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.

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 ……. Imię i Nazwisko ……

Stanowisko …….. Stanowisko ……

Data ……..…… Data ……..

Podpis …… Podpis ……..……

REGULAMIN EKSPLOATACJI SYSTEMÓW TELEINFORMATYCZNYCH

Spis treści:

§ 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 przetwarzania 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 defoult);
   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 defoult).

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

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.

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

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 .