojawienia się w systemie teleinformatycznym nieautoryzowanego oprogramowania.
8. Do przeprowadzenia przeglądu zgodności zainstalowanego oprogramowania z posiadanymi licencjami, a także zgodności z konfiguracją standardową, Administrator Systemu może stosować narzędzia programowe umożliwiające m.in.:
   1) automatyczne sprawdzanie stacji roboczych i serwerów,
   2) centralne zarządzanie spisem licencjonowanego oprogramowania,
   3) automatyczne ostrzeganie przed przekroczeniem liczby licencji.
9. Nieautoryzowane oprogramowanie jest niezwłocznie usuwane z systemu teleinformatycznego, a informacje o przypadkach używania nieautoryzowanego oprogramowania są przedstawiane przez Administratora Systemu Komitetowi z rekomendacją podjęcia odpowiednich działań.

§ 6.

Zarządzanie kopiami zapasowymi i archiwalnymi

1. Kopie zapasowe systemów, aplikacji baz danych i dokumentów użytkowanych w Agencji służą do zapewnienia możliwości odtworzenia w przypadku utraty aktualnie użytkowanych danych i/lub konfiguracji systemów i aplikacji.
2. Kopie zapasowe sporządza się w następujących przypadkach:
   1) przed dokonaniem zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych),
   2) po przeprowadzeniu udanej zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych).
   3. Kopie archiwalne sporządza się w celu utrwalenia istotnych dokumentów, systemów, baz danych i aplikacji, które nie są aktualnie wykorzystywane, a których obowiązek przechowywania wynika z obowiązujących aktów prawnych lub potrzeb wewnętrznych Agencji.
4. Kopie archiwalne przechowywane są przez okres wynikający z uwarunkowań prawnych lub wewnętrznych Agencji.
5. Kopie zapasowe i archiwalne są wykonywane dla systemów, baz danych i aplikacji oraz dokumentów użytkowanych w Agencji.
6. Za tworzenie kopii zapasowych i archiwalnych odpowiedzialny jest Administrator Systemu, któremu Właściciel Procesu/Właściciel Zasobu zlecił wykonywanie kopii.
7. Dla wskazanych dokumentów, systemów, baz danych i aplikacji podlegających tworzeniu kopii Właściciel Procesu/Właściciel Zasobu w porozumieniu z Administratorem Systemu określa:
   1) strategię tworzenia kopii uwzględniającą: częstotliwość tworzenia kopii, rodzaj kopii (przyrostowa, pełna, różnicowa), ilość kopii, miejsce, okres i sposób przechowywania kopii, rotację nośników,
   2) warunki techniczne realizacji procesu zarządzania kopiami zapasowymi i archiwalnymi, w tym określenie urządzenia/oprogramowania do wykonywania kopii, rodzaj nośnika, sposób wykonywania kopii (automatyczny, ręczny), okno eksploatacyjne wykonywania kopii (jeśli ma zastosowanie), sposób weryfikacji poprawności wykonanej kopii.
8. Użytkownicy mogą zlecać Administratorowi Systemu wykonanie kopii przetwarzanych przez nich danych (np. kopii folderów osobistych skrzynek pocztowych).
9. Postępowanie dotyczące nagrywania na nośnikach optycznych danych, zawierających informacje przetwarzane w Agencji opisane zostało w Książce Procedur KP-611-186-ARiMR.
10. Tworzenie kopii odbywa się zgodnie z procedurą tworzenia i odtwarzania kopii zapasowych i podlega rejestracji. Wzór rejestru określa załącznik nr 1 do niniejszego Regulaminu. Rejestr prowadzony jest w postaci papierowej lub elektronicznej.
11. Po utworzeniu kopii automatycznie (jeżeli jest technicznie realizowalne) jest generowany raport o przebiegu wykonania kopii. Raport podlega weryfikacji przez Administratora Systemu.
12. Miejsce przechowywania kopii jest zabezpieczone przed nieuprawnionym dostępem oraz skutkami zdarzeń takich, jak pożar, zalanie, oddziaływanie silnego pola elektromagnetycznego, promieniowanie, zanieczyszczenie środowiska na takim poziomie, jak jest zabezpieczony system, z którego kopia zapasowa została wykonana.
13. Kopie są przechowywane w bezpiecznej odległości (w innej lokalizacji) od miejsca, w którym jest prowadzona eksploatacja systemów. Proces przekazywania nośników zawierających kopie zapasowe i archiwalne do innej lokalizacji jest udokumentowany.

14. Regularnie, co najmniej raz w roku, Administrator Systemu w porozumieniu z Właścicielem Procesu/Właścicielem Zasobu przeprowadza testowe sprawdzenie odtworzenia systemu, aplikacji, bazy danych lub dokumentów z kopii. Testowe odtworzenie podlega udokumentowaniu w dzienniku pracy systemu.
15. W przypadku, gdy okres trwałości zapisu na nośniku elektronicznym lub magnetycznym jest krótszy od wymaganego okresu przechowywania wynikającego z uwarunkowań prawnych dane z nośników są przenoszone na inny nośnik.
16. Kopię na inny nośnik wykonuje Administrator Systemu. Nośnik, z którego przeniesiono zapis, jest niszczony zgodnie z zasadami obowiązującymi w Agencji, a całość operacji przeniesienia jest dokumentowana.
17. Po upływie wymaganego okresu przechowywania kopie archiwalne są niszczone zgodnie z zasadami obowiązującymi w Agencji.
18. Usługi transportowania lub przechowywania kopii zapasowych lub archiwalnych mogą być powierzone podmiotowi zewnętrznemu.
19. Umowa z podmiotem zewnętrznym na transportowanie lub przechowywanie kopii zapasowych lub archiwalnych powinna zawierać:
    1) wymagania bezpieczeństwa transportowania (przechowywania) kopii zapasowych,
    2) tryb przekazywania (odbierania) kopii zapasowych lub archiwalnych:
        a) zwykły (rotacja kopii zapasowych),
        b) awaryjny (w celu użycia kopii zapasowej lub archiwalnej),
    3) sposoby komunikowania się Agencji z usługodawcą, w tym potwierdzania dostarczenia kopii zapasowych w trybie awaryjnym,
    4) zakres odpowiedzialności usługodawcy za utratę lub uszkodzenie kopii zapasowych lub archiwalnych.

§ 7.

Zarządzanie poprawkami technicznymi

1. Zarządzanie poprawkami ma na celu eliminowanie lub ograniczanie zidentyfikowanych podatności systemów teleinformatycznych.
2. Administrator Systemu zobowiązany jest do monitorowania pojawiania się poprawek do poszczególnych usług sieciowych, systemów operacyjnych i aplikacji ARiMR.
3. Administrator Systemu obowiązany jest do wprowadzania poprawek w oparciu informacje uzyskane od producentów urządzeń sieciowych, systemów operacyjnych i aplikacji oraz od profesjonalnych organizacji zajmujących się tematyką bezpieczeństwa informacji i systemów teleinformatycznych.
4. Poprawki techniczne, w zależności od ich krytyczności, są testowane w środowisku testowym zanim zostaną wprowadzone do środowiska produkcyjnego. Administrator Systemu prowadzi rejestr dokonywanych zmian.
5. Wprowadzanie poprawek bezpośrednio do środowiska produkcyjnego może być wykonane wyłącznie po uzyskaniu akceptacji Właściciela Procesu / Właściciela Zasobu. Wprowadzanie poprawek podlega dokumentowaniu w Dzienniku pracy systemu.

Rozdział 2.
Zasady bezpieczeństwa sieci

§ 8.

Ogólne mechanizmy bezpieczeństwa sieci

1. Agencja zapewnia bezpieczeństwo sieci za pomocą następujących mechanizmów:
    1) aplikacji i urządzeń typu firewall oraz systemów wykrywania i przeciwdziałania włamaniom na poziomie sieci i hostów,
    2) aplikacji antywirusowych stosowanych podczas wymiany danych pomiędzy siecią Agencji a sieciami należącymi do innych organizacji lub sieciami publicznymi,
    3) rozdzielania sieci; użytkownicy poszczególnych komórek i jednostek organizacyjnych są grupowani w logicznie rozdzielonych segmentach sieciowych (VLAN),
    4) uwierzytelniania użytkowników i urządzeń (o ile istnieją możliwości techniczne),
    5) wyłączenia (zablokowania) usług sieciowych, które są niewykorzystywane, nie mają uzasadnienia biznesowego lub technicznego albo są uznawane za niebezpieczne, niezależnie do tego czy są udostępniane wewnątrz sieci Agencji, czy także na zewnątrz,
    6) właściwie (z punktu widzenia bezpieczeństwa informacji) skonfigurowanie aplikacji, usług lub systemów operacyjnych,
    7) aktualizowanie aplikacji, systemów operacyjnych oraz usług sieciowych do najnowszej oraz bezpiecznej i stabilnej wersji,
    8) fizycznych zabezpieczeń dostępu do systemów,
    9) rozdzielenia środowisk produkcyjnych od testowych.

2. Podsieci logiczne VLAN wewnątrz sieci Agencji tworzy się dla elementów systemu o różnych wymaganiach bezpieczeństwa. Każda z takich podsieci stanowi odrębną strefę bezpieczeństwa, do której dostęp musi być kontrolowany z wykorzystaniem zapory ogniowej zapewniającej realizację ścisłej kontroli oraz selektywnego dostępu do wybranych usług i systemów w danej strefie.
3. Ruch między podsieciami jest kontrolowany za pomocą reguł filtrujących wprowadzonych w urządzeniach sieciowych oraz serwerach.
4. W Agencji wdrożono mechanizmy kontroli rutingu w sieciach oparte na zdefiniowaniu możliwych tras pakietów w sieci.
5. Sygnatury systemów wykrywania i przeciwdziałania włamaniom podlegają regularnej aktualizacji.
6. Komunikacja systemów zewnętrznych z systemami Agencji musi być realizowana poprzez routery dostępowe przyłączone w jednej ze stref zapory ogniowej – strefy dostępowej dedykowanej dla komunikacji z systemami zewnętrznymi.
7. Do realizacji połączeń z systemami zewnętrznymi wymagane jest wykorzystanie łączy dedykowanych. W szczególnych przypadkach oraz do celów testowych zezwala się na dostęp do systemów aplikacyjnych Agencji za pośrednictwem łączy wirtualnych realizowanych poprzez sieć publiczną z wykorzystaniem technologii VPN (połączenia terminowane w zaporze ogniowej lub koncentratorze VPN zlokalizowanym w strefie dostępowej).

§ 9.

Uwierzytelnianie węzłów

1. Agencja wykorzystuje mechanizm identyfikacji urządzeń do uwierzytelniania połączeń z określonych lokalizacji lub urządzeń. Identyfikacja urządzeń realizowana jest w oparciu o przydzielanie stałego adresu IP, na podstawie unikalnego adresu MAC, dla każdego urządzenia podłączanego do sieci Agencji.
2. Agencja może nie stosować mechanizmu określonego w ust. 1, jeśli wynika to z uzasadnionych potrzeb biznesowych.

§ 10.

Ochrona urządzeń sieciowych

1. Wszelkie zmiany topologii sieci lub konfiguracji urządzeń sieciowych są przeprowadzane w oparciu o proces zarządzania zmianami.
2. Wszędzie, gdzie jest to technicznie możliwe, urządzenia sieciowe są chronione hasłem dostępu przechowywanym w postaci zaszyfrowanej.
3. Zarządzanie siecią odbywa się z wydzielonych stacji roboczych zlokalizowanych w sieci lokalnej lub przez konsole podłączone bezpośrednio do urządzeń sieciowych.

§ 11.

Bezpieczeństwo zdalnego dostępu do portów diagnostycznych i konfiguracyjnych

1. Ustawienia parametrów konfiguracyjnych oraz przeprowadzenie diagnostyki urządzeń systemu teleinformatycznego wykonuje się z lokalnej konsoli administracyjnej, wykorzystując do tego celu dedykowane konta administracyjne (lokalny dostęp administracyjny).
2. W szczególnych przypadkach przewidzianych umowami z podmiotami zewnętrznymi oraz sytuacjach awaryjnych, działania administracyjne można wykonywać w trybie zdalnego dostępu. Zdalny dostęp administracyjny jest realizowany wyłącznie ze stacji dedykowanych dla systemów administracyjnych.
3. Do nawiązywania zdalnych połączeń administracyjnych stosuje się:
   1) mechanizmy zapewniające uwierzytelnianie stacji i użytkownika,
   2) szyfrowanie komunikacji z wykorzystaniem bezpiecznych protokołów, zapewniających poufność i integralność przesyłanych danych,
   3) ograniczenie dostępu do określonej grupy adresacji oraz usług niezbędnych do realizacji powierzonych zadań.
4. Warunki techniczne zdalnego dostępu podlegają zatwierdzeniu przez Komitet.

§ 12.

Bezpieczeństwo dostępu do sieci publicznych (Internet)

1. Sieć teleinformatyczna Agencji, w tym sieci lokalne jednostek organizacyjnych, może być podłączona do sieci ogólnodostępnych (np. sieć publiczna Internet) tylko na poziomie WAN'u i jedynie przy użyciu specjalnych systemów zabezpieczających (aplikacje i urządzenia typu firewall, systemy IDS/IPS).
2. Za zgodą Komitetu, sieć teleinformatyczna Agencji może być połączona z innymi sieciami zewnętrznymi. Warunki takiego połączenia określane są przez reguły filtrowania zapór sieciowych ustalane przez Administratora Systemu we współpracy z dyrektorem komórki właściwej ds. bezpieczeństwa informacji.
3. Wszystkie połączenia pomiędzy sieciami publicznymi a siecią Agencji są realizowane przy użyciu specjalnych systemów zabezpieczających (aplikacje i urządzenia typu firewall, systemy wykrywania włamań).
4. Architekturę zapory ogniowej (firewall) oddzielającej sieć publiczną od sieci wewnętrznych Agencji skonfigurowano na zasadzie przepuszczania tylko ściśle zdefiniowanego ruchu przychodzącego i wychodzącego.
5. Serwery zewnętrznych usług sieciowych muszą być zlokalizowane w wydzielonych strefach DMZ.

6. Usługi udostępniane w sieci publicznej oraz uprawnienia dostępu użytkowników do tych usług są autoryzowane przez Komitet. Wykaz dostępnych usług prowadzi Administrator Systemu. Wykaz ten zawiera zestawienia usług oraz profile użytkowników uprawnionych do korzystania z określonych usług.

Rozdział 3.
Bezpieczeństwo systemów operacyjnych
§ 13.
Ogólne mechanizmy bezpieczeństwa

1. W Agencji stosuje się następujące mechanizmy bezpieczeństwa systemów operacyjnych:
1) uwierzytelnianie użytkowników, zgodnie z przyjętymi w Agencji zasadami kontroli dostępu,
2) rejestrowanie nieudanych prób dostępu do systemu,
3) rejestrowanie korzystania z przywilejów systemowych,
4) generowanie alarmów w przypadku naruszenia reguł bezpieczeństwa systemu,
5) ograniczanie czasu nieaktywności sesji użytkowników.
2. Systemy operacyjne pracujące w Agencji muszą mieć włączone mechanizmy bezpiecznego logowania zapewniające (w zależności od możliwości technicznych):
   1) ujawnianie minimum informacji o systemie,
   2) wyświetlanie ostrzeżenia, że dostęp do systemu jest dozwolony jedynie dla uprawnionych użytkowników,
   3) unikanie wyświetlania komunikatów pomocniczych, które mogłyby pomóc nieuprawnionemu użytkownikowi przy nieautoryzowanych próbach dostępu,
   4) unikanie wskazywania, która część danych jest poprawna lub niepoprawna w przypadku wystąpienia błędu podczas logowania,
   5) ograniczenie liczby nieudanych prób logowania się do systemu,
   6) blokowanie konta po co najwyżej sześciu następujących po sobie nieudanych próbach logowania,
   7) wykonywanie zapisu każdego nieudanego logowania w logach zdarzeń,
   8) ograniczenie możliwości zalogowania się do systemu tylko w określonych przedziałach czasowych („oknach logowania”),
   9) blokowanie wyświetlania hasła w trakcie jego wprowadzania,
   10) blokowanie domyślnego wyświetlania identyfikatora (konieczność wpisania identyfikatora),
   11) szyfrowanie przesyłanych haseł.

§ 14.
Identyfikacja i uwierzytelnianie użytkowników

1. Wszyscy użytkownicy systemów muszą posiadać unikalne identyfikatory użytkownika (ID użytkownika) do swojego wyłącznego użytku.
2. Stosowane identyfikatory użytkownika nie wskazują na poziom uprawnień danego użytkownika.
3. W celu uwierzytelnienia użytkowników Agencja wykorzystuje hasła lub klucze kryptograficzne chronione hasłem.
4. Dostęp do systemu dla użytkownika, który sześciokrotnie pod rząd podał błędne hasło jest blokowany; odblokowania dokonuje ręcznie Administrator Systemu na wniosek złożony zgodnie z KP-611-101-ARiMR. Tworzenie automatów (skryptów) programowych odblokowujących dostęp np. po określonym czasie jest zabronione.

§ 15.
System zarządzania hasłami

1. Ustawienia zasad zarządzania hasłami w systemach teleinformatycznych zapewniają:
   1) wymuszanie użycia indywidualnych haseł,
   2) wybór i zmianę haseł przez użytkowników,
   3) potwierdzanie zmiany haseł dla uniknięcia błędów podczas ich wprowadzania,
   4) wymuszenie wyboru haseł o odpowiedniej jakości, tj.: składających się co najmniej z 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne,
   5) wymuszenie zmiany haseł z ustaloną częstotliwością, w przypadku systemów przetwarzających dane osobowe zmiana hasła następuje nie rzadziej niż co 30 dni,
   6) wymuszenie zmiany haseł tymczasowych przy pierwszym rejestrowaniu się w systemie,
   7) pamiętanie haseł przez system w celu zapobiegania ponownemu ich użyciu, minimalna liczba haseł pamiętanych przez system wynosi 5.
2. Hasła administracyjne mogą być w szczególnych sytuacjach stosowane dłużej niż zaznaczono to w ust. 1 pkt 5, jednak nie dłużej niż 6 miesięcy.

§ 16.

Użycie programów narzędziowych

1. Uprawnienia umożliwiające uruchamianie programów narzędziowych są przydzielane na czas niezbędny do wykonania określonego zadania, na podstawie wniosku złożonego przez kierownika komórki organizacyjnej lub Właściciela Procesu / Właściciela Zasobu, którego wzór zamieszczono w załączniku nr 4 do niniejszego Regulaminu.
2. Poziom uprawnień umożliwiający uruchamianie programów narzędziowych jest udokumentowany.
3. Administrator Systemu rejestruje w Dzienniku pracy systemu, którego wzór zamieszczono w załączniku nr 3 do niniejszego Regulaminu, wszystkie przypadki użycia systemowych programów narzędziowych.
4. Systemowe programy narzędziowe oraz aplikacje, które nie są wykorzystywane przez użytkowników podczas pracy w systemach teleinformatycznych, są w miarę możliwości technicznych usuwane ze stacji roboczych i serwerów.

§ 17.

Ograniczenia czasowe sesji połączeniowej

1. W celu wymuszenia ochrony urządzeń systemu teleinformatycznego stosuje się następujące mechanizmy włączane w przypadku stwierdzenia braku aktywności użytkownika:
   1) blokowanie lub wyłączanie stacji roboczej (sesji połączeniowej),
   2) powtarzanie identyfikacji i uwierzytelnianie użytkownika.
2. System operacyjny po ustalonym okresie bezczynności użytkownika, jednak nie dłużej niż 10 minut, przechodzi w stan nieaktywny, w którym blokowany jest dostęp do konsoli. Powrót do stanu aktywności wymaga podania hasła.
3. Dla zapewnienia bezpieczeństwa systemów teleinformatycznych Agencji stosuje się ograniczenia czasu pracy w systemach operacyjnych do godzin pracy Agencji.
4. O ograniczeniu czasu trwania połączenia decyduje Właściciel Procesu/Właściciel Zasobu odpowiedzialny za funkcjonowanie i bezpieczeństwo danego systemu teleinformatycznego.
5. W przypadku konieczności pracy w systemie w innym czasie niż wyżej określony, zgodę wydaje Właściciel Procesu/Właściciel Zasobu na wniosek kierownika komórki organizacyjnej, której pracownicy potrzebują dostępu do systemu poza ustalonymi godzinami pracy.

§ 18.

Eksploatacja aplikacji w systemach teleinformatycznych Agencji

1. O przyznawaniu dostępu i zakresie nadanych uprawnień użytkowników do aplikacji decyduje Właściciel Procesu / Właściciel Zasobu w Centrali oraz, w razie potrzeby, dyrektor oddziału regionalnego dla użytkowników w oddziale regionalnym i biurze powiatowym, na podstawie upoważnienia nadanego przez Właściciela Procesu / Właściciela Zasobu.
2. Uprawnienia administratora są nadawane ograniczonej liczbie użytkowników.
3. Mechanizm dziedziczenia uprawnienia administratora aplikacji na podstawie uprawnień administratora nadanych w systemie operacyjnym lub na platformie bazodanowej jest zablokowany.
4. Właściciel Procesu / Właściciel Zasobu jest odpowiedzialny za aktualność i dokumentowanie przydzielonych uprawnień udzielonych użytkownikom do pracy w aplikacjach Agencji. Dotyczy to uprawnień wszystkich użytkowników w tym również pracowników podmiotów zewnętrznych świadczących usługi informatyczne dla Agencji.

§ 19.

