



25 lat

Agencja Restrukturyzacji
i Modernizacji Rolnictwa

Al. Jana Pawła II 70, 00-175 Warszawa

Adres korespondencyjny:

**Agencja Restrukturyzacji i Modernizacji Rolnictwa
ul. Poleczki 33
02-822 Warszawa**

numer referencyjny sprawy: DPiZP.2610.38.2019

**Specyfikacja Istotnych
Warunków Zamówienia**

w postępowaniu o udzielenie zamówienia publicznego
o wartości powyżej 144 000 €
prowadzonym w trybie przetargu nieograniczonego

na:

**„Zakup i wdrożenie 2 szt. urządzeń Load Balancer wraz z gwarancją
i konsultacjami”**

wszczętym na podstawie ustawy z dnia 29 stycznia 2004 r.
- Prawo zamówień publicznych (tj.: Dz. U. z 2019 r. poz. 1843)

INFORMACJE OGÓLNE DOTYCZĄCE PROWADZONEGO POSTĘPOWANIA

1. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w języku polskim. Komunikacja między Zamawiającym a Wykonawcami w niniejszym postępowaniu odbywa się przy użyciu środków komunikacji elektronicznej, tj. „Platformy Zakupowej” dostępnej pod adresem <https://platformazakupowa.pl/pn/arimr> (dalej: „Platforma Zakupowa”).
2. Informacje i dokumenty związane z przedmiotowym postępowaniem zostały zamieszczone w zakładce „Postępowania”. W celu zapoznania się z zamieszczonymi informacjami lub dokumentami należy przejść na formularz postępowania.
3. Poniżej Zamawiający przedstawia wymagania techniczno-organizacyjne związane z udziałem Wykonawców w postępowaniu o udzielenie zamówienia publicznego:
 - 1) Złożenie oferty możliwe jest przez Wykonawców, którzy posiadają konto na Platformie Zakupowej oraz przez Wykonawców nie posiadających konta na Platformie Zakupowej. W celu założenia konta na Platformie Zakupowej należy wybrać zakładkę „Zaloguj się” w kolejnym kroku należy wybrać „Założ konto”, następnie należy wypełnić formularze i postępować zgodnie z poleceniami wyświetlającymi się na ekranie monitora. W przypadku Wykonawców niezalogowanych w celu złożenia oferty niezbędne jest podanie adresu e-mail (na który wysłane będzie potwierdzenie złożenia oferty), nr NIP oraz nazwy firmy, nieobowiązkowo nr telefonu.
 - 2) Złożenie oferty oraz oświadczenia, o którym mowa w art. 25a z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (tj.: Dz. U. z 2018 r. poz. 1986 z późn. zm.; dalej: „ustawa”), w tym Jednolitego Europejskiego Dokumentu Zamówienia składanych w trakcie toczącego się postępowania wymaga od Wykonawcy posiadania kwalifikowanego podpisu elektronicznego.
 - 3) Wykonawca składa ofertę, która w przypadku prawidłowego złożenia oferty zostaje automatycznie zaszyfrowana przez system. Nie jest możliwe zapoznanie się z treścią złożonej oferty przed upływem terminu otwarcia ofert.
 - 4) Podpisanie dokumentów w formie skompresowanej poprzez opatrzenie całego pliku jednym podpisem kwalifikowanym jest równoznaczne z poświadczaniem za zgodność z oryginałem wszystkich elektronicznych kopii dokumentów. Dokumenty, co do których wymagana jest forma oryginału, muszą zostać podpisane indywidualnie (każdy z nich) kwalifikowanym podpisem elektronicznym. Podpisanie skompresowanego pliku, w którym umieszczono dokument w formie oryginału nie stanowi podpisania tego dokumentu.
4. Zamawiający, zgodnie z § 3 ust. 3 Rozporządzenia Prezesa Rady Ministrów w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępnienia i przechowywania dokumentów elektronicznych (Dz. U. z 2017 r. poz. 1320; dalej: „Rozporządzenie w sprawie środków komunikacji”), określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na Platformie Zakupowej, tj.:
 - 1) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
 - 2) komputer klasy PC lub MAC, o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10.4, Linux, lub ich nowsze wersje,
 - 3) zainstalowana dowolna przeglądarka internetowa; w przypadku Internet Explorer minimalnie wersja 10.0.,
 - 4) włączona obsługa JavaScript,
 - 5) zainstalowany program Adobe Acrobat Reader, lub inny obsługujący format plików .pdf.
5. Zamawiający, zgodnie z § 3 ust. 3 Rozporządzenia w sprawie środków komunikacji, określa dopuszczalne formaty przesyłanych danych, tj. plików o wielkości do 75 MB. Zalecany format: .pdf.
6. Zamawiający, zgodnie z § 3 ust. 3 Rozporządzenia w sprawie środków komunikacji, określa informacje na temat kodowania i czasu odbioru danych, tj.:
 - 1) Plik załączony przez Wykonawcę na Platformie Zakupowej i zapisany nie jest widoczny dla Zamawiającego, gdyż jest w systemie jako zaszyfrowany. Możliwość otworzenia pliku dostępna jest dopiero po odszyfrowaniu przez system, co następuje po terminie otwarcia ofert,
 - 2) Oznaczenie czasu odbioru danych przez Platformę stanowi przypiętą do oferty elektronicznej datę oraz dokładny czas (hh:mm:ss), znajdujące się w kolumnie dotyczącej danej oferty, w sekcji - "Data złożenia oferty".
7. Zamawiający, zgodnie z § 4 Rozporządzenia w sprawie środków komunikacji, określa dopuszczalny format kwalifikowanego podpisu elektronicznego jako:
 - 1) dokumenty w formacie .pdf zaleca się podpisywać formatem PAdES;
 - 2) dopuszcza się podpisanie dokumentów w formacie innym niż .pdf, wtedy zaleca się użyć formatu XAdES.
8. Wykonawca przystępując do niniejszego postępowania o udzielenie zamówienia publicznego, akceptuje warunki korzystania z Platformy Zakupowej, określone w Regulaminie zamieszczonym na stronie internetowej pod adresem <https://platformazakupowa.pl/pn/arimr> w zakładce „Regulamin” oraz uznaje go za wiążący.
9. Zamawiający informuje, że instrukcje korzystania z Platformy Zakupowej dotyczące w szczególności logowania, pobrania dokumentacji, składania wniosków o wyjaśnienie treści siwz, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu Platformy Zakupowej znajdują się w zakładce „Instrukcje dla Wykonawców” na stronie internetowej pod adresem <https://platformazakupowa.pl/pn/arimr>.
10. Korzystanie z Platformy Zakupowej jest bezpłatne. W celu ułatwienia Wykonawcom korzystania z Platformy Zakupowej operator platformy uruchomił Centrum Wsparcia Klienta, które służy pomocą techniczną od 7:00 do 17:00 od poniedziałku do piątku pod numerem telefonu 22 101 02 02 lub e-mai: cwk@platformazakupowa.pl

Rozdział I. Przedmiot zamówienia.**I.1. Opis przedmiotu zamówienia.**

1. Kod Wspólnego Słownika Zamówień (CPV).
Główny kod: 32420000 – 3 [Urządzenia sieciowe].
2. Przedmiotem zamówienia jest zakup wraz z dostawą 2 sztuk fabrycznie nowych, nienoszących śladów uprzedniego używania jednakowych urządzeń Load Balancer wraz z Oprogramowaniem, (dalej „Sprzęt IT”), spełniających co najmniej parametry i funkcjonalności określone w Załączniku nr 1 do wzoru umowy wraz z załącznikami, stanowiącej załącznik nr 6 do specyfikacji istotnych warunków zamówienia [dalej: siwz];
3. Zamawiający wymaga, aby wykonanie przedmiotu zamówienia nastąpiło na warunkach i zasadach określonych we wzorze Umowy wraz z załącznikami stanowiącym Załącznik nr 6 do siwz.

I.2. Opis części zamówienia.

Zamawiający nie dopuszcza składania przez Wykonawcę ofert częściowych w rozumieniu art. 2 pkt 6) ustawy.

I.3. Powierzenie Podwykonawcy wykonania części zamówienia.

1. Zamawiający dopuszcza powierzenie Podwykonawcom wykonania części zamówienia.
2. Wykonawca zobowiązany jest do wskazania w ofercie części zamówienia, której wykonanie zamierza powierzyć Podwykonawcy oraz do podania firm Podwykonawców.

I.4. Pozostałe istotne elementy związane z przedmiotem zamówienia.

1. Zamawiający nie przewiduje udzielenia zamówień, o których mowa w art. 67 ust. 1 pkt 7) ustawy.
2. Zamawiający nie dopuszcza składania ofert wariantowych w rozumieniu art. 2 pkt 7) ustawy.
3. Zamawiający nie przewiduje zawarcia umowy ramowej na podstawie art. 99 ustawy, jak również nie przewiduje przeprowadzenia aukcji elektronicznej.
4. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
5. Wszelkie rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).

Rozdział II. Termin wykonania zamówienia.

Zamawiający wymaga realizacji zamówienia w następujących terminach:

1. Zamawiający wymaga dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów oraz Wdrożenia w lokalizacjach COPD (Centralne Ośrodki Przetwarzania Danych Zamawiającego) nie później niż w terminie do 20 Dni Roboczych od dnia zawarcia Umowy.
2. Zamawiający wymaga świadczenia konsultacji technicznych w okresie 36 miesięcy od dnia zawarcia Umowy.

Rozdział III. Warunki udziału w postępowaniu oraz podstawy wykluczenia.

1. O zamówienie mogą ubiegać się Wykonawcy, którzy:
 - 1.1. Nie podlegają wykluczeniu z postępowania na podstawie art. 24 ust. 1 pkt 12 – 23 ustawy oraz art. 24 ust. 5 ustawy;
 - 1.2. Spełniają warunki udziału w postępowaniu w zakresie zdolności zawodowej. Zamawiający uzna, że Wykonawca spełnia warunek udziału we wskazanym zakresie, jeżeli Wykonawca wykaże, że:
 - 1.2.1. wykonał, w okresie ostatnich trzech (3) lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, co najmniej 2 (dwie) dostawy urządzeń typu Load Balancer, wraz z wdrożeniem, o wartości każdej z nich nie mniejszej niż 300 000,00 zł brutto (słownie: trzysta tysięcy złotych 00/100).

UWAGA 1

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

1.2.2. dysponuje następującymi osobami, które zostaną skierowane przez Wykonawcę do realizacji zamówienia, legitymującymi się odpowiednimi kwalifikacjami zawodowymi, wykształceniem i doświadczeniem niezbędnymi do wykonania zamówienia, tj.: dysponuje **co najmniej jedną osobą, która posiada:**

- 1.2.2.1. co najmniej 12 miesięczne doświadczenie przy realizacji zamówień o zakresie jak w pkt 1.2.1. z wyłączeniem wartości zamówień;
- 1.2.2.2. certyfikat F5 Certified Solutions Expert Security lub równoważny.

UWAGA 2

Przez certyfikat równoważny, o którym mowa powyżej Zamawiający rozumie certyfikat, który:

- 1) jest analogiczny co do zakresu z przykładowym certyfikatem wskazanym z nazwy dla danej roli, co jest rozumiane jako:
 - a) analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat,
 - b) analogiczny stopień poziomu kompetencji,
 - c) analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu,
- 2) potwierdzony jest egzaminem (dotyczy tylko tych ról, których przykładowe certyfikaty muszą być potwierdzone egzaminem).

UWAGA 3

Zamawiający wymaga, aby Wdrożenie objęte przedmiotem zamówienia odbywało się co najmniej przez osobę wykazaną przez Wykonawcę na potwierdzenie spełnienia opisanego przez Zamawiającego warunku udziału w postępowaniu w zakresie dysponowania osobami zdolnymi do realizacji zamówienia

UWAGA 4

W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia:

- 1) brak podstaw wykluczenia, o których mowa w pkt 1.1 musi spełniać każdy Wykonawca z osobna,
 - 2) warunki udziału w postępowaniu określone w pkt 1.2 musi spełniać co najmniej jeden Wykonawca lub wszyscy Wykonawcy łącznie.
2. Ocena spełniania ww. warunków dokonana zostanie w oparciu o informacje zawarte we właściwych dokumentach wyszczególnionych w Rozdziale IV niniejszej SIWZ. Z treści załączonych dokumentów musi wynikać jednoznacznie, iż ww. warunki Wykonawca spełnił.
 3. Jeżeli Wykonawca nie złożył oświadczenia, o którym mowa w art. 25a ust. 1 ustawy, oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy, lub innych dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, Zamawiający wzywa do ich złożenia, uzupełnienia lub poprawienia lub do udzielania wyjaśnień w terminie przez siebie wskazanym, chyba że mimo ich złożenia, uzupełnienia lub poprawienia lub udzielenia wyjaśnień oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.
 4. Jeżeli Wykonawca nie złożył wymaganych pełnomocnictw albo złożył wadliwe pełnomocnictwa, Zamawiający wzywa do ich złożenia w terminie przez siebie wskazanym, chyba że mimo ich złożenia oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.
 5. Z postępowania o udzielenie zamówienia Zamawiający wykluczy Wykonawcę:
 - 5.1. na podstawie art. 24 ust. 1 pkt 12 – 23 ustawy,
 - 5.2. na podstawie art. 24 ust. 5 ustawy, tj.:
 - 5.2.1. art. 24 ust. 5 pkt 1 ustawy, tj. Wykonawcę w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz. U. z 2017 r. poz. 1508 ze zm.) lub którego upadłość ogłoszono, z wyjątkiem Wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (Dz. U. z 2017 r. poz. 2344 z późn. zm.),
 - 5.2.2. art. 24 ust. 5 pkt 2 ustawy, tj. Wykonawcę który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy Wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych,
 - 5.2.3. art. 24 ust. 5 pkt 3 ustawy, tj. jeżeli Wykonawca lub osoby, o których mowa w art. 24 ust. 1 pkt 14 ustawy, uprawnione do reprezentowania Wykonawcy pozostają w relacjach określonych w art. 17 ust. 1 pkt 2 – 4 ustawy z:
 - 5.2.3.1. Zamawiającym,
 - 5.2.3.2. osobami uprawnionymi do reprezentowania Zamawiającego,
 - 5.2.3.3. członkami komisji przetargowej,
 - 5.2.3.4. osobami, które złożyły oświadczenie, o których mowa w art. 17 ust. 2a ustawy,
 - chyba że jest możliwe zapewnienie bezstronności po stronie Zamawiającego w inny sposób niż przez wykluczenie Wykonawcy z udziału w postępowaniu;
 - 5.2.4. art. 24 ust. 5 pkt 4 ustawy, tj. Wykonawcę który, z przyczyn leżących po jego stronie, nie wykonał albo nienależycie wykonał w istotnym stopniu wcześniejszą umowę w sprawie zamówienia publicznego lub umowę koncesji, zawartą z zamawiającym, o którym mowa w art. 3 ust. 1 pkt 1–4 ustawy, co doprowadziło do rozwiązania umowy lub zasądzenia odszkodowania,
 - 5.2.5. art. 24 ust. 5 pkt 5 ustawy, tj. Wykonawcę będącego osobą fizyczną, którego prawomocnie skazano za wykroczenie przeciwko prawom pracownika lub wykroczenie przeciwko środowisku, jeżeli za jego popełnienie wymierzono karę aresztu, ograniczenia wolności lub karę grzywny nie niższą niż 3 000 złotych,
 - 5.2.6. art. 24 ust. 5 pkt 6 ustawy, tj. Wykonawcę, jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za wykroczenie przeciwko prawom pracownika lub wykroczenie przeciwko środowisku, jeżeli za jego popełnienie wymierzono karę aresztu, ograniczenia wolności lub karę grzywny nie niższą niż 3 000 złotych,
 - 5.2.7. art. 24 ust. 5 pkt 7 ustawy, tj. Wykonawcę, wobec którego wydano ostateczną decyzję administracyjną o naruszeniu obowiązków wynikających z przepisów prawa pracy, prawa ochrony środowiska lub przepisów o zabezpieczeniu społecznym, jeżeli wymierzono tą decyzją karę pieniężną nie niższą niż 3 000 złotych,
 - 5.2.8. art. 24 ust. 5 pkt 8 ustawy, tj. Wykonawcę który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych, z wyjątkiem przypadku, o którym mowa w ust. 1 pkt 15 ustawy, chyba że Wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności.
 6. Wykonawca jest zobowiązany wykazać, że spełnia warunki udziału w postępowaniu i nie podlega wykluczeniu z postępowania.
 7. Zamawiający informuje, że zgodnie z procedurą wskazaną w art. 24aa ustawy, najpierw dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza (na podstawie kryteriów oceny ofert określonych w SIWZ) nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

Rozdział IV. Zawartość ofert, wykaz oświadczeń lub dokumentów potwierdzających brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu.

