Załącznik nr 2 do Umowy nr FDZZ.226.18.2024

Informacje o Zamawiającym

Dane Zamawiającego:

	Dane zarejestrowane:	**Dane poprawne (korekta)**
Nazwa jednostki:		
Adres:		
Główny adres e-mail Zamawiającego*:		
Akceptacja dostarczania informacji dotyczących pakietu Oprogramowania Aplikacyjnego na w/w adres e-mail (TAK/NIE):		
Nr telefonu:		
Nr faksu:		
NIP		
REGON		
Wpis do KRS prowadzonego przez:		
KRS		
Adres WWW:		
Identyfikator Zamawiającego w Systemie CHD: (przydziela administrator Systemu CHD)		

Osoby upoważnione do administrowania użytkownikami CHD ze Strony Zamawiającego i/lub osoby upoważnione do reprezentowania Zamawiającego przy zawieraniu umów handlowych oraz umów powierzenia przetwarzania danych osobowych związanych z nabywaniem produktów Wykonawcy zgodnie z § 4 ust.1:

TYTUL	IMIONA	NAZWISKO	STANOWISKO	TELEFON KOM.	E_MAIL	REPREZ_I_ODO	ADM_CHD	KOD_OSOBY

Legenda:
e-mail -indywidualny służbowy adres pracownika,
Reprez_I_ODO- osoba uprawniona do reprezentowania Zamawiającego przy zawieraniu umów handlowych i umów powierzenia przetwarzania danych osobowych (wartości: TAK/NIE),
Adm_CHD- osoba uprawniona do administrowania w imieniu Zamawiającego użytkownikami CHD uprawnionymi do rejestrowania i obsługi zgłoszeń, koordynowania obsługi zgłoszeń i udostępniania baz danych dla systemów dostarczanych przez Wykonawcę (wartości: TAK/NIE),
Kod_Osoby - identyfikator przydzielany przez administratora Systemu CHD po stronie Wykonawcy – przydziela Wykonawca.

Uwaga ! Ważne !
Bardzo prosimy o podanie indywidualnych służbowych adresów e-mail dla każdego pracownika zaangażowanego w przesyłanie zgłoszeń.
Maksymalnie można wskazać 2 osoby REPREZ_I_ODO.
Maksymalnie można wskazać 2 osoby ADM_CHD.
W przypadku zmian na liście osób upoważnionych do reprezentowania Zamawiającego i/lub osób upoważnionych REPREZ_i_ODO oraz ADM_CHD, Zamawiający ma obowiązek poinformować Wykonawcę poprzez przesłanie zaktualizowanego załącznika nr 2.

Zamawiający wyraża zgodę na przetwarzanie podanego powyżej Głównego adresu e-mail Zamawiającego przez …..... z siedzibą w …..... w celach marketingowych, w tym również w celu marketingu bezpośredniego oraz na doręczanie korespondencji za pomocą środków komunikacji elektronicznej w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.
Powyższa zgoda może być wycofana przez Zamawiającego w każdym czasie, w sposób wolny od opłat.

Załącznik nr 3 do Umowy nr FDZZ.226.18.2024
Zasady udzielenia zdalnego dostępu do zasobów

Niniejszy załącznik ustala zasady udzielenia Wykonawcy zdalnego dostępu do zasobów sieci teleinformatycznej Zamawiającego w celu umożliwienia Wykonawcy realizacji jego zobowiązań wynikających z Umowy.

§ 1. Udostępnienie

1. W celu realizacji usług, o których mowa w § 2 Umowy, zdalny dostęp zostanie udostępniony Wykonawcy przez Zamawiającego niezwłocznie na wezwanie Wykonawcy w terminie szczegółowo uzgodnionym przez Strony.
2. Bezpośredni dostęp do systemów Zamawiającego jest możliwy tylko i wyłącznie po udostępnieniu go przez administratora Zamawiającego i po przekazaniu wymaganych uprawnień i haseł.
3. Zamawiający zapewni sprawne działanie zdalnego dostępu.