Świadczenie usług informatycznych przez podmioty zewnętrzne

1. Dostęp podmiotu zewnętrznego do systemów Agencji wymaga przeprowadzenia udokumentowanego szacowania ryzyka.
2. Szacowanie ryzyka przeprowadza Właściciel Procesu/Właściciel Zasobu na podstawie informacji dostarczonych przez Administratora Systemu.
3. W szczególności, Właściciel Procesu/Właściciel Zasobu otrzymuje następujące informacje:
   1) podstawę udzielenia dostępu dla danego podmiotu zewnętrznego,
   2) zakres i sposób dostępu do sieci Agencji, w tym zakres przydzielanych uprawnień,
   3) proponowane rozwiązania techniczne i organizacyjne służące ograniczeniu ryzyka dla bezpieczeństwa systemów teleinformatycznych Agencji.
4. Zgodę na udzielenie dostępu podmiotowi zewnętrznemu wydaje Właściciel Procesu/ Właściciel Zasobu, po zaakceptowaniu i wdrożeniu rozwiązań, o których mowa w ust. 3 pkt 3.
5. W umowie z podmiotem zewnętrznym dotyczącej utrzymania systemów teleinformatycznych Agencji uwzględnia się zapis zobowiązujący podmiot zewnętrzny do stosowania zasad i procedur wynikających z dokumentów polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji. Umowa z podmiotem zewnętrznym może zawierać uszczegółowienie bądź rozszerzenie zasad wynikających z dokumentów polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji wynikające ze specyfiki danego projektu.
6. Doraźne działania serwisowe podmiotów zewnętrznych (nie mające charakteru stałego utrzymania systemów teleinformatycznych) są dokumentowana przez Administratora Systemu w dzienniku pracy systemu. Zapis w dzienniku zawiera, co najmniej:

1) dokładny czas rozpoczęcia i zakończenia działania serwisowego,
2) identyfikacja osoby realizującej działania serwisowe po stronie podmiotu zewnętrznego oraz nadzorującej te działania po stronie Agencji,
3) dokładny opis przeprowadzonych działań wraz ze wskazaniem statusu tych działań (wymagające kontynuacji, zakończone).

7. Doraźne działania serwisowe w systemie teleinformatycznym osób, nie będących uprawnionymi pracownikami Agencji dokonywane są w obecności Administratora Systemu.
8. Osobie reprezentującej podmiot zewnętrzny, wykonującej działania serwisowe, nie mogą zostać nadane uprawnienia administratora. Jeśli wyjątkowa sytuacja uzasadnia taką potrzebę, to nadanie uprawnienia wymaga zgody Właściciela Procesu/Właściciela Zasobu. Niezwłocznie po zakończeniu pracy uprawnienia administratora oraz jakiekolwiek inne uprawnienia nadane osobie reprezentującej podmiot zewnętrzny muszą zostać odebrane.
9. W przypadku dokonywania zmian konfiguracji (naprawy, rekonfiguracje) przez stronę trzecią Agencja zapewnia odpowiednie uprawnienia do użycia oprogramowania narzędziowego służącego do celów zarządzania konfiguracją.

Rozdział 4.

Zarządzanie zmianami w systemach teleinformatycznych Agencji

§ 20.

Odbiór systemu teleinformatycznego

1. Kryteria odbioru obejmują dostarczenie:

1) w przypadku oprogramowania - dokumentacji technicznej, instrukcji dla administratora i użytkownika,
2) w przypadku infrastruktury – dokumentacji powykonawczej obejmującej w szczególności schemat połączeń fizycznych i logicznych elementów infrastruktury.

2. Ponadto, kryteria odbioru obejmują:
   1) wymagania wydajnościowe i pojemnościowe systemu teleinformatycznego,
   2) dokumenty potwierdzające, że instalacja nowych systemów nie będzie miała negatywnego wpływu na istniejące systemy, szczególnie w chwilach największego obciążenia (jeżeli ma zastosowanie),
   3) dokumenty potwierdzające, że wpływ nowych systemów na bezpieczeństwo informacji został uwzględniony,
   4) szkolenia z zakresu posługiwania się i działania nowych systemów,
   5) w przypadku oprogramowania, odbiór obejmuje dodatkowo zapisy zawarte w § 7 Regulaminu rozwoju aplikacji.

§ 21.

Kontrola zmian w eksploatacji

1. Kontrola zmian sieci, systemów operacyjnych i aplikacji ma na celu zapewnianie poprawnego i bezpiecznego działania systemów teleinformatycznych pracujących w Agencji.
2. Zarządzanie zmianami polega na koordynacji, nadawaniu priorytetów, zatwierdzaniu, planowaniu zasobów i oceny ryzyka w związku ze zmianami dokonywanymi w systemach teleinformatycznych Agencji.
3. Każda zmiana w systemie teleinformatycznym Agencji musi być udokumentowana.
4. Zasady wskazane w niniejszym rozdziale odnoszą się do:
   1) zmian infrastruktury technicznej systemów sprowadzających się do wprowadzenia nowego elementu infrastruktury, zmodyfikowania lub usunięcia istniejącego elementu infrastruktury, poprawiania błędu w infrastrukturze, przy czym:
      a) zmiana infrastruktury regularna – oznacza zmianę, która nie wymaga natychmiastowego wdrożenia,
      b) zmiana infrastruktury awaryjna - stosowana w sytuacjach awaryjnych, gdzie czas implementacji zmiany jest krytyczny, z pominięciem lub uproszczeniem niektórych etapów (np. testów) przy założonym ryzyku,
      c) zmiana infrastruktury rutynowa - zaakceptowane wcześniej działanie związane z relatywnie prostymi czynnościami np. wymiana drukarki lub monitora,
   2) zmian aplikacyjnych będących poprawkami (w tym usuwanie błędów) albo modyfikacjami, zmiany aplikacyjne są klasyfikowane jako:
      a) zmiany aplikacyjne regularne – oznaczają zmiany, które nie wymagają natychmiastowego wdrożenia,
      b) zmiany aplikacyjne awaryjne – wprowadzane w stanie pilnej konieczności z powodu zagrożenia działania aplikacji,
   3) zmian w sposobie i/ lub zakresie świadczenia usług przez podmiot zewnętrzny.
5. Za proces zarządzania zmianami w poszczególnych obszarach jest odpowiedzialny Właściciel Procesu/Właściciel Zasobu, zaś za wykonywane zmian Administrator Systemu (jeżeli działania te zostały na niego delegowane).
6. Każda zmiana regularna jest poprzedzona udokumentowanym:
   1) opisem zmiany,
   2) opisem przyczyny zmiany (wraz z podaniem aktów prawnych uzasadniających zmianę – jeżeli ma zastosowanie),

3) opisem rodzaju wymaganych działań,
4) szacowaniem ryzyka potencjalnego wpływu zmian,
5) harmonogramem wprowadzanych zmian,
6) wykonaniem kopii zapasowej z możliwością odtworzenia stanu poprzedniego na wypadek nieprzewidzianych zdarzeń (jeżeli ma zastosowanie),
7) przetestowaniem zmian.

7. Jeżeli zmiana ma charakter awaryjny, dokumentacja może być opracowana najpóźniej w przeciągu 7 dni od dokonania zmiany.
8. Zmiana mająca charakter awaryjny, którą trzeba wprowadzić bezzwłocznie w celu ograniczenia ryzyka poważnego zakłócenia działalności Agencji wymaga zgody Właściciela Procesu / Właściciela Zasobu.
9. Dokonywane zmiany: regularne, awaryjne i rutynowe podlegają rejestracji w Dzienniku pracy systemu prowadzonym przez Administratora Systemu.
10. Wpisu dokonuje osoba przeprowadzająca zmianę. Wpis zawiera w szczególności odnośniki do dokumentów określonych w ust. 6.

§ 22.

Bezpieczeństwo dokumentacji systemu

1. Dokumentacja powykonawcza infrastruktury oraz dokumentacja techniczna systemu podlega ochronie zgodnie z zasadami ochrony informacji wrażliwych przedstawionymi w Polityce.
2. Osobą odpowiedzialną za aktualność i kompletność dokumentacji jest dyrektor komórki właściwej ds. informatyki.
3. Dokumentacja systemów jest udostępniana na zasadzie „wiedzy koniecznej". Udostępnienie dokumentacji jest rejestrowane.

Rozdział 5.

Zarządzanie wymiennymi nośnikami komputerowymi

§ 23.

Użytkowanie nośników

1. Nośniki komputerowe są przechowywane i eksploatowane zgodnie z zaleceniami producenta, z uwzględnieniem wymagań w zakresie ochrony informacji, które są umieszczone na nośnikach.
2. Nośniki zawierające informacje wrażliwe przechowywane są w specjalnych, atestowanych szafach (np. S120 DIS) zlokalizowanych w strefie administracyjnej. Szafy do przechowywania nośników zapewniają ochronę przed:
   1) pożarem,
   2) eksplozją towarzyszącą pożarowi,
   3) działaniem gazów powstałych podczas pożaru,
   4) zalaniem,
   5) działaniem pola elektromagnetycznego.
3. Wymienne nośniki komputerowe takie, jak: przenośne dyski twarde, kamery taśmy magnetyczne, optyczne nośniki danych, pamięci typu flash, podlegają ewidencji prowadzonej przez Administratora Systemu. Rejestr wymiennych nośników komputerowych prowadzony jest w postaci papierowej lub elektronicznej.
4. Etykiety nośników informacji posiadają identyfikator lub numer umożliwiający ich jednoznaczną identyfikację (np.: nr seryjny, kod kreskowy, itp.). Na podstawie etykiety nośnika informacji i danych zawartych w ewidencji nośników możliwe jest ustalenie:
   1) numeru ewidencyjnego nośnika,
   2) typu nośnika,
   3) daty zapisu na nośniku (informacja nieobowiązkowa dla nośników wielokrotnego zapisu),
   4) nazwy komórki organizacyjnej składującej informacje,
   5) określenia rodzaju przechowywanej informacji (informacja nieobowiązkowa dla nośników wielokrotnego zapisu),
   6) imienia i nazwiska osoby dokonującej zapisu (w przypadku nośników wielokrotnego zapisu imię i nazwisko osoby, na stanie której jest dany nośnik).
5. Nośniki wymienne zawierające informacje wrażliwe przewożone są przez pracowników Agencji do innych lokalizacji w pojemniku zapewniającym ochronę nośników przed zagrożeniami wskazanymi w ust. 2.

§ 24.

Wycofanie z eksploatacji nośników komputerowych

1. Wycofanie z eksploatacji wymiennych nośników komputerowych, przekazanie do naprawy lub ponownego użycia jest poprzedzone archiwizacją, a następnie skutecznym usunięciem zapisanych danych.
2. Uszkodzone wymienne nośniki komputerowe zawierające informacje wrażliwe są niszczone w sposób uniemożliwiający odczytanie zapisanych na nich informacji.

3. Zasady i tryb postępowania z nośnikami przekazanymi do archiwum określają odrębne przepisy Agencji.

Rozdział 6.

Bezpieczeństwo wymiany danych

§ 25.

Bezpieczeństwo serwisów intranetowych i ekstranetowych

1. Serwisy intranetowe i ekstranetowe są lokalizowane na serwerach, do których dostęp wymaga identyfikacji i uwierzytelnienia.
2. Udostępnienie informacji w serwisach intranetowych i ekstranetowych wymaga zatwierdzenia przez Właściciela Procesu/Właściciela Zasobu.
3. Dostęp do serwisów ekstranetowych posiadają wyłącznie pracownicy Agencji.
4. Dostęp do serwisów ekstranetowych mogą posiadać uprawnione z mocy prawa podmioty zewnętrzne współpracujące z Agencją.

§ 26.

Bezpieczeństwo wymiany poczty elektronicznej wewnętrznej i zewnętrznej

1. System poczty elektronicznej zapewnia:
   1) ochronę przed szkodliwym oprogramowaniem rozpowszechnianym za pomocą poczty elektronicznej,
   2) ochronę antywirusową załączników przesyłanych w poczcie elektronicznej,
   3) ochronę antyspamową,
   4) możliwość użycia dostępnych technik kryptograficznych do ochrony poufności i integralności wiadomości poczty elektronicznej,
   5) monitorowanie i rejestrowanie poczty elektronicznej.
2. Zasoby poczty elektronicznej (wszystkie skrzynki pocztowe) podlegają sporządzaniu kopii zapasowej. Kopia zapasowa sporządzana jest każdego dnia. Okres przechowywania kopii zapasowych wynosi co najmniej 3 dni.
3. System poczty elektronicznej nakłada ograniczenia, co do rozmiaru pojedynczej skrzynki pocztowej oraz wielkości przesyłanej wiadomości.

Rozdział 7.

Konserwacja i naprawy sprzętu

§ 27.

Konserwacja i naprawa sprzętu

1. Konserwacja sprzętu i urządzeń pracujących w systemach teleinformatycznych Agencji ma na celu zapewnienie nieprzerwanej i bezpiecznej pracy tych systemów, zapobieganie utraty, uszkodzenia lub naruszenia bezpieczeństwa.
2. Sprzęt podlega konserwacji według ustalonego planu, wynikającego z zaleceń producentów.
3. Konserwacja i naprawy muszą być prowadzone jedynie przez uprawnionych pracowników Agencji lub podmiot zewnętrzny świadczącą usługi konserwacyjne na podstawie umowy lub w ramach gwarancji.
4. W przypadku, gdy na nośnikach komputerowych, stanowiących integralną część sprzętu przekazywanego do naprawy, znajdują się informacje wrażliwe, sprzęt taki naprawiany jest pod nadzorem Administratora Systemu. Jeżeli zaś taki nadzór nie jest możliwy, to informacje wrażliwe są, po zapewnieniu możliwości ich odtworzenia, skutecznie usuwane z nośnika.
5. Wszelkie konserwacje i naprawy są odnotowywane w dzienniku pracy danego sprzętu.

§ 28.

Zabezpieczenie sprzętu poza siedzibą

1. Wynoszenie sprzętu (np. komputery przenośne, notesy elektroniczne itp.) jest możliwe tylko w przypadku uzyskania zgody Właściciela Procesu/Właściciela Zasobu.
2. Pracownik wyznaczony przez Właściciela Procesu/Właściciela Zasobu prowadzi ewidencję sprzętu pracującego poza Agencją.
3. Wszelkie informacje wrażliwe nie mogą być przechowywane w urządzeniach przenośnych, które pracują poza Agencją w postaci niezaszyfrowanej.
4. Sprzęt wykorzystywany poza Agencją podlega ubezpieczeniu.
5. Ustala się, że wynoszenie sprzętu komputerowego poza Agencję, w tym sposób programowego zabezpieczenia komputerów, odbywa się w sposób opisany w „Procedurze wydawania zezwoleń na wynoszenie sprzętu komputerowego z ARiMR" zawartej w Książce Procedur KP-611-206-ARiMR.
6. Wynoszenie sprzętu komputerowego poza Agencję dotyczy również sytuacji, kiedy praca odbywa się na terenie Agencji, ale poza pomieszczeniami przystosowanymi do przetwarzania informacji wrażliwych.

Rozdział 8.
Zarządzanie dostępem do systemów teleinformatycznych
§ 29.
Rejestrowanie użytkowników i przypisanie praw dostępu

1. Użytkownik systemu teleinformatycznego jest jednoznacznie identyfikowany poprzez indywidualny identyfikator (nazwę) użytkownika.
2. Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego użytkownika (chyba, że z przyczyn technicznych nie ma możliwości stosowania osobistych identyfikatorów).
3. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.
4. Uprawnienia dostępu są nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzeby wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień administratora (przywilejów) będzie kwalifikowane jako incydent związany z bezpieczeństwem informacji.
5. Nadawanie uprawnień dostępu do systemu teleinformatycznego Agencji odbywa się zgodnie z procedurą nadawania/zmiany/odbierania uprawnień pracownikom ARiMR zawartą w Książce Procedur KP-611-101-ARiMR.
6. W przypadku konieczności natychmiastowego odebrania/ograniczenia praw dostępu dopuszcza się możliwość zastosowania uproszczonego trybu polegającego na przekazaniu stosownej informacji pocztą elektroniczną od bezpośredniego przełożonego do Administratora Systemu, która niezwłocznie jest potwierdzana w zwykłym trybie.
7. Rejestr użytkowników wraz z przyznanymi uprawnieniami do systemu lub aplikacji prowadzi Administrator Systemu. Rejestr publikowany jest w sieci wewnętrznej na stronie intranetowej Agencji i aktualizowany nie rzadziej niż raz na miesiąc. Weryfikację aktualności tego rejestru prowadzą Właściciele Procesów/Właściciele Zasobów w odniesieniu do nadzorowanych przez siebie zasobów.
8. Prawa dostępu do wielu aktywów (plików, katalogów, aplikacji, stron internetowych) jednocześnie przydzielane są dla każdego z aktywów za osobną zgodą danego Właściciela Procesu/Właściciela Zasobu. W przypadku, gdy w Agencji wykorzystuje się domenowe mechanizmy zarządzania dostępem (usługi katalogowe, active directory, itp.) aktywa są grupowane, za uprzednią zgodą odpowiednich Właścicieli Procesów / Właścicieli Zasobów.
9. Administrator Systemu raz na miesiąc dokonuje przeglądu stanu aktywności kont użytkowników.
10. Konta nieużywane przez okres 30 dni są automatycznie blokowane.

§ 30.
Zarządzanie przywilejami

1. Nadawane przywileje (większe uprawnienia niż wynika to z realizowanych rutynowych zadań użytkownika) podlegają ścisłej ewidencji prowadzonej przez Administratora Systemu.
2. Przywileje w systemie nadaje Administrator Systemu zgodnie z procedurami obsługi kont użytkowników systemów informatycznych zamieszczonymi w Książce Procedur KP-611-101-ARiMR.
3. Uprzywilejowane konto nie może służyć do realizacji przez użytkownika rutynowych zadań.
4. Przywileje podlegają cofnięciu niezwłocznie po ustaniu potrzeby uzasadniającej ich nadanie.
5. Przywileje nadawane są osobie zastępującej danego administratora na czas jego nieobecności.
6. Osobie zastępującej przekazywane są hasła dostępu oraz procedury wykonywane nadanym stanowisku.
7. Nadawane przywileje podlegają regularnym przeglądom i kontroli.

§ 31.
Zarządzanie hasłami użytkowników

1. Niedopuszczalne jest występowanie w systemie teleinformatycznym kont niezabezpieczonych hasłem.
2. Administrator Systemu, za pomocą ustawień systemowych, wymusza natychmiastową zmianę hasła początkowego, przydzielonego użytkownikowi, na nowe przez niego wybrane (o ile istnieją możliwości techniczne wymuszenia).
3. Zabronione jest przekazywanie haseł przez osoby trzecie lub za pośrednictwem otwartych wiadomości poczty elektronicznej (nie dotyczy to haseł tymczasowych do systemów wyposażonych w mechanizm wymuszający zmianę hasła przy pierwszej próbie uwierzytelnienia się w danym systemie).
4. Hasła tymczasowe, dostarczane w przypadku utraty hasła, są wydawane dopiero po pozytywnej weryfikacji tożsamości użytkownika.
5. Przy konfigurowaniu mechanizmów logowania do systemów uwzględnia się następujące zasady:
   1) użytkownik musi podać swój identyfikator oraz hasło,
   2) w polu logowania nie jest prezentowana ostatnio użyta nazwa użytkownika (o ile system to umożliwia),
   3) wpisywane hasło nie pojawia się w postaci jawnej na ekranie logowania,
   4) hasło przesyłane jest w postaci zaszyfrowanej (o ile system to umożliwia).
6. Systemy operacyjne i aplikacje spełniają wymagania dotyczące możliwości ustawienia następujących parametrów haseł:

1) siły hasła (długość i złożoność haseł),
2) maksymalnego okresu ważności,

3) ograniczenia możliwości ponownego wykorzystania hasła (pamięć ostatnio używanych haseł).
7. Specjalne warunki przechowywania duplikatów haseł dotyczą:
   1) elementów aktywnych sieci teleinformatycznej,
   2) haseł administracyjnych do systemów, aplikacji i baz danych,
   3) konfiguracji komputerów, w tym hasła do BIOS.
8. Hasła administracyjne przechowuje się w postaci zaszyfrowanej. Dopuszcza się przechowywanie haseł w wersji elektronicznej poprzez zastosowanie oprogramowania typu „password manager" z bazą szyfrowaną algorytmem AES lub Twofish.
9. Do przechowywania hasła głównego do zaszyfrowanej bazy haseł, bądź innych haseł zapisanych na papierze, stosuje się wyłącznie koperty, które uniemożliwiają otwarcie bez uszkodzenia ich struktury (tzw. „koperty bezpieczne"). Koperty z hasłami przechowuje się w sejfie, w miejscu zapewniającym dostęp tylko osobom upoważnionym.
10. Dane umieszczone na bezpiecznej kopercie zawierają:
1) numer koperty adekwatny do numeru ewidencyjnego podanego w książce ewidencji haseł,
2) datę jej złożenia i podpis osoby składającej kopertę,
3) skróconą nazwę przynależności hasła.
11. Koperty z hasłami podlegają oznaczaniu zgodnie z załącznikiem nr 2 do niniejszego Regulaminu oraz ścisłej ewidencji prowadzonej przez Administratora Systemu.
12. Ewidencja haseł przechowywana jest w miejscu zabezpieczonym przed utratą i dostępem osób niepowołanych.
13. Za aktualność przechowywanych haseł odpowiedzialny jest Administrator Systemu.
14. Awaryjne otwarcie bezpiecznej koperty oraz pobranie kopii hasła znajdującego się w kopercie wymaga uprzedniej pisemnej akceptacji Właściciela Procesu / Właściciela Zasobu lub osoby przez niego upoważnionej i jest udokumentowane w ewidencji kopert.
15. Po użyciu, hasło ulega zniszczeniu, a w to miejsce jest generowane nowe hasło, którego kopia jest przechowywana na identycznych zasadach jak w przypadku zniszczonego hasła.

§ 32.