W zakresie nieuregulowanym postanowieniami SIWZ zastosowanie mają przepisy rozporządzenia Ministra Rozwoju z dnia 26 lipca 2016r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz. U. z 2016 r. poz. 1126 ze zm. dalej: „Rozporządzenie w sprawie rodzajów dokumentów”).

IV.1. Zawartość ofert.

1. Ofertę należy złożyć pod rygorem nieważności w postaci elektronicznej, podpisaną kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Wykonawca składa ofertę na Formularzu Ofertowym (wg Załącznika nr 1 do SIWZ) za pośrednictwem Platformy Zakupowej.
2. Wykonawca obowiązany jest złożyć wraz z ofertą następujące dokumenty:
 - 2.1. Pełnomocnictwo do podpisania oferty pod rygorem nieważności w postaci elektronicznej, opatrzone kwalifikowanym podpisem elektronicznym przez osobę/y upoważnione do reprezentacji wskazane we właściwym rejestrze, jeżeli oferta nie została podpisana przez osoby upoważnione do tych czynności dokumentem rejestracyjnym. Zamawiający dopuszcza złożenie elektronicznej kopii pełnomocnictwa poświadczonej przez notariusza.
 - 2.2. Dowód wniesienia wadium - dokument wadium, oryginał gwarancji/poręczenia, jeżeli Wykonawca wnosi wadium w innej formie niż pieniądź opatrzone kwalifikowanym podpisem elektronicznym osób upoważnionych do jego wystawienia (wystawców dokumentu). W przypadku wniesienia wadium w innej formie niż pieniądź, powinno ono obowiązywać przez cały okres związania ofertą.
 - 2.3. Zobowiązanie podmiotu trzeciego lub inny dokument potwierdzający, że Wykonawca będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia, jeżeli Wykonawca powołuje się na zasoby innych podmiotów. Zobowiązanie należy złożyć pod rygorem nieważności w postaci elektronicznej, podpisane kwalifikowanym podpisem elektronicznym przez osobę upoważnioną do reprezentacji wskazane we właściwym rejestrze. Zapisy Rozdziału IV.5 SIWZ stosuje się odpowiednio.
 - 2.4. Aktualne na dzień składania ofert oświadczenie w formie jednolitego europejskiego dokumentu zamówienia (dalej: „JEDZ”) sporządzone zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji Europejskiej wydanym na podstawie art. 59 ust. 2 Dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE. Dokument JEDZ należy złożyć pod rygorem nieważności w postaci elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym.
 - 2.5. Ogólnodostępny dokument producenta lub wyciąg z tego dokumentu, wraz ze wskazaniem dokładnego miejsca w dokumencie potwierdzającego spełnianie wymagań określonych w Rozdziale XI, pkt 1.4 SIWZ i oferowanych przez wykonawcę w Tabeli nr 2 Formularza ofertowego, jeżeli wykonawca oferuje dodatkowe parametry techniczne punktowane w ramach kryterium oceny ofert „Parametry techniczne Sprzętu IT”.

IV.2 Oświadczenie w formie Jednolitego Europejskiego Dokumentu Zamówienia.

1. Wykonawca wypełnia JEDZ, tworząc dokument w postaci elektronicznej. Wykonawca może korzystać z narzędzia ESPD lub innych dostępnych narzędzi lub oprogramowania, które umożliwiają wypełnienie JEDZ i utworzenie dokumentu w postaci elektronicznej.
 - 1.1. Zamawiający udostępnił Wykonawcom plik, w formacie xml, wygenerowany z narzędzia ESPD, który stanowi Załącznik nr 7 do SIWZ.
 - 1.2. Zamawiający informuje, że pod adresem: <https://espd.uzp.gov.pl> Urząd Zamówień Publicznych udostępnił nieodpłatne narzędzie umożliwiające zamawiającym i wykonawcom utworzenie, wypełnienie i ponowne wykorzystanie standardowego formularza JEDZ (JEDZ/ESPD) w wersji elektronicznej (eESPD).
2. Oświadczenia podmiotów składających ofertę wspólnie oraz podmiotów udostępniających potencjał składane na formularzu JEDZ muszą mieć formę dokumentu w postaci elektronicznej podpisanego kwalifikowanym podpisem elektronicznym przez każdy z tych podmiotów w zakresie w jakim potwierdzają okoliczności, o których mowa w treści art. 22 ust. 1 ustawy.
3. Środkiem komunikacji elektronicznej, służącym złożeniu JEDZ przez Wykonawcę, jest Platforma Zakupowa.
4. Dokument elektroniczny JEDZ należy złożyć w formacie .pdf).
5. Obowiązek złożenia JEDZ w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym w sposób określony powyżej dotyczy również JEDZ składanego na wezwanie w trybie art. 26 ust. 3 ustawy; W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenie o którym mowa w Rozdziale IV.1. pkt 2.4. SIWZ składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Dokumenty te potwierdzają spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.
6. Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania, w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu składa także oświadczenia JEDZ, o którym mowa w Rozdziale IV.1. pkt 2.4. SIWZ, dotyczące tych podmiotów.

IV.3. Oświadczenia lub dokumenty, potwierdzające spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.

1. Wykonawca obowiązany jest w terminie 3 dni od dnia zamieszczenia na stronie internetowej Zamawiającego (Platformie Zakupowej) - www.platformazakupowa.pl/pn/arimr informacji, o których mowa w art. 86 ust. 5 ustawy, do przekazania Zamawiającemu oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy. Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia. Wzór oświadczenia stanowi Załącznik nr 3 do SIWZ.

2. Zamawiający przed udzieleniem zamówienia wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia za pośrednictwem Platformy Zakupowej, w wyznaczonym, nie krótszym niż 10 dni, terminie aktualnych na dzień złożenia oświadczeń lub dokumentów podpisanych kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności w poniższym zakresie:
 - 2.1. braku podstaw wykluczenia Wykonawcy z postępowania o udzielenie zamówienia:
 - 2.1.1. informacji z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy oraz, odnośnie skazania za wykroczenie na karę aresztu, w zakresie określonym przez zamawiającego na podstawie art. 24 ust. 5 pkt 5 i 6 ustawy, wystawionej nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert,
 - 2.1.2. zaświadczenia właściwego naczelnika urzędu skarbowego potwierdzającego, że Wykonawca nie zalega z opłacaniem podatków, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że Wykonawca zawarł porozumienie z właściwym organem podatkowym w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu,
 - 2.1.3. zaświadczenia właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego albo innego dokumentu potwierdzającego, że Wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że Wykonawca zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu,
 - 2.1.4. odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt 1 ustawy,
 - 2.1.5. oświadczenia Wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne albo – w przypadku wydania takiego wyroku lub decyzji – dokumentów potwierdzających dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności,
 - 2.1.6. oświadczenia Wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne,
 - 2.1.7. oświadczenia Wykonawcy o niezaleganiu z opłacaniem podatków i opłat lokalnych, o których mowa w ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz. U. z 2018 r. poz. 1445 z późn. zm.),
 - 2.1.8. oświadczenia Wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu skazującego za wykroczenie na karę ograniczenia wolności lub grzywny w zakresie określonym w art. 24 ust. 5 pkt 5 i 6 ustawy,
 - 2.1.9. oświadczenia Wykonawcy o braku wydania wobec niego ostatecznej decyzji administracyjnej o naruszeniu obowiązków wynikających z przepisów prawa pracy, prawa ochrony środowiska lub przepisów o zabezpieczeniu społecznym w zakresie określonym w art. 24 ust. 5 pkt 7 ustawy.
 - 2.2. potwierdzenia spełniania warunków udziału w postępowaniu dotyczących zdolności zawodowej:
 - 2.2.1. wykazu dostaw wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane, oraz załączeniem dowodów określających czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy; w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert. Wzór oświadczenia stanowi Załącznik nr 4 do SIWZ.
 - 2.2.2. wykazu osób, skierowanych przez Wykonawcę do realizacji zamówienia publicznego wraz z informacjami na temat ich kwalifikacji zawodowych niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami. Wzór oświadczenia stanowi Załącznik nr 5 do SIWZ.
 - 2.3. potwierdzenia spełniania przez oferowane dostawy wymagań:
 - 2.3.1. ogólnodostępnego dokumentu producenta lub wyciągu z tego dokumentu, wraz ze wskazaniem dokładnego miejsca w dokumencie potwierdzającego spełnianie wymagań dla każdego z parametrów **określonych w załączniku nr 1 do wzoru Umowy**.
3. Wykonawca mający siedzibę na terytorium Rzeczypospolitej Polskiej, w odniesieniu do osoby mającej miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, której dotyczy dokument wskazany w Rozdziale IV.3 pkt 2.1.1 SIWZ, składa na Platformie Zakupowej, podpisany kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności dokument, o którym mowa w Rozdziale IV.4 pkt 1.1 SIWZ, w zakresie określonym w art. 24 ust. 1 pkt 14 i 21 oraz ust. 5 pkt 6 ustawy. Jeżeli w kraju, w którym miejsce zamieszkania ma osoba, której dokument miał dotyczyć, nie wydaje się takich dokumentów, zastępuje się go dokumentem zawierającym oświadczenie tej osoby złożonym przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na miejsce zamieszkania tej osoby. Postanowienia Rozdziału IV.4 pkt 2 SIWZ zdanie pierwsze stosuje się.
4. Jeżeli treść informacji przekazanych przez Wykonawcę w JEDZ odpowiada zakresowi informacji, których Zamawiający wymaga poprzez żądanie dokumentów, w szczególności o których mowa w pkt 2.2, Zamawiający zastrzega sobie prawo do odstąpienia od żądania tych dokumentów od Wykonawcy. W takim przypadku dowodem spełniania przez Wykonawcę warunków udziału w

postępowaniu oraz braku podstaw wykluczenia są odpowiednie informacje przekazane przez Wykonawcę lub odpowiednio przez podmioty, na których zdolnościach lub sytuacji Wykonawca polega na zasadach określonych w art. 22a ustawy, w JEDZ.

IV.4. Dokumenty składane przez Wykonawców mających siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej.

1. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentów, o których mowa w Rozdziale:
 - 1.1. IV.3 pkt 2.1.1 SIWZ – składa informację z odpowiedniego rejestru albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument, w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 oraz ust. 5 pkt 5 i 6 ustawy,
 - 1.2. IV.3 pkt 2.1.2 – 2.1.4 SIWZ – składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:
 - 1.2.1. nie zalega z opłacaniem podatków, opłat, składek na ubezpieczenie społeczne lub zdrowotne albo że zawarł porozumienie z właściwym organem w sprawie spłat należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu,
 - 1.2.2. nie otwarto jego likwidacji ani nie ogłoszono upadłości.
2. Dokumenty, o których mowa w pkt 1.1 oraz 1.2.2, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert. Dokument, o którym mowa w pkt 1.2.1, powinien być wystawiony nie wcześniej niż 3 miesiące przed upływem tego terminu.
3. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa w pkt 1, zastępuje się je dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy lub miejsce zamieszkania tej osoby. Postanowienia pkt 2 stosuje się.

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

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
2. Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.
3. W celu oceny, czy Wykonawca polegając na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a ustawy, będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia publicznego oraz oceny, czy stosunek łączący Wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów, Zamawiający żąda złożenia przez Wykonawcę dokumentów, które określają w szczególności:
 - 3.1. zakres dostępnych Wykonawcy zasobów innego podmiotu,
 - 3.2. sposób wykorzystania zasobów innego podmiotu, przez Wykonawcę, przy wykonywaniu zamówienia publicznego,
 - 3.3. zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia publicznego.
4. Zamawiający żąda od Wykonawcy, który polega na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a ustawy, przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych w Rozdziale IV.3 pkt 2.1.1 – 2.1.9 SIWZ.

IV.6. Klauzule informacyjne w zakresie danych osobowych.

1. W związku z treścią z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2.), dalej: „RODO” Zamawiający informuje, że:
 - 1.1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w toku postępowania jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, al. Jana Pawła II, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
 - 1.2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazanych w pkt 1.1.
 - 1.3. Pani/Pana dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu przeprowadzenia niniejszego postępowania o udzielenie zamówienia publicznego.
 - 1.4. Odbiorcami Pani/Pana danych osobowych mogą być:
 - 1.4.1. osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy,
 - 1.4.2. organy kontrolne,
 - 1.4.3. osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2018.1330 j.t.),

- 1.4.4. podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa.
- 1.5. Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do przeprowadzenia niniejszego postępowania. Ponadto, zgodnie z art. 97 ust. 1 ustawy przechowywane będą przez okres 4 lat od dnia zakończenia niniejszego postępowania. Okres przechowywania danych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora. Ponadto, okres przechowywania danych może zostać przedłużony na okres 5 lat, na potrzeby archiwizacji.
- 1.6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych.
- 1.7. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
- 1.8. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego, a konsekwencje niepodania określonych danych wynikają z ustawy.