§ 2. Zasady korzystania

1. Korzystając ze Zdalnego Dostępu Wykonawca:

a) będzie wykorzystywał Zdalny Dostęp wyłącznie w celu realizacji Umowy;

b) nie będzie pozyskiwał ani przetwarzał żadnych innych danych, za wyjątkiem danych niezbędnych do realizacji Umowy;

2. Wykonawca może wnioskować o dane logowania tylko i wyłącznie dla osób upoważnionych do przetwarzania danych osobowych, powierzonych do przetwarzania na potrzeby należytej realizacji Umowy.

3. Zabrania się Wykonawcy przekazywania danych logowania (login lub hasło) innym osobom niż osoby wskazane do realizacji Umowy.

4. Zdalny dostęp udostępnia się do realizacji usług wynikających z Umowy.

§ 3. Warunki Techniczne do uzyskania Zdalnego Dostępu

1. Zamawiający zapewni jeden z czterech rodzajów połączeń:

a) VPN – zapewni bezpieczny sposób komunikacji z siecią poprzez udostępnienie bezpiecznego kanału VPN;

b) Udostępnienie terminala – zapewni bezpieczny sposób komunikacji z siecią poprzez udostępnienie bezpiecznego terminala;

c) Udostępnienie portu do bazy danych – zapewni bezpieczny sposób komunikacji z siecią poprzez udostępnienie IP i portu pozwalającego na komunikację z bazą danych.

d) Udostępnienie dostępu poprzez aplikację Team Viewer lub Anydesk

2. Na wezwanie Wykonawcy, Zamawiający przekaże, osobie realizującej wynikające z zapisów Umowy prace, identyfikator użytkownika (login) wraz z innymi parametrami niezbędnymi do zestawienia zdalnego połączenia. Hasło zostanie przekazane bezpiecznym kanałem ustalonym przez strony. Użytkownicy po stronie Wykonawcy zobowiązują się do nie udostępniania tych identyfikatorów i haseł innym osobom oraz wykorzystywania dostępu wyłącznie w celu realizacji Umowy.

3. Wszystkie dane dotyczące parametrów logowania zostaną przekazane na indywidualne konta e-mail. Tą samą drogą dostarczone zostanie również oprogramowanie Klienta VPN lub klienta terminalowego. Oprogramowanie zostanie zainstalowane na komputerach użytkowników staraniem Wykonawcy. Parametry logowania mogą być także przekazane poprzez system CHD