Zasady dostępu do plików i katalogów

1. Uprawnienia dostępu do plików i katalogów z poziomu systemu operacyjnego są nadawane przez Administratora Systemu po zatwierdzeniu przez Właściciela Procesu/Właściciela Zasobu odpowiedzialnego za dany zasób.
2. Uprawnienia dostępu do katalogów i plików aplikacji, w tym do baz danych, są nadawane przez Administratora Systemu po zatwierdzeniu przez Właściciela Procesu/Właściciela Zasobu odpowiadającego za dany zasób.

Rozdział 9.
Zasady monitorowania systemów i ich użycia

§ 33.

Mechanizmy monitorowania systemów

1. Monitorowanie systemów i ich użycia ma na celu wykrywanie nieuprawnionych działań.
2. Rejestrowane i monitorowane są wszystkie zdarzenia polegające na użyciu urządzeń przetwarzania informacji oraz programów narzędziowych, diagnostycznych zapewniając weryfikację i rozliczalność użytkowników wykonujących zadania, do których zostali uprawnieni. W szczególności rejestrowaniu podlegają:
   1) identyfikatory użytkowników,
   2) daty i czasy zarejestrowania i wyrejestrowania w systemie,
   3) identyfikator stacji roboczej lub terminala (nazwę komputera w systemie),
   4) nieudane próby logowania do systemu,
   5) zmiany zapisów w rejestrach,
   6) błędy systemu i procedury obsługi tych błędów,
   7) zawieszenie i ponowne uruchomienia systemu,
   8) uruchamianie programów narzędziowych,
   9) zmiany w plikach konfiguracyjnych i krytycznych zmiennych systemowych,
   10) wersje systemu i stan uaktualnień w porównaniu z zalecanymi przez producenta, (jeśli ma zastosowanie).
3. Rejestry są utrzymywane i przechowywane dla wszystkich krytycznych dla Agencji systemów i aplikacji.
4. Systemy rejestrów są objęte standardową procedurą tworzenia kopii archiwalnych. Kopie archiwalne rejestrów przechowywane są przez 2 lata.
5. Serwery kontrolujące dostęp do Internetu tworzą zdalne pliki rejestrów lub mają wdrożony system przesyłania rejestrów zdarzeń na inne, wewnętrzne serwery.

6. W celu wykrywania incydentów związanych z bezpieczeństwem Administrator Systemu regularnie monitoruje zapisy dokonywane automatycznie przez systemy w rejestrach zdarzeń pod kątem właściwego wykorzystania systemu teleinformatycznego i zarządzania nim.
7. Systemy zapisu zdarzeń są zabezpieczone przed manipulacją i nieuprawnionymi zmianami.
8. W ramach weryfikacji zgodności systemów teleinformatycznych względem standardów bezpieczeństwa przeprowadzane są, na podstawie zatwierdzonego przez Prezesa Agencji harmonogramu oraz procedury KP-611-298-ARiMR, testy bezpieczeństwa systemów teleinformatycznych ARiMR.

§ 34.

Dziennik pracy systemu

1. Administrator Systemu prowadzi dziennik wykonywanych czynności oraz zdarzeń zachodzących w systemie. Dzienniki pracy systemu, zgodnie ze wzorem zamieszczonym w załączniku nr 3 do niniejszego Regulaminu, zawierają zapisy dotyczące następujących zdarzeń lub czynności:
   1) informacje o nadaniu, modyfikacji lub cofnięciu przywilejów w systemie,
   2) przejęcie obowiązków administratora,
   3) błędy systemowe i podjęte działania naprawcze,
   4) zdarzenie związane z bezpieczeństwem informacji,
   5) błędy zgłaszane przez użytkowników oraz innych administratorów, a także uzyskane od stron trzecich świadczących usługi na rzecz systemu użytkowanego w Agencji oraz podjęte działania naprawcze,
   6) informacje o sesjach połączeń zdalnych wykonywanych przez podmioty zewnętrzne (jeżeli ma zastosowanie) zawierające:
      a) cel połączenia,
      b) opis działań,
      c) specyfikację danych i systemów, do których firma serwisowa będzie miała dostęp,
      d) nazwisko osoby nawiązującej połączenie ze strony firmy zewnętrznej oraz nazwę firmy,
      e) datę i godzinę połączenia,
   7) instalacje oprogramowania lub zmiany wersji,
   8) użycie programów narzędziowych,
   9) zmiany konfiguracji sprzętu i systemu operacyjnego.
2. Każdy zapis w dzienniku pracy systemu zawiera informacje dodatkowe o czynnościach lub zdarzeniu, takie jak:
   1) czas rozpoczęcia i zakończenia pracy w systemie;
   2) nazwisko osoby wykonującej wpis do dziennika,
   3) identyfikator konta, z którego wykonano czynności (jeśli ma zastosowanie).
3. Administrator Systemu odnotowuje w dzienniku wszelkie dodatkowe informacje, które pozwolą zlokalizować przyczynę błędu:
   1) w przypadku awarii sprzętu lub usługi, w szczególności:

a) powtórzenie błędu (np. analogiczny wcześniejszy zapis w dzienniku),
b) objawy towarzyszące (np. komunikaty systemowe, logi połączeń),
c) krytyczność awarii, zgodnie z klasyfikacją uzgodnioną z dostawcą usług (np. w umowie SLA),

   2) w przypadku awarii oprogramowania, w szczególności:
      a) powtórzenie błędu (np. analogiczny wcześniejszy zapis w dzienniku),
      b) zrzuty ekranów,
      c) konfiguracje oprogramowania i baz danych (np. otwarte pliki, zapisy w logach),
      d) krytyczność błędu, zgodnie z klasyfikacją uzgodnioną z dostawcą oprogramowania.
4. Lista działań wykonywanych przez administratorów podlegających bezwzględnemu odnotowywaniu w dziennikach może zostać poszerzona lub ograniczona dla danego systemu teleinformatycznego po ówczesnym przeprowadzeniu udokumentowanego
   szacowanie ryzyka i zatwierdzeniu przez Komitet.
5. Dzienniki mogą być prowadzone oddzielnie dla każdego serwera, urządzenia sieciowego, aplikacji.
6. Dzienniki prowadzone są przez administratora odpowiedzialnego za dany serwer, urządzenie sieciowe, aplikację.
7. Dzienniki systemowe lub ich części prowadzone są w formie elektronicznej lub papierowej.
8. Rejestracja błędów może być prowadzona poza dziennikiem administratora, w dedykowanym rejestrze.

§ 35.

Synchronizacja zegarów

1. Odpowiednia dokładność i możliwość korelacji rejestrów zdarzeń, których zapisy mogą służyć jako dowody w postępowaniu w przypadku wykrycia naruszenia bezpieczeństwa, jest zapewniona przez właściwe ustawienie zegarów urządzeń teleinformatycznych.

2. Do synchronizacji czasu wykorzystuje się protokół NTP.
3. Źródłem synchronizacji powinien być zewnętrzny wzorzec czasu.
4. Stacje robocze synchronizują czas z kontrolerów domen.

§ 36.

Bezpieczeństwo okablowania

1. W Agencji przyjęto następujące zasady instalowania i ochrony okablowania:
   1) sposób instalacji okablowania uwzględnia ochronę okablowania przed nieautoryzowanym dostępem lub uszkodzeniem, poprzez prowadzenie kabli w rurach kablowych, listwach PCV, podłogach technologicznych,
   2) okablowanie, w miarę możliwości, nie jest prowadzone przez ogólnie dostępne strefy; w przypadku prowadzenia okablowania przez takie miejsca stosowane są środki uniemożliwiające bądź ograniczające dostęp do okablowania przez osoby nieupoważnione,
   3) przy projektowaniu przebiegu linii sieci teleinformatycznej poza strefami administracyjnymi wykorzystywane są w maksymalnym stopniu rozwiązania wykorzystujące technologie światłowodowe,
   4) w instalacji okablowania oddzielono kable zasilające od okablowania komunikacyjnego w celu unikania interferencji,
   5) w instalacji okablowania zastosowano jednoznaczne i wyraźne oznakowanie umożliwiające identyfikację kabli i sprzętu w celu zmniejszenia ryzyka błędów takich, jak niewłaściwe połączenie lub zastosowanie nieodpowiedniego kabla,
   6) kable komunikacyjne wyposażone są w zabezpieczenia odgromowe (jeżeli ma zastosowanie),
   7) prowadzi się kompletną i aktualną dokumentację połączeń fizycznych i logicznych w celu zmniejszenia prawdopodobieństwa błędów.
2. Pomieszczenia, w których znajdują się panele połączeniowe, węzły telekomunikacyjne i szafy dystrybucyjne objęte są systemem kontroli dostępu.
3. Niewykorzystywane segmenty sieci strukturalnej są odłączane od sieci teleinformatycznej.
4. W przypadku systemów wskazanych w procesie szacowania ryzyka jako kluczowe, są uwzględnione następujące zabezpieczenia obejmujące:
   1) stosowanie zapasowych (awaryjnych) dróg komunikacyjnych lub mediów transmisyjnych zapewniających odpowiedni poziom bezpieczeństwa,
   2) korzystanie z kabli światłowodowych.
5. Badanie właściwości transmisyjnych okablowania strukturalnego przeprowadzane jest przez Administratora Systemu nie rzadziej niż raz na 2 lata.

§ 37.

Eksploatacja urządzeń zasilających

1. Wszystkie urządzenia sieci teleinformatycznej są zasilane napięciem o parametrach zgodnych z wymaganiami producenta.
2. Urządzenia teleinformatyczne muszą być zasilane z wydzielonej instalacji elektrycznej.
3. Urządzenia sieci teleinformatycznej, od ciągłości pracy, których zależne jest realizowanie podstawowych zadań Agencji, muszą być zasilane z gwarantowanych źródeł.
4. Gwarantowane zasilanie uzyskiwane jest przez zastosowanie dywersyfikacji zewnętrznych źródeł energii elektrycznej z samoczynnym załączaniem rezerwy (SZR), zastosowanie zasilaczy bezprzerwowych (UPS), zastosowanie awaryjnych agregatów prądotwórczych.
5. Konfiguracja zasilania gwarantowanego wynika z Planu Zapewnienia Ciągłości Działania Agencji.
6. Dobór urządzeń podtrzymujących zasilanie pod względem wydajności mocowej poprzedzane jest przeprowadzeniem udokumentowanego bilansu mocy.
7. Każde urządzenie sieci teleinformatycznej jest opatrzone tabliczką, z której wynika skąd dane urządzenie jest zasilane, zawierającą nazwę rozdzielnicy lub tablicy zabezpieczeń oraz nazwę pola w rozdzielnicy lub bezpiecznika na tablicy zabezpieczeń.
8. Stan zasilania zasobów sieci teleinformatycznej, którym nadano status zasobu kluczowego, jest na bieżąco monitorowany przez Administratora Systemu. Jakość zasilania pozostałych zasobów sieci teleinformatycznej musi być okresowo sprawdzana.
9. Zasilacze bezprzerwowe, zasilające kluczowe zasoby sieci teleinformatycznej, raportują stan swojej pracy (zasilanie z sieci, zasilanie z baterii) oraz parametry baterii (jej stopień naładowania i przewidziany czas pracy z baterii przy danym obciążeniu)
   systemom operacyjnym serwerów. W przypadku, gdy stopień naładowania baterii osiągnie w czasie pracy z baterii poziom, którego przekroczenie nie gwarantuje podtrzymania ciągłości pracy, system operacyjny wymusza automatyczne zamknięcie aplikacji i baz danych oraz kontrolowane wyłączenie serwera.

10. W przypadku, gdy automatyczne raportowanie nie jest technicznie możliwe Administrator Systemu dokonuje okresowych, raz na tydzień, oględzin polegających na sprawdzeniu wskazań paneli sterujących (według instrukcji techniczno-eksploatacyjnych). Oględziny muszą być odnotowywane w dzienniku pracy systemu.
11. Elementy systemu zasilania gwarantowanego podlegają okresowym przeglądom i konserwacjom w zakresie określonym przez producenta.
12. Akumulatory podlegają wymianie po okresach eksploatacji przewidzianych w instrukcjach użytkowania.
13. Serwisowanie urządzeń zasilających przeprowadzane jest wyłącznie przez autoryzowane podmioty zewnętrzne.
14. Przeglądy, konserwacje i serwisowanie podlega odnotowaniu w dzienniku pracy systemu.
15. Agregaty prądotwórcze są okresowo uruchamiane w okresach i zakresie przewidzianych przez ich producentów.

Załącznik nr 1 do Regulaminu eksploatacji systemów teleinformatycznych - Rejestr kopii zapasowych

L.p.	Nazwa systemu lub aplikacji	Lokalizacja jednostki danych	Nazwa serwera	Typ danych (system operacyjny, baza danych, pliki, poczta, inne)	Typ backupu (pełny, przyrostowy, różnicowy)	Wolumen [GB]
1						
2						
3						
4						
5						
6						
7						

cd.:

L.p.	Nazwa systemu lub aplikacji	Częstotliwość wykonywania backupu	Ilość kopii zapasowych	Sposób wykonywania kopii	Okres przechowywania	Miejsce przechowywania kopii zapasowych	Okno czasowe backupu
1							
2							
3							
4							
5							
6							
7							

Załącznik nr 2 do Regulaminu eksploatacji systemów teleinformatycznych - Ewidencja bezpiecznych kopert

1. Ewidencja bezpiecznych kopert prowadzona jest w książce ewidencji haseł, która zawiera:
    1) Numer ewidencyjny,
    2) Oznaczenie przynależności hasła zawartego w kopercie (nazwa systemu, zasobu, komputera, elementu aktywnego, itp.),
    3) Imię i nazwisko, pełnioną funkcję oraz podpis osoby składającej kopertę (właściciela hasła),
    4) Datę złożenia koperty z hasłem,
    5) Podpis osoby przyjmującej kopertę na przechowanie,
    6) Datę wygaśnięcia ważności hasła zawartego w kopercie,
    7) Adnotację o wydaniu koperty z hasłem (użyciu awaryjnym).

Wzór etykiety na kopercie:

Właściciel hasła	**Imię i nazwisko**
Nazwa systemu, zasobu lub komputera, do którego przynależy hasło	Nazwa
Numer kolejny hasła	01, 02, ...
Daty początku i końca okresu ważności hasła	dd-mm-rr - dd-mm-rr
Data złożenia	dd-mm-rrrr

Załącznik nr 3 do Regulaminu eksploatacji systemów teleinformatycznych - Dziennik pracy systemu

Lp.	Rodzaj zdarzenia	Opis zdarzenia	Rozpoczęcie pracy [data, godzina]	Zakończenie pracy [data, godzina]	Nazwisko i imię osoby dokonującej wpisu	Konto, które zostało użyte do obsługi zdarzenia	Podjęte działania naprawcze
1	2	3	4	5	6	7	8

Załącznik nr 4 do Regulaminu eksploatacji systemów teleinformatycznych
- Wniosek dotyczący użytkowania programu narzędziowego

Część I
(Wypełnia kierownik komórki/jednostki organizacyjnej/Właściciel Zasobu)

1) Komórka organizacyjna:
.....

2) Nazwa programu narzędziowego, wersja i krótki opis
.....

Program wewnętrzny (część systemu lub aplikacji)		☐
Program zewnętrzny		☐
Wymagane uprawnienia w systemie (zwykły użytkownik, administrator, supervisor itp.) – opcjonalnie, jeśli Wypełniający dysponuje taką wiedzą	.....	
Szczegółowe informacje techniczne i dostępność (np. URL producenta, dostawcy)	.....	
Okres użytkowania programu:	Regularnie, z częstotliwością <....>, bezterminowo Regularnie, z częstotliwością <....> do: (data) Jednorazowo	☐ ☐ ☐

3) Imiona i nazwiska użytkowników:
.....

4) Uzasadnienie wniosku:
.....

…….……
(data i podpis kierownika komórki/jednostki organizacyjnej/Właściciela Zasobu)

Część II Ocena zasadności wniosku (w aspekcie bezpieczeństwa informacji i systemów teleinformatycznych)
(wypełnia dyrektor komórki właściwej ds. bezpieczeństwa informacji)

Decyzja pozytywna	☐	Decyzja negatywna	☐

Uzasadnienie:
.....
.....

……
(data i podpis dyrektora komórki właściwej ds. bezpieczeństwa informacji)

Część III Informacje o realizacji wniosku
(Wypełnia Administrator Systemu)

Identyfikator wniosku: .....

.....
.....
.....

Nadany(e) identyfikator(y) (ID) użytkownika(ów) .....

Poziom uprawnień (przywilejów) .....

……
(data i podpis Administratora Systemu)

Załącznik nr 14 do Polityki bezpieczeństwa informacji w ARiMR

REGULAMIN OCHRONY DANYCH OSOBOWYCH

Spis treści:

Rozdział 1
Definicje
§ 1.

Użyte w regulaminie określenia oznaczają:

1) Administrator danych – Agencja Restrukturyzacji i Modernizacji Rolnictwa;
2) UODO – Urząd Ochrony Danych Osobowych;
3) PUODO – Prezes Urzędu Ochrony Danych Osobowych;
4) RODO - Rozporządzenie Parlamentu Europejskiego Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
5) Ustawa – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
6) Inspektor Ochrony Danych (IOD) – wyznaczony przez Administratora danych pracownik realizujący zadania, o których mowa w art. 39 RODO;
7) Właściciel zbioru – dyrektor komórki organizacyjnej w Centrali Agencji, któremu powierzono zbiór danych osobowych;
8) Współadministrator – administrator, który wspólnie z innym lub innymi administratorami ustala cele i sposoby przetwarzania. W drodze wspólnych uzgodnień współadministratorzy określają zakres swojej odpowiedzialności, dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą przysługujących jej praw oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 RODO, chyba, że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo krajowe, któremu administratorzy ci podlegają;
9) Przedstawiciel administratora – osoba fizyczna lub prawna mająca miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora na mocy art. 27 do reprezentowania administratora w zakresie jego obowiązków wynikających z RODO;
10) Podmiot przetwarzający – podmiot przetwarzający dane osobowe na podstawie umowy lub innego instrumentu prawnego w imieniu Administratora danych, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób których dane dotyczą;
11) Zbiór danych osobowych – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

12) Naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przetwarzanych danych osobowych;
13) Privacy by design – zasady ochrony danych osobowych na etapie projektowania systemu służącego do przetwarzania danych osobowych;
14) Privacy by default – zasady ochrony danych osobowych w zakresie podstawowym (domyślne);
15) Privacy Impact Assessment – ocena skutków dla ochrony danych osobowych;
16) Osoba, której dane dotyczą – każda osoba fizyczna, których dane są przetwarzane przez Administratora danych;
17) Prawa osób, których dane dotyczą – prawa, o których mowa w art. 15-21 RODO;
18) Nowy Projekt – każda nowa inicjatywa, której realizacja będzie wiązać się z przetwarzaniem danych osobowych. Nowym projektem będzie w szczególności: zorganizowanie konkursu, stworzenie nowej lub modyfikacja istniejącej aplikacji, wdrożenie nowej lub modyfikacja istniejącej usługi, jeśli w ramach jej świadczenia będzie dochodzić do przetwarzania danych, lub wdrożenie nowego procesu przetwarzania danych osobowych.

Rozdział 2
Cel przetwarzania danych osobowych
§ 2.

1. Agencja przetwarza dane osobowe w celu realizacji zadań określonych w ustawie o Agencji Restrukturyzacji i Modernizacji Rolnictwa oraz w związku z wykonywaniem innych ustaw.
2. Dane osobowe są przetwarzane do czasu realizacji celu, dla którego zostały pozyskane, chyba, że przepisy innych ustaw stanowią inaczej.
3. Niniejszy regulamin ma zastosowanie do danych osobowych przetwarzanych we wszystkich zasobach Agencji, a w szczególności w systemach teleinformatycznych, poza systemami teleinformatycznymi oraz na wszelkich nośnikach danych.

Rozdział 3
Organizacja bezpieczeństwa
§ 3.

1. Przestrzeganie zasad ochrony danych osobowych należy do obowiązków wszystkich pracowników jednostek i komórek organizacyjnych Agencji oraz podmiotów zewnętrznych współpracujących z Agencją.
2. Właściciel zbioru wykonuje obowiązki Administratora danych wobec powierzonego mu zbioru danych osobowych za wyjątkiem tych obowiązków, które zostały przekazane innym podmiotom.
3. Właściciel zbioru jest obowiązany zapewnić ochronę przetwarzanych danych osobowych przez zastosowanie środków technicznych i organizacyjnych zapewniających ochronę odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed dostępem do nich osób nieupoważnionych, zabraniem przez osobę nieuprawnioną, ich zmianą, utratą, uszkodzeniem lub zniszczeniem oraz zapewnić, aby dane były przetwarzane zgodnie z przepisami prawa.
4. Szczegółowe zakresy obowiązków i odpowiedzialności Właściciela Zasobu ustanowione w Polityce bezpieczeństwa informacji w ARiMR stosuje się odpowiednio do Właściciela zbioru.
5. Właściciel zbioru nie może delegować swoich zadań do podmiotów zewnętrznych.
6. Dyrektor oddziału regionalnego nie jest Właścicielem zbioru.

§ 4.