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

1. Komunikacja między Zamawiającym, a Wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują wyłącznie za pośrednictwem Platformy Zakupowej, z zachowaniem formy elektronicznej. Za datę wpływu oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się ich datę wczytania do Platformy Zakupowej.
2. Postępowanie prowadzone jest pod numerem referencyjnym sprawy: **DPIZP.2610.38.2019**, Wykonawcy powinni we wszelkich kontaktach z Zamawiającym powoływać się na wskazany numer referencyjny.
3. Wykonawcy powinni kierować do Zamawiającego wszelką korespondencję z zachowaniem formy elektronicznej za pośrednictwem Platformy Zakupowej.
4. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści Specyfikacji istotnych warunków zamówienia (SIWZ). Wniosek należy przesłać za pośrednictwem Platformy Zakupowej. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 6 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SIWZ wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. Treść pytań (bez ujawnienia źródła) wraz z wyjaśnieniami bądź informacje o dokonaniu modyfikacji SIWZ, Zamawiający przekaze Wykonawcom za pośrednictwem Platformy Zakupowej.
5. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynął do Zamawiającego po upływie terminu jego składania, o którym mowa w pkt 4 lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.
6. W uzasadnionym przypadku Zamawiający może przed terminem składania ofert zmienić treść dokumentów składających się na niniejszą SIWZ.
7. Zamawiający nie zamierza zwoływać zebrania Wykonawców.
8. Osobami uprawnionymi ze strony Zamawiającego do kontaktów z Wykonawcami są:
 - 8.1. Pan Henryk Żywno, tel.: +48 22 595-00-67 w godz. 9.00 – 15.00.
 - 8.2. Pani Agnieszka Skarzyńska, tel.: +48 22 595-00-65 w godz. 9.00 – 15.00.

Rozdział VI. Wymagania dotyczące wadium.

1. Wykonawca zobowiązany jest wnieść wadium w wysokości: 20 000,00 zł (słownie: dwadzieścia tysięcy złotych zero groszy).
2. Wadium może być wniesione w:
 - 2.1. pieniądzu,
 - 2.2. poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że poręczenie kasy jest zawsze poręczeniem pieniężnym,
 - 2.3. gwarancjach bankowych,
 - 2.4. gwarancjach ubezpieczeniowych,
 - 2.5. poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (tj.: Dz. U. z 2018 r., poz. 110 z późn. zm.).
3. Wadium w formie pieniądza należy wnieść przelewem na rachunek bankowy w Banku Gospodarstwa Krajowego III Oddział w Warszawie numer rachunku - 45 1130 1062 8000 0000 0002 8175, z dopiskiem na przelewie: „wadium w postępowaniu na „Zakup i wdrożenie 2 szt. urządzeń Load Balancer wraz z gwarancją i konsultacjami”.
4. W przypadku wnoszenia wadium w innej formie niż pieniądź Wykonawca wnosi w formie elektronicznej poprzez wczytanie na Platformie Zakupowej oryginału dokumentu wadialnego tj. opatrzonego kwalifikowanym podpisem elektronicznym osób upoważnionych do jego wystawienia (wystawców dokumentu). Wadium powinno być oznaczone w następujący sposób: WADIUM – numer referencyjny i nazwa postępowania lub w inny sposób umożliwiający identyfikację postępowania, którego dotyczy.
5. Dokument wadium musi wyraźnie wskazywać na wszystkie okoliczności jego utraty określone w art. 46 ust. 4a i ust. 5 ustawy.
6. Z treści gwarancji/poręczenia powinno wynikać bezwarunkowe, na każde pisemne żądanie zgłoszone przez Zamawiającego, zobowiązanie Gwaranta do wypłaty Zamawiającemu pełnej kwoty wadium w okolicznościach określonych w art. 46 ust. 4a i ust. 5 ustawy.
7. Oferta Wykonawcy, który nie wnieśli wadium lub wnieśli je w sposób nieprawidłowy zostanie odrzucona.
8. W przypadku wniesienia wadium i niezłożenia oferty, Wykonawca jest zobowiązany złożyć do Zamawiającego wniosek o zwrot wadium.

Rozdział VII. Termin związania ofertą.

Wykonawcy pozostają związani złożoną ofertą przez 60 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

Rozdział VIII Opis sposobu przygotowywania ofert.**VIII.1. Przygotowanie ofert.**

1. Ofertę należy złożyć pod rygorem nieważności w postaci elektronicznej, podpisaną kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Wykonawca składa ofertę na Formularzu Ofertowym (wg Załącznika nr 1 do SIWZ). Oferta oraz dokumenty, co do których wymagana jest forma oryginału, muszą zostać podpisane indywidualnie (każdy z nich) kwalifikowanym podpisem elektronicznym (każdy plik osobno podpisany kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności).
2. Treść złożonej oferty musi odpowiadać treści niniejszej SIWZ. Wykonawca ma prawo złożyć tylko jedną ofertę. Oferta powinna być sporządzona w języku polskim, w postaci elektronicznej pod rygorem nieważności i podpisana kwalifikowanym podpisem elektronicznym wyłącznie za pośrednictwem Platformy Zakupowej.
3. Oferta powinna zawierać jedną, jednoznacznie opisaną propozycję.
4. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.
5. Zamawiający informuje, iż zgodnie z art. 96 ust. 3 ustawy oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeśli Wykonawca nie później niż w terminie składania ofert zastrzegł, że nie mogą one być udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji określonych w art. 86 ust. 4 ustawy, tj. nazwa (firma) Wykonawcy, adres Wykonawcy, informacje dotyczące ceny, terminu wykonania zamówienia, okresu gwarancji, warunków płatności zawarte w ofercie.

Uwaga: Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2018 r. poz. 419), które Wykonawca pragnie zastrzec jako tajemnicę przedsiębiorstwa, muszą zostać załączone na Platformie Zakupowej w osobnym pliku w miejscu właściwym dla informacji stanowiących tajemnicę przedsiębiorstwa.

6. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia, w takim przypadku:
 - 6.1. oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia musi być podpisana w taki sposób, by prawnie zobowiązywała wszystkich Wykonawców występujących wspólnie,
 - 6.2. każdy z Wykonawców wspólnie ubiegających się o udzielenie zamówienia musi udokumentować, że nie podlega wykluczeniu z postępowania na podstawie art. 24 ust. 1 pkt 12 – 23 oraz art. 24 ust. 5 ustawy, a także złożyć informację lub listę, o której mowa w Rozdziale IV.3 pkt 1 SIWZ,
 - 6.3. zgodnie z art. 23 ust. 2 ustawy muszą ustanowić pełnomocnika do reprezentowania ich w postępowaniu o udzielenie niniejszego zamówienia lub do reprezentowania ich w postępowaniu oraz zawarcia umowy o udzielenie przedmiotowego zamówienia publicznego,
 - 6.4. wszelka korespondencja oraz rozliczenia dokonywane będą wyłącznie z pełnomocnikiem,
 - 6.5. przed podpisaniem umowy przedłożą pełnomocnictwo do zawarcia umowy w sprawie zamówienia publicznego, jeżeli pełnomocnictwo takie nie zostało dołączone do oferty.

VIII.2. Forma dokumentów składanych w postępowaniu.

1. Wszystkie dokumenty wchodzące w skład oferty oraz składane w trakcie postępowania należy złożyć na Platformie Zakupowej w postaci elektronicznej, podpisane kwalifikowanym podpisem elektronicznym, wystawionym przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne - podpis elektroniczny spełniający wymogi bezpieczeństwa określone w ustawie z dnia 5 września 2016 r. – o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r. poz. 1579 z późn. zm.).
2. Dokumenty i oświadczenia wchodzące w skład oferty oraz składane w trakcie postępowania, sporządzone w językach obcych muszą być złożone wraz z tłumaczeniami na język polski.
3. Dokumenty lub oświadczenia, o których mowa w Rozporządzeniu w sprawie rodzajów dokumentów, składane są w oryginale w postaci dokumentu elektronicznego lub w elektronicznej kopii dokumentu lub oświadczenia poświadczonej za zgodność z oryginałem.
4. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów lub oświadczeń, które każdego z nich dotyczą.
5. Poświadczenia za zgodność z oryginałem elektronicznej kopii dokumentu lub oświadczenia, o której mowa w pkt 4 następuje przy użyciu kwalifikowanego podpisu elektronicznego.
6. Ilekroć w SIWZ, a także w załącznikach do SIWZ występuje wymóg podpisywania dokumentów lub oświadczeń lub też potwierdzania dokumentów lub oświadczeń za zgodność z oryginałem, należy przez to rozumieć że oświadczenia i dokumenty te powinny być opatrzone kwalifikowanym podpisem elektronicznym osoby (osób) uprawnionej (uprawnionych) do reprezentowania Wykonawcy/podmiotu na zasobach lub sytuacji, którego Wykonawca polega, zgodnie z zasadami reprezentacji wskazanymi we właściwym rejestrze lub osobę (osoby) upoważnioną do reprezentowania Wykonawcy/podmiotu na zasobach lub sytuacji, którego Wykonawca polega na podstawie pełnomocnictwa.

Rozdział IX. Miejsce oraz termin składania i otwarcia ofert, warunki zmiany albo wycofania oferty.**IX.1. Miejsce oraz termin składania ofert i otwarcia ofert.**

- Ofertę pod rygorem nieważności należy złożyć w postaci elektronicznej, podpisaną kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Ofertę należy złożyć na Platformie Zakupowej udostępnionej przez Zamawiającego na stronie internetowej <https://platformazakupowa.pl/pn/arimr>.
- Termin składania ofert upływa w dniu **08.01.2020 r. o godzinie 12:00** Oferty otrzymane przez Zamawiającego po tym terminie zostaną zwrócone po upływie terminu przewidzianego na wniesienie odwołania, po uprzednim zawiadomieniu Wykonawcy o fakcie złożenia oferty po terminie.
- Otwarcie ofert odbędzie się w dniu **08.01.2020 r. o godzinie 12:15** w biurze Zamawiającego, pod adresem ul. Poleczki 33, 02-822 Warszawa.
- Zamawiający nie bierze odpowiedzialności za nieprawidłowe złożenie oferty wynikające z niezastosowania się przez Wykonawcę do wymagań niniejszej SIWZ.

IX.2. Warunki zmiany i wycofania złożonej oferty.

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

Rozdział X. Opis sposobu obliczenia ceny.

- Wykonawca zobowiązany jest do wyliczenia i podania cen jednostkowych, ceny ofertowej netto, należnego podatku od towarów i usług VAT oraz ceny ofertowej brutto, w sposób określony w Formularzu Ofertowym stanowiącym Załącznik nr 1 do SIWZ.
- Ceny określone w Formularzu Ofertowym powinny zawierać wszystkie koszty związane z wykonaniem przedmiotu zamówienia. Podane ceny nie podlegają zmianom przez okres obowiązywania umowy, z zastrzeżeniem postanowień Rozdziału XIV pkt 4 niniejszej SIWZ.
- Ceny określone w formularzu ofertowym muszą być podane i wyliczone w zaokrągleniu do dwóch miejsc po przecinku (wg zasady zaokrąglenia: poniżej 5 należy końcówkę pominać, powyżej i równe 5 należy zaokrąglić w górę).
- Wszystkie ceny podane w Formularzu Ofertowym powinny być wyrażone w złotych polskich.
- Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, obowiązany jest do poinformowania Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.

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

- Przy wyborze oferty najkorzystniejszej Zamawiający będzie się kierował poniższymi kryteriami:
 - kryterium **cena (P_c) – waga 60% [60 pkt]**, wg poniższego wzoru

$$P_c = \frac{C_{min}}{C_b} \times 60 \text{ pkt}$$

gdzie:

 P_c – ilość punktów oferty badanej w kryterium cena C_{min} – cena najniższa spośród ważnych ofert C_b – cena oferty badanej

- kryterium „okres serwisu gwarancyjnego” (P_g), o którym mowa w § 6 ust. 1 wzoru Umowy stanowiącej Załącznik nr 6 do SIWZ – waga 25% [25 pkt], wg poniższego wzoru:

$$P_g = \frac{t_b}{60} \times 25 \text{ pkt}$$

gdzie:

 P_g – oznacza ilość punktów oferty badanej w kryterium „okres serwisu gwarancyjnego.”

60 – maksymalny oczekiwany przez Zamawiającego okres serwisu gwarancyjnego (wyrażony w miesiącach).

 t_b – oznacza „okres serwisu gwarancyjnego” oferty badanej (wyrażony w miesiącach).**Uwaga:**

- a) Minimalny okres serwisu gwarancyjnego, o którym mowa w § 6 ust. 1 wzoru Umowy stanowiącej Załącznik nr 6 do SIWZ wynosi 36 miesięcy od daty podpisania bez zastrzeżeń przez Zamawiającego Protokołu odbioru Dokumentacji powykonawczej, o którym mowa w § 4 ust. 10 wzoru Umowy stanowiącej Załącznik nr 6 do SIWZ.
- b) Jeżeli Wykonawca zaoferuje okres serwisu gwarancyjnego krótszy niż 36 miesięcy – oferta takiego Wykonawcy zostanie odrzucona jako niezgodna z treścią SIWZ;
- c) W przypadku, gdy Wykonawca nie wskaże oferowanego okresu serwisu gwarancyjnego, Zamawiający uzna, że Wykonawca zaoferował minimalny wskazany przez Zamawiającego okres serwisu gwarancyjnego, tj. 36 miesięcy.
- d) Jeżeli Wykonawca zaoferuje okres serwisu gwarancyjnego dłuższy niż 60 miesięcy Zamawiający wpisze ten termin w § 6 ust. 1 wzoru Umowy stanowiącej Załącznik nr 6 do SIWZ, natomiast do celów oceny ofert uzna, iż Wykonawca zaoferował okres serwisu gwarancyjnego wynoszący 60 miesięcy.

1.3. Kryterium „dodatkowe godziny konsultacji technicznych” (P_k), o których mowa w § 2 ust. 4 wzoru Umowy – waga 6% [6 pkt], wg poniższego wzoru:

$$P_k = \frac{t_b}{200} \times 6 \text{ pkt}$$

gdzie:

P_k – oznacza ilość punktów oferty badanej w kryterium „dodatkowe godziny konsultacji technicznych.”

200 – maksymalna oczekiwana przez Zamawiającego wielkość dodatkowych godzin konsultacji technicznych (wyrażona w godzinach).

t_b – oznacza „dodatkowe godziny konsultacji technicznych” oferty badanej (wyrażone w godzinach).

Uwagi:

- a) W przypadku braku wskazania ilości godzin konsultacji technicznych w Formularzu Ofertowym, Zamawiający uzna, że Wykonawca zaoferował 0 (zero) godzin dodatkowych konsultacji technicznych.
- b) Jeżeli Wykonawca zaoferuje ilość dodatkowych godzin konsultacji technicznych powyżej 200 godzin, Zamawiający wpisze tą ilość do postanowień Umowy (§ 2 ust. 4 pkt 2 wzoru Umowy stanowiącej Załącznik nr 6 do SIWZ), natomiast do celów oceny ofert uzna, iż Wykonawca zaoferował 200 godzin dodatkowych godzin konsultacji technicznych.

1.4. kryterium „Parametry techniczne Sprzętu IT” (PT) – waga 9% [9 pkt], wg poniższych zasad.

W ramach tego kryterium oferta może otrzymać łącznie nie więcej niż 9 pkt. Sumowaniu będą podlegały punkty przyznane badanej ofercie w poszczególnych pozycjach.

W przypadku gdy zaoferowany Sprzęt IT (poza wymaganiami podstawowymi) będzie posiadał dodatkowo parametry techniczne określone w poniższej tabeli, oferta takiego Wykonawcy otrzyma punkty według poniższej tabeli.