Załącznik nr 4 do Umowy nr FDZZ.226.18.2024
UMOWA LICENCYJNA

Warunki licencji

<table>
<tr><td>A.</td><td>Licencjodawca</td><td colspan="4">.....</td></tr>
<tr><td>B.</td><td>Licencjobiorca</td><td colspan="4">Zespół Zakładów Opieki Zdrowotnej w Ostrowie Wielkopolskim, ul. Limanowskiego 20/22, NIP 622-22-56-387, REGON P-000314187</td></tr>
<tr><td>C.</td><td>Przedmiot umowy</td><td colspan="4">Licencjodawca udziela Licencjobiorcy niewyłącznej, nieograniczonej w czasie, odwołalnej, licencji na korzystanie z poszczególnych Modułów(1) Oprogramowania Aplikacyjnego określonych w pkt. E wyłącznie na terytorium Rzeczypospolitej Polskiej, na polach eksploatacji wymienionych w pkt. F
(1) Moduł - oznacz wyodrębniona poprzez udzielenie licencji część Oprogramowania Aplikacyjnego.</td></tr>
<tr><td>D.</td><td>Nadzór Autorski</td><td colspan="4">Oprogramowanie Aplikacyjne objęte jest do dnia …….. r. gwarancyjnym nadzorem autorskim Wykonawcy. W ramach gwarancyjnego nadzoru autorskiego Wykonawca zapewnia rozwój Oprogramowania Aplikacyjnego objętego niniejszą umową, zgodnie ze zmieniającymi się powszechnie obowiązującymi przepisami prawa oraz przepisami wewnętrznymi obowiązującymi Zamawiającego, wydanymi na podstawie upoważnienia ustawowego.</td></tr>
<tr><td rowspan="4">E.</td><td rowspan="4">Oprogramowanie Aplikacyjne</td><td>Lp.</td><td>Nazwa Modułu / Funkcjonalności i oznaczenie Oprogramowania Aplikacyjnego</td><td>Ilość Jednoczesnych Użytkowników(1) / Open(2)</td><td>Termin udzielenia licencji</td></tr>
<tr><td>1</td><td>Grafiki</td><td>Open</td><td rowspan="2">z dniem podpisania protokołu odbioru certyfikatów licencji</td></tr>
<tr><td>2</td><td>Interfejs integracji z RCP</td><td>1 System zew.</td></tr>
<tr><td colspan="4">* Użytkownik - oznacza osoby, upoważnione przez Licencjobiorcę do korzystania z Oprogramowania Aplikacyjnego, z zastrzeżeniem, że są to osoby realizujące czynności w ramach działalności Licencjobiorcy (wyłączone jest upoważnienie dla przedstawicieli innych firm, niewskazanych przez producenta)
(1) Jednoczesny Użytkownik – oznacza Użytkowników w tym samym momencie zalogowanych do danego Modułu Oprogramowania Aplikacyjnego, na jednej instalacji bazy danych Oprogramowania Aplikacyjnego.
(2) Licencja Open - oznacza możliwość korzystania z Oprogramowania Aplikacyjnego przez nieograniczoną ilość Jednoczesnych Użytkowników, w wielu Lokalizacjach.</td></tr>
<tr><td rowspan="5">F.</td><td rowspan="5">Pola eksploatacji</td><td colspan="3">Zwielokrotnienie Modułów Oprogramowania Aplikacyjnego w pamięci, serwerów, komputerów oraz urządzeń mobilnych.</td><td>Tak</td></tr>
<tr><td colspan="3">Korzystanie z Modułów Oprogramowania Aplikacyjnego przez liczbę Jednoczesnych Użytkowników określonych dla każdego Modułu w pkt. E.</td><td>Tak</td></tr>
<tr><td colspan="3">Instalacja na serwerze sieciowym Licencjobiorcy z udostępnieniem dla ilości Jednoczesnych Użytkowników określonych w pkt. E dla każdego Modułu Oprogramowania Aplikacyjnego.</td><td>Tak</td></tr>
<tr><td colspan="3">Sporządzenie 1 kopii zapasowej (-ych) każdego nośnika Oprogramowania Aplikacyjnego.</td><td>Tak</td></tr>
<tr><td colspan="3">Korzystanie z Oprogramowania Aplikacyjnego wyłącznie przez Jednoczesnych Użytkowników, zalogowanych na jednej instalacji bazy danych Oprogramowania Aplikacyjnego.</td><td>Tak</td></tr>
<tr><td>G.</td><td>Czas eksploatacji</td><td colspan="4">Nieoznaczony</td></tr>
</table>