1. Do zadań Inspektora Ochrony Danych należy:
   1) kreowanie polityki ochrony danych osobowych oraz dokonywanie jej wykładni poprzez:
      a) określanie zasad przetwarzania danych osobowych m.in. ich udostępniania i powierzania, a także zasad ochrony danych osobowych i zarządzania danymi osobowymi,
      b) określenie jednolitego dla całej Agencji sposobu prowadzenia dokumentacji, o której mowa w RODO oraz dokumentowania wykonania czynności wymaganych w RODO,
      c) sporządzanie i przedstawianie stanowiska w sprawie stosowania obowiązującego w tym zakresie prawa,
      d) inicjowanie, tworzenie i aktualizacja procedur oraz innych dokumentów wynikających z zadań powierzonych w polityce ochrony danych osobowych,
      e) opiniowanie, pod względem zgodności z przepisami o ochronie danych osobowych oraz polityką ochrony danych osobowych, umów (w tym umów powierzenia przewarzania danych), porozumień, procedur i innych dokumentów wytworzonych w Agencji, dotyczących bezpieczeństwa i przetwarzania danych osobowych,
      f) wspieranie dyrektora komórki ds. bezpieczeństwa w zakresie opiniowania nowych projektów pod kątem zgodności z zasadami ochrony w fazie projektowania oraz domyślnej ochrony danych (Privacy by design, Privacy by defoult);

2) monitorowanie przestrzegania RODO, innych przepisów o ochronie danych osobowych oraz polityki ochrony danych osobowych, w szczególności poprzez:
   a) zbieranie informacji w celu identyfikacji procesów przetwarzania,
   b) zbieranie informacji w celu zapewnienia przestrzegania polityki ochrony danych osobowych,
   c) nadzorowanie i koordynowanie prowadzenia przez Właścicieli zbiorów rejestrów czynności przetwarzania danych osobowych oraz rejestrów kategorii czynności przetwarzania,
   d) prowadzenie zbiorczych rejestrów czynności przetwarzania oraz zbiorczych rejestrów kategorii czynności przetwarzania,
   e) prowadzenie zbiorczego rejestru umów powierzenia na podstawie danych przekazywanych przez Właścicieli zbiorów,
   f) wykonywanie czynności audytowych weryfikujących zgodność przetwarzania danych oraz rekomendowanie określonych działań w tym zakresie. Realizując uprawnienie, o którym mowa w zdaniu pierwszym Inspektor Ochrony Danych w szczególności:
      – audytuje sposób przetwarzania danych osobowych we wszystkich komórkach i jednostkach organizacyjnych Agencji,
      – audytuje sposób przestrzegania obowiązujących standardów ochrony danych osobowych w odniesieniu do zastosowanych środków technicznych i organizacyjnych we wszystkich komórkach i jednostkach organizacyjnych Agencji,
   g) wydawanie zaleceń Właścicielom zbiorów, dyrektorom oddziałów regionalnych i innym osobom odpowiedzialnym za ochronę i zgodne z prawem przetwarzanie danych osobowych w Agencji;
3) zwiększanie świadomości personelu uczestniczącego w operacjach przetwarzania danych osobowych, poprzez prowadzenie szkoleń (z wyjątkiem szkoleń podstawowych dla osób nowozatrudnionych) i udzielanie konsultacji w zakresie ochrony danych osobowych;
4) udzielanie na żądanie Właściciela zbioru/dyrektora oddziału regionalnego zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania, zgodnie z art. 35 RODO. Dokonując oceny Właściciel zbioru/dyrektor oddziału regionalnego może konsultować z Inspektorem Ochrony Danych m.in. następujące kwestie:
   a) czy zasadne jest przeprowadzenie oceny skutków dla ochrony danych,
   b) metodologię przeprowadzania oceny skutków dla ochrony danych,
   c) czy zasadne jest przeprowadzenie wewnętrznej oceny czy zlecenie jej podmiotowi zewnętrznemu,
   d) zabezpieczenia (w tym środki techniczne i organizacyjne) stosowane do minimalizowania wszelkich zagrożeń praw i interesów osób, których dane dotyczą,
   e) prawidłowości przeprowadzenia oceny skutków dla ochrony danych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie oraz jakie zabezpieczenia należy zastosować);
5) współpraca z PUODO (organem nadzorczym) w kwestiach związanych z przetwarzaniem danych osobowych, w tym reprezentowanie Administratora danych w postępowaniach skargowych prowadzonych przed PUODO;
6) pełnienie funkcji punktu kontaktowego dla PUODO w kwestiach związanych z przetwarzaniem danych osobowych, w tym z uprzednimi konsultacjami związanymi z dokonywaniem oceny skutków dla ochrony danych, o których mowa w art. 36 RODO, oraz – w stosownych przypadkach – prowadzenie konsultacji we wszelkich innych sprawach;
7) pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą;
8) ocena, czy istnieje w danym stanie faktycznym wymóg zgłaszania naruszenia ochrony danych osobowych;
9) ocena, czy istnieje w danym stanie faktycznym wymóg zawiadamiania osób, których dane dotyczą, o naruszeniu ochrony danych osobowych;
10) prowadzenie rejestru naruszeń ochrony danych osobowych.

2. Osoby zatrudnione w ARiMR na podstawie umowy o pracę oraz osoby wykonujące pracę na podstawie innych form zatrudnienia, a także stażyści, praktykanci i wolontariusze mają obowiązek współpracy z Inspektorem Ochrony Danych, w związku z realizacją jego zadań, a także niezwłocznego informowania, w szczególności o incydentach lub podejrzeniach incydentów związanych z ochroną danych osobowych, w tym naruszeniach ochrony danych.

§ 5.

1. Każdy zbiór danych osobowych przetwarzanych w Agencji posiada Właściciela zbioru ustanowionego w formie zarządzenia.
2. Właściciel zbioru odpowiada za realizację ustawowych obowiązków Administratora danych, a w szczególności odpowiada za:
   1) przetwarzanie danych osobowych zgodne z zasadami określonymi w art. 5 RODO, tj.:
      a) zasadą legalności, rzetelności i przejrzystości danych – przetwarzanie zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Właściciel zbioru zapewnia przejrzystość przetwarzania danych, w szczególności poprzez informowanie osób, których dane dotyczą o przetwarzaniu danych z chwilą ich pozyskania, w tym o celu i podstawie prawnej przetwarzania. Właściciel zbioru zapewnia, aby dane były zbierane tylko w zakresie niezbędnym do wskazanego celu i przetwarzane tylko przez okres, w jakim jest to niezbędne,
      b) zasadą celowości (ograniczenia celu) – dane osobowe powinny być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz nieprzetwarzane dalej w sposób niezgodny z tymi celami,
      c) zasadą adekwatności (minimalizacji danych) – dane osobowe powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,
      d) zasadą merytorycznej poprawności (prawidłowości danych) – dane osobowe powinny być merytorycznie poprawne, a ich zakres i rodzaj adekwatny do celu, w jakim są przetwarzane, oraz w razie potrzeby uaktualniane. Dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania powinny zaś zostać niezwłocznie usunięte lub sprostowane,
      e) zasadą ograniczenia czasowego (ograniczenia przechowywania) – dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Właściciel zbioru po osiągnięciu celów przetwarzania danych powinien usunąć te dane albo je zanonimizować,
      f) zasadą zabezpieczenia danych (integralności i poufności danych) – dane osobowe powinny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych,

      Zasady, o których mowa w pkt 1 lit. a – f powinny być spełnione łącznie, a Właściciel zbioru jest odpowiedzialny za ich przestrzeganie. Mając na względzie „zasadę rozliczalności", o której mowa w ust. 2 art. 5 RODO, Właściciel zbioru powinien być w stanie wykazać ich przestrzeganie;
   2) prowadzenie w formie papierowej lub w formie elektronicznej rejestru czynności przetwarzania danych osobowych, którego jest właścicielem, zawierającego:
      a) nazwę oraz dane kontaktowe Administratora danych oraz wszelkich współadministratorów, a także Inspektora Ochrony Danych,
      b) cele przetwarzania,
      c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
      d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
      e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
      f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
      g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa adekwatnych do rodzaju danych, okoliczności ich przetwarzania oraz ryzyka naruszeń ochrony danych;
   3) zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane i/lub udostępniane;
   4) nadawanie upoważnień do przetwarzania danych osobowych;
   5) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
   6) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną w oparciu o szacowanie ryzyka;
   7) nadzorowanie systemów teleinformatycznych służących do przetwarzania powierzonych zbiorów danych osobowych za pośrednictwem Administratora Systemu;
   8) terminowe przekazywanie dyrektorowi komórki ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych – informacji i wyjaśnień niezbędnych do wykonywania wyznaczonych im zadań;
   9) zapewnienie warunków i pomocy osobom dokonującym kontroli, o której mowa w § 22 ust. 1;

10) przed przystąpieniem do przetwarzania danych dokonanie analizy ryzyka, a w przypadku stwierdzenia występowania wysokiego ryzyka, przeprowadzenie oceny skutków dla ochrony danych, przy uwzględnieniu charakteru, zakresu, kontekstu i celu przetwarzania oraz źródła ryzyka;
11) obsługę wniosków osób, których dane dotyczą związanych z realizacją ich praw, w zakresie przetwarzania ich danych osobowych;
12) prowadzenie rejestru wniosków osób, których dane dotyczą, związanych z realizacją ich praw w zakresie przetwarzania ich danych osobowych.

3. W przypadku, gdy Właściciel zbioru występuje w roli podmiotu przetwarzającego zobowiązany jest do prowadzenia w formie papierowej lub w formie elektronicznej rejestru kategorii czynności przetwarzania danych osobowych, którego jest właścicielem, zawierającego:
   1) nazwę oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora oraz Inspektora Ochrony Danych,
   2) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,
   3) gdy ma to zastosowanie - przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
   4) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa adekwatnych do rodzaju danych, okoliczności ich przetwarzania oraz ryzyka naruszeń ochrony danych.

§ 6.

Administrator Systemu jest odpowiedzialny za utrzymanie i bezpieczeństwo systemów teleinformatycznych służących do przetwarzania danych osobowych.

§ 7.

1. Dyrektor oddziału regionalnego ponosi odpowiedzialność za stosowanie w oddziale regionalnym i podległych biurach powiatowych obowiązujących środków technicznych i organizacyjnych, niezbędnych do zapewnienia odpowiedniej ochrony danych osobowych, oraz przetwarzanie tych danych na zasadach określonych w § 5 ust. 2 pkt 1.
2. Obowiązki Właściciela zasobu i przypisana mu odpowiedzialność, ustanowione w Polityce bezpieczeństwa informacji w ARiMR stosuje się odpowiednio do dyrektora oddziału regionalnego administrującego w oddziale regionalnym zbiorami danych osobowych.
3. Dyrektor oddziału regionalnego jest zobowiązany w szczególności do:
   1) nadawania upoważnień do przetwarzania danych osobowych i prowadzenia ewidencji osób upoważnionych;
   2) rozpatrywania wniosków o udostępnienie danych;
   3) zawierania umów powierzenia przetwarzania danych realizowanych w oddziale regionalnym;
   4) terminowego przekazywania dyrektorowi komórki właściwej ds. bezpieczeństwa informacji oraz Inspektorowi Ochrony Danych - informacji i wyjaśnień niezbędnych do wykonywania wyznaczonych im zadań;
   5) zapewnienia warunków i pomocy osobom dokonującym audytu w oddziale regionalnym i podległych biurach powiatowych;
   6) obsługi wniosków osób, których dane dotyczą związanych z realizacją ich praw w zakresie przetwarzania ich danych osobowych.

§ 8.

Do obowiązków Inspektora Bezpieczeństwa Informacji w OR należy w szczególności:
1) rozpatrywanie wniosków o udostępnienie danych osobowych;
2) dokonywanie wpisów w ewidencji udostępnień danych osobowych w systemie teleinformatycznym;
3) przechowywanie i aktualizacja wykazu umów powierzenia przetwarzania danych osobowych;
4) przechowywanie aktualnego wykazu osób wyznaczonych do rozpatrywania wniosków o udostępnianie danych osobowych w biurach powiatowych oraz dokumentacji szkoleń przeprowadzonych dla tych osób zawierającej m.in. prezentację na szkolenie i listy obecności uczestników;
5) przechowywanie dokumentacji szkoleń, o których mowa w § 15 ust. 4 przeprowadzonych dla kierowników biur powiatowych, zawierającej m.in. prezentację na szkolenie i listy obecności uczestników.

§ 9.

1. Dyrektor komórki ds. bezpieczeństwa nadzoruje przestrzeganie w Agencji polityki ochrony danych osobowych, w tym stosowanie środków technicznych i organizacyjnych zapewniających ochronę danych osobowych.
2. Nadzorowanie przestrzegania polityki ochrony danych osobowych następuje m.in. przez wykonywanie czynności audytowych, wydawanie wiążących poleceń Właścicielom zbiorów, dyrektorom oddziałów regionalnych i innym osobom odpowiedzialnym za ochronę i zgodne z prawem przetwarzanie danych osobowych w Agencji oraz poprzez sporządzanie pisemnych wystąpień w tym zakresie.

3. Wyznaczone zadania w zakresie nadzoru nad przestrzeganiem polityki ochrony danych osobowych w Agencji wykonują Inspektorzy Bezpieczeństwa Informacji z Centrali. Inspektorzy Bezpieczeństwa Informacji z Centrali wykonują zadania m.in. w zakresie:
   1) opiniowania, pod względem zgodności z przepisami o ochronie danych osobowych oraz polityką ochrony danych osobowych, umów (w tym umów powierzenia przewarzania danych), porozumień, dokumentów wewnętrznych oraz aktów prawnych wewnętrznych i zewnętrznych;
   2) opiniowania nowych projektów pod kątem zgodności z zasadami ochrony w fazie projektowania oraz domyślnej ochrony danych (Privacy by design, Privacy by default);
   3) audytowania sposobu przetwarzania danych osobowych w Agencji;
   4) audytowania sposobu przestrzegania obowiązujących standardów ochrony danych osobowych w odniesieniu do zastosowanych środków technicznych i organizacyjnych w Agencji;
   5) prowadzenia szkoleń dotyczących przestrzegania polityki ochrony danych osobowych w Agencji.
4. Bieżący nadzór nad przestrzeganiem polityki ochrony danych osobowych w oddziale regionalnym i podległych biurach powiatowych wykonuje dyrektor oddziału regionalnego za pośrednictwem Inspektorów Bezpieczeństwa Informacji w oddziale regionalnym. Inspektorzy Bezpieczeństwa Informacji w oddziale regionalnym wykonują m.in. zadania w zakresie:
   1) prowadzenia przeglądów w zakresie przetwarzania danych osobowych w oddziale regionalnym i biurach powiatowych;
   2) prowadzenia przeglądów w zakresie przestrzegania w oddziale regionalnym i biurach powiatowych obowiązujących standardów ochrony danych osobowych w odniesieniu do zastosowanych środków technicznych i organizacyjnych w Agencji;
   3) prowadzenia szkoleń dotyczących przestrzegania polityki ochrony danych osobowych w oddziale regionalnym i biurach powiatowych;
   4) opiniowanie nowych projektów pod kątem zgodności z zasadami ochrony w fazie projektowania oraz domyślnej ochrony danych (Privacy by design, Privacy by default).
5. Dyrektor komórki ds. bezpieczeństwa może wyznaczać dyrektorowi oddziału regionalnego zadania i żądać wyjaśnień w tym zakresie, wydawać polecenia, a także żądać informacji i opinii dotyczących przestrzegania polityki ochrony danych osobowych.
6. Upoważnienie do realizacji czynności audytowych/przeglądów Inspektorom Bezpieczeństwa Informacji w Centrali/oddziale regionalnym wydaje odpowiednio:
   1) Prezes ARiMR;
   2) dyrektor oddziału regionalnego.

Rozdział 4

Prowadzenie dokumentacji w zakresie bezpieczeństwa danych osobowych i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

§ 10.

1. Obszar przetwarzania danych osobowych w Agencji stanowi wykaz adresów obiektów:
   1) w których są przetwarzane dane osobowe przez Agencję;
   2) stanowiących lokalizację Równoległego Ośrodka Przetwarzania Danych;
   3) stanowiących lokalizację Centrum Przetwarzania Danych.
2. Wykaz adresów obiektów stanowiących obszar przetwarzania danych osobowych na druku stanowiącym załącznik nr 1 do niniejszego regulaminu, w terminie do dnia 31 grudnia każdego roku kalendarzowego, dostarcza dyrektorowi komórki ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych:
   1) Administrator Zabezpieczeń Fizycznych w Centrali Agencji – w odniesieniu do obiektów (budynków) Centrali, oddziałów regionalnych i biur powiatowych,
   2) Administrator Systemu - w odniesieniu do Centrum Przetwarzania Danych i Równoległego Ośrodka Przetwarzania Danych.
3. Osoby wymienione w ust. 2 pkt 1 i 2 informują dyrektora komórki ds. bezpieczeństwa oraz Inspektora Ochrony Danych o wszelkich zmianach dotyczących lokalizacji obszarów przetwarzania w terminie 7 dni od wystąpienia zmiany.
4. Administrator Systemu sporządza:
   1) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
   2) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, który może być sporządzony w wersji elektronicznej;
   3) informację o sposobie przepływu danych pomiędzy poszczególnymi systemami;

4) opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

5. Środki techniczne i organizacyjne dobierane są adekwatnie do rodzaju danych, okoliczności ich przetwarzania oraz ryzyka naruszeń ochrony.
6. Administrator Systemu aktualizuje informacje, o których mowa w ust. 4 pkt 1 – 4 w terminie 7 dni od wystąpienia zmian i przesyła aktualne wersje dyrektorowi komórki ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych.

§ 11.

1. Dokument „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych", zawiera opis sposobu realizacji wymogów dotyczących ochrony danych osobowych.
2. Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz regulaminy z nią powiązane i procedury w niej wskazane opracowuje i aktualizuje Administrator Systemu.
3. Administrator Systemu w terminie 7 dni od wystąpienia zmiany, przesyła dyrektorowi komórki właściwej ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych aktualną wersję Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
4. Administrator Systemu zapewnia domyślną ochronę systemów teleinformatycznych służących do przetwarzania danych osobowych.
5. Właściciel zbioru nadzoruje Administratora Systemu w zakresie zapewnienia wymaganych funkcjonalności dla systemów teleinformatycznych służących do przetwarzania zbiorów danych osobowych.
6. Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych określa regulamin zarządzania incydentami bezpieczeństwa informacji.

Rozdział 5

Tworzenie i usuwanie zbiorów danych osobowych

§ 12.

1. Właściciel zbioru zobowiązany jest zawiadomić dyrektora komórki ds. bezpieczeństwa oraz Inspektora Ochrony Danych o utworzeniu nowego zbioru nie później niż w terminie 7 dni od rozpoczęcia tworzenia zbioru.
2. Zawiadomienie następuje przez przesłanie informacji w zakresie:
   1) nazwy zbioru danych osobowych;
   2) podstawy prawnej przetwarzania;
   3) celu przetwarzania;
   4) opisu kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   5) kategorii odbiorców, którym dane osobowe zostaną ujawnione, w tym odbiorców państw trzecich lub w organizacjach międzynarodowych;
   6) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
   7) planowanych terminów usunięcia poszczególnych kategorii danych;
   8) ogólnego opisu technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO uwzględniających ryzyko przetwarzania danych w zgłaszanym zbiorze.
3. Na wniosek Właściciela zbioru, w przypadku tworzenia nowego zbioru Administrator Systemu określa warunki techniczne dotyczące zabezpieczeń zbioru w systemie teleinformatycznym.
4. Właściciel zbioru jest zobowiązany zawiadomić dyrektora komórki ds. bezpieczeństwa oraz Inspektora Ochrony Danych o wszelkich zmianach dotyczących przetwarzania danych osobowych w zbiorze nie później niż w terminie 14 dni od ich wystąpienia.
5. Administrator Systemu jest zobowiązany zgłosić Właścicielowi zbioru wszelkie zmiany dotyczące sposobu przetwarzania danych osobowych oraz ich zabezpieczenia w systemie teleinformatycznym w ciągu 7 dni od daty zaistnienia tych zmian.

§ 13.

1. W przypadku zaprzestania przetwarzania danych w zbiorze Właściciel Zbioru jest zobowiązany niezwłocznie poinformować dyrektora komórki ds. bezpieczeństwa oraz Inspektora Ochrony Danych o tym fakcie. Informacja, o której mowa w zdaniu pierwszym powinna zawierać uzasadnienie.
2. Właściciel zbioru decyduje o trwałym usunięciu zbioru danych osobowych. O tym fakcie informuje dyrektora komórki ds. bezpieczeństwa oraz Inspektora Ochrony Danych. W razie wątpliwości, przed usunięciem zbioru danych osobowych Właściciel zbioru zasięga opinii Inspektora Ochrony Danych.
3. Właściciel zbioru podejmuje działania w celu usunięcia zbioru danych osobowych ze wszystkich nośników.
4. Zbiory danych osobowych są likwidowane komisyjnie.
5. W skład komisji powołanej przez Administratora danych wchodzą:

1) Administrator Systemu, jeżeli zbiór jest przetwarzany w systemie informatycznym;
2) dwie osoby reprezentujące Właściciela zbioru.

6. Właściciel Zbioru przekazuje dyrektorowi komórki ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych kopię protokołu komisyjnie zlikwidowanego zbioru.

Rozdział 6

Nadawanie, zmiana i odbieranie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych

§ 14.

1. Przetwarzanie danych osobowych w Agencji wymaga uzyskania upoważnienia do przetwarzania danych osobowych.
2. Upoważnienie nadaje się przed dopuszczeniem osoby do przetwarzania danych osobowych.

§ 15.