Lp.	„Parametry techniczne Sprzętu IT” (P_T)	Ilość punktów w przypadku zaoferowania Sprzętu IT spełniającego poniższe parametry techniczne opisane w danej pozycji
1.	Klucze prywatne zapisane na dysku urządzenia przechowywane w formie zaszyfrowanej. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej.	3 pkt
2.	Wsparcie dla przynajmniej 2 wersji oprogramowania (multi-boot).	3 pkt
3.	W ramach klastra możliwość jednoczesnego wykorzystania różnych modeli urządzeń sprzętowych oraz maszyn wirtualnych.	3 pkt

Uwagi:

- a) W przypadku nie przekreślenia żadnego ze zwrotów lub łącznego przekreślenia obu zwrotów „TAK/NIE” przez Wykonawcę dla danej pozycji w Formularzu Ofertowym, Zamawiający uzna że zaoferowany Sprzęt IT nie spełnia parametrów technicznych opisanych i wymaganych w danym kryterium technicznym i oferta takiego Wykonawcy otrzyma dla tej pozycji 0 pkt.
- b) Wykonawca może zaoferować Sprzęt IT spełniający wymagania opisane przez Zamawiającego na wszystkie ww. pozycje (tj. 3 pozycji) lub na dowolnie wybrane przez siebie pozycje. Zamawiający będzie oceniał oferowane parametry techniczne Sprzętu IT dla każdej z pozycji, punkty będą przyznawane adekwatnie do dokonanej oceny oferty.

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

$$P = P_c + P_g + P_k + P_T$$

gdzie:

- P – ilość punktów oferty w łącznym kryterium oceny ofert;
- P_c – ilość punktów oferty w kryterium „Cena”;
- P_g – ilość punktów oferty w kryterium „okres serwisu gwarancyjnego”;
- P_k – ilość punktów oferty w kryterium „dodatkowe godziny konsultacji technicznych”;
- P_T – ilość punktów oferty w kryterium „Parametry techniczne Sprzętu IT”.

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

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

Rozdział XIII. Wymagania dotyczące zabezpieczenia należytego wykonania umowy.

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

Rozdział XIV. Informacje dotyczące umowy w sprawie zamówienia publicznego.

1. Zawarcie umowy nastąpi wg wzoru Umowy Zamawiającego, stanowiącego Załącznik nr 6 do niniejszej SIWZ.
2. Postanowienia ustalone we wzorze Umowy nie podlegają negocjacom.
3. Przyjęcie niniejszych postanowień umowy stanowi jeden z istotnych warunków przyjęcia oferty.
4. Zamawiający dopuszcza zmiany postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy. Warunki zmian zostały opisane przez Zamawiającego we wzorze Umowy wraz z załącznikami, stanowiącym Załącznik nr 6 do SIWZ.

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

1. Wykonawcom, którzy mają lub mieli interes w uzyskaniu danego zamówienia oraz ponieśli lub mogą ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy przysługują środki ochrony prawnej określone w dziale VI ustawy.
2. Odwołanie przysługuje wyłącznie od niezgodnej z przepisami ustawy czynności Zamawiającego podjętej w postępowaniu o udzielenie zamówienia lub zaniechania czynności, do której Zamawiający jest zobowiązany na podstawie ustawy.
3. Odwołanie powinno wskazywać czynność lub zaniechanie czynności Zamawiającego, której zarzuca się niezgodność z przepisami ustawy, zawierać zwięzłe przedstawienie zarzutów, określać żądanie oraz wskazywać okoliczności faktyczne i prawne uzasadniające wniesienie odwołania.
4. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej w postaci papierowej albo w postaci elektronicznej, opatrzone odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym.
5. Odwołujący przesyła kopię odwołania Zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, iż Zamawiający mógł zapoznać się z treścią

odwołania przed upływem terminu do jego wniesienia, jeżeli przesłanie jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.

6. Odwołanie wnosi się w terminie:

- 6.1. 10 (dziesięciu) dni od dnia przesłania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przesłane przy użyciu środków komunikacji elektronicznej, albo w terminie 15 (piętnastu) dni – jeżeli zostały przesłane w inny sposób;
- 6.2. 10 (dziesięciu) dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia SIWZ na stronie internetowej – wobec treści ogłoszenia oraz wobec postanowień SIWZ;
- 6.3. 10 (dziesięciu) dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia – wobec czynności innych niż określone w pkt 6.1 i 6.2 powyżej.

7. W przypadku wniesienia odwołania wobec treści ogłoszenia o zamówieniu lub postanowień SIWZ Zamawiający może przedłużyć termin składania ofert.

8. W przypadku wniesienia odwołania po upływie terminu składania ofert bieg terminu związania ofertą ulega zawieszeniu do czasu ogłoszenia przez Krajową Izbę Odwoławczą orzeczenia.

Załączniki do SIWZ:

1. Załącznik nr 1 wzór Formularza Ofertowego.
2. Załącznik nr 2 - wzór Oświadczenie o braku podstaw wykluczenia.
3. Załącznik nr 3 - wzór Oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej.
4. Załącznik nr 4 - wzór Oświadczenia – Wykaz dostaw (*warunek udziału w postępowaniu*)
5. Załącznik nr 5 - wzór Oświadczenia – Wykaz osób (*warunek udziału w postępowaniu*).
6. Załącznik nr 6 – wzór Umowy wraz z załącznikami.
7. Załącznik nr 7 - ESPD – plik, w formacie xml, wygenerowany z narzędzia ESPD – do przygotowania Formularza Jednolitego Europejskiego Dokumentu Zamówienia (JEDZ).

Zatwierdzam SIWZ wraz z załącznikami:

Warszawa, 15.11.2019 r.  p.o. PREZESA
Tomasz Nowakowski
podpis Zamawiającego

Załącznik nr 1 do SIWZ wzór Formularza Ofertowego

Formularz Ofertowy
DPIZP.2610.38.2019

Ja(my) niżej podpisany(-i)
 Działając w imieniu i na rzecz

W odpowiedzi na ogłoszone postępowanie prowadzone w trybie przetargu nieograniczonego na „Zakup i wdrożenie 2 szt. urządzeń Load Balancer wraz z gwarancją i konsultacjami”, zgodnie z wymaganiami określonymi w specyfikacji istotnych warunków zamówienia i wzorze Umowy wraz z załącznikami, oferuję(-emy) realizację przedmiotu zamówienia za cenę:

Tabela nr 1A

Load Balancer wraz z Oprogramowaniem – 2 szt.

Lp.	Parametry wymagane – minimalne wymagane przez Zamawiającego parametry dla pojedynczego Load Balancer wraz z Oprogramowaniem	Parametry oferowane (zaznacza Wykonawca)
1.	Sprzęt IT musi być dedykowaną platformą sprzętową typu appliance	TAK/NIE*
	Sprzęt IT musi realizować następujące funkcje: a) rozkład ruchu pomiędzy serwerami aplikacji Web; b) selektywny http caching; c) selektywna kompresja danych; d) terminowanie sesji SSL; e) optymalizacja i akceleracja aplikacji	TAK/NIE*
2.	Wszystkie wymienione funkcje muszą być dostępne w obrębie jednego Sprzętu IT	TAK/NIE*
3.	Sprzęt IT musi posiadać następujące metody równoważenia obciążenia: a) cykliczna; b) ważona; c) najmniejsza liczba połączeń; d) najszybsza odpowiedź serwera; e) najmniejsza liczba połączeń i najszybsza odpowiedź serwera; f) najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie; g) dynamicznie ważona oparta na SNMP/WMI; h) definiowana na podstawie grupy priorytetów dla serwerów	TAK/NIE*
4.	Sprzęt IT musi posiadać wbudowany w system operacyjny język skryptowy, posiadający następujące cechy: a) analiza, zmiana oraz zastępowanie parametrów w nagłówku http oraz w zawartości pakietów; b) obsługa protokołów: http, tcp, xml, rtp, sip; c) musi posiadać funkcję inspekcji protokołów LDAP oraz RADIUS	TAK/NIE*
5.	Język skryptowy musi bazować na języku programowania Tool Command Language lub równoważnym, z własnymi komendami	TAK/NIE*
6.	Musi istnieć możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego	TAK/NIE*
7.		TAK/NIE*

8.	<p>Producent Sprzęt IT musi dostarczyć darmową, specjalizowaną aplikację do analizy poprawności składni skryptów pisanych przy wykorzystaniu języka skryptowego opisanego w pkt. 6. Aplikacja musi posiadać wbudowane szablony skryptów oraz funkcję automatycznego uzupełniania wpisywanych komend lub posiadać mechanizm analizy poprawności składni skryptów w graficznym interfejsie zarządzania</p> <p>Rozwiązanie musi pracować w trybie pełnego proxy</p>	TAK/NIE*
9.		TAK/NIE*
10.	Praca w trybie pełnego proxy nie może powodować degradacji wydajności rozwiązania	TAK/NIE*
11.	Rozwiązanie musi posiadać programowalny interfejs API do integracji z zewnętrznymi systemami oraz automatyzacji wykonywania operacji	TAK/NIE*
12.	<p>Funkcjonalność lokalnego równoważenia obciążenia:</p> <ul style="list-style-type: none"> a) wspierane mechanizmy równoważenia obciążenia: round robin, ważona, dynamicznie ważona (na podstawie SNMPv1), najmniejsza liczba połączeń, największa odpowiedź, observer, predictive, grupy priorytetów, możliwość modyfikacji za pomocą języka skryptowego; b) buforowanie połączeń TCP w przypadku osiągnięcia zadanej ilości sesji dla danego serwera; c) obsługiwane mechanizmy monitorowania stanu serwerów: ICMP, echo (port 7/TCP), TCP, TCP half-open, UDP, SSL, http/https, LDAP, zapytania do baz MS SQL i Oracle, FTP, SIP, SMB/CIFS, RADIUS, SIP, POP3, IMAP, SMTP, SNMP, SOAP, sprawdzanie odpowiedzi w oparciu o wyrażenia regularne. Dodatkowo musi istnieć możliwość wykorzystania skryptów do tworzenia złośliwych monitorów sprawdzających aktywność usług; d) obsługiwane mechanizmy przywiązywania sesji: cookie (hash, rewrite, custom, insert, passive), adres docelowy, SSL ID, RDP login name, JSESSIONID, SIP call ID; e) wsparcie dla usług warstw 4-7: inspekcja warstw 7, wstrzykiwanie nagłówków http, ukrywanie zasobów, zmiana odpowiedzi serwera, zaszyfrowane cookies, przepisywanie odpowiedzi, ochrona przed atakami DoS/DDoS i SYN Flood, multipleksacja zapytań HTTP, kompresja i cache'owanie http <p>Optymalizacja i akceleracja aplikacji:</p> <ul style="list-style-type: none"> a) Sprzęt IT musi optymalizować protokół TCP i posiadać predefiniowane profile dla następujących charakterystyk sieci: <ul style="list-style-type: none"> i. LAN; ii. WAN; iii. urządzeń mobilnych; iv. urządzeń sieciowych; b) Sprzęt IT powinien implementować TCP proxy z mechanizmem zamykania okna w stronę serwera www w przypadku zbyt wolnego odbierania danych przez zdalnego klienta; c) Sprzęt IT musi mieć możliwość włączenia ignorowania nagłówków przegladarki dotyczących cachowania (Cache-control); d) Sprzęt IT musi wspierać multipleksację wielu zapytań http w tej samej sesji TCP; e) Sprzęt IT musi umożliwiać kompresję zwracanej zawartości http. Użycie kompresji powinno być zależne od: <ul style="list-style-type: none"> i. listy dozwolonych URI; ii. listy wykluczonych URI; iii. listy kompresowalnych Content-Type; iv. listy wykluczonych Content-Type. 	TAK/NIE*
13.		TAK/NIE*
14.	<p>Sprzęt IT musi posiadać następujące interfejsy administracyjne:</p> <ul style="list-style-type: none"> a) GUI przy wykorzystaniu protokołu https; b) zarządzanie poprzez SSH; c) zarządzanie poprzez API REST 	TAK/NIE*
15.	Autoryzacja administratorów Sprzętu IT musi bazować na rolach użytkowników	TAK/NIE*
16.	<p>Sprzęt IT musi posiadać funkcje przywiązywania sesji (Session persistence) przy wykorzystaniu następujących atrybutów:</p> <ul style="list-style-type: none"> a) Cookie (hash, rewrite, custom, insert, passive); b) adres źródła; c) SIP call ID; d) identyfikator sesji SSL; e) Microsoft Terminal Services (RDP) – nazwa użytkownika; f) adres docelowy; g) tworzone przez administratora przy wykorzystaniu języka skryptowego z pkt. 5. 	TAK/NIE*
17.	Sprzęt IT musi posiadać funkcję definiowania maksymalnej ilości obsługiwanych przez dany serwer połączeń, w przypadku przekroczenia zdefiniowanej wartości musi istnieć możliwość wysłania klientowi strony błędu lub przekierowania klienta na inny serwer	TAK/NIE*

18.	Sprzęt IT musi zapewnić możliwość klonowania puli serwerów umożliwiając wysyłanie kopii ruchu do zewnętrznych systemów monitoringu lub urządzeń typu IDS/IPS	TAK/NIE*
19.	Sprzęt IT musi zapewniać obsługę certyfikatów z kluczami typu ECDSA wykorzystującymi krzywe eliptyczne (ECC) zarówno od strony klienta, jak i od strony puli serwerów	TAK/NIE*
20.	Sprzętowe wsparcie dla algorytmów AES, AES-GCM, RSA, DSA, DH, ECDSA, ECDH, SHA2. Wsparcie dla Perfect Forward Secrecy	TAK/NIE*
21.	Dla protokołu TLS 1.2 wymagana jest obsługa AES-GCM zarówno od strony klienta, jak i od strony puli serwerów	TAK/NIE*
22.	Wsparcie dla protokołu TLS 1.3.	TAK/NIE*
23.	Sprzęt IT musi zapewniać obsługę certyfikatów podpisanych funkcją skrótu SHA-2 zarówno od strony klienta, jak i od strony puli serwerów	TAK/NIE*
24.	Sprzęt IT musi obsługiwać sieci VLAN w standardzie 802.1q.	TAK/NIE*
25.	Sprzęt IT musi obsługiwać agregację linków w standardzie 802.3ad (LACP).	TAK/NIE*
26.	Sprzęt IT musi obsługiwać Jumbo Frames	TAK/NIE*
27.	Sprzęt IT musi posiadać funkcjonalność bramy VXLAN oraz NVGRE.	TAK/NIE*
28.	Sprzęt IT musi świadczyć następujące usługi w warstwach 4-7: a) inspekcja warstwy aplikacji, w tym inspekcja nagłówka http; b) ukrywanie zasobów; c) zmiana odpowiedzi serwera; d) przepisywanie odpowiedzi (response rewriting); e) ochrona przed atakami typu DoS/DDoS; f) ochrona przed atakami typu SYN Flood; g) multipleksowanie połączeń http.	TAK/NIE*
29.	Sprzęt IT musi posiadać następujące funkcje zarządzania siecią: a) obsługa protokołu SNMP v1/v2/v3; b) możliwość budowania własnych zdarzeń SNMP z własnymi numerami OID; c) zewnętrzny syslog; d) zbieranie danych i ich wyświetlanie; e) zbieranie danych zgodnie z ustawieniami administratora; f) osobna brama domyślna dla interfejsu zarządzającego; g) zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy); h) dedykowany podsystem monitorowania stanu pracy Sprzętu IT (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu Sprzętu IT.	TAK/NIE*
30.	Sprzęt IT musi posiadać funkcję integracji z zewnętrznymi serwerami uwierzytelnienia użytkowników LDAP, RADIUS, TACACS.	TAK/NIE*
31.	Sprzęt IT musi posiadać funkcję definiowania i edycji szablonów konfiguracji aplikacji. Szablony powinny służyć do optymalizacji procesu wdrażania Sprzętu IT zarówno dla znanych aplikacji biznesowych, jak i własnych aplikacji klienta. W ramach opisanych szablonów musi istnieć możliwość automatycznej kontroli poszczególnych elementów konfiguracji szablonu i zabezpieczenie ich przed modyfikacją i usunięciem	TAK/NIE*
32.	Sprzęt IT musi posiadać moduł analizy ruchu http. Moduł powinien zbierać następujące metryki: a) czas odpowiedzi per serwer; b) czas odpowiedzi per URI; c) ilość sesji użytkownika; d) przepustowość; e) adres źródła; f) kraj; g) User Agent (wykorzystywana przez klienta aplikacja); h) metoda dostępu	TAK/NIE*
33.	Sprzęt IT musi posiadać funkcję walidacji certyfikatów klientów łączących się przy wykorzystaniu protokołu SSL.	TAK/NIE*
34.	Sprzęt IT musi oferować podział na tzw. partycje administracyjne. Zdefiniowany użytkownik może zarządzać konfiguracją tylko i wyłącznie wewnątrz swojej partycji.	TAK/NIE*