H.	Postanowienia Dodatkowe	Sublicencja	Niedopuszczalna
		Przeniesienie licencji	Niedopuszczalne
I.	Zobowiązanie Licencjobiorcy	Licencjobiorca zobowiązuje się zorganizować i utrzymywać środki bezpieczeństwa zapobiegające jakiemukolwiek nieautoryzowanemu wykorzystaniu Oprogramowania Aplikacyjnego wskazanego w pkt. E niniejszej umowy.	
		Korzystanie z Oprogramowania Aplikacyjnego przez Jednoczesnych Użytkowników w więcej niż jednej instalacji bazy danych Oprogramowania Aplikacyjnego stanowi naruszenie warunków niniejszej umowy.	
		Korzystanie z Modułów Oprogramowania, na które została udzielona licencja, w więcej, aniżeli wskazane Lokalizacje, wymaga zapłaty wynagrodzenia za prawo korzystania z tych Modułów w kolejnych Lokalizacjach.	
		Licencjobiorca nie ma prawa do dokonywania modyfikacji, zmian układu czy jakichkolwiek zmian w Modułach Oprogramowania Aplikacyjnego, za wyjątkiem realizacji praw Licencjobiorcy przyznanych bezwzględnie obowiązującymi przepisami prawa. Zmodyfikowane przez Licencjobiorcę Moduły Oprogramowania Aplikacyjnego, w zakresie w jakim zostały zmodyfikowane, nie są objęte gwarancyjnym nadzorem autorskim Licencjodawcy.	
J.	Odpowiedzialność Licencjodawcy	Licencjobiorca zobowiązuje się zorganizować i utrzymywać środki bezpieczeństwa zapobiegające jakiemukolwiek nieautoryzowanemu wykorzystaniu Oprogramowania Aplikacyjnego wskazanego w pkt. E niniejszej umowy.	
		Licencjodawca nie odpowiada za szkody, jakie Licencjobiorca poniósł w związku z korzystaniem z Oprogramowania Aplikacyjnego, z wyjątkiem przypadków, gdy taką odpowiedzialność przewidują bezwzględnie obowiązujące przepisy prawa.	
		Licencjodawca nie ponosi odpowiedzialności za: a) skutki korzystania z Oprogramowania; b) treść i integralność (zawartość) danych, otrzymywanych i przechowywanych przez Licencjobiorcę; c) jakiekolwiek szkody wynikłe z nieprawidłowego działania lub zaprzestania funkcjonowania Oprogramowania Aplikacyjnego związane z nieprawidłowym korzystaniem z Oprogramowania Aplikacyjnego; d) korzystanie z Oprogramowania Aplikacyjnego przez osoby nieupoważnione; e) dokonywanie modyfikacji Oprogramowania Aplikacyjnego przez osoby inne niż upoważnione przez Licencjodawcę; f) udostępnienie hasła lub jakichkolwiek innych informacji identyfikujących użytkowników; g) wadliwe działanie sieci telekomunikacyjnej; h) nieprawidłowe działanie lub brak działania Oprogramowania Aplikacyjnego osób trzecich; i) nieautoryzowaną ingerencję Licencjobiorcy lub osób trzecich, w struktury baz danych Oprogramowania Aplikacyjnego; j) siłę wyższą	

		Odpowiedzialność odszkodowawcza Licencjodawcy ogranicza się do rzeczywistej straty, bez utraconych korzyści Licencjobiorcy. Odpowiedzialność odszkodowawcza Licencjodawcy ograniczona także jest do 20% wartości wynagrodzenia netto należnego Licencjodawcy z tytułu udzielenia licencji. Strony oświadczają, że wszelka odpowiedzialność Licencjodawcy z tytułu rękojmi za wady fizyczne na podstawie art. 55 ustawy o prawie autorskim i prawach pokrewnych jak i na podstawie jakiegokolwiek tytułu prawnego, ulega wyłączeniu.
K.	Rozwiązanie umowy licencyjnej	Licencjodawca może rozwiązać niniejszą umowę licencyjną bez zachowania terminów wypowiedzenia, gdy Licencjobiorca: a) narusza warunki niniejszej umowy licencji w odniesieniu do miejsca, zakresu lub sposobu korzystania z każdego z Modułów Oprogramowania Aplikacyjnego lub jego części; b) uniemożliwia przedstawicielom Licencjodawcy sprawdzenie sposobu wykorzystywania Oprogramowania Aplikacyjnego; c) w inny sposób narusza warunki licencji, prawa autorskie do Oprogramowania Aplikacyjnego lub postanowienia niniejszej umowy. W terminie 14 dni od rozwiązania umowy, Licencjobiorca ma obowiązek zaprzestania korzystania z Oprogramowania Aplikacyjnego - w tym celu Licencjobiorca ma obowiązek usunięcia Oprogramowania Aplikacyjnego z serwerów oraz stacji roboczych, na których zostało ono zainstalowane. Art. 59 ustawy o prawie autorskim i prawach pokrewnych nie stosuje się.
L.	Postanowienia końcowe	W zakresie nieuregulowanym niniejszą umową zastosowanie mają przepisy prawa polskiego w szczególności przepisy Kodeksu cywilnego i Ustawy z 4 lutego 1994 o prawie autorskim i prawach pokrewnych (t. jedn. Dz.U.2016.666 z pózn. zm.).