1. Upoważnienie do przetwarzania danych osobowych poza zbiorami (upoważnienie ogólne) może być nadane:
   1) osobom przyjmowanym do pracy, bez względu na podstawę prawną zatrudnienia, po odbyciu szkolenia podstawowego;
   2) innym osobom, jeżeli przepisy tak stanowią lub jeżeli zachodzi uzasadniona potrzeba nadania upoważnienia.
2. Dyrektor komórki właściwej ds. kadrowych w Centrali/wyznaczona osoba z komórki właściwej ds. kadrowych w oddziale regionalnym/kierownik biura powiatowego w przypadku, o którym mowa w ust. 4, zapoznają osoby przyjmowane do pracy z aktami prawnymi zawierającymi przepisy o ochronie danych osobowych.
3. Inspektor Ochrony Danych publikuje na stronie internetowej Agencji w zakładce Ochrona Danych Osobowych wykaz aktów prawnych zawierających przepisy o ochronie danych osobowych.
4. Dyrektor komórki właściwej ds. kadrowych w Centrali/wyznaczona osoba z komórki właściwej ds. kadrowych w oddziale regionalnym kierują osoby przyjmowane do pracy na szkolenie podstawowe z zakresu ochrony danych osobowych i w razie potrzeby na szkolenie w zakresie przetwarzania szczególnych kategorii danych. Szkolenie prowadzi Inspektor Bezpieczeństwa Informacji odpowiedni dla jednostki organizacyjnej ARiMR, po uprzednim uzgodnieniu terminu szkolenia. W wyjątkowych przypadkach szkolenie dla stażystów, praktykantów i wolontariuszy może przeprowadzić, uprzednio przeszkolony przez Inspektora Bezpieczeństwa Informacji w OR, kierownik biura powiatowego, do którego osoby te zostały skierowane do pracy. Prezentację przeznaczoną na potrzeby szkolenia podstawowego dla kierownika BP przygotowuje Inspektor Bezpieczeństwa Informacji w OR.
5. Szkoleniu, o którym mowa w ust. 4, podlegają również:
   1) osoby zatrudnione, a niewykonujące pracy w Agencji przez okres co najmniej 12 miesięcy;
   2) osoby, które w wyniku awansu obejmują stanowisko kierownika komórki organizacyjnej albo kierownika jednostki organizacyjnej lub jego zastępcy.
6. Fakt przeprowadzenia szkolenia jest dokumentowany przez sporządzenie listy obecności uczestników. Listę obecności sporządza się na druku stanowiącym załącznik nr 3 do Regulaminu bezpieczeństwa informacji w zarządzaniu zasobami ludzkimi (załącznik nr 10 do Polityki).
7. Dyrektor komórki właściwej ds. bezpieczeństwa zawiadamia dyrektora komórki właściwej ds. kadrowych w Centrali oraz odpowiednio Inspektora Bezpieczeństwa Informacji w OR - komórkę właściwą ds. kadrowych w oddziale regionalnym, o osobach uczestniczących w szkoleniu podstawowym w zakresie bezpieczeństwa informacji. Zawiadomienie następuje przez doręczenie listy obecności uczestników. Osoby, które nie odbyły szkolenia podstawowego nie mogą zostać dopuszczone do pracy związanej z przetwarzaniem danych osobowych.
8. Osoba przeszkolona potwierdza uczestnictwo w szkoleniu, zapoznanie się z przepisami o ochronie danych osobowych i zobowiązuje się do zachowania w poufności przetwarzanych danych i innych informacji prawnie chronionych oraz zastosowanych w Agencji środków ochrony.
9. Treść oświadczenia zamieszczona jest na druku stanowiącym załącznik nr 2 do niniejszego regulaminu. Dokument po wypełnieniu dołącza się do akt osobowych lub podobnych akt prowadzonych dla osób wykonujących pracę w Agencji na innej podstawie niż stosunek pracy.
10. Kopie list obecności uczestników szkoleń podstawowych przeprowadzanych przez kierowników biur powiatowych oraz oryginały dokumentów zawierających oświadczenie przesyłane są do Inspektora Bezpieczeństwa Informacji w OR. Kopie list obecności z BP przechowywane są przez Inspektora Bezpieczeństwa Informacji w OR i składają się na prowadzoną przez niego ewidencję szkoleń. Oryginały dokumentów zawierających oświadczenie otrzymane z BP są niezwłocznie przekazywane do komórki właściwej ds. kadrowych w OR. Kierownik biura powiatowego wysyła wymienione dokumenty najpóźniej w dniu roboczym następującym po dniu jego sporządzenia.
11. Upoważnienie do przetwarzania danych osobowych w Centrali, osobom wskazanym w ust. 1 nadaje dyrektor komórki właściwej ds. kadrowych oraz odpowiednio w oddziale regionalnym i biurach powiatowych - dyrektor oddziału regionalnego, wypełniając druk stanowiący załącznik nr 2 do niniejszego regulaminu. Dyrektorom wszystkich komórek organizacyjnych w Centrali oraz dyrektorom oddziałów regionalnych i zastępcom dyrektora upoważnienie nadaje

Prezes Agencji lub osoba przez niego upoważniona. Upoważnienie przechowuje się w aktach osobowych lub aktach prowadzonych dla osób zatrudnionych na podstawie innej formy zatrudnienia niż umowa o pracę.

12. W szczególnie uzasadnionych przypadkach, dyrektor komórki właściwej ds. kadrowych w Centrali/dyrektor oddziału regionalnego mogą nadać upoważnienie osobom wskazanym w ust. 1 pkt 2 bez ich przeszkolenia, równocześnie wskazując obowiązek odbycia ww. szkolenia w terminie nie przekraczającym jednego miesiąca od nadania upoważnienia.
13. Dyrektor komórki właściwej ds. kadrowych oraz dyrektor oddziału regionalnego w komórce właściwej ds. kadrowych prowadzą w formie elektronicznej, z zachowaniem chronologii, wykaz osób, którym nadano upoważnienia, wg wzoru stanowiącego
załącznik nr 3 do niniejszego regulaminu. Wykaz składa się na ewidencję osób upoważnionych.
14. Upoważnienie do przetwarzania danych osobowych, bez obowiązku uczestniczenia w szkoleniu podstawowym z zakresu ochrony danych osobowych, z dniem zatrudnienia nabywają:
    1) Prezes ARiMR;
    2) Zastępcy Prezesa.
15. Osoby, o których mowa w ust. 14, podpisują oświadczenie na druku upoważnienia, którego wzór stanowi załącznik nr 2 do niniejszego regulaminu, przekazanym przez dyrektora komórki właściwej ds. kadrowych, w którym zobowiązują się do zachowania w tajemnicy/poufności przetwarzanych danych oraz zastosowanych w Agencji środków ochrony.
16. Oświadczenie, o którym mowa w ust. 15 przechowywane jest w ich aktach osobowych.

§ 16.

1. Upoważnienie do przetwarzania danych w zbiorach (upoważnienie szczególne) może być nadane:
    1) osobom zatrudnionym (wykonującym pracę) w Agencji bez względu na podstawę prawną zatrudnienia, jeżeli uzyskały one upoważnienie do przetwarzania danych osobowych poza zbiorami (upoważnienie ogólne);
    2) innym osobom, jeżeli przepisy tak stanowią lub jeżeli zachodzi uzasadniona potrzeba nadania upoważnienia; osobom tym można nadać upoważnienie bez obowiązku uprzedniego uzyskania upoważnienia ogólnego.
2. Upoważnienie do przetwarzania danych w zbiorach przetwarzanych w systemie informatycznym jest nadawane w wyniku zaakceptowania przez Właściciela zbioru wniosku o nadanie uprawnień do pracy w systemie. Druk wniosku określono w Książce procedur KP-611-101-ARiMR „Obsługa kont użytkowników systemów informatycznych ARiMR".
3. Wobec zbiorów przetwarzanych w systemie informatycznym w Centrali Agencji, z wnioskiem o nadanie uprawnień do pracy w systemie występują osoby określone w KP-611-101-ARiMR.
4. Wniosek o nadanie uprawnień do pracy w systemie jest zatwierdzany przez wszystkich Właścicieli zbiorów, do których zbiorów danych osobowych będzie miała dostęp osoba, której zostaną nadane uprawnienia, z zastrzeżeniem ust. 7.
5. Wniosek o nadanie uprawnień po uprzednim zatwierdzeniu przez Właściciela(i) zbioru(ów), realizuje Administrator Systemu.
6. Zbiór wszystkich zrealizowanych wniosków o nadanie uprawnień do pracy w systemie informatycznym, przechowywany przez Administratora Systemu, jest częścią ewidencji osób upoważnionych.
7. Wobec zbiorów przetwarzanych w systemie informatycznym w oddziałach regionalnych i biurach powiatowych Agencji wniosek o nadanie uprawnień do pracy w systemie, w mieniu Właścicieli zbiorów, zatwierdza dyrektor oddziału regionalnego.
8. Wniosek o nadanie uprawnień zatwierdzony przez dyrektora oddziału regionalnego lub osobę przez niego upoważnioną jest przechowywany w oddziale regionalnym w dokumentacji pracowniczej osoby uprawnionej.
9. Zbiór wszystkich wniosków zrealizowanych w oddziale regionalnym o nadanie uprawnień do pracy w systemie, przechowywany w oddziale regionalnym, jest częścią ewidencji osób upoważnionych.
10. Upoważnienie do przetwarzania danych osobowych w zbiorach przetwarzanych wyłącznie w formie papierowej nadają:
    1) w Centrali Agencji – Właściciel zbioru;
    2) w oddziale regionalnym i biurze powiatowym – dyrektor oddziału regionalnego.
11. Upoważnienie, o którym mowa w ust. 10 nadawane jest poprzez zatwierdzenie wniosku sporządzonego na druku stanowiącym załącznik nr 4 do niniejszego Regulaminu.
12. Do sporządzania wniosku, o którym mowa w ust. 10, stosuje się odpowiednio zasady kompetencyjne obowiązujące przy sporządzaniu wniosku o nadanie uprawnień do przetwarzania danych w systemie informatycznym.
13. Zatwierdzone wnioski o nadanie upoważnienia do przetwarzania danych w zbiorach przetwarzanych wyłącznie w formie papierowej są przechowywane odpowiednio przez Właścicieli zbiorów w Centrali Agencji i przez dyrektorów oddziałów regionalnych. Są one częścią ewidencji osób upoważnionych.

§ 17.

1. Zmiany upoważnienia do przetwarzania danych osobowych dokonują osoby uprawnione do jego nadawania.

2. Utrata upoważnienia do przetwarzania danych osobowych w zbiorach następuje w wyniku jego odebrania przez osobę uprawnioną. Dokument dotyczący odebrania uprawnienia przechowuje się u właściciela zasobu i w dokumentacji pracowniczej
osoby.
3. Ważność upoważnienia ogólnego wygasa z chwilą zakończenia zatrudnienia.
4. Osobę uprawnioną mogą wskazywać przepisy niniejszego regulaminu lub innych regulaminów ustanowionych w ramach SZBI, a w szczególności Regulaminu bezpieczeństwa w zarządzaniu zasobami ludzkimi.

Rozdział 7
Ewidencja osób upoważnionych do przetwarzania danych osobowych
§ 18.

1. W Agencji prowadzi się ewidencję osób upoważnionych do przetwarzania danych osobowych.
2. Ewidencja osób upoważnionych do przetwarzania danych osobowych w Agencji zawiera łącznie:
   1) zbiór osób, które uzyskały upoważnienia do przetwarzania danych osobowych, do którego należą:
      a) osoby, których wykaz jest prowadzony w formie elektronicznej przez dyrektora komórki właściwej ds. kadrowych w Centrali oraz dyrektorów oddziałów regionalnych,
      b) Prezes i Zastępcy Prezesa;
   2) zbiór osób, które uzyskały upoważnienia do przetwarzania danych w zbiorach:
      a) przetwarzanych w systemie informatycznym,
      b) przetwarzanych wyłącznie w formie papierowej;
   3) zbiór osób, które uzyskały upoważnienia do przetwarzania danych w Agencji na mocy przepisów wcześniej obowiązujących.
3. Administrator Systemu prowadzi ewidencję identyfikatorów użytkowników systemu informatycznego, w którym są przetwarzane dane osobowe.

Rozdział 8
Realizacja praw osób, których dane dotyczą
§ 19.

1. Każdej osobie przysługuje prawo dostępu do danych osobowych, które jej dotyczą oraz do wydania kopii danych, sprostowania danych, usunięcia danych („prawo do bycia zapomnianym"), ograniczenia przetwarzania, przeniesienia danych oraz prawo do sprzeciwu, zgodnie z art. 15-21 RODO.
2. Wniosek o realizację praw osób, których dane dotyczą może być złożony w formie: pisemnej, elektronicznej (zawierającej podpis elektroniczny lub potwierdzony profil zaufany) lub osobiście. Wniosek nie może zostać odrzucony z tego względu, że został on złożony w piśmie dotyczącym innej sprawy.
3. Szczegółowe zasady w zakresie realizacji praw osób, których dane dotyczą oraz tryb postępowania z wnioskami tych osób określają „Wytyczne dotyczące realizacji praw osób, których dane dotyczą", opracowane i udostępniane, a w razie konieczności aktualizowane przez Inspektora Ochrony Danych w sieci wewnętrznej na stronie intranetowej Agencji.
4. Wniosek osoby, której dane dotyczą, w sprawach właściwych dla Centrali rozpatruje Właściciel zbioru. Wniosek w sprawach właściwych dla oddziału regionalnego lub biura powiatowego rozpatruje dyrektor oddziału regionalnego.
5. Inspektor Ochrony Danych udziela, w razie uzasadnionej potrzeby, niezbędnego wsparcia Właścicielowi zbioru/dyrektorowi oddziału regionalnego przy rozpatrywaniu wniosków w zakresie realizacji praw osób, których dane dotyczą.
6. Wniosek osoby, której dane dotyczą Właściciel zbioru/dyrektor oddziału regionalnego powinien rozpatrzyć bez zbędnej zwłoki, jednak w terminie nie dłuższym niż jeden miesiąc od otrzymania żądania w przedmiotowym zakresie.
7. W przypadku zamiaru przesłania odpowiedzi drogą pocztową, Właściciel zbioru/dyrektor oddziału regionalnego zapewnia, aby odpowiedź została wysłana nie później niż w terminie 3 dni roboczych przed upływem jednego miesiąca od daty otrzymania wniosku.
8. W razie potrzeby termin, o którym mowa w ust. 7, może zostać przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W takim przypadku, w terminie miesiąca od otrzymania żądania Właściciel zbioru/dyrektor oddziału regionalnego powinien poinformować osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.
9. Właściciel zbioru/dyrektor oddziału regionalnego może odmówić podjęcia działań w związku ze złożonym wnioskiem osoby, której dane dotyczą w przypadku, gdy:
   1) wniosek jest ewidentnie nieuzasadniony;
   2) żądania osoby, której dane dotyczą są nadmierne, w szczególności, gdy ich zgłaszanie ma charakter ustawiczny.

10. O odmowie podjęcia działań, z uwagi na okoliczności, o których mowa w ust. 9 Właściciel zbioru/dyrektor oddziału regionalnego informuje osobę, której dane dotyczą w terminie miesiąca od otrzymania wniosku. Informacja udzielana jest zgodnie z wzorem formularza wniosku, określonym w załączniku do instrukcji, o której mowa w ust. 3.

Rozdział 9
Udostępnianie danych osobowych
§ 20.

1. Dane osobowe udostępniane są na wniosek.
2. Wniosek o udostępnienie danych osobowych, który wpłynął do biura powiatowego lub oddziału regionalnego załatwia dyrektor oddziału regionalnego.
3. Wniosek o udostępnienie danych osobowych, który z przyczyn formalnych lub merytorycznych nie może zostać załatwiony przez dyrektora oddziału regionalnego, załatwia Właściciel zbioru.
4. Wnioski o udostępnienie danych osobowych załatwiane przez dyrektora oddziału regionalnego rozpatruje Inspektor Bezpieczeństwa Informacji w OR. W tym celu m.in.:
   1) dokonuje oceny wniosków pod względem formalnym i merytorycznym;
   2) przygotowuje projekty pism w sprawie usunięcia nieprawidłowości, uzupełnienia wniosków, udzielenia niezbędnych wyjaśnień oraz projekty odpowiedzi na wnioski, które przedkłada do podpisu dyrektorowi oddziału regionalnego;
   3) występuje do komórek organizacyjnych oddziału regionalnego lub biura powiatowego o przekazanie informacji merytorycznej niezbędnej do przygotowania odpowiedzi na wnioski; za terminowość i integralność przekazanej informacji odpowiedzialność ponosi kierownik biura powiatowego lub kierownik komórki organizacyjnej oddziału regionalnego przekazujący informację.
5. Osoba zatrudniona na stanowisku Radcy prawnego w oddziale regionalnym opiniuje projekt pisma w sprawie usunięcia nieprawidłowości, uzupełnienia wniosku lub udzielenia niezbędnych wyjaśnień oraz projekt odpowiedzi na wniosek, jeżeli taki projekt zostanie mu przedstawiony do zaopiniowania przez Inspektora Bezpieczeństwa Informacji w OR; akceptując projekt pisma, osoba zatrudniona na stanowisku Radcy prawnego w oddziale regionalnym składa na nim czytelny podpis.
6. Wniosek o udostępnienie danych osobowych z Systemu Identyfikacji i Rejestracji Zwierząt, od osoby zatrudnionej w Inspekcji Weterynaryjnej, który wpłynął do biura powiatowego załatwia kierownik biura powiatowego.
7. Kierownik biura powiatowego zgłasza do dyrektora oddziału regionalnego wykaz osób wyznaczonych do rozpatrywania wniosków o udostępnienie danych i odpowiada za jego aktualizację. Osoby te podlegają co najmniej raz w roku szkoleniom doskonalącym prowadzonym przez Inspektorów Bezpieczeństwa Informacji z OR.
8. Wniosek o udostępnienie danych osobowych załatwiany w biurze powiatowym, którego sposób rozpatrzenia budzi uzasadnione wątpliwości, może zostać przesłany do oddziału regionalnego w celu uzyskania opinii Inspektora Bezpieczeństwa Informacji w OR. Do kopii wniosku dołącza się informacje niezbędne do jego rozpatrzenia oraz stanowisko kierownika BP.
9. Wniosek, który wpłynął do Centrali Agencji załatwia Właściciel zbioru. Wniosek organu egzekucyjnego może zostać przekazany przez Właściciela zbioru do załatwienia dyrektorowi oddziału regionalnego.
10. Właściciel zbioru jest obowiązany wyznaczyć co najmniej dwie osoby do rozpatrywania wniosków o udostępnienie danych (osoby wyznaczone), o których informuje dyrektora komórki właściwej ds. bezpieczeństwa oraz Inspektora Ochrony Danych. Tylko osoby wyznaczone rozpatrują wnioski o udostępnienie danych osobowych, które załatwia Właściciel zbioru.
11. Dyrektor komórki właściwej ds. bezpieczeństwa prowadzi wykaz osób wyznaczonych, które podlegają okresowemu szkoleniu. Za przekazywanie informacji niezbędnych do prowadzenia aktualnego wykazu odpowiadają Właściciele zbiorów.
12. Wniosek o udostępnienie danych osobowych, którego sposób rozpatrzenia budzi uzasadnione wątpliwości, może zostać przesłany wraz z informacjami niezbędnymi dla jego rozpatrzenia, do Inspektora Ochrony Danych w celu zajęcia stanowiska w sprawie. Do wniosku dołącza się projekt odpowiedzi. Projekt odpowiedzi przesłany z oddziału regionalnego wymaga podpisu osoby zatrudnionej na stanowisku radcy prawnego.
13. Dane osobowe udostępnia się na wniosek sporządzony w formie pisemnej, spełniający wymagania formalne, określone w przepisach prawa. Szczegółowe zasady postępowania przy rozpatrywaniu wniosków o udostępnienie danych osobowych określają „Wytyczne dotyczące rozpatrywania wniosków o udostępnienie danych osobowych". Obowiązujące Wytyczne są opracowywane i udostępniane, a w razie konieczności aktualizowane przez Inspektora Ochrony Danych w sieci wewnętrznej na stronie intranetowej Agencji.
14. Informacje zawierające dane osobowe są udostępniane uprawnionym podmiotom:
   1) w formie pisemnego wydruku, listem poleconym lub za potwierdzeniem osobistego odbioru;

2) za pomocą elektronicznej skrzynki podawczej e-PUAP – z użyciem podpisu kwalifikowanego lub potwierdzonego profilem zaufanym;
3) w drodze teletransmisji danych (w sposób gwarantujący poufność przesyłanych danych);
4) na elektronicznych nośnikach informacji, za potwierdzeniem odbioru;
5) w inny sposób określony przepisami prawa lub umową.

15. Podstawową formą przekazywania danych osobowych jest metoda określona w ust. 14 pkt 1.
16. W szczególnie uzasadnionych przypadkach stosuje się metody określone w ust. 14 pkt 2 – 5. Uzasadnienie takiego przypadku, sporządzone na piśmie, dołącza się do akt sprawy.
17. Zawartość elektronicznych nośników informacji podlega kontroli i pisemnej akceptacji bezpośredniego przełożonego - osoby przygotowującej informację określoną w ust. 14.
18. Jeżeli tryb udostępniania danych osobowych określa umowa, przepisów niniejszego rozdziału nie stosuje się w zakresie postanowień umowy.
19. Ewidencja przypadków udostępnienia danych prowadzona jest w wyznaczonym systemie informatycznym. Ewidencję prowadzą:
    1) w Centrali Agencji – Właściciel zbioru;
    2) w oddziale regionalnym – dyrektor;
    3) w biurze powiatowym – kierownik.

Rozdział 10
Powierzanie przetwarzania danych osobowych innym podmiotom
§ 21.