35.	Sprzęt IT musi oferować wsparcie dla tzw. domen routing (Virtual Routing and Forwarding). Rozwiązanie takie oferuje separację ruchu sieciowego do różnych aplikacji. Musi umożliwiać poprawnie działanie rozwiązań, kiedy podłączone VLANy do Sprzętu IT mają takie same podsieci i adresy IP.	TAK/NIE*
36.	Sprzęt IT musi oferować stworzenie minimum 10 partycji administracyjnych oraz 100 jednocześnie domen routing. Partycje administracyjne i domeny routing muszą być dostępne również, jeżeli Sprzęt IT pracuje w formie klastra	TAK/NIE*
37.	Rozwiązanie musi być dostarczone w formie klastra wysokiej dostępności (HA) złożonego z dwóch urządzeń tego samego typu pracujących w trybie active – standby z możliwością realizacji trybu active-active oraz rozbudowy do klastra N+1.	TAK/NIE*
38.	Sprzęt IT musi umożliwiać podział urządzenia na wirtualne części, przy czym każda taka część musi pracować logicznie jako niezależne urządzenie z niezależnym oprogramowaniem (każda część może posiadać inną wersję oprogramowania oraz osobną tablicę routing). Sprzęt IT musi umożliwić podział na minimum 8 wirtualnych części.	TAK/NIE*
39.	Klastrer wysokiej dostępności musi zapewniać kopiowanie informacji o sesji SSL i stanu sesji TCP pomiędzy urządzeniami, aby uniknąć ponownej negocjacji po przelazczeniu ruchu	TAK/NIE*
40.	Klastrer wysokiej dostępności musi zapewniać synchronizację: a) konfiguracji; b) stanu połączeń; c) przywiązywania sesji (<i>Session persistence</i>).	TAK/NIE*
41.	Wykrycie awarii Sprzętu IT w klastrze odbywać się musi przy użyciu weryfikacji stanu pracy Sprzętu IT poprzez analizę aktywności w sieci (Network failover).	TAK/NIE*
42.	Sprzęt IT musi być dostarczony z 4 sztukami licencji testowych do wykorzystania w środowiskach testowo-deweloperskich.	TAK/NIE*
43.	Licencje testowe muszą być rozwiązaniem wirtualnym działającym w następujących środowiskach: a) VMware ESXi 5.5 U3, 6.0 U2, 6.5; b) Microsoft Hyper-V dla Windows 2008 R2 SP1, Windows 2012, Windows 2012 R2 RTM i Update 1, Windows Server 2016; c) Linux KVM dla CentOS/RHEL od 6.3, Ubuntu od 14.04, Debian od 7.1; d) Microsoft Azure	TAK/NIE*
44.	Licencje testowe muszą zawierać w sobie wszystkie wyspecyfikowane wyżej funkcjonalności z wyłączeniem subskrypcji dla serwisu reputacyjnego i z kampaniami oraz wymagań wydajnościowych.	TAK/NIE*
45.	Sprzęt IT w postaci jednego urządzenia musi spełniać wymagania przedstawione w Tabeli 1B (poniżej).	TAK/NIE*

Uwaga 1

*-niewłaściwie przekreślić.

Tabela nr 1B

Wymagania minimalne dla pojedynczego Sprzętu IT.

Lp.	Parametr:	Minimalne wartości parametru:	Parametry oferowane (zaznacza Wykonawca)
1	Pamięć	48 GB	TAK/NIE**
2	Dysk twardy	Jeden dysk SSD o pojemności 480 GB	TAK/NIE**
3	Przebiegłość dla warstwy 4	60 Gbps	TAK/NIE**
4	Przebiegłość dla warstwy 7	35 Gbps	TAK/NIE**
5	Przebiegłość wewnętrznej magistrali	640 Gbps	TAK/NIE**
6	Ilość jednocześnie obsługiwanych połączeń	40 000 000	TAK/NIE**
7	Ilość transakcji SSL na sekundę dla klucza o długości 2048	35 000	TAK/NIE**
8	Ilość transakcji SSL na sekundę dla szyfrowania ECC (ECDHE-ECDHE-AES128-SHA256)	20 000	TAK/NIE**
9	Przebiegłość ruchu szyfrowanego	20 Gbps	TAK/NIE**
10	Ilość połączeń na sekundę w warstwie 4	800 000	TAK/NIE**
11	Kompresja sprzętowa	20 Gbps	TAK/NIE**
12	Sprzętowa ochrona DDoS	50 000 000 SYN cookies na sekundę	TAK/NIE**

13	Gęstość interfejsów	8 interfejsów z możliwością obsadzenia wkładkami SFP (T, SX lub LX) lub SFP+ 10G (SR lub LR). 4 interfejsy z możliwością obsadzenia wkładkami 40Gb QSFP+. oddzielny interfejs zarządzania, port konsolowy, interfejs szeregowy failover, port USB. 2 wkładki QSFP+ 40Gb. 2 wkładki QSFP+ 40Gb do switcha Cisco Nexus 6004, do którego zostanie podłączony Sprzęt IT. Wymagane jest dostarczenie odpowiednich kabli transmisyjnych w ilości 2 sztuk dla każdego Sprzętu IT w celu połączenia z dostarczonymi wkładkami do switchy Cisco Nexus 6004. Dostarczone wkładki muszą być oficjalnie wspierane przez producentów zarówno Sprzętu IT jak i urządzeń, do którego zostaną podłączone. Dostarczone wkładki nie mogą nieść ze sobą ryzyka odmowy świadczenia gwarancji, serwisu bądź pomocy technicznej przez producenta. Dostarczone wkładki muszą być objęte takimi samymi świadczeniami serwisowo-gwarancyjnymi jak Sprzęt IT oraz pochodzić z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej. Panel i wyświetlacz LCD z funkcjami: ustawienia adresu IP na potrzeby zarządzania, ustawienia parametrów portu szeregowego, wyświetlania podstawowych alarmów, możliwości restartu Sprzętu IT, wyświetlania informacji o Sprzęcie IT. Funkcjonalność „Always On Management”. Przeznaczona do montażu w szafie rack 19", wysokość nie większa niż 2U. 2 redundantne zasilacze - prąd zmienny 230V AC. EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A EN 61000-3-2:2014 EN 61000-3-3:2013 EN 55024:2010 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013 69 000 godzin	TAK/NIE**
14	Zarządzanie		TAK/NIE**
15	Obudowa		TAK/NIE**
16	Zasilanie		TAK/NIE**
17	Wymagana certyfikacja		TAK/NIE**
18	MTBF		TAK/NIE**

Uwaga 2

**-niewłaściwe przekreślić.

TABELA nr 2 – Wymagania dodatkowe punktowane w ramach kryterium „Parametry techniczne Sprzętu IT”

Lp.	„Parametry techniczne Sprzętu IT” (P _T)	Parametr oferowany zaznacza Wykonawca
1.	Klucze prywatne zapisane na dysku urządzenia przechowywane w formie zaszyfrowanej. Nie dopuszcza się rozwiązań przechowywujących klucze prywatne w formie jawnej.	TAK/NIE***
2.	Wsparcie dla przynajmniej 2 wersji oprogramowania (multi-boot).	TAK/NIE ***
3.	W ramach klastra możliwość jednoczesnego wykorzystania różnych modeli urządzeń sprzętowych oraz maszyn wirtualnych.	TAK/NIE ***

Uwaga 3:

***- niewłaściwe przekreślić. W przypadku nie przekreślenia żadnego ze zwrotów lub łącznego przekreślenia obu zwrotów „TAK/NIE” przez Wykonawcę dla danej pozycji. Zamawiający uzna że zaoferowany Sprzęt IT nie spełnia parametrów technicznych opisanych i wymaganych w danym kryterium technicznym i oferta takiego Wykonawcy otrzyma dla tej pozycji 0 pkt.

TABELA nr 3

Oferujemy Sprzęt IT o parametrach technicznych wymienionych w Tabeli nr 1A i nr 1B oraz w Tabeli nr 2 (punktowane w ramach kryteriów oceny ofert****), oraz na warunkach określonych we wzorze Umowy, który stanowi Załącznik nr 6 do SIWZ za cenę:

Uwagi:

**** - o ile są oferowane

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł)	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	[b]	[c]	[d]	[e] = [c] x [d]	[f]	[g] = [e] x [f]	[h] = [e] + [g]
1	Sprzęt IT (Load Balancer - 1 szt. wraz z Oprogramowaniem), spełniający wymagania określone w Tabeli nr 1A, Tabeli 1B i Tabeli nr 2 oraz Serwisem gwarancyjnym świadczonym wg wymagań zdefiniowanych w § 6 wzoru umowy. <i>Producent</i> <i>Model Load Balancer</i>	2					
2	Wdrożenie i Dokumentacja powykonawcza, zgodnie z § 7 ust. 1 pkt. 2) wzoru Umowy	1					
		Razem [Σ1+2]:				X	

Tabela nr 4

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł) (cena za 1 godz. konsultacji)	Podatek VAT		Cena ofertowa brutto (zł)
				%	zł	
[a]	[b]	[c]	[d]	[e] = [c] x [d]	[f] = [e] x [f]	[h] = [e] + [g]
1	Konsultacje, o których mowa w § 2 ust. 4 pkt 1 wzoru Umowy	300 godz.				

Tabela nr 5 - Łączna cena oferty

[a]	Przedmiot	Cena netto [zł]	Podatek VAT [zł]	Cena brutto [zł]
1	<p>[b]</p> <p>Sprzęt IT (Load Balancer - 2 szt. wraz z Oprogramowaniem), spełniający wymagania określone w Tabeli nr 1 i Tabeli nr 2 oraz Serwisem gwarancyjnym świadczonym wg wymagań zdefiniowanych w § 6 wzoru Umowy oraz</p> <p>Wdrożenie i Dokumentacja powykonawcza, zgodnie z § 7 ust. 1 pkt. 2) wzoru umowy, - wg Tabeli nr 3 (należy wpisać odpowiednio wartości z Tabeli nr 3 z pozycji „Razem”: kol. „b”, „d” i „e”)</p>	[c]	[d]	[e]
2	<p>Konsultacje, o których mowa w § 2 ust. 4 pkt 1 wzoru Umowy – wg Tabeli nr 4 (należy wpisać odpowiednio wartości z Tabeli nr 4: kol. „e”, „g” i „h”)</p>			
Łączna cena oferty [Σ1÷2]:				

Łączna cena netto oferty zł słownie:

Łączna cena brutto oferty zł słownie:

Oświadczamy, że:

1. W cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia.
2. Zapoznaliśmy się z treścią SIWZ (w tym ze wzorem Umowy) i nie wnosimy do niej zastrzeżeń oraz przyjmujemy warunki w niej zawarte.
3. Okres serwisu gwarancyjnego, o którym mowa w § 6 ust. 1 wzoru Umowy stanowiącej Załącznik nr 6 do SIWZ, wyniesie miesięcy.

Uwaga:

- a) Minimalny okres serwisu gwarancyjnego, o którym mowa w § 6 ust. 1 wzoru Umowy stanowiącej Załącznik nr 6 do SIWZ wynosi 36 miesięcy od daty podpisania bez zastrzeżeń przez Zamawiającego Protokołu odbioru Dokumentacji powykonawczej, o którym mowa w § 4 ust. 10 wzoru Umowy stanowiącej Załącznik nr 6 do SIWZ.
- b) Jeżeli Wykonawca zaofertuje okres serwisu gwarancyjnego krótszy niż 36 miesięcy – oferta takiego Wykonawcy zostanie odrzucona jako niezgodna z treścią SIWZ.
- c) W przypadku, gdy Wykonawca nie wskaże oferowanego okresu serwisu gwarancyjnego, Zamawiający uzna, że Wykonawca zaofertował minimalny wskazany przez Zamawiającego okres serwisu gwarancyjnego, tj. 36 miesięcy.

d) Jeżeli Wykonawca zaofertuje okres gwarancyjnego dłuższy niż 60 miesięcy Zamawiający wpisze ten termin w § 6 ust. 1 wzoru Umowy stanowiącej Załącznik nr 6 do SIWZ, natomiast do celów oceny ofert uzna, iż Wykonawca zaofertował okres serwisu gwarancyjnego wynoszący 60 miesięcy.

4. Oferujemy dodatkowe godziny konsultacji technicznych, o którym mowa w § 2 ust. 4 pkt 2 wzoru Umowy stanowiącej Załącznik nr 6.1 do SIWZ, w ilości godzin.

Uwaga:

a) W przypadku braku wskazania ilości godzin konsultacji technicznych w Formularzu Ofertowym, Zamawiający uzna, że Wykonawca zaofertował 0 (zero) godzin dodatkowych konsultacji technicznych.

b) Jeżeli Wykonawca zaofertuje ilość dodatkowych godzin konsultacji technicznych powyżej 200 godzin, Zamawiający wpisze tą ilość do postanowień Umowy (§ 2 ust. 4 pkt 2 wzoru Umowy stanowiącej Załącznik nr 6 do SIWZ), natomiast do celów oceny ofert uzna, iż Wykonawca zaofertował 200 godzin dodatkowych godzin konsultacji technicznych.