……
w imieniu Licencjobiorcy

Załącznik nr 5 do Umowy nr FDZZ.226.18.2024

Lista głównych rozwiązań technicznych i organizacyjnych, zapewniających bezpieczne i prawidłowe wykonywanie czynności oraz ochronę techniczną tajemnicy prawnie chronionej, w szczególności ochronę danych osobowych i tajemnicy bankowej.

I. ŚRODKI ORGANIZACYJNE:

1) Została opracowana i wdrożona polityka bezpieczeństwa;
2) Organizowane są cykliczne szkolenia dla pracowników/współpracowników z zasad bezpieczeństwa informacji, cyberbezpieczeństwa oraz ochrony danych osobowych;
3) Realizowany jest zatwierdzony program podnoszenia świadomości z zakresu bezpieczeństwa informacji (szkolenia adaptacyjne, e-learning, pigułki wiedzy, szkolenia dedykowane, artykuły, symulowane ataki);
4) Oświadczenia do zachowania w poufności wszelkich informacji stanowiących tajemnicę przedsiębiorstwa są podpisywane przez pracowników/współpracowników przed rozpoczęciem pracy w organizacji;
5) Do przetwarzania informacji zostały dopuszczone wyłącznie uprawnione osoby;
6) Dane są klasyfikowane zgodnie z wytycznymi spółki. Klasyfikacja wspierana jest narzędziowo. Informację sklasyfikowane jako poufne podlegają dodatkowej ochronie wykorzystując mechanizmy szyfrujące;
7) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
8) Stosuje się politykę czystego biurka oraz czystego ekranu (blokowanie komputerów przy pustych stanowiskach, niepozostawanie dokumentacji na biurkach, zamykanie szafek z dokumentacją, itd.);
9) Realizowane są regularne audyty\kontrole bezpieczeństwa przetwarzania informacji;
10) Wdrożono skuteczny proces zgłaszania oraz obsługi zdarzeń/incydentów związanych z naruszeniem bezpieczeństwa informacji w tym naruszeniem ochrony danych osobowych;
11) Zdefiniowano i stosowana jest polityka kontroli dostęp do informacji. Przydzielanie uprawnień do informacji oraz ich modyfikacje realizowane są w oparciu o zasady minimalnych uprawnień i wiedzy koniecznej na postawie udokumentowanych wniosków dostępowych;
12) Utworzono i uruchomiono jednostkę SOC (Security Operation Center) pracującą w trybie 24/7/365 w celu monitorowania infrastruktury i reagowania na incydenty cyberbezpieczeństwa;
13) Opracowano i wdrożono wewnętrzne standardy bezpieczeństwa wymagające stosowania zabezpieczeń adekwatnych do stopnia krytyczności i wrażliwości aktywów informacyjnych;
14) Zidentyfikowano krytyczne procesy i usługi oraz opracowano dla nich plany ciągłości działania oraz plany awaryjne w celu zapewnia zdolności do szybkiego przywrócenia dostępności danych wrażliwych i dostępu do nich i usług krytycznych w razie incydentu fizycznego lub technicznego;
15) Wprowadzono do stosowania politykę prywatności: Polityka prywatności - Asseco Poland
16) Wprowadzono zasady bezpiecznej pracy zdalnej.

II. ŚRODKI OCHRONY TECHNICZNEJ DANYCH:

1) Stosowane są mechanizmy ochrony kont użytkowników identyfikujące podejrzane aktywności na ich kontach;
2) Logowanie do krytycznych usług realizowane jest z zastosowaniem dwuskładnikowego logowania;
3) Dostęp do informacji oraz systemu operacyjnego komputera, w którym przetwarzane są informacje sklasyfikowane jako poufne (np. dane osobowe),, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. Stosowana

jest silna polityka haseł dostępowych;