1. Powierzenie przetwarzania danych nie wyłącza, ani nie ogranicza odpowiedzialności Właściciela zbioru/dyrektora oddziału regionalnego za zgodne z prawem przetwarzanie tych danych.
2. Powierzenie przetwarzania danych osobowych odbywa się na podstawie umowy zawartej zgodnie z RODO.
3. Przed przekazaniem danych osobowych w ramach wykonania umowy powierzenia danych Właściciel zbioru/dyrektor oddziału regionalnego dokonuje weryfikacji czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odbywało się zgodnie z RODO i chroniło prawa osób, których dane dotyczą. Ocena spełnienia przez podmiot przetwarzający wymogów, o których mowa powyżej przeprowadzana jest za pomocą ankiety. Formularz ankiety jest opracowywany, aktualizowany i udostępniany przez dyrektora komórki właściwej ds. bezpieczeństwa w sieci wewnętrznej na stronie intranetowej Agencji, przy czym wymagana jest uprzednia akceptacja w tym zakresie Inspektora Ochrony Danych.
4. Umowa powierzenia przetwarzania danych osobowych powinna zawierać elementy określone w art. 28 RODO, a zatem co najmniej:
    1) przedmiot przetwarzania (jakie dane i w jakim zakresie zostają powierzone podmiotowi przetwarzającemu);
    2) czas trwania przetwarzania;
    3) charakter i cel przetwarzania;
    4) rodzaj danych osobowych;
    5) kategorie osób, których dane dotyczą;
    6) obowiązki i prawa Administratora danych, w tym w szczególności: postanowienia określające sposób sprawowania przez Agencję kontroli należytego wykonania umowy w powyższym zakresie; postanowienia określające sposób dochodzenia roszczeń Agencji w przypadku, gdy nastąpi naruszenie ochrony danych z przyczyn leżących po stronie podmiotu, któremu powierza się ich przetwarzanie;
    7) zobowiązanie podmiotu, któremu powierza się dane osobowe do zastosowania odpowiednich środków zabezpieczających te dane, wymaganych na mocy art. 32 RODO;
    8) postanowienia dotyczące wydawania upoważnień do przetwarzania danych osobowych;
    9) zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.
5. Inspektor Ochrony Danych określa wzór umowy powierzenia przetwarzania danych osobowych obowiązujący w Agencji.
6. Ostateczny projekt umowy powierzenia przetwarzania danych osobowych, a także każdej innej umowy zawartej w Centrali Agencji, której realizacja może wiązać się z przetwarzaniem powierzonych danych osobowych Agencji, wymaga akceptacji w wyniku złożenia czytelnych podpisów przez:
    1) wszystkich Właścicieli zbiorów, których dane są powierzane;
    2) Inspektora Ochrony Danych;
    3) dyrektora komórki właściwej ds. bezpieczeństwa;
    4) Administratora Systemu.

7. Ostateczny projekt umowy powierzenia przetwarzania danych osobowych, a także każdej innej umowy zawartej w OR Agencji, której realizacja może wiązać się z przetwarzaniem powierzonych danych osobowych, wymaga akceptacji w wyniku złożenia czytelnych podpisów przez:
   1) Dyrektora OR;
   2) kierownika komórki organizacyjnej przygotowującej projekt;
   3) Inspektora Bezpieczeństwa Informacji w OR;
   4) osoby zajmującej samodzielne stanowisko radcy prawnego w OR.
8. Właściciel zbioru nadzoruje wykonywanie umów powierzenia przetwarzania danych osobowych zawartych w Centrali i wykonywanych na terenie właściwości Centrali Agencji. Dyrektor oddziału regionalnego nadzoruje wykonywanie umów powierzenia przetwarzania danych osobowych zawartych w oddziale regionalnym oraz wszystkich umów wykonywanych na terenie właściwości oddziału regionalnego chyba, że Właściciel zbioru postanowi inaczej.
9. Właściciele zbiorów i dyrektorzy oddziałów regionalnych prowadzą wykaz umów powierzenia przetwarzania danych według wzoru stanowiącego załącznik nr 6 do niniejszego regulaminu.

Rozdział 11

Postępowanie w przypadku kontroli PUODO

§ 22.

1. PUODO lub upoważnieni przez PUODO pracownicy UODO, zwani dalej „kontrolującymi", mają prawo do przeprowadzania kontroli w Agencji. Kontrolę przeprowadza się po okazaniu przez kontrolującego imiennego upoważnienia wraz z legitymacją służbową. Imienne upoważnienie do przeprowadzania kontroli powinno zawierać elementy wskazane w art. 81 ust. 2 Ustawy.
2. Czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej. Kontrolowany jest obowiązany do pisemnego wskazania osoby upoważnionej do reprezentowania go w trakcie kontroli (przedstawiciela kontrolowanej komórki lub jednostki organizacyjnej). Szczegółowe warunki i zasady przeprowadzania kontroli określa Ustawa.
3. Inspektor Ochrony Danych jest zawiadamiany bez zbędnej zwłoki o kontroli PUODO w Agencji i może być obecny podczas wykonywania przez kontrolujących czynności kontrolnych w Agencji.
4. Właściciel zbioru, Administrator Systemu, Administrator Zabezpieczeń Fizycznych, dyrektor oddziału regionalnego, kierownik biura powiatowego i inne osoby poddawane kontroli zobowiązani są do ścisłej współpracy z Inspektorem Ochrony Danych.
5. Inspektor Ochrony Danych zapewnia pod względem organizacyjnym warunki niezbędne do przeprowadzenia kontroli PUODO w Centrali Agencji.
6. Merytoryczną obsługę kontroli PUODO polegającą m.in. na udzieleniu kontrolującym niezbędnych informacji, wyjaśnień, dostępu do dokumentów i systemów teleinformatycznych w Centrali Agencji zapewniają w granicach swoich kompetencji i uprawnień:
   1) Właściciel zbioru wobec powierzonych mu zbiorów;
   2) Administrator Systemu;
   3) Administrator Zabezpieczeń Fizycznych;
   4) Inspektor Ochrony Danych;
   5) dyrektor komórki właściwej ds. bezpieczeństwa;
   6) kierownik komórki organizacyjnej, w której są przetwarzane dane osobowe;
   7) pracownicy i inne osoby wykonujące pracę na rzecz Agencji w odniesieniu do wykonywania obowiązków związanych z przetwarzaniem danych osobowych, tylko w obecności przełożonego lub osoby nadzorującej ich pracę.
7. Dyrektor oddziału regionalnego zapewnia warunki i obsługę kontroli PUODO w oddziale regionalnym.
8. Merytoryczną obsługę kontroli PUODO w oddziale regionalnym zapewniają kierownicy jednostek i komórek organizacyjnych w granicach swoich kompetencji i uprawnień. Pracownicy i inne osoby wykonujące pracę w oddziale regionalnym, związaną z przetwarzaniem danych osobowych, uczestniczą w czynnościach kontrolnych tylko w obecności przełożonego lub osoby nadzorującej ich pracę.
9. W trakcie czynności kontrolnych wykonywanych przez kontrolujących w oddziale regionalnym uczestniczy Inspektor Bezpieczeństwa Informacji z OR. Dyrektor oddziału regionalnego może wyznaczyć też inne osoby, które będą brały udział w tych czynnościach.
10. Kierownicy komórek organizacyjnych w oddziale regionalnym, kierownicy biur powiatowych i inne osoby poddawane kontroli są zobowiązane do ścisłej współpracy z Inspektorem Bezpieczeństwa Informacji w OR oraz innymi osobami wyznaczonymi przez dyrektora oddziału regionalnego.

Rozdział 12

Odpowiedzialność za naruszenie zasad ochrony danych osobowych

§ 23.

Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi i administracyjnymi określonymi w Ustawie oraz w Kodeksie karnym. Niezależnie od powyższego naruszenie zasad ochrony danych osobowych obowiązujących w Agencji może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną pracowników.

Załącznik nr 1 do Regulaminu ochrony danych osobowych.

Znak sprawy:

Wykaz obszarów przetwarzania danych osobowych w Agencji Restrukturyzacji i Modernizacji Rolnictwa na dzień
.....

Obszary przetwarzania danych osobowych stanowi strefa administracyjna i strefa bezpieczeństwa w użytkowanych budynkach.

Nazwa obiektu	Województwo	Powiat	Adres

Załącznik nr 2 do Regulaminu Ochrony Danych Osobowych

Agencja Restrukturyzacji i Modernizacji Rolnictwa
Al. Jana Pawła II 70
00-175 Warszawa
Adres do korespondencji:
ul. Poleczki 33
02-822 Warszawa
(dane administratora)

……., dnia……. r.
(miejscowość, data)

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych*) (Dz. Urz. UE L 119 z 04.05.2016 r., s. 1 oraz Dz. Urz. UE. L 127 z 23.05.2018 r., str. 2) zwanego dalej: „Rozporządzeniem", upoważniam:
Panią/Pana*……,
posiadającą/ego nr. KIP* – ……., zatrudnioną/ego w ……..* Agencji Restrukturyzacji i Modernizacji Rolnictwa, do przetwarzania i polecam przetwarzanie:

- ☐ danych osobowych zwykłych;
- ☐ danych osobowych szczególnych kategorii**

w zakresie niezbędnym do wykonywania powierzonej pracy***.

Niniejsze upoważnienie obejmuje uprawnienie do przetwarzania danych osobowych w okresie wykonywania powierzonej pracy.

Jednocześnie zobowiązuje Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami Rozporządzenia, ustawy z dnia 10.05.2018 r. *o ochronie danych osobowych* (Dz. U. z 2018 r., poz. 1000 z późn.zm.), ustawy z dnia 26.06.1974 r. *Kodeks Pracy* (Dz. U. z 2018 r. poz. 917 z późn. zm.), innymi przepisami prawa powszechnie obowiązującymi, a także z przepisami wewnątrzzakładowymi ARiMR w zakresie Polityki ochrony danych osobowych Pracodawcy.

……
(podpis osoby uprawnionej do nadania upoważnienia)

Oświadczam, że znane są mi przepisy z zakresu ochrony danych osobowych oraz zasady ochrony i przetwarzania danych osobowych obowiązujące w Agencji Restrukturyzacji i Modernizacji Rolnictwa. Zobowiązuję się do zachowania w tajemnicy/poufności danych osobowych przetwarzanych w Agencji Restrukturyzacji i Modernizacji Rolnictwa oraz sposobu ich zabezpieczenia w czasie trwania zatrudnienia oraz po zaprzestaniu wykonywania pracy, a także do przetwarzania danych wyłącznie w granicach upoważnienia, w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych i organizacyjnych.

……
(data i podpis osoby upoważnionej)

Pouczenie:

*- wypełnić wstawiając: imię i nazwisko, indywidualny numer pracownika nadany w systemie kadrowo-płacowym ARiMR (KIP), jednostka organizacyjna, w której wykonywana jest praca.
Dla innej osoby niż pracownik: imię i nazwisko, określenie statusu prawnego (np. wolontariusz, stażysta, praktykant, zleceniobiorca itp.) ze wskazaniem jednostki organizacyjnej ARiMR, w której wykonuje pracę.

** **należy zaznaczyć obydwa checkbox-y jedynie w przypadku, gdy zakres czynności obejmuje przetwarzanie danych osobowych zwykłych i przetwarzanie danych osobowych szczególnych kategorii, o których mowa w art. 9 Rozporządzenia, tj. ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu**

jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej. W pozostałych przypadkach należy zaznaczyć jedynie checkbox dotyczący danych osobowych zwykłych i przekreślić checkbox dotyczący danych szczególnych kategorii.

*** - wynika z zakresu obowiązków pracowniczych lub innej podstawy wykonywania pracy.

Załącznik nr 3 do Regulaminu ochrony danych osobowych

Wykaz osób upoważnionych do przetwarzania danych poza zbiorami w Centrali ARiMR/..... OR ARiMR*								
Lp.	**Imię i Nazwisko**	**Jednostka organiz.**	**Komórka organiz.****	**Data nadania upoważnienia**	**Upoważniony (a) w zakresie wykonywania *** **		**Data odbioru upoważnienia**	**Uwagi**
					obowiązków pracowniczych	**innych obowiązków**		
1	2	3	4	5	6	7	8	9

* Niepotrzebne skreślić

** Wypełniać tylko dla osób nie będących pracownikami

*** Wstawić X w odpowiedniej kolumnie

Załącznik nr 4 do Regulaminu ochrony danych osobowych

Znak sprawy:

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH
w zbiorach przetwarzanych w formie papierowej

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych*) (Dz. Urz. UE L 119 z 04.05.2016 r., s. 1 oraz Dz. Urz. UE. L 127 z 23.05.2018 r., str. 2) zwanego dalej: „Rozporządzeniem”,
upoważniam / odbieram upoważnienie*:
Panią/Pana*……..,
posiadającą/ego nr. KIP – ……..,
zatrudnioną/ego w …….. ARiMR,
(komórka organizacyjna)
do przetwarzania danych osobowych w zbiorze:
……
……
w następującym zakresie:
……
……
……

.....
*(data, pieczątka imienna i podpis Właściciela zbioru/dyrektora OR)**

* Niepotrzebne skreślić

Załącznik nr 5 do Regulaminu ochrony danych osobowych

Wykaz umów powierzenia przetwarzania danych osobowych zawartych w Centrali/..... OR* ARiMR w ..... roku						
Lp.	**Data i nr umowy na wykonanie usługi oraz opis przedmiotu umowy ****	**Data i nr Umowy powierzenia przetwarzania**	**Strona Umowy powierzenia przetwarzania**	**Komórka organizacyjna nadzorująca wykonanie Umowy**	**Właściciel zbioru lub zbiór danych podlegający powierzeniu**	**Uwagi**
1	**2**	**3**	**4**	**5**	**6**	**7**

* Wypełnić właściwe, niepotrzebne skreślić.

****** Dotyczy umowy, do której zawarto umowę powierzenia przetwarzania danych osobowych.

Załącznik nr 7 do Umowy

Klauzula informacyjna w zakresie przetwarzania danych osobowych [2]

W związku z treścią z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2)), dalej: „RODO" Zamawiający informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w związku z zawarciem Umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazany w pkt 1.
3. Dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. b RODO w celu zawarcia oraz wykonania niniejszej Umowy.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
   1) organy kontrolne,
   2) osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2019 r., poz. 1429 ze zm.),
   3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
   4) podmioty przetwarzające dane osobowe w imieniu Administratora na mocy zawartych innych umów, m. in. dostawcy IT.
5. Pani/Pana dane osobowe będą przechowywane przez okres obowiązywania Umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa. Okres przechowywania danych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora. Ponadto, okres przechowywania danych może zostać przedłużony na okres 5 lat, na potrzeby archiwizacji.
6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych w przypadkach określonych w RODO oraz prawo do przenoszenia Pani/Pana danych osobowych oraz prawo do usunięcia danych, zgodnie z art. 17 RODO.
7. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
8. Podanie przez Panią/Pana danych osobowych jest konieczne w celu określonym w pkt 3 powyżej, dla zawarcia i wykonania Umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa, a konsekwencją niepodania Pani/Pana danych osobowych będzie brak możliwości zawarcia Umowy.

[2] Niniejsza klauzula w zakresie przetwarzania danych osobowych, znajdzie zastosowanie w przypadku bezpośredniego pozyskania danych od drugiej strony umowy będącej osobą fizyczną/osobą fizyczną prowadzącą działalność gospodarczą.

Klauzula informacyjna w zakresie przetwarzania danych osobowych[3]

W związku z treścią z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U.UE.L 2016.119. z 04.05.2016 r., s. 1 oraz Dz. Urz. UE L 127 z 23.05.2018 r., s. 2.), dalej: „RODO" Zamawiający informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w związku z zawarciem umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazany w pkt 1.
3. Dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu zawarcia oraz wykonania niniejszej umowy.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
   1) organy kontrolne,
   2) osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2019 r. poz. 1429 ze zm.),
   3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
   4) podmioty przetwarzające w imieniu Administratora na mocy zawartej umowy, m. in. dostawcy IT.
5. Pani/Pana dane osobowe będą przechowywane przez okres obowiązywania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa. Okres przechowywania danych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora. Ponadto, okres przechowywania danych może zostać przedłużony na okres 5 lat, na potrzeby archiwizacji.
6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, usunięcia oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych, w przypadkach określonych w RODO.
7. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
8. Podanie przez Panią/Pana danych osobowych jest konieczne w celu określonym w pkt 3 powyżej, dla zawarcia i wykonania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa, a konsekwencją niepodania Pani/Pana danych osobowych będzie brak możliwości zawarcia umowy.

[3] Niniejsza klauzula w zakresie przetwarzania danych osobowych, znajdzie zastosowanie w przypadku bezpośredniego pozyskania danych pełnomocnika drugiej strony umowy będącej osobą fizyczną/osobą fizyczną prowadzącą działalność gospodarczą oraz reprezentantów drugiej strony umowy będącej spółką prawa handlowego/ spółką cywilną.

Klauzula informacyjna w zakresie przetwarzania danych osobowych[4]

W związku z treścią z art. 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U.UE.L 2016.119. z 04.05.2016 r., s. 1 oraz Dz. Urz. UE L 127 z 23.05.2018 r., s. 2.) dalej: „RODO" Zamawiający informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w związku z zawarciem umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazany w pkt 1.
3. Dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu zawarcia oraz wykonania niniejszej umowy.
4. Administrator będzie przetwarzał następujące kategorie Pani/Pana danych: dane identyfikacyjne oraz dane kontaktowe.
5. Odbiorcami Pani/Pana danych osobowych mogą być:
   1) organy kontrolne,
   2) osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2019 r. poz. 1429 ze zm.),
   3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
   4) podmioty przetwarzające w imieniu Administratora na mocy zawartej umowy, m. in. dostawcy IT.
6. Pani/Pana dane osobowe będą przechowywane przez okres obowiązywania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa. Okres przechowywania danych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora. Ponadto, okres przechowywania danych może zostać przedłużony na okres 5 lat, na potrzeby archiwizacji.
7. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, usunięcia oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych. w przypadkach określonych w RODO.
8. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
9. Pani/Pana dane Administrator uzyskał od firmy […*].

*należy wskazać źródło pozyskania danych [nazwę firmy, od której Administrator pozyskał dane].

[4] Niniejsza klauzula w zakresie przetwarzania danych osobowych, znajdzie zastosowanie w przypadku pośredniego pozyskania danych pełnomocników drugiej strony umowy będącej osobą fizyczną/osobą fizyczną prowadzącą działalność gospodarczą oraz reprezentantów drugiej strony umowy będącej spółką prawa handlowego/ spółką cywilną.

Załącznik nr 7 A do Umowy

Oświadczenie o wypełnieniu obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO
(wzór)

…… (dane Wykonawcy), którą reprezentuje:

1. ……,
2. ……,

zwana „**Wykonawcą**”

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[5] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu zawarcia oraz wykonania Umowy[6].

(podpisy)

1. ……,
2. ……,

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2).

[6] W przypadku, gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie składa.

Załącznik nr 8 do Umowy

Umowa powierzenia przetwarzania danych osobowych z Wykonawcą - wzór

Umowa powierzenia przetwarzania danych osobowych
zawarta w dniu …… 20… r. w Warszawie
(dalej zwana także – „Umową Powierzenia").

pomiędzy:
Agencją Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie przy al. Jana Pawła II nr 70, 00-175 Warszawa, REGON nr 010613083, zarejestrowanym podatnikiem podatku od towarów i usług, NIP 526-19-33-940, zwaną w dalszej części umowy **„Zamawiającym"** lub **„Administratorem"**, którą reprezentuje:
……..

……..
a
…….. – zwaną dalej **„Wykonawcą",** którą reprezentuje:
……..

Zamawiający i Wykonawca w dalszej części niniejszej Umowy Powierzenia zwani są także pojedynczo **„Stroną"** i łącznie **„Stronami"**.

§ 1.
Powierzenie przetwarzania danych osobowych.