5. Realizację przedmiotu zamówienia wykonamy w terminach określonych w Rozdziale II SIWZ oraz wzorze Umowy.

6. Uwazamy się za związanych niniejszą ofertą na okres wskazany w SIWZ.

7. Wadium w wysokości 20 000,00 zł (słownie: dwadzieścia tysięcy złotych zero groszy) wnieśliśmy przed upływem terminu składania ofert.

8. Wadium wniesione w formie pieniądza należy zwrócić na rachunek bankowy nr prowadzony w banku

9. Zobowiązujemy się do wniesienia przed podpisaniem umowy zabezpieczenia należytego wykonania umowy w wysokości 5% ceny całkowitej podanej w ofercie.

10. W przypadku przyznania nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.

11. Podwykonawcom zamierzamy powierzyć wykonanie następującej(-ych) części zamówienia (należy podać zakres prac oraz firmę Podwykonawcy):

a)

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

12. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na poniższy adres:

Dane kontaktowe: imię i nazwisko, nr tel., adres e-mail:

13. Dokumenty wymienione od strony do strony stanowią tajemnicę przedsiębiorstwa i nie mogą być ujawnione uczestnikom postępowania.

UWAGA:

Zamawiający przypomina, że stosownie do art. 8 ust. 3 ustawy Wykonawca winien nie później niż w terminie składania ofert wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.

14. Wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO* wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.**

* rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2016, str. 2.).

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

15. Jednocześnie zgodnie z treścią art. 91 ust. 3a ustawy oświadczam, że wybór przedmiotowej oferty:*

a) nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego

b) będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług

(należy wskazać: nazwę (rodzaj) towarów/usług, których dostawa/świadczenie będzie prowadzić do jego powstania oraz wartość bez kwoty podatku od towarów i usług)

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

16. Oferta została złożona na _____ stronach kolejno ponumerowanych od nr _____ do nr _____.

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

Załącznik nr 2 do SIWZ wzór Oświadczenia o braku podstaw wykluczenia

()

Dane Wykonawcy
(nazwa; adres)

()

Oświadczenie o braku podstaw wykluczenia

DPIZP.2610.38.2019

Przystępując do udziału w postępowaniu o zamówienie publiczne na „Zakup i wdrożenie 2 szt. urządzeń Load Balancer wraz z gwarancją i konsultacjami” oświadczam(-y), że:

- 1) nie wydano wobec nas prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne* / wydano wobec nas prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, wobec czego składamy niżej wymienione dokumenty potwierdzające dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności*:
 - a)
 - b)
 - c)
 - d)
- 2) nie wydano orzeczenia wobec nas tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne,
- 3) nie zalegamy z opłacaniem podatków i opłat lokalnych, o których mowa w ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz. U. z 2018 r. poz. 1445 ze zm.),
- 4) nie wydano wobec nas prawomocnego wyroku sądu skazującego za wykroczenie na karę ograniczenia wolności lub grzywny w zakresie określonym na podstawie art. 24 ust. 5 pkt 5 i 6 ustawy,
- 5) nie wydano wobec nas ostatecznej decyzji administracyjnej o naruszenie obowiązków wynikających z przepisów prawa pracy, prawa ochrony środowiska lub przepisów o zabezpieczeniu społecznym w zakresie określonym na podstawie art. 24 ust. 5 pkt 7 ustawy.

* UWAGA: niepotrzebne skreślić

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

(Dane Wykonawcy
(nazwa; adres))

Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej

DPIZP.2610.38.2019

Przystępując do udziału w postępowaniu o zamówienie publiczne na „Zakup i wdrożenie 2 szt. urządzeń Load Balancer wraz z gwarancją i konsultacjami”

- 1) Oświadczamy, że nie należymy do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2019 r., poz. 369)* z żadnym z Wykonawców, którzy złożyli ofertę w przedmiotowym postępowaniu o udzielenie zamówienia publicznego.
- 2) Oświadczamy, że należymy do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2019 r., poz. 369)* z następującymi Wykonawcami, którzy złożyli ofertę w przedmiotowym postępowaniu o udzielenie zamówienia publicznego:

Lp.	Nazwa podmiotu	Siedziba

[Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia]

* UWAGA: niepotrzebne skreślić

Załącznik nr 4 do SIWZ wzór Oświadczenia – Wykaz dostaw
[warunek udziału w postępowaniu]

[
Dane Wykonawcy
(nazwa; adres)
]

Oświadczenie – Wykaz dostaw
DPIZP.2610.38.2019

Przystępując do udziału w postępowaniu o zamówienie publiczne na „Zakup i wdrożenie 2 szt. urządzeń Load Balancer wraz z gwarancją i konsultacjami”, składamy wykaz dostaw wykonanych (wykonywanych) w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, na potwierdzenie spełnienia warunku udziału w postępowaniu, o którym mowa w Rozdziale III pkt.1.2.1 SIWZ.

Lp.	Przedmiot wykonanych/wykonywanych dostaw (wg warunku udziału w postępowaniu: zawołanie polegające na dostawie urządzeń typu Load Balancer, wraz z wdrożeniem	Wartość brutto dostawy w zł (w przypadku gdy zakres dostawy jest szerszy, należy podać wyłącznie wartość dostawy odpowiadającej treści warunku udziału w postępowaniu w badanym zakresie, wg warunku udziału w postępowaniu: co najmniej 300 000,00 zł brutto)	Podmiot na rzecz którego wykonano dostawę (nazwa i adres)		Daty wykonania		Dowody	Informacje uzupełniające	
			Od dd-mm-rrrr	Do dd-mm-rrrr	Zasoby innego podmiotu	Nazwa innego podmiotu			
1	2	3	4	5	6	7	8	9	
1									
2									

Uwaga do kol. 7:

1. Do wykazu należy dołączyć dowody potwierdzające, że powyższe dostawy zostały wykonane lub są wykonywane należycie, tj.:
 - 1.1. referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane należycie,
 - 1.2. oświadczenie Wykonawcy - jeżeli z uzasadnionych przyczyn o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać dokumentów, o którym mowa wyżej w pkt 1.1.
2. Należy wpisać nazwę dowodu (dokumentu), potwierdzającego, że dostawy zostały wykonane/wykonywane należycie (podać numer strony w ofercie);

Uwaga do kol. 8:

1. Zaznaczyć „TAK”, tylko w przypadku gdy Wykonawca polega na zasobach innego podmiotu dla wykazania spełnienia warunku udziału;
2. Dla wykazania spełnienia warunku udziału w postępowaniu, opisanego w Rozdziale III pkt 1.2.1 SIWZ, Wykonawca może polegać, na zasadach określonych w art.22a ustawy. W tym celu Wykonawca składa dokumenty i oświadczenia zgodnie z zasadami określonymi w Rozdziale IV.5 SIWZ.

Załącznik nr 5 do SIWZ wzór Oświadczenia — Wykaz osób
[warunek udziału w postępowaniu]

[
Dane Wykonawcy
(nazwa; adres)
]

Oświadczenie – Wykaz osób, które będą uczestniczyć w wykonywaniu zamówienia
DPIZP.2610.38.2019

Przystępując do udziału w postępowaniu o zamówienie publiczne na „Zakup i wdrożenie 2 szt. urządzeń Load Balancer wraz z gwarancją i konsultacjami”, składamy wykaz osób w celu potwierdzenia spełnienia warunku udziału w postępowaniu, o którym mowa w Rozdziale III pkt 1.2.2 SIWZ, skierowanych przez Wykonawcę do realizacji zamówienia, które będą uczestniczyć w jego wykonaniu:

1. Jedna osoba spełniająca poniższe wymagania:

Wymagania Zamawiającego wskazane w SIWZ		Wypełnia Wykonawca		
<p>Osoba, która posiada:</p> <p>1) co najmniej 12 miesięczne doświadczenie przy realizacji zamówień o zakresie jak w pkt 1.2.1. SIWZ z wyłączeniem wartości zamówień;</p> <p>2) certyfikat F5 Certified Solutions Expert Security lub równoważny.</p> <p>Uwaga: Przez certyfikat równoważny, o którym mowa powyżej Zamawiający rozumie certyfikat, który: 1) jest analogiczny co do zakresu z przykładowym certyfikatem wskazanym z nazwy dla danej roli, co jest rozumiane jako: a) analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat, b) analogiczny stopień poziomu kompetencji, c) analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu, 2) potwierdzony jest egzaminem (dotyczy tylko tych ról, których przykładowy certyfikat musi być potwierdzony egzaminem).</p>	1.1	Imię i Nazwisko		
	1.2.	Wskazana osoba spełnia wymagania zdefiniowane w Rozdziale III pkt 1.2.2.SIWZ		
	1.3	Posiadany certyfikat	1.3.1	Nazwa certyfikatu
			1.3.2	Podmiot wydający certyfikat
			1.3.3	Nr certyfikatu (o ile dotyczy)
	1.3.4	Data ważności certyfikatu (DD-MM-RRRR) (o ile dotyczy)		
1.4	Podstawa dysponowania osobą	1.4.1	Dysponowanie bezpośrednie	
		1.4.2	Dysponowanie osobą na podstawie art. 22a ustawy – Prawo zamówień publicznych	

Uwaga:

- Dla wykazania spełnienia warunku udziału w postępowaniu opisanego w Rozdziale III pkt 1.2.2. SIWZ, Wykonawca może polegać, na osobach zdolnych do wykonania zamówienia oddanych mu do dyspozycji przez inne podmioty.
- W odniesieniu do podstawy dysponowania osobą Wykonawca wypełnia kolumnę „Dysponowanie bezpośrednie” albo „Dysponowanie osobą na podstawie art. 22a ustawy – Prawo zamówień publicznych”.
- W przypadku dysponowania przez Wykonawcę osobą na podstawie art. 22a ustawy – Prawo zamówień publicznych jest obowiązany udowodnić Zamawiającemu, iż będzie dysponował niezbędnymi osobami zdolnymi do wykonania zamówienia, w szczególności przedstawiając w tym celu dokumenty i oświadczenia w zakresie wskazanym w Rozdziale IV.5 SIWZ.

Załącznik nr 6 do SIWZ wzór Umowy

Umowa nr ____/DI/20.../2610

zawarta w dniu _____ 20..... r. w Warszawie pomiędzy:

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

_____ – Zastępca Prezesa ARiMR, Pełnomocnik;
 _____ – Dyrektor Departamentu Księgowości, w ramach zajmowanego stanowiska wykonująca obowiązki Głównego Księgowego, Pełnomocnik;

a

_____, zwaną dalej "**Sprzedawcą**", którą reprezentuje:

_____ – _____;
 _____ – _____;

zwanych łącznie „**Stronami**”.

W wyniku wyboru oferty w postępowaniu o udzielenie zamówienia publicznego przeprowadzonego w trybie przetargu nieograniczonego zgodnie z art. 39 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843 ze zm.), zawarto umowę o następującej treści:

§ 1. Definicje

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

- 1) **Strony** – Sprzedawca i Kupujący wymienieni w komparycji Umowy;
- 2) **Umowa** – niniejsza umowa wraz z załącznikami regulująca prawa i obowiązki Stron z niej wynikające i związane z jej wykonaniem;
- 3) **Sprzęt IT** – urządzenia informatyczne, pełniące funkcje load balancer'ów – 2 szt., wraz z Oprogramowaniem, posiadające parametry i funkcjonalności szczegółowo opisane w Załączniku nr 1 do Umowy;
- 4) **Oprogramowanie** – programy komputerowe dostarczone przez Sprzedawcę, z których Kupujący korzysta na podstawie Licencji udzielonych przez producenta, niezbędne do zachowania wyspecyfikowanej funkcjonalności Sprzętu IT i korzystania ze Sprzętu IT;
- 5) **Licencja** – prawo do bezterminowego korzystania z Oprogramowania, zgodnie z warunkami określonymi przez producenta Oprogramowania, potwierdzone dokumentem licencyjnym;
- 6) **Serwis gwarancyjny** – usługa opieki serwisowej i wsparcia technicznego dla Sprzętu IT oraz Oprogramowania, świadczona w zakresie i na zasadach określonych w Umowie oraz zgodnie z warunkami określonymi przez producenta Sprzętu IT i Oprogramowania;
- 7) **Dokumenty** - instrukcje eksploatacyjne, instrukcje obsługi Sprzętu IT oraz dokumenty licencyjne dla Oprogramowania;
- 8) **Wdrożenie** – czynności wykonywane przez Sprzedawcę, mające na celu uruchomienie dostarczonego Sprzętu IT, instalacje Oprogramowania oraz przeniesienie konfiguracji z dotychczas użytkowanych urządzeń na Sprzęt IT – szczegółowo opisane w Załączniku nr 1 do Umowy;
- 9) **Dokumentacja powykonawcza** - dokumentacja zawierająca schemat fizyczny i logiczny podłączenia Sprzętu IT, konfigurację Sprzętu IT oraz opis zastosowanych rozwiązań i technologii;
- 10) **COPD** – Centralne Ośrodki Przetwarzania Danych Kupującego znajdujące się w Piasecznie ul. Jana Pawła II 66, 05-500 Piaseczno oraz w Warszawie, ul. Poleczki 23, 02-822 Warszawa;
- 11) **Dni Robocze** – dni w godzinach pracy (7.30-15.30) Kupującego od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych od pracy u Kupującego, o których Kupujący powiadomi Sprzedawcę.

§ 2. Przedmiot Umowy

1. Na podstawie Umowy Sprzedawca:
 - 1) sprzedaje i dostarczy fabrycznie nowy, nienoszący śladów uprzedniego używania Sprzęt IT wraz z Oprogramowaniem, zgodnie ze specyfikacją stanowiącą Załącznik nr 1 do Umowy oraz z Formularzem ofertowym, stanowiącym Załącznik nr 7 do Umowy;
 - 2) wykona Wdrożenie;
 - 3) świadczył będzie Serwis gwarancyjny dla Sprzętu IT i Oprogramowania przez okres ____ (zostanie wypełniony zgodnie z deklaracją Sprzedawcy złożoną w Formularzu Ofertowym) miesięcy;

- a Kupujący kupuje Sprzęt IT i Oprogramowanie.
2. Wraz z dostawą Sprzętu IT wraz z Oprogramowaniem Sprzedawca dostarczy Kupującemu Dokumenty.
 3. W ramach realizacji Umowy Sprzedawca wykona Dokumentację powykonawczą i dostarczy ją Kupującemu w formie papierowej i elektronicznej do akceptacji i odbioru.
 4. W ramach Umowy Sprzedawca zapewni Kupującemu:
 - 1) 300 godzin konsultacji technicznych, w okresie pierwszych 36 miesięcy obowiązywania Umowy, w zakresie problemów dotyczących Sprzętu IT lub Oprogramowania. Konsultacje będą obejmowały analizy, audyty oraz rekomendację dot. Sprzętu IT lub Oprogramowania, jak również wszelkiego rodzaju prace rekonfiguracyjne Sprzętu IT lub Oprogramowania oraz pomoc przy pracach technicznych przeprowadzanych przez Kupującego w COPD, w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 pkt 3 Umowy. Konsultacje będą świadczone w języku polskim.
 - 2) _____ dodatkowych godzin konsultacji (zostanie wypełnione zgodnie z deklaracją Sprzedawcy złożoną w Formularzu Ofertowym), w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 pkt 1 Umowy, w okresie i zakresie wskazanym w pkt 1, które Zamawiający wykorzysta w pierwszej kolejności przed konsultacjami, o których mowa w pkt 1.
 5. W ramach konsultacji technicznych Sprzedawca na wniosek Kupującego przeprowadzi warsztaty lub prezentacje dot. wskazanego elementu Sprzętu IT oraz Oprogramowania w Centrali Kupującego przy ul. Poleczki 33 w Warszawie. Czas dojazdu do Sprzedawcy nie będzie wliczony jako wykorzystanie dostępnej puli godzin.
 6. Sprzedawca będzie przyjmował zgłoszenia konsultacyjne od poniedziałku do piątku, w godzinach od 8.00 do 18.00, telefonicznie pod numerem: + _____ lub na adres poczty elektronicznej _____@_____. Przyjęcie zgłoszenia zostanie przez Sprzedawcę potwierdzone (drogą elektroniczną na adresy e-mail pracowników Kupującego, wskazanych w § 3 ust. 2 pkt 1 Umowy) w ciągu 1 godziny od otrzymania zgłoszenia. Niepotwierdzenie zgłoszenia w powyższym terminie Kupujący uznaje za przyjęcie zgłoszenia. O każdej zmianie adresu lub numeru telefonu wskazanego powyżej, Sprzedawca zobowiązany jest niezwłocznie powiadomić na piśmie Kupującego. Zmiana danych, o których mowa w zdaniu poprzedzającym nie wymaga zmiany Umowy w formie pisemnego aneksu, a jedynie poinformowania drugiej Strony o zmianie.
 7. Na koniec każdego kwartału Sprzedawca przedstawi Protokół odbioru konsultacji ze zgłoszonych i przeprowadzonych konsultacji, którego wzór został określony w Załączniku nr 4b do Umowy.