4) Komputery, na których dochodzi do przetwarzania danych:
   a) pracują pod kontrolą aktualnego, wspieranego przez producenta systemu operacyjnego,
   b) posiadają uruchomioną systemową zaporę sieciową,
   c) posiadają aktualne systemy do ochrony przed złośliwym oprogramowaniem klasy EDR,
   d) posiadają zaszyfrowane dyski twarde, przy pomocy silnych protokołów szyfrujących,
   e) posiadają wygaszacze ekranów zabezpieczone hasłem.
   f) są centralnie nadzorowane i konfigurowane przez organizację (SOC+SIEM).
5) Stosowane są rozwiązanie do automatyzacji konfiguracji i zabezpieczania stacji roboczych oraz mechanizmy identyfikujące stacje niezgodne z przyjętymi standardami bezpieczeństwa;
6) Urządzenia mobilne (smartfon, tablet), na których dochodzi do przetwarzania informacji:
   a) pracują pod kontrolą aktualnego, wspieranego przez producenta systemu operacyjnego,
   b) posiadają zaszyfrowaną pamięć urządzenia,
   c) posiadają blokadę dostępu zabezpieczoną trudnym do odgadnięcia hasłem (litery i cyfry - najmniej 6 znaków), kodem PIN (minimum 6 cyfr), wzorem graficznym (minimum 6 znaków) lub zabezpieczeniem biometrycznym,
   d) posiadają automatyczną blokadę dostępu do urządzenia po czasie nie dłuższym niż 1 minuta.
7) Dane sklasyfikowane jako poufne są w sposób automatyczny szyfrowane i ograniczone w dostępie z wykorzystaniem dedykowanego rozwiązania do klasyfikacji i ochrony informacji;
8) W uzasadnionych przypadkach stosowane są nośniki wymienne, które są szyfrowane (pendrive, CD/DVD, dysk zewnętrzny, itp.);
9) Informacje utrwalone w formie papierowej przechowywane są w zamknięciu;
10) Stosowany jest proces bezpiecznego niszczenia nośników informacji oparty na normie DIN 66399. Po ustaniu przydatności dokumentacja papierowa, magnetyczne dyski twarde oraz optyczne i elektroniczne nośniki danych podlegają procesowi bezpiecznego zniszczenia;
11) Zastosowano system rejestracji dostępu do systemu/bazy danych oraz użycia;
12) Stosowany jest system Web Application Firewall do ochrony krytycznych aktywów informacyjnych Spółki;
13) Zastosowano system Firewall do ochrony dostępu do sieci komputerowej;
14) Stosowane jest szyfrowanie komunikacji zewnętrznej oraz wewnętrznej przy pomocy silnych protokołów szyfrujących;
15) Identyfikowane są podatności systemów informatycznych. Ustalono proces zarządzania podatnościami technicznymi. Ustalono czasy remediacji podatności oraz ścieżki raportowania i eskalacji o przekroczeniach.
16) Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii informacji wrażliwych;
17) Zastosowano narzędzia klasy EDR (Endpoint Detection and Response – EDR) w celu wykrywania i reagowania na podejrzane aktywności urządzeń końcowych.

III. ŚRODKI OCHRONY FIZYCZNEJ DANYCH DLA OBIEKTÓW BIUROWYCH ASSECO:

1) Dostęp do pomieszczeń objęty jest systemem kontroli dostępu. Dostęp do stref Data Center mają tylko upoważnieni pracownicy Asseco Poland, którzy świadczą bezpośrednio usługi utrzymania systemów w Data Center.
2) Pomieszczenia, w którym przetwarzane są informacje wyposażone są w system alarmowy przeciwwłamaniowy,
3) Dostęp do pomieszczeń, w których przetwarzane są informacje, kontrolowany jest przez system monitoringu z zastosowaniem kamer,
4) Dostęp do pomieszczeń, jest nadzorowany przez służbę ochrony. Funkcjonuje ochrona

fizyczna obiektów Data Center w postaci koncesjonowanej służby ochrony. Uruchomiony jest elektroniczny monitoring wideo obiektów i stref bezpieczeństwa w obiektach, w trybie 24/365.

5) Zastosowano procedury zarządzania dostępem gości.