1. W celu wykonania Umowy nr ……./DI/2019/2308 z dnia ……2019 r. (dalej zwana także – „Umową") zawartej pomiędzy wyżej wymienionymi Stronami, Zamawiający powierza Wykonawcy w trybie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z dnia 04.05.2016 r., str. 1, ze zm.), zwanego również „Rozporządzenie" lub „ogólne rozporządzenie o ochronie danych", przetwarzanie danych osobowych znajdujących się w systemie teleinformatycznym ARiMR w zbiorze/zbiorach/zasobach: ……., a Wykonawca zobowiązuje się do przetwarzania powierzonych danych osobowych w powyższym celu, w zakresie i w sposób niezbędny do wykonania Umowy.
2. Wykonawca zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi ogólnego rozporządzenia o ochronie danych i chroniło prawa osób, których te dane dotyczą. Wykonawca zobowiązuje się do przekazania Administratorowi - celem spełnienia wymogu rozliczalności - niezbędnych informacji i dokumentów lub innych dowodów potwierdzających realizację obowiązku, o którym mowa w zdaniu pierwszym.
3. Na podstawie Umowy powierzenia przetwarzania danych osobowych Strony określają jej przedmiot w następujący sposób:
   1) Zamawiający powierza Wykonawcy przetwarzanie danych osobowych w zakresie[7]:
      a) charakter przetwarzania:……;
      b) kategoria osób, których dane dotyczą:……;
      c) rodzaj danych osobowych:……;
   2) Zamawiający powierza Wykonawcy przetwarzanie danych osobowych poprzez wykonanie następujących operacji na powierzonych danych osobowych[8]:

[7] Należy dokładnie określić: charakter przetwarzania (tj. zespół cech właściwych całemu procesowi lub poszczególnych operacji przetwarzania, np. przetwarzanie danych może odbywać się elektronicznie lub w formie papierowej, w sposób zautomatyzowany, półautomatycznie lub ręcznie; przetwarzanie danych może odbywać się także w sposób ciągły, systematyczny lub sporadyczny; charakter (operacji) przetwarzania danych to sposób ich dokonywania – częstotliwość/powtarzalność, czasowość, długoterminowość, masowość z uwzględnieniem zastosowanych technologii); kategorię osób, których dane dotyczą (tj. informacje dotyczące charakterystyki określonej grupy podmiotów danych, np. dane pracowników Administratora, dane producenta rolnego/beneficjenta); rodzaj danych osobowych (np. dane zwykłe lub dane szczególnych kategorii, o których mowa w art. 9 ogólnego rozporządzenia o ochronie danych lub dane z art. 10 ogólnego rozporządzenia o ochronie danych, w postaci: np. imienia i nazwiska, adresu zamieszkania, nr PESEL, nr telefonu, nr producenta rolnego, nr działki ewidencyjnej).
[8] Należy dokładnie określić rodzaj wykonywanych operacji na powierzonych danych osobowych, np. utrwalanie (tj. kopiowanie, zapisywanie), przechowywanie (tj. archiwizowanie, wykonywanie kopii bezpieczeństwa, zapisywanie na nośnikach danych i w pamięci komputerów), opracowywanie (tj. analizowanie, porównywanie, testowanie), zmienianie (tj. modyfikowanie, dezintegrowanie), usuwanie (tj. kasowanie z nośników danych i pamięci komputerów, niszczenie danych) itp.

a) ……;
b) ……;
c) ……;
d) ……

4. Dane osobowe będą przekazane Wykonawcy przez Zamawiającego poprzez nadanie osobom wskazanym przez Wykonawcę praw dostępu do systemu teleinformatycznego ARiMR, w którym te dane się znajdują, dostępnego w[9] ……
5. Wniosek o nadanie uprawnień dostępu do systemu teleinformatycznego ARiMR przez Zamawiającego osobom wskazanym przez Wykonawcę, potwierdzać będzie na piśmie upoważniony pełnomocnik Wykonawcy.
6. Dane osobowe zostaną przekazane przez Zamawiającego po dostarczeniu mu przez Wykonawcę wykazu obszarów przetwarzania, przez który należy rozumieć wykaz budynków, pomieszczeń lub części pomieszczeń, w których powierzone dane będą przetwarzane. Wykaz obszarów przetwarzania będzie aktualizowany przez Wykonawcę, który w terminie 3 dni po każdej zmianie obszarów przetwarzania powierzonych danych jest obowiązany dostarczyć Zamawiającemu nowy wykaz obszarów ich przetwarzania.
7. Strony ustalają, że odwołanie przez Wykonawcę umocowania udzielonego pełnomocnikowi, o którym mowa w ust. 5 dokonywane będzie na piśmie. O każdorazowym odwołaniu wskazanego powyżej upoważnienia Wykonawca zobowiązany jest niezwłocznie poinformować Zamawiającego w formie pisemnej.
8. Wykonawca zobowiązuje się przetwarzać dane osobowe wyłącznie na udokumentowane polecenie Administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego. W przypadku, gdy obowiązek przetwarzania danych osobowych przez Wykonawcę wynika z obowiązujących przepisów prawa unijnego lub krajowego, Wykonawca informuje Administratora na piśmie lub drogą elektroniczną, na adresy wskazane w § 7 ust. 4 Umowy Powierzenia – przed rozpoczęciem przetwarzania – o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
9. Wykonawca zobowiązuje się niezwłocznie informować Administratora, jeżeli jego zdaniem wydane mu polecenie, o którym mowa w ust. 8 stanowi naruszenie ogólnego rozporządzenia o ochronie danych lub innych przepisów Unii lub państwa członkowskiego o ochronie danych. Informacja ta powinna zawierać wskazanie przepisu prawa, który w ocenie Wykonawcy został naruszony i uzasadnienie oraz powinna być przekazana na piśmie lub drogą elektroniczną, na adres Administratora wskazany w § 7 ust. 4 Umowy Powierzenia.

§ 2.

Zasady przetwarzania powierzonych danych osobowych.

1. Zamawiający jest administratorem danych osobowych w rozumieniu przepisów ogólnego rozporządzenia o ochronie danych.
2. Stosownie do przepisów ogólnego rozporządzenia o ochronie danych, Zamawiający powierza, a Wykonawca przyjmuje do przetwarzania dane osobowe wyłącznie w celu i zakresie niezbędnym do wykonania Umowy, o której mowa w § 1 ust. 1 Umowy Powierzenia.
3. Wykonawca nie jest uprawniony do dalszego przekazywania (tzw. podpowierzania) danych osobowych uzyskanych od Zamawiającego w trybie powierzenia.
4. Wykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z Umową powierzenia, ogólnym rozporządzeniem o ochronie danych oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
5. Wykonawca zobowiązuje się wykonać wszelkie czynności i zobowiązania wynikające z Umowy Powierzenia i ogólnego rozporządzenia o ochronie danych z najwyższą starannością.
6. W przypadku wystąpienia zagrożeń mogących mieć wpływ na odpowiedzialność Zamawiającego za przetwarzanie powierzonych danych osobowych, Wykonawca zobowiązuje się niezwłocznie zawiadomić o tych zagrożeniach Zamawiającego i podjąć wszelkie działania niezbędne dla usunięcia tych zagrożeń oraz natychmiast zawiadomić Zamawiającego o podjętych działaniach.
7. Wykonawca zobowiązuje się niezwłocznie, ale nie później niż w ciągu 3 (trzech) dni roboczych (rozumianych jako dni od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy) do informowania Administratora o jakimkolwiek postępowaniu (w tym sądowym lub administracyjnym), którego przedmiot stanowi przetwarzanie powierzonych danych osobowych, o jakiejkolwiek decyzji administracyjnej lub rozstrzygnięciu odnoszącym się do przetwarzania tych danych, skierowanym do Wykonawcy, a także o wszelkich zaplanowanych lub prowadzonych kontrolach i inspekcjach u Wykonawcy, dotyczących przetwarzania powierzonych danych.
8. W przypadku wszczęcia przeciwko Zamawiającemu przez osobę trzecią jakiegokolwiek postępowania (w szczególności administracyjnego lub sądowego) opartego na twierdzeniu, że przetwarzanie powierzonych danych osobowych nastąpiło z naruszeniem przepisów Rozporządzenia, przepisów prawa krajowego wprowadzonych na mocy Rozporządzenia oraz innych przepisów prawa powszechnie obowiązującego, chroniących prawa osób, których dane dotyczą, Wykonawca zobowiązuje się na

[9] Należy dokładnie określić miejsce (tj. adres), w którym będzie umożliwiony dostęp do systemu teleinformatycznego ARiMR (np. siedziba Wykonawcy).

żądanie Zamawiającego do udzielenia Zamawiającemu wszelkich informacji i wyjaśnień oraz przekazania Zamawiającemu wszelkich dokumentów wymaganych przez Zamawiającego, potrzebnych mu do wzięcia udziału w tym postępowaniu. Wykonawca niniejszym zobowiązuje się do zapewnienia Zamawiającemu na swój koszt ochrony sądowej oraz do poniesienia konsekwencji zapadłego wyroku sądowego.

9. Wykonawca zobowiązuje się do udostępniania Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia oraz umożliwiania Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji i przyczynianie się do nich.

§ 3.

Zabezpieczenie powierzonych danych osobowych.

1. Wykonawca oświadcza, że będzie przetwarzał powierzone dane osobowe przy użyciu urządzeń i systemów informatycznych zapewniających odpowiedni poziom bezpieczeństwa przetwarzania, o którym mowa w art. 32 ogólnego rozporządzenia o ochronie danych, odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, których powierzone dane dotyczą.
2. Wykonawca zobowiązuje się spełnić warunki, w tym podjąć środki zabezpieczające powierzone dane osobowe, o których mowa w art. 32 ogólnego rozporządzenia o ochronie danych. W szczególności Wykonawca zobowiązuje się do:
   1) zapewnienia kontroli nad prawidłowością przetwarzania powierzonych danych osobowych,
   2) zastosowania odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia powierzonych danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przypadkową lub niezgodną z prawem modyfikacją, utratą, zniszczeniem lub uszkodzeniem,
   3) dopuszczenia do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład służących do przetwarzania powierzonych danych osobowych wyłącznie osób, których dostęp do danych osobowych jest niezbędny dla realizacji Umowy i posiadających wydane przez niego upoważnienie,
   4) prowadzenia aktualnej ewidencji osób upoważnionych do przetwarzania powierzonych danych osobowych,
   5) zapewnienia, aby osoby upoważnione do przetwarzania powierzonych danych osobowych zachowały je w tajemnicy także po wygaśnięciu niniejszej Umowy Powierzenia, między innymi poprzez poinformowanie tych osób o prawnych konsekwencjach naruszenia poufności powierzonych danych osobowych i wykorzystania tych danych niezgodnie z przeznaczeniem oraz odebranie od tych osób oświadczeń o zachowaniu w tajemnicy wskazanych danych osobowych,
   6) niewykorzystywania powierzonych danych osobowych dla celów innych niż wykonywanie Umowy, o której mowa w §1 ust. 1 Umowy Powierzenia,
   7) uwzględniając charakter przetwarzania, pomagania Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą w zakresie wykonywania jej praw określonych w rozdziale III ogólnego rozporządzenia o ochronie danych,
   8) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomagania Administratorowi wywiązać się z obowiązków określonych w art. 32-36 ogólnego rozporządzenia o ochronie danych,
   9) w razie stwierdzenia naruszenia ochrony danych osobowych, zawiadomienia Zamawiającego o takim naruszeniu niezwłocznie (na piśmie i drogą elektroniczną, na adresy wskazane w §7 ust. 4 Umowy Powierzenia), lecz nie później niż w ciągu 12 godzin od jego wykrycia. Zawiadomienie o stwierdzeniu naruszenia powinno zostać przesłane Administratorowi wraz z niezbędną dokumentacją odnoszącą się do naruszenia - w szczególności opisującą charakter naruszenia ochrony danych osobowych, jego skalę, możliwe konsekwencje naruszenia ochrony danych, czas zdarzenia, osoby odpowiedzialne i osoby poszkodowane - celem umożliwienia Administratorowi spełnienia obowiązku powiadomienia organu nadzoru,
   10) prowadzenia w formie pisemnej (w tym elektronicznej) rejestru wszystkich kategorii czynności przetwarzania, dokonywanych w imieniu Zamawiającego.

§ 4.

Nadzór nad wykonywaniem Umowy Powierzenia.

1. Zamawiający jest uprawniony w każdym czasie do przeprowadzania audytów sposobu wykonywania Umowy Powierzenia przez Wykonawcę, w tym sprawdzania czy środki techniczne i organizacyjne zabezpieczające przetwarzanie powierzonych danych, zastosowane przez Wykonawcę, odpowiadają ryzyku naruszenia praw lub wolności osób, których dane dotyczą. Ponadto Zamawiający ma prawo dokonać weryfikacji, czy Wykonawca przetwarzając powierzone dane osobowe przestrzega przepisów ogólnego rozporządzenia o ochronie danych oraz innych mających zastosowanie przepisów w zakresie, w jakim ewentualne naruszenie tych przepisów mogłoby prowadzić do ponoszenia odpowiedzialności przez Zamawiającego, w tym zagrażało bezpieczeństwu powierzonych danych osobowych lub naruszało prawa osób trzecich.
2. W celu wykonania audytu upoważnieni pracownicy Zamawiającego mają prawo:
   1) wstępu do obszarów przetwarzania powierzonych danych osobowych (m.in. pomieszczeń) i przeprowadzania czynności audytowych,
   2) pozyskania informacji o sposobie przetwarzania powierzonych danych,

3) żądania od Wykonawcy udostępnienia dokumentów, złożenia pisemnych i ustnych wyjaśnień w celu ustalenia stanu faktycznego,
4) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych Wykonawcy służących do przetwarzania powierzonych danych osobowych,
5) [10].....

3. Z czynności audytowych przeprowadzający audyt pracownicy Zamawiającego sporządzają protokół w dwóch egzemplarzach – podpisany przez przedstawicieli obu Stron – z których jeden egzemplarz doręcza się Wykonawcy.
4. Wykonawca zapewnia możliwość niezwłocznego przeprowadzenia czynności audytowych przez Zamawiającego w każdym z obszarów przetwarzania powierzonych danych osobowych. Osoby uprawnione do przeprowadzenia audytu mają prawo niezwłocznego wstępu do obszarów przetwarzania powierzonych danych osobowych, w dniach i w godzinach wykonywania pracy u Wykonawcy, na ustne żądanie skierowane do osób zapewniających ochronę fizyczną wraz z okazaniem upoważnienia do przeprowadzenia audytu.
5. W przypadku ujawnienia okoliczności uznanych przez Zamawiającego za nieprawidłowości w zakresie wykonywania Umowy Powierzenia lub ogólnego rozporządzenia o ochronie danych, Wykonawca zobowiązuje się do ich usunięcia w wyznaczonym przez Zamawiającego terminie. W razie niezastosowania się przez Wykonawcę do wydanych mu poleceń, w tym m.in. w przypadku nieusunięcia przez Wykonawcę wskazanej mu nieprawidłowości w wyznaczonym terminie, Zamawiający może naliczyć Wykonawcy karę umowną w wysokości 10.000 zł (słownie złotych: dziesięć tysięcy 00/100) za każdy przypadek stwierdzonej i nieusuniętej w terminie nieprawidłowości.
6. Jeżeli nieprawidłowości wskazane w ust. 5 zostaną ponownie ujawnione, Zamawiający może naliczyć Wykonawcy karę umowną w wysokości wskazanej w ust. 5 bez wyznaczania terminu do usunięcia tych nieprawidłowości.
7. W przypadku naliczenia kary umownej, Zamawiający może według własnego wyboru:
   1) potrącać karę umowną z łącznego wynagrodzenia za wykonanie Umowy, o której mowa w § 1 ust. 1 Umowy Powierzenia.
   2) skorzystać z zabezpieczenia należytego wykonania Umowy, o której mowa w § 1 ust. 1 Umowy Powierzenia.
   3) wezwać Wykonawcę do zapłaty kary umownej w terminie 14 dni od dnia doręczenia pisemnego wezwania do jej zapłaty.

§ 5.

Przetwarzanie powierzonych danych osobowych po wygaśnięciu Umowy Powierzenia.

1. Umowa Powierzenia wygasa z upływem 14 dni od dnia wykonania, rozwiązania, wygaśnięcia, unieważnienia lub odstąpienia od Umowy, o której mowa w § 1 ust. 1 Umowy Powierzenia.
2. W przypadku wystąpienia okoliczności, o której mowa w ust. 1, Wykonawca zobowiązuje się niezwłocznie, nie później jednak niż w terminie 14 dni od dnia wystąpienia tej okoliczności, trwale usunąć wszelkie powierzone mu na podstawie Umowy Powierzenia dane osobowe oraz wszelkie ich istniejące kopie, w tym skutecznie usunąć te dane z nośników elektronicznych pozostających w jego dyspozycji lub zwrócić dane, chyba że prawo Unii lub prawo państwa członkowskiego nakazują dalej przechowywanie danych osobowych. Zamawiający celem zweryfikowania wykonania przez Wykonawcę zobowiązań wskazanych w zdaniu pierwszym niniejszego ustępu uprawniony jest do przeprowadzenia audytu na zasadach wskazanych w §4 ust. 1-4 Umowy Powierzenia.
3. Powierzenie przetwarzania danych osobowych trwa do upływu terminu wskazanego w ust. 1.
4. Celem usunięcia wątpliwości Strony ustalają, że pomimo wygaśnięcia Umowy Powierzenia zachowują moc obowiązującą wszelkie postanowienia nakładające lub mogące nałożyć na Wykonawcę jakiekolwiek zobowiązanie względem Zamawiającego, po terminie wygaśnięcia Umowy Powierzenia, w tym m.in. postanowienia §2 ust. 8, §5 ust. 2 i §5 ust. 5 Umowy Powierzenia.
5. W przypadku niewykonania przez Wykonawcę zobowiązania wynikającego z treści §5 ust. 2 Umowy Powierzenia Zamawiający uprawniony jest do naliczenia Wykonawcy kary umownej w wysokości 10.000 zł (słownie złotych: dziesięć tysięcy 00/100). W przypadku naliczenia kary umownej wskazanej w zdaniu pierwszym niniejszego ustępu stosuje się odpowiednio postanowienia §4 ust. 7 Umowy Powierzenia.
6. W przypadku naruszenia przez Wykonawcę zobowiązania, o którym mowa w § 3 ust. 2 pkt 5, Zamawiający uprawniony jest do naliczenia Wykonawcy kary umownej w wysokości 10.000 zł (słownie złotych: dziesięć tysięcy 00/100) za każdy przypadek naruszenia. W przypadku naliczenia kary umownej wskazanej w zdaniu pierwszym niniejszego ustępu stosuje się odpowiednio postanowienia § 4 ust. 7 Umowy Powierzenia.
7. Jeżeli na skutek niewykonania lub nienależytego wykonania Umowy Powierzenia powstanie szkoda przewyższająca zastrzeżoną karę umowną, Zamawiającemu, oprócz tej kary, przysługuje prawo do dochodzenia odszkodowania uzupełniającego. Jeżeli szkoda powstanie z innych przyczyn, niż te, ze względu na które zastrzeżono karę umowną, Zamawiającemu przysługuje prawo do dochodzenia odszkodowania na zasadach ogólnych Kodeksu cywilnego.

§ 6.

Wykonywanie Umowy Powierzenia.

[7] Wymienić inne uprawnienia upoważnionych pracowników Zamawiającego, związane z wykonaniem audytu, np. uczestniczenie w procesie migracji danych osobowych.

1. Wynagrodzenie z tytułu wykonania Umowy Powierzenia zawarte jest w wynagrodzeniu przewidzianym dla Wykonawcy w § 7 ust. 1 Umowy.
2. Wykonanie Umowy Powierzenia nie może być podstawą dodatkowych roszczeń Wykonawcy wobec Zamawiającego.
3. Uprawnienie Zamawiającego względem Wykonawcy do kary umownej oraz odszkodowań wskazanych w niniejszej Umowie Powierzenia nie wyłącza odpowiedzialności Wykonawcy w przypadku wystąpienia zdarzenia, o którym mowa w §2 ust. 8 niniejszej Umowy Powierzenia.

§ 7.

Postanowienia końcowe.

1. Wszelkie zmiany Umowy Powierzenia dokonywane będą w formie pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych Umową Powierzenia mają zastosowanie w szczególności przepisy Kodeksu cywilnego oraz przepisy ogólnego rozporządzenia o ochronie danych.
3. Sądem właściwym dla rozstrzygania sporów powstałych w związku z zawarciem lub wykonywaniem Umowy Powierzenia jest sąd powszechny właściwy dla siedziby Zamawiającego.
4. Wszelka korespondencja w sprawach związanych z Umową Powierzenia będzie kierowana do:
   a) Administratora na następujące dane kontaktowe: adres (…), tel. (…), e-mail (…);
   b) Wykonawcy na następujące dane kontaktowe: adres (…), tel. (…), e-mail (…).
5. Dane przedstawicieli Stron:
   a) Administratora w kontaktach z Wykonawcą w zakresie ustaleń Umowy Powierzenia reprezentować będą następujące osoby: (…);
   b) Wykonawcę w kontaktach z Administratorem w zakresie ustaleń Umowy Powierzenia reprezentować będą następujące osoby: (…).
6. Zmiana adresów i danych osób wskazanych w ust. 4 i 5 nie stanowi zmiany Umowy Powierzenia. O każdej zmianie powyższych danych Strony powiadomią się na piśmie, za potwierdzeniem odbioru lub drogą elektroniczną.
7. Umowa Powierzenia wchodzi w życie z dniem jej podpisania przez Strony.
8. Umowę Powierzenia sporządzono w czterech jednobrzmiących egzemplarzach – trzy dla Zamawiającego i jeden dla Wykonawcy

Wykonawca	**Zamawiający**
……	……
……	……

Załącznik nr 8 A do Umowy

Umowa powierzenia przetwarzania danych osobowych z Podwykonawcą - wzór

Umowa powierzenia przetwarzania danych osobowych
zawarta w dniu …… 20… r. w Warszawie
(dalej zwana także – „**Umową Powierzenia**")

pomiędzy:
Agencją Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie przy al. Jana Pawła II nr 70, 00-175 Warszawa, REGON nr 010613083, zarejestrowanym podatnikiem podatku od towarów i usług, NIP 526-19-33-940, zwaną w dalszej części umowy **„Zamawiającym"** lub **„Administratorem"**, którą reprezentuje:

……
……

a
……
z siedzibą w …… przy ul. ……., wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy……., (…) Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem ……, NIP (…), REGON (...), posiadającą kapitał zakładowy w kwocie ……. zł, wpłacony w całości/
…….. zamieszkałą/ym …… legitymującą/ym się ……., prowadzącą/ym działalność gospodarczą pod nazwą ……., na podstawie wpisu do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, z miejscem prowadzenia działalności gospodarczej w ……, REGON……, zarejestrowanym podatnikiem podatku od towarów i usług, NIP……., zwaną/ym dalej **„Podwykonawcą",** którą reprezentuje:

……..

Zamawiający i Podwykonawca w dalszej części niniejszej Umowy Powierzenia zwani są także pojedynczo **„Stroną"** i łącznie **„Stronami"**.

§ 1.
Powierzenie przetwarzania danych osobowych.

1. W celu wykonania Umowy nr ……./DI/2019/2308 z dnia ……2019 r. (dalej zwana także – „Umową") zawartej pomiędzy Zamawiającym a[11] …… (Wykonawcą), Zamawiający powierza Podwykonawcy w trybie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z dnia 04.05.2016 r., str. 1, ze zm.), zwanego również „Rozporządzenie" lub „ogólne rozporządzenie o ochronie danych", przetwarzanie danych osobowych znajdujących się w systemie teleinformatycznym ARiMR w zbiorze/zbiorach/zasobach: ……., a Podwykonawca zobowiązuje się do przetwarzania powierzonych danych osobowych w powyższym celu, w zakresie i w sposób niezbędny do wykonania Umowy.
2. Podwykonawca zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi ogólnego rozporządzenia o ochronie danych i chroniło prawa osób, których te dane dotyczą. Podwykonawca zobowiązuje się do przekazania Administratorowi - celem spełnienia wymogu rozliczalności - niezbędnych informacji i dokumentów lub innych dowodów potwierdzających realizację obowiązku, o którym mowa w zdaniu pierwszym.
3. Na podstawie Umowy powierzenia przetwarzania danych osobowych Strony określają jej przedmiot w następujący sposób:
   1) Zamawiający powierza Podwykonawcy przetwarzanie danych osobowych w zakresie[12]:

[11] Należy wpisać Wykonawcę, na rzecz którego Podwykonawca wykonuje obowiązki w ramach Umowy głównej.
[12] Należy dokładnie określić: charakter przetwarzania (tj. zespół cech właściwych całemu procesowi lub poszczególnych operacji przetwarzania, np. przetwarzanie danych może odbywać się elektronicznie lub w formie papierowej, w sposób zautomatyzowany, półautomatycznie lub ręcznie; przetwarzanie danych może odbywać się także w sposób ciągły, systematyczny lub sporadyczny; charakter (operacji) przetwarzania danych to sposób ich dokonywania – częstotliwość/powtarzalność, czasowość, długoterminowość, masowość z uwzględnieniem zastosowanych technologii); kategorię osób, których dane dotyczą (tj. informacje dotyczące charakterystyki określonej grupy podmiotów danych, np. dane pracowników Administratora, dane producenta

a) charakter przetwarzania:……;
b) kategoria osób, których dane dotyczą:……;
c) rodzaj danych osobowych:……;

2) Zamawiający powierza Podwykonawcy przetwarzanie danych osobowych poprzez wykonanie następujących operacji na powierzonych danych osobowych[13]:
a) ……;
b) ……;
c) ……;
d) ……

4. Dane osobowe będą przekazane Podwykonawcy przez Zamawiającego poprzez nadanie osobom wskazanym przez Podwykonawcę praw dostępu do systemu teleinformatycznego ARiMR, w którym te dane się znajdują, dostępnego w[14] ……
5. Wniosek o nadanie uprawnień dostępu do systemu teleinformatycznego ARiMR przez Zamawiającego osobom wskazanym przez Podwykonawcę, potwierdzać będzie na piśmie upoważniony pełnomocnik Wykonawcy i pełnomocnik Podwykonawcy.
6. Dane osobowe zostaną przekazane przez Zamawiającego po dostarczeniu mu przez Podwykonawcę wykazu obszarów przetwarzania, przez który należy rozumieć wykaz budynków, pomieszczeń lub części pomieszczeń, w których powierzone dane będą przetwarzane. Wykaz obszarów przetwarzania będzie aktualizowany przez Podwykonawcę, który w terminie 3 dni po każdej zmianie obszarów przetwarzania powierzonych danych jest obowiązany dostarczyć Zamawiającemu nowy wykaz obszarów ich przetwarzania.
7. Strony ustalają, że odwołanie przez Podwykonawcę umocowania udzielonego pełnomocnikowi, o którym mowa w ust. 5 dokonywane będzie na piśmie. O każdorazowym odwołaniu wskazanego powyżej upoważnienia Podwykonawca zobowiązany jest niezwłocznie poinformować Zamawiającego w formie pisemnej.
8. Podwykonawca zobowiązuje się przetwarzać dane osobowe wyłącznie na udokumentowane polecenie Administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego. W przypadku, gdy obowiązek przetwarzania danych osobowych przez Podwykonawcę wynika z obowiązujących przepisów prawa unijnego lub krajowego, Podwykonawca informuje Administratora na piśmie lub drogą elektroniczną, na adresy wskazane w § 7 ust. 4 Umowy Powierzenia – przed rozpoczęciem przetwarzania – o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
9. Podwykonawca zobowiązuje się niezwłocznie informować Administratora, jeżeli jego zdaniem wydane mu polecenie, o którym mowa w ust. 8 stanowi naruszenie ogólnego rozporządzenia o ochronie danych lub innych przepisów Unii lub państwa członkowskiego o ochronie danych. Informacja ta powinna zawierać wskazanie przepisu prawa, który w ocenie Podwykonawcy został naruszony i uzasadnienie oraz powinna być przekazana na piśmie lub drogą elektroniczną, na adres Administratora wskazany w § 7 ust. 4 Umowy Powierzenia.

§ 2.

Zasady przetwarzania powierzonych danych osobowych.

1. Zamawiający jest administratorem danych osobowych w rozumieniu przepisów ogólnego rozporządzenia o ochronie danych.
2. Stosownie do przepisów ogólnego rozporządzenia o ochronie danych, Zamawiający powierza, a Podwykonawca przyjmuje do przetwarzania dane osobowe wyłącznie w celu i zakresie niezbędnym do wykonania Umowy, o której mowa w § 1 ust. 1 Umowy Powierzenia.
3. Podwykonawca nie jest uprawniony do dalszego przekazywania (tzw. podpowierzania) danych osobowych uzyskanych od Zamawiającego w trybie powierzenia.
4. Podwykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z Umową Powierzenia, ogólnym rozporządzeniem o ochronie danych oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
5. Podwykonawca zobowiązuje się wykonać wszelkie czynności i zobowiązania wynikające z Umowy Powierzenia i ogólnego rozporządzenia o ochronie danych z najwyższą starannością.

rolnego/beneficjenta); rodzaj danych osobowych (np. dane zwykłe lub dane szczególnych kategorii, o których mowa w art. 9 ogólnego rozporządzenia o ochronie danych lub dane z art. 10 ogólnego rozporządzenia o ochronie danych, w postaci: np. imienia i nazwiska, adresu zamieszkania, nr PESEL, nr telefonu, nr producenta rolnego, nr działki ewidencyjnej.

[13] Należy dokładnie określić rodzaj wykonywanych operacji na powierzonych danych osobowych, np. utrwalanie (tj. kopiowanie, zapisywanie), przechowywanie (tj. archiwizowanie, wykonywanie kopii bezpieczeństwa, zapisywanie na nośnikach danych i w pamięci komputerów), opracowywanie (tj. analizowanie, porównywanie, testowanie), zmienianie (tj. modyfikowanie, dezintegrowanie), usuwanie (tj. kasowanie z nośników danych i pamięci komputerów, niszczenie danych) itp.

[14] Należy dokładnie określić miejsce (tj. adres), w którym będzie umożliwiony dostęp do systemu teleinformatycznego ARiMR (np. siedziba Podwykonawcy).

6. W przypadku wystąpienia zagrożeń mogących mieć wpływ na odpowiedzialność Zamawiającego za przetwarzanie powierzonych danych osobowych, Podwykonawca zobowiązuje się niezwłocznie zawiadomić o tych zagrożeniach Zamawiającego i podjąć wszelkie działania niezbędne dla usunięcia tych zagrożeń oraz natychmiast zawiadomić Zamawiającego o podjętych działaniach.
7. Podwykonawca zobowiązuje się niezwłocznie, ale nie później niż w ciągu 3 (trzech) dni roboczych (rozumianych jako dni od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy) do informowania Administratora o jakimkolwiek postępowaniu (w tym sądowym lub administracyjnym), którego przedmiot stanowi przetwarzanie powierzonych danych osobowych, o jakiejkolwiek decyzji administracyjnej lub rozstrzygnięciu odnoszącym się do przetwarzania tych danych, skierowanym do Podwykonawcy, a także o wszelkich zaplanowanych lub prowadzonych kontrolach i inspekcjach u Podwykonawcy, dotyczących przetwarzania powierzonych danych.
8. W przypadku wszczęcia przeciwko Zamawiającemu przez osobę trzecią jakiegokolwiek postępowania (w szczególności administracyjnego lub sądowego) opartego na twierdzeniu, że przetwarzanie powierzonych danych osobowych nastąpiło z naruszeniem przepisów Rozporządzenia, przepisów prawa krajowego wprowadzonych na mocy Rozporządzenia oraz innych przepisów prawa powszechnie obowiązującego, chroniących prawa osób, których dane dotyczą, Podwykonawca zobowiązuje się na żądanie Zamawiającego do udzielenia Zamawiającemu wszelkich informacji i wyjaśnień oraz przekazania Zamawiającemu wszelkich dokumentów wymaganych przez Zamawiającego, potrzebnych mu do wzięcia udziału w tym postępowaniu. Podwykonawca niniejszym zobowiązuje się do zapewnienia Zamawiającemu na swój koszt ochrony sądowej oraz do poniesienia konsekwencji zapadłego wyroku sądowego.
9. Podwykonawca zobowiązuje się do udostępniania Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia oraz umożliwiania Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji i przyczynianie się do nich.

§ 3.

Zabezpieczenie powierzonych danych osobowych.

1. Podwykonawca oświadcza, że będzie przetwarzał powierzone dane osobowe przy użyciu urządzeń i systemów informatycznych zapewniających odpowiedni poziom bezpieczeństwa przetwarzania, o którym mowa w art. 32 ogólnego rozporządzenia o ochronie danych, odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, których powierzone dane dotyczą.
2. Podwykonawca zobowiązuje się spełnić warunki w tym podjąć środki zabezpieczające powierzone dane osobowe, o których mowa w art. 32 ogólnego rozporządzenia o ochronie danych. W szczególności Podwykonawca zobowiązuje się do:
   1) zapewnienia kontroli nad prawidłowością przetwarzania powierzonych danych osobowych,
   2) zastosowania odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia powierzonych danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przypadkową lub niezgodną z prawem modyfikacją, utratą, zniszczeniem lub uszkodzeniem,
   3) dopuszczenia do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład służących do przetwarzania powierzonych danych osobowych wyłącznie osób, których dostęp do danych osobowych jest niezbędny dla realizacji Umowy i posiadających wydane przez niego upoważnienie,
   4) prowadzenia aktualnej ewidencji osób upoważnionych do przetwarzania powierzonych danych osobowych,
   5) zapewnienia, aby osoby upoważnione do przetwarzania powierzonych danych osobowych zachowały je w tajemnicy także po wygaśnięciu niniejszej Umowy Powierzenia, między innymi poprzez poinformowanie tych osób o prawnych konsekwencjach naruszenia poufności powierzonych danych osobowych i wykorzystania tych danych niezgodnie z przeznaczeniem oraz odebranie od tych osób oświadczeń o zachowaniu w tajemnicy wskazanych danych osobowych,
   6) niewykorzystywania powierzonych danych osobowych dla celów innych niż wykonywanie Umowy, o której mowa w §1 ust. 1 Umowy Powierzenia,
   7) uwzględniając charakter przetwarzania, pomagania Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą w zakresie wykonywania jej praw określonych w rozdziale III ogólnego rozporządzenia o ochronie danych,
   8) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomagania Administratorowi wywiązać się z obowiązków określonych w art. 32-36 ogólnego rozporządzenia o ochronie danych,
   9) w razie stwierdzenia naruszenia ochrony danych osobowych, zawiadomienia Zamawiającego o takim naruszeniu niezwłocznie (na piśmie i drogą elektroniczną, na adresy wskazane w §7 ust. 4 Umowy Powierzenia), lecz nie później niż w ciągu 12 godzin od jego wykrycia. Zawiadomienie o stwierdzeniu naruszenia powinno zostać przesłane Administratorowi wraz z niezbędną dokumentacją odnoszącą się do naruszenia – w szczególności opisującą charakter naruszenia ochrony danych osobowych, jego skalę, możliwe konsekwencje naruszenia ochrony danych, czas zdarzenia, osoby odpowiedzialne i osoby poszkodowane - celem umożliwienia Administratorowi spełnienia obowiązku powiadomienia organu nadzoru,
   10) prowadzenia w formie pisemnej (w tym elektronicznej) rejestru wszystkich kategorii czynności przetwarzania, dokonywanych w imieniu Zamawiającego.

§ 4.

Nadzór nad wykonywaniem Umowy Powierzenia.

1. Zamawiający jest uprawniony w każdym czasie do przeprowadzania audytów sposobu wykonywania Umowy Powierzenia przez Podwykonawcę, w tym sprawdzania, czy środki techniczne i organizacyjne zabezpieczające przetwarzanie powierzonych danych, zastosowane przez Podwykonawcę, odpowiadają ryzyku naruszenia praw lub wolności osób, których dane dotyczą. Ponadto Zamawiający ma prawo dokonać weryfikacji, czy Podwykonawca przetwarzając powierzone dane osobowe przestrzega przepisów ogólnego rozporządzenia o ochronie danych oraz innych mających zastosowanie przepisów w zakresie, w jakim ewentualne naruszenie tych przepisów mogłoby prowadzić do ponoszenia odpowiedzialności przez Zamawiającego, w tym zagrażało bezpieczeństwu powierzonych danych osobowych lub naruszało prawa osób trzecich.
2. W celu wykonania audytu upoważnieni pracownicy Zamawiającego mają prawo:
    1) wstępu do obszarów przetwarzania powierzonych danych osobowych (m.in. pomieszczeń)i przeprowadzania czynności audytowych,
    2) pozyskania informacji o sposobie przetwarzania powierzonych danych,
    3) żądania od Podwykonawcy udostępnienia dokumentów, złożenia pisemnych i ustnych wyjaśnień w celu ustalenia stanu faktycznego,
    4) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych Podwykonawca służących do przetwarzania powierzonych danych osobowych,
    5) [15.] ……
3. Z czynności audytowych przeprowadzający audyt pracownicy Zamawiającego sporządzają protokół w dwóch egzemplarzach – podpisany przez przedstawicieli obu Stron - z których jeden egzemplarz doręcza się Podwykonawcy.
4. Podwykonawca zapewnia możliwość niezwłocznego przeprowadzenia czynności audytowych przez Zamawiającego w każdym z obszarów przetwarzania powierzonych danych osobowych. Osoby uprawnione do przeprowadzenia audytu mają prawo niezwłocznego wstępu do obszarów przetwarzania powierzonych danych osobowych, w dniach i w godzinach wykonywania pracy u Podwykonawcy, na ustne żądanie skierowane do osób zapewniających ochronę fizyczną wraz z okazaniem upoważnienia do przeprowadzenia audytu.
5. W przypadku ujawnienia okoliczności uznanych przez Zamawiającego za nieprawidłowości w zakresie wykonywania Umowy Powierzenia lub ogólnego rozporządzenia o ochronie danych, Podwykonawca zobowiązuje się do ich usunięcia w wyznaczonym przez Zamawiającego terminie. W razie niezastosowania się przez Podwykonawcę do wydanych mu poleceń, w tym m.in. w przypadku nieusunięcia przez Podwykonawcę wskazanej mu nieprawidłowości w wyznaczonym terminie, Zamawiający może naliczyć Podwykonawcy karę umowną w wysokości 10.000 zł (słownie złotych: dziesięć tysięcy 00/100) za każdy przypadek stwierdzonej i nieusuniętej w terminie nieprawidłowości.
6. Jeżeli nieprawidłowości wskazane w ust. 5 zostaną ponownie ujawnione, Zamawiający może naliczyć Podwykonawcy karę umowną w wysokości wskazanej w ust. 5 bez wyznaczania terminu do usunięcia tych nieprawidłowości.
7. W przypadku naliczenia kary umownej, Zamawiający wezwie Podwykonawcę do zapłaty kary umownej w terminie 14 dni od dnia doręczenia pisemnego wezwania do jej zapłaty.

§ 5.

Przetwarzanie powierzonych danych osobowych po wygaśnięciu Umowy Powierzenia.

1. Umowa Powierzenia wygasa z upływem 14 dni od dnia wykonania, rozwiązania, wygaśnięcia, unieważnienia lub odstąpienia od Umowy, o której mowa w § 1 ust. 1 Umowy Powierzenia.
2. W przypadku wystąpienia okoliczności, o której mowa w ust. 1, Podwykonawca zobowiązuje się niezwłocznie, nie później jednak niż w terminie 14 dni od dnia wystąpienia tej okoliczności, trwale usunąć wszelkie powierzone mu na podstawie Umowy Powierzenia dane osobowe oraz wszelkie ich istniejące kopie, w tym skutecznie usunąć te dane z nośników elektronicznych pozostających w jego dyspozycji lub zwrócić dane, chyba że prawo Unii lub prawo państwa członkowskiego nakazują dalej przechowywanie danych osobowych. Zamawiający celem zweryfikowania wykonania przez Podwykonawcę zobowiązań wskazanych w zdaniu pierwszym niniejszego ustępu uprawniony jest do przeprowadzenia audytu na zasadach wskazanych w §4 ust. 1-4 Umowy Powierzenia.
3. Powierzenie przetwarzania danych osobowych trwa do upływu terminu wskazanego w ust. 1.
4. Celem usunięcia wątpliwości Strony ustalają, że pomimo wygaśnięcia Umowy Powierzenia zachowują moc obowiązującą wszelkie postanowienia nakładające lub mogące nałożyć na Podwykonawcę jakiekolwiek zobowiązanie względem Zamawiającego, po terminie wygaśnięcia Umowy Powierzenia, w tym m.in. postanowienia §2 ust. 8, §5 ust. 2 i §5 ust. 5 Umowy Powierzenia.
5. W przypadku niewykonania przez Podwykonawcę zobowiązania wynikającego z treści §5 ust. 2 Umowy Powierzenia Zamawiający uprawniony jest do naliczenia Podwykonawcy kary umownej w wysokości 10.000 zł (słownie złotych: dziesięć tysięcy 00/100). W

[15.] Wymienić inne uprawnienia upoważnionych pracowników Zamawiającego, związane z wykonaniem audytu, np. uczestniczenie w procesie migracji danych osobowych.

przypadku naliczenia kary umownej wskazanej w zdaniu pierwszym niniejszego ustępu stosuje się odpowiednio postanowienia § 4 ust. 7 Umowy Powierzenia.

6. W przypadku naruszenia przez Podwykonawcę zobowiązania, o którym mowa w § 3 ust. 2 pkt 5, Zamawiający uprawniony jest do naliczenia Podwykonawcy kary umownej w wysokości 10.000 zł (słownie złotych: dziesięć tysięcy 00/100) za każdy przypadek naruszenia. W przypadku naliczenia kary umownej wskazanej w zdaniu pierwszym niniejszego ustępu stosuje się odpowiednio postanowienia § 4 ust. 7 Umowy Powierzenia.
7. Jeżeli na skutek niewykonania lub nienależytego wykonania Umowy Powierzenia powstanie szkoda przewyższająca zastrzeżoną karę umowną, Zamawiającemu, oprócz tej kary, przysługuje prawo do dochodzenia odszkodowania uzupełniającego. Jeżeli szkoda powstanie z innych przyczyn, niż te, ze względu na które zastrzeżono karę umowną, Zamawiającemu przysługuje prawo do dochodzenia odszkodowania na zasadach ogólnych Kodeksu cywilnego.

§ 6.

Wykonywanie Umowy Powierzenia.

1. Z tytułu wykonania Umowy Powierzenia Podwykonawcy nie przysługuje wynagrodzenie.
2. Wykonanie Umowy Powierzenia nie może być podstawą dodatkowych roszczeń Podwykonawcy wobec Zamawiającego.
3. Uprawnienie Zamawiającego względem Podwykonawcy do kary umownej oraz odszkodowań wskazanych w niniejszej Umowie Powierzenia nie wyłącza odpowiedzialności Podwykonawcy w przypadku wystąpienia zdarzenia, o którym mowa w §2 ust. 8 niniejszej Umowy Powierzenia.

§ 7.

Postanowienia końcowe.

1. Wszelkie zmiany Umowy Powierzenia dokonywane będą w formie pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych Umową Powierzenia mają zastosowanie w szczególności przepisy Kodeksu cywilnego oraz przepisy ogólnego rozporządzenia o ochronie danych.
3. Sądem właściwym dla rozstrzygania sporów powstałych w związku z zawarciem lub wykonywaniem Umowy Powierzenia jest sąd powszechny właściwy dla siedziby Zamawiającego.
4. Wszelka korespondencja w sprawach związanych z Umową Powierzenia będzie kierowana do:
   a) Administratora na następujące dane kontaktowe: adres (…), tel. (…), e-mail (…);
   b) Podwykonawcy na następujące dane kontaktowe: adres (…), tel. (…), e-mail (…).
5. Dane przedstawicieli Stron:
   a) Administratora w kontaktach z Podwykonawcą w zakresie ustaleń Umowy Powierzenia reprezentować będą następujące osoby: (…);
   b) Podwykonawcę w kontaktach z Administratorem w zakresie ustaleń Umowy Powierzenia reprezentować będą następujące osoby: (…).
6. Zmiana adresów i danych osób wskazanych w ust. 4 i 5 nie stanowi zmiany Umowy Powierzenia. O każdej zmianie powyższych danych Strony powiadomią się na piśmie, za potwierdzeniem odbioru lub drogą elektroniczną.
7. Umowa Powierzenia wchodzi w życie z dniem jej podpisania przez Strony.
8. Umowę Powierzenia sporządzono w czterech jednobrzmiących egzemplarzach – trzy dla Zamawiającego i jeden dla Podwykonawcy.

Podwykonawca	**Zamawiający**
……	……
……	……

Załącznik nr 8 do SWZ – plik, w formacie XML, wygenerowany z narzędzia ESPD

Plik, w formacie XML, wygenerowany z narzędzia ESPD („*ESPD*") znajduje się w odrębnym pliku o nazwie „Załącznik nr 8 do SWZ_ESPD". Plik należy pobrać i zapisać na dysk komputera oraz wypełnić przy pomocy narzędzia udostępnionego przez Urząd Zamówień Publicznych pod adresem https://espd.uzp.gov.pl.

Po uruchomieniu wyżej wymienionej strony internetowej Urzędu, należy wybrać „pl Polski", a w dalszej kolejności zaznaczyć „Jestem wykonawcą". Następnie należy zaimportować „ESPD" wczytując plik w formacie XML będący Załącznikiem nr 8 do SWZ. Po sporządzeniu oświadczenia w formie jednolitego europejskiego dokumentu zamówienia („*JEDZ*") należy je podpisać przez osobę lub osoby uprawnione.

Aktualne na dzień składania ofert oświadczenie w formie JEDZ należy złożyć w formie elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym, za pomocą środka komunikacji elektronicznej, tj. Platformę Zakupową.
Szczegółowy zakres wymagań określony został w Rozdz. IV.2 SWZ.