§ 3. Wymagania dotyczące wykonania Umowy

1. Sprzedawca oświadcza, że posiada konieczne doświadczenie i profesjonalne kwalifikacje niezbędne do prawidłowego wykonania Umowy i zobowiązuje się do wykonania Umowy przy zachowaniu należytej staranności określonej w art. 355 § 2 Kodeksu Cywilnego.
2. Osobami upoważnionymi do rozpatrywania bieżących spraw i podpisywania protokołów odbioru związanych z wykonaniem Umowy, przy zachowaniu określonych w niej warunków, w tym terminów:
 - 1) po stronie Kupującego są:

Pan _____ tel.: (22) _____; e-mail: _____@arimr.gov.pl

Pan _____ tel.: (22) _____; e-mail: _____@arimr.gov.pl

Pan _____ tel.: (22) _____; e-mail: _____@arimr.gov.pl
 - 2) po stronie Sprzedawcy są:

Pan _____ tel.: (XX) _____; e-mail: _____@_____

Pan _____ tel.: (XX) _____; e-mail: _____@_____
3. Zmiana osób, o których mowa w ust. 2 powyżej, nie stanowi zmiany Umowy wymagającej sporządzenia aneksu.
4. Sprzedawca oświadcza, że Sprzęt IT posiada wszelkie certyfikaty i homologacje niezbędne do eksploatacji na terytorium Rzeczypospolitej Polskiej oraz gwarantuje, że Sprzęt IT jest zgodny z Polskimi Normami niezawodności i bezpieczeństwa.
5. Kupujący wymaga a Sprzedawca oświadcza, że Wdrożenie będzie wykonywane bezpośrednio przez minimum 1 osobę posiadającą uprawnienia F5 Certified Solutions Expert Security lub równoważne. W ramach Wdrożenia wymagane będzie przeniesienie funkcjonalności z czterech urzędzeń F5 BIG IP.
6. W terminie do 3 Dni Roboczych po podpisaniu przez upoważnionych przedstawicieli Stron Umowy, Kupujący prześle Sprzedawcy aktualną konfigurację urzędzeń, o których mowa w ust. 5 oraz fragmenty konfiguracji do przeniesienia z urzędzeń F5 BIG IP pracujących w sieci LAN Kupującego.

§ 4. Terminy i odbiory

1. Dostarczenie Sprzętu IT wraz z Oprogramowaniem, Dokumentów oraz Wdrożenie nastąpi w lokalizacjach COPD nie później niż w terminie do 20 Dni Roboczych od dnia zawarcia Umowy.
2. Sprzedawca powiadomi, w formie pisemnej, Kupującego o terminie dostarczenia Sprzętu IT wraz z Oprogramowaniem, i Dokumentów oraz o terminie rozpoczęcia Wdrożenia w poszczególnych lokalizacjach COPD, z wyprzedzeniem co najmniej 5 Dni Roboczych. W terminie do 2 Dni Roboczych Kupujący potwierdzi wskazany termin lub wskaże inny, jednak nie później niż 2 Dni Robocze od daty otrzymania przez Kupującego ww. powiadomienia.
3. Dostarczenie Sprzętu IT wraz z Oprogramowaniem i Dokumentów odbędzie się na koszt i ryzyko Sprzedawcy. Sprzedawca dostarczy Sprzęt IT wraz z Oprogramowaniem i Dokumenty zgodnie z warunkami Umowy i poniesie pełne ryzyko związane z niebezpieczeństwem utraty albo uszkodzenia Sprzętu IT wraz z Oprogramowaniem do dokonania ich odbioru przez osobę upoważnioną przez Kupującego, zgodnie z ust. 4 - 10.
4. Odbiór Sprzętu IT wraz z Oprogramowaniem i Dokumentów zostanie dokonany komisyjnie z udziałem upoważnionych przedstawicieli Sprzedawcy i Kupującego. Odbiór i zawiadomienia Stron dotyczące odbioru i Wdrożenia będą dokonywane w Dniach Roboczych.
5. Podczas odbioru Sprzętu IT wraz z Oprogramowaniem i Dokumentów Sprzedawca w obecności Kupującego:

- 1) rozpakuje dostarczony Sprzęt IT oraz sprawdzi czy nie nosi znamion uszkodzeń mechanicznych oraz czy jest fabrycznie nowy i zgodny z Załącznikiem nr 1 i nr 7 do Umowy;
 - 2) podłączy Sprzęt IT do sieci zasilającej i zainstaluje Oprogramowanie;
 - 3) usunie z miejsca dostarczenia i zutilizuje wszelkie opakowania, pozostałe po dostarczeniu i zainstalowaniu Sprzętu IT;
 - 4) wykona Wdrożenie, zgodnie z ust. 7.
6. Po dokonaniu przez Kupującego bez zastrzeżeń odbioru Sprzętu IT wraz z Oprogramowaniem, Dokumentów w ostatniej lokalizacji COPD, Kupujący podpisze Protokół odbioru Sprzętu IT, Oprogramowania i Dokumentów, którego wzór stanowi Załącznik nr 2a do Umowy.
 7. W ramach Wdrożenia Sprzedawca w obecności pracownika Kupującego wykona czynności wskazane w Załączniku nr 1 do Umowy, co zostanie potwierdzone podpisaniem przez upoważnionych przedstawicieli Stron Protokołem odbioru Wdrożenia, którego wzór stanowi Załącznik nr 2b do Umowy.
 8. W przypadku stwierdzenia podczas odbioru, że:
 - 1) Sprzęt IT lub Oprogramowanie są niezgodne z Załącznikiem nr 1 lub Załącznikiem nr 7 do Umowy lub posiadają ślady zewnętrznego uszkodzenia lub
 - 2) nie dostarczono wszystkich wymaganych Dokumentów, o których mowa w ust. 1 lub
 - 3) Wdrożenie nie zostało wykonane prawidłowo lub
 - 4) Sprzęt IT wraz z Oprogramowaniem, Dokumenty lub Wdrożenie budzą inne zastrzeżenia niż określone w pkt 1-3,
 Kupujący odmówi podpisania Protokołu odbioru, jednocześnie przekaze Sprzedawcy protokół przedstawiający powód odmowy odbioru ze wskazaniem terminu dostarczenia Sprzętu IT wraz z Oprogramowaniem lub Dokumentów wolnych od wad lub ponownego wykonania Wdrożenia. Procedura czynności odbioru zostanie przeprowadzona ponownie.
 9. W przypadku stwierdzenia podczas powtórnej procedury czynności odbioru którejkolwiek z okoliczności wskazanych w ust. 8, Kupujący odmówi odbioru przedmiotu Umowy i jednocześnie przekaze Sprzedawcy protokół przedstawiający powód odmowy odbioru Sprzętu IT wraz z Oprogramowaniem i Dokumentów Sprzedawca ma obowiązek odbioru dostarczonego Sprzętu IT wraz z Oprogramowaniem i Dokumentów w terminie 5 Dni Roboczych od daty przekazania Sprzedawcy protokołu przedstawiającego powody odmowy odbioru Sprzętu IT.
 10. W terminie do 5 Dni Roboczych od dnia podpisania Protokołu odbioru, o którym mowa w ust. 7, Sprzedawca dostarczy do Kupującego Dokumentację powykonawczą. Odbiór zostanie potwierdzony Protokołem odbioru Dokumentacji powykonawczej, którego wzór stanowi Załącznik nr 3. Kupujący zastrzega sobie prawo zgłaszania uwag do Dokumentacji powykonawczej. Sprzedawca zobowiązany jest uwzględnić uwagi Kupującego lub zgłosić zastrzeżenia w terminie 3 Dni Roboczych od dnia otrzymania uwag od Kupującego.
 11. Wszystkie powiadomienia dotyczące odbiorów Sprzętu IT wraz z Oprogramowaniem, Dokumentów, Dokumentacji powykonawczej lub wykonania Wdrożenia powinny być dokonywane w Dni Robocze.

§ 5. Udzielenie Licencji

1. Kupujący, w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 pkt 2 Umowy, nabywa Licencję upoważniającą do bezterminowego korzystania z Oprogramowania w celu zachowania funkcjonalności Sprzętu IT.
2. Kupujący, w ramach udzielonej Licencji, zgodnie z warunkami producenta Oprogramowania, ma prawo do trwałego lub czasowego zwielokrotnienia Oprogramowania w całości lub w części, jakimikolwiek środkami i w jakiegokolwiek formie; w zakresie, w którym jest to niezbędne dla wprowadzania, wyświetlania, stosowania, przekazywania, przechowywania Oprogramowania dla własnych potrzeb Kupującego, z uwzględnieniem treści ust. 3, zgodnie z jego charakterem i przeznaczeniem, Dokumentami i warunkami Umowy.
3. Licencja uzyskana zgodnie z zapisami ust. 2, może być wykorzystywana wyłącznie dla celów działalności Kupującego i nie obejmuje prawa do wprowadzania Oprogramowania do obrotu lub przekazywania ani w części ani w całości osobom trzecim zarówno odpłatnie, jak i nieodpłatnie w żadnej formie prawnej.
4. W ramach udzielonej Licencji Kupujący jest upoważniony do korzystania z Dokumentów dostarczonych z Oprogramowaniem, na polach eksploatacji wskazanych w ust. 2.

§ 6. Serwis gwarancyjny

1. Serwis gwarancyjny świadczony będzie przez Sprzedawcę przez okres ____ (zostanie wypełniony zgodnie z deklaracją Sprzedawcy złożoną w Formularzu Ofertowym) miesięcy od dnia podpisania Protokołu odbioru Dokumentacji powykonawczej, o którym mowa w § 4 ust. 10 Umowy.
2. Sprzedawca zobowiązuje się, że podczas trwania Serwisu gwarancyjnego, po otrzymaniu zgłoszenia serwisowego od Kupującego, na własny koszt i ryzyko, naprawi lub wymieni w terminach określonych w niniejszym paragrafie wadliwy Sprzęt IT na wolny od wad oraz usunie skutki tych wad. Naprawy będą dokonywane bezpośrednio przez Sprzedawcę w lokalizacji COPD, w której dokonano Wdrożenia Sprzętu IT, którego dotyczy wada.
3. Serwis gwarancyjny obejmuje dokonanie naprawy, w tym wymianę podzespołów na nowe, a także dojazd serwisanta, transport Sprzętu IT oraz podstawienie urządzeń zastępczych.
4. W ramach Serwisu gwarancyjnego Sprzedawca dokona naprawy Sprzętu IT najpóźniej w ciągu 6 godzin od otrzymania zgłoszenia serwisowego, o którym mowa w ust. 2, przy czym naprawa Sprzętu IT powinna być dokonana przez serwisanta posiadającego właściwe kwalifikacje techniczne.
5. Sprzedawca, w przypadku niemożności dokonania naprawy w terminie wskazanym w ust. 4, zobowiązany jest dokonać w tym terminie wymiany wadliwego Sprzętu IT na fabrycznie nowy, wolny od wad. Obowiązek, o którym mowa w zdaniu poprzednim dotyczy również sytuacji, gdy wada, usterka lub inna nieprawidłowość Sprzętu IT nie zostanie usunięta w wyniku dokonania naprawy po raz trzeci, przy czym termin na dostarczenie Sprzętu IT w takim wypadku wynosi 12

- godzin od otrzymania przez Sprzedawcę czwartego zgłoszenia serwisowego dotyczącego tego samego Sprzętu IT. W przypadku, gdy dostarczenie takiego samego Sprzętu IT nie będzie możliwe, Sprzedawca dostarczy nowy Sprzęt IT o parametrach technicznych nie gorszych od określonych w Załączniku nr 1 i 6 do Umowy. Dostarczenie zastępcze wymaga zgody Kupującego.
6. Sprzedawca będzie przyjmował zgłoszenia serwisowe Kupującego od osób wskazanych pisemnie przez Kupującego, w trybie 24 godziny na dobę 7 dni w tygodniu (tryb 24/7) telefonicznie pod numerem: (XX) _____, faksem pod numerem (XX) _____ lub na adres poczty elektronicznej: _____@_____ Przyjęcie zgłoszenia zostanie przez Sprzedawcę potwierdzone (drogą elektroniczną na wskazany przez Kupującego adres e-mail) w ciągu 1 godziny od otrzymania zgłoszenia. Niepotwierdzenie zgłoszenia w powyższym terminie Kupujący uznaje za przyjęcie zgłoszenia. O każdej zmianie adresu lub numerów telefonów i faksów wskazanych powyżej, Sprzedawca zobowiązany jest niezwłocznie powiadomić na piśmie Kupującego. Zmiana danych, o których mowa w zdaniu poprzedzającym nie wymaga zmiany Umowy w formie aneksu, a jedynie poinformowania drugiej Strony. Usunięcie wady lub wymiana Sprzętu IT zostaną potwierdzone Protokołem odbioru Serwisu gwarancyjnego / usunięcia wady podpisanym przez upoważnionych przedstawicieli Stron, sporządzonym według wzoru stanowiącego Załącznik nr 4a do Umowy.
 7. Dla Sprzętu IT przez naprawę należy rozumieć przywrócenie takiego stanu, w którym Sprzęt IT pracuje poprawnie i spełnia wszystkie funkcjonalności określone w Załączniku nr 1 do Umowy.
 8. Wszelkie koszty związane ze świadczeniem Serwisu gwarancyjnego obciążają Sprzedawcę.
 9. Niezależnie od uprawnień z tytułu Serwisu gwarancyjnego (gwarancji) Kupującemu przysługują wobec Sprzedawcy uprawnienia z tytułu rękojmi. Jeżeli w ramach rękojmi Kupujący zażąda wykonania przez Sprzedawcę obowiązków, określonych w niniejszym paragrafie, do terminów realizacji poszczególnych obowiązków z tytułu rękojmi mają odpowiednie zastosowanie terminy określone dla tych obowiązków w ust. 4 lub 5.
 10. Kupujący zastrzega sobie prawo do zmiany lokalizacji COPD (w obrębie Warszawy). Kupujący odinstaluje, przewiezie, dokona instalacji i uruchomi Sprzęt IT w nowej lokalizacji COPD. Uruchomienie Sprzętu IT odbędzie się w asyście przedstawiciela Sprzedawcy, jeśli Sprzedawca poinformuje Kupującego o zamiarze uczestniczenia w uruchomieniu Sprzętu IT w nowej lokalizacji COPD. Nieobecność przedstawiciela Sprzedawcy podczas uruchomienia Sprzętu IT w nowej lokalizacji nie wpływa na uruchomienie przez Kupującego Sprzętu IT oraz nie zwalnia Sprzedawcy z obowiązku świadczenia zobowiązań wynikających z Umowy zgodnie z jej postanowieniami. Zmiana lokalizacji COPD nie wymaga zmiany Umowy w formie pisemnego aneksu a jedynie poinformowania osób wskazanych przez Sprzedawcę w § 3 ust. 2 Umowy o takiej zmianie na 5 Dni Roboczych przed planowaną zmianą lokalizacji COPD. Od momentu przekazania informacji o uruchomieniu Sprzętu IT w nowej lokalizacji COPD, Sprzedawca świadczyć będzie zobowiązania wynikające z Umowy dla zmienionej lokalizacji COPD.
 11. W ramach Serwisu gwarancyjnego Kupujący będzie miał prawo dostępu do serwisu producenta Oprogramowania, w tym do:
 - 1) aktualizacji wersji Oprogramowania (*updates, upgrade, patches*) oraz nowych wersji Oprogramowania i udoskonalień do wersji bieżących Oprogramowania (nowych edycji Oprogramowania, wydań uzupełniających, poprawek programistycznych); Kupujący, w ramach wynagrodzenia, uzyskuje prawo do zainstalowania, uruchamiania, przechowywania i nieograniczonego w czasie korzystania z aktualizacji,
 - 2) monitorowania statusu zgłoszeń serwisowych;
 - 3) samodzielnego oraz za pośrednictwem Sprzedawcy zgłaszania awarii do producenta;
 - 4) samodzielnego oraz za pośrednictwem Sprzedawcy dostępu do bazy Oprogramowania, bazy wiedzy, dokumentacji i forum dyskusyjnego producenta Sprzętu IT, o ile takie istnieje;
 - 5) dostępu do bazy Oprogramowania, bazy wiedzy, dokumentacji i forum dyskusyjnego producenta, o ile takie istnieje.

§ 7. Wynagrodzenie

1. Łączne wynagrodzenie z tytułu wykonania Umowy wynosi netto zł (słownie złotych: XX/100), powiększone o należny VAT co daje kwotę brutto zł (słownie złotych: XX/100), z czego:
 - 1) wynagrodzenie za sprzedaż i dostarczenie Sprzętu IT wraz z Oprogramowaniem oraz za Serwis gwarancyjny wynosi netto zł (słownie złotych: XX/100), powiększone o należny VAT co daje kwotę brutto zł (słownie złotych: XX/100),
 - 2) wynagrodzenie za Wdrożenie i Dokumentację powykonawczą wynosi netto zł (słownie złotych: XX/100), powiększone o należny VAT co daje kwotę brutto zł (słownie złotych: XX/100),
 - 3) maksymalne wynagrodzenie z tytułu konsultacji, o których mowa w § 2 ust 4 pkt 1 Umowy wynosi netto _____,XX zł (słownie złotych: _____ XX/100) powiększone o należny podatek od towarów i usług, co daje kwotę brutto _____,XX zł (słownie złotych: _____ XX/100).
2. Wynagrodzenie, o którym mowa w:
 - 1) ust. 1 pkt 1-2 płatne będzie na podstawie faktury VAT wystawionej przez Sprzedawcę, w terminie do 28 dni licząc od dnia otrzymania przez Kupującego prawidłowo wystawionej faktury VAT łącznie z podpisanym bez zastrzeżeń przez upoważnionych przedstawicieli Stron Protokołem odbioru Dokumentacji powykonawczej, o którym mowa w § 4 ust. 10 Umowy, oraz Protokołem odbioru, o którym mowa w § 6 ust. 6, stanowiącymi podstawę wystawienia faktury VAT;
 - 2) w ust. 1 pkt 3 płatne będzie każdorazowo w terminie do 28 dni licząc od daty otrzymania przez Kupującego prawidłowo wystawionej faktury oraz podpisanego bez zastrzeżeń przez upoważnionych przedstawicieli Stron protokołu konsultacji o którym mowa w § 2 ust. 7 Umowy. Wynagrodzenie o którym mowa w zdaniu poprzednim (za konsultacje), rozliczane jest kwartalnie i wyliczane jako iloczyn ilości godzin konsultacji odebranych w danym kwartale i ceny za jedną godzinę

konsultacji określonej zgodnie z ofertą Sprzedawcy na kwotę netto ____XX zł (słownie złotych: _____ XX/100) powiększoną o należny podatek VAT, co daje kwotę brutto ____XX zł (słownie złotych: _____ XX/100).

3. Wynagrodzenie, o którym mowa w ust. 1, wyczerpuje wszelkie roszczenia finansowe Sprzedawcy z tytułu wykonania Umowy, w tym uwzględnia konsultacje, o których mowa w § 2 ust. 4 Umowy.
4. Za termin wykonania płatności uznaje się dzień obciążenia rachunku bankowego Kupującego.
5. Błędnie wystawiona faktura VAT lub brak podpisanego przez umocowanych przedstawicieli Stron Protokołu odbioru Dokumentacji powykonawczej, o którym mowa w § 4 ust. 10 Umowy spowodują naliczenie ponownego, 28-dniowego terminu płatności od dostarczenia prawidłowo wystawionej faktury VAT lub podpisanego Protokołu odbioru Dokumentacji powykonawczej.
6. Błędnie wystawiona faktura VAT lub brak podpisanego przez umocowanych przedstawicieli Stron Protokołu odbioru Serwisu gwarancyjnego / usunięcia wady lub Protokołu odbioru konsultacji, o których mowa odpowiednio w § 6 ust. 6 lub § 2 ust. 7 Umowy spowodują naliczenie ponownego, 28-dniowego terminu płatności od dostarczenia prawidłowo wystawionej faktury VAT lub podpisanego Protokołu odbioru Serwisu gwarancyjnego / usunięcia wady lub Protokołu odbioru konsultacji.
7. Jeżeli w trakcie realizacji Umowy nastąpi:
 - 1) zmiana stawki podatku od towarów i usług,
 - 2) zmiana wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej ustalonych na podstawie przepisów ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (Dz. U. z 2018, poz. 2177 tj.),
 - 3) zmiana zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne,
 - 4) zmiana zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych,
 a zmiany te będą miały wpływ na koszty wykonania Umowy – zastosowanie mają zasady wprowadzania zmian wysokości wynagrodzenia należnego Sprzedawcy określone w ust. 8-15 poniżej.
8. Zmiana wysokości wynagrodzenia wymaga zmiany Umowy w drodze aneksu.
9. Sprzedawca najpóźniej w terminie 30 dni od dnia wejścia w życie przepisów wprowadzających zmiany o których mowa w ust. 7 uprawniony jest do wystąpienia do Kupującego z pisemnym wnioskiem o dokonanie zmiany Umowy w zakresie wysokości wynagrodzenia wraz z jej uzasadnieniem oraz dokumentami niezbędnymi do oceny przez Kupującego, czy zmiany, o których mowa w ust. 7, mają wpływ na koszty wykonania Umowy przez Sprzedawcę oraz w jakim stopniu zmiany tych kosztów uzasadniają zmianę wysokości wynagrodzenia Sprzedawcy określonego w niniejszej Umowie, a w szczególności:
 - 1) szczegółową kalkulację proponowanej zmienionej wysokości wynagrodzenia Sprzedawcy oraz wykazanie adekwatności propozycji do zmiany wysokości kosztów wykonania Umowy przez Sprzedawcę.
 - 2) przyjęte przez Sprzedawcę zasady kalkulacji wysokości kosztów wykonania Umowy oraz założenia co do wysokości dotychczasowych oraz przyszłych kosztów wykonania Umowy, wraz z dokumentami potwierdzającymi prawidłowość przyjętych założeń - takimi jak np. umowy o pracę, dokumenty potwierdzające zgłoszenie pracowników do ubezpieczeń.
10. W terminie 30 dni od otrzymania wniosku o którym mowa w ust. 9, Kupujący może zwrócić się do Sprzedawcy o jego uzupełnienie lub przekazanie dodatkowych wyjaśnień lub dokumentów (np. zażądać: oryginałów do wglądu, przekazania kopii dokumentów potwierdzonych za zgodność z oryginałami).
11. Kupujący w terminie 30 dni od dnia otrzymania kompletnego wniosku zajmie w stosunku do niego pisemne stanowisko. Za dzień przekazania stanowiska uznaje się dzień jego wystania na adres właściwy dla doręczeń pism dla Sprzedawcy.
12. Kupujący najpóźniej w terminie 30 dni od dnia wejścia w życie przepisów wprowadzających zmiany, o których mowa w ust. 7 może przekazać Sprzedawcy pisemny wniosek o dokonanie zmiany Umowy. Wniosek powinien zawierać co najmniej propozycję zmiany Umowy w zakresie wysokości wynagrodzenia oraz powołanie zmian przepisów.
13. Przed przekazaniem wniosku, o którym mowa w ust. 12, Kupujący może zwrócić się do Sprzedawcy o złożenie wyjaśnień lub dokumentów (oryginałów do wglądu lub kopii potwierdzonych za zgodność z oryginałem) niezbędnych do oceny przez Kupującego, czy zmiany, o których mowa w ust. 7, mają wpływ na koszty wykonania Umowy przez Sprzedawcę oraz w jakim stopniu zmiany tych kosztów uzasadniają zmianę wysokości wynagrodzenia. Rodzaj i zakres tych informacji określi Kupujący. Postanowienia ust. 10-15 stosuje się odpowiednio, z tym, że Sprzedawca jest zobowiązany w każdym przypadku do zajęcia pisemnego stanowiska w terminie 30 dni od dnia otrzymania wniosku od Kupującego.
14. W przypadku niewykonania lub nienależytego wykonania przez Sprzedawcę zobowiązania określonego w ust. 13 w terminie określonym w ust. 13, Sprzedawca zapłaci na rzecz Kupującego karę umowną w wysokości 0,1 % wynagrodzenia brutto określonego w ust.1 za każdy rozpoczęty dzień kalendarzowy opóźnienia. Jeżeli w terminie określonym w ust. 13 Sprzedawca nie przedłoży wyjaśnień lub dokumentów, o których mowa w ust. 13 lub przedłożone przez Sprzedawcę wyjaśnienia lub dokumenty będą niewystarczające do dokonania przez Kupującego oceny, o której mowa w ust. 13 – Kupujący wyznaczy Sprzedawcy dodatkowy termin, nie dłuższy niż 10 dni, na dostarczenie lub uzupełnienie wyjaśnień lub dokumentów. W przypadku bezskutecznego upływu terminu wyznaczonego zgodnie ze zdaniem drugim, Kupujący uprawniony będzie do wypowiedzenia Umowy z zachowaniem miesięcznego terminu wypowiedzenia.
15. Jeżeli w trakcie procedury opisanej w ust. 9-14 zostanie wykazane, że zmiany, o których mowa w ust. 7 uzasadniają zmianę wysokości wynagrodzenia, Strony uzgodnią treść aneksu do Umowy oraz podpiszą aneks, z zachowaniem zasady zmiany

wysokości wynagrodzenia w kwocie odpowiadającej zmianie kosztów wykonania Umowy wywołanych przyczynami określonymi w ust. 10.

§ 8. Kary umowne i roszczenia odszkodowawcze

1. W przypadku opóźnienia Sprzedawcy w dostarczeniu Sprzętu IT wraz z Oprogramowaniem, Dokumentów oraz w realizacji Wdrożenia w terminie wskazanym w § 4 ust. 1 lub ust. 2 Umowy Kupującemu przysługuje kara umowna w wysokości 2.000,00 zł (słownie złotych: dwa tysiące 00/100) za każdy rozpoczęty dzień kalendarzowy opóźnienia.
2. Jeśli opóźnienie, o którym mowa w ust. 1 trwało będzie dłużej niż 14 dni, Kupujący może, bez wyznaczenia dodatkowego terminu, odstąpić od Umowy (w terminie 14 dni od wystąpienia przestanki uprawniającej do odstąpienia) oraz zażądać kary umownej w wysokości 20 % kwoty łącznego wynagrodzenia brutto określonego w § 7 ust. 1 Umowy.
3. W przypadku opóźnienia Sprzedawcy w wymianie Sprzętu IT na fabrycznie nowy, wolny od wad w okresie Serwisu gwarancyjnego (gwarancji) lub rękomi, w stosunku do terminów, o którym mowa w § 6 ust. 4 lub 5 Umowy, Kupującemu przysługuje kara umowna w wysokości 0,1 % kwoty łącznego wynagrodzenia brutto określonego w § 7 ust. 1 Umowy za każdy rozpoczęty dzień kalendarzowy, jeżeli termin liczony jest w dniach lub odpowiednio kara umowna w wysokości 0,02 % kwoty łącznego wynagrodzenia brutto określonego w § 7 ust. 1 Umowy, za każdą rozpoczętą godzinę opóźnienia, jeżeli termin liczony jest w godzinach.
4. Jeżeli opóźnienie, o którym mowa w ust. 3 trwało będzie dłużej niż 24 godziny (dla terminów liczonych w godzinach) lub odpowiednio 3 dni (dla terminów liczonych w dniach), Kupujący, w terminie 14 dni od upływu terminu powyższego opóźnienia, ma prawo, według własnego wyboru:
 - 1) odstąpić od Umowy bez konieczności wyznaczenia dodatkowego terminu na usunięcie wad oraz żądać kary umownej w wysokości 20 % kwoty łącznego wynagrodzenia brutto określonego w § 7 ust. 1 Umowy,
 - 2) dokonać zastępczej wymiany Sprzętu IT na koszt Sprzedawcy,
 - 3) naliczyć 2-krotność kary umownej określonej w ust. 3, począwszy odpowiednio od 25 godziny opóźnienia lub od 4 dnia opóźnienia, do terminu, w którym zostanie wymieniony Sprzęt IT.
5. W przypadku opóźnienia Sprzedawcy w dostarczeniu Sprzętu IT wraz z Oprogramowaniem lub Dokumentów wolnych od wad lub ponownego wykonania Wdrożenia, w stosunku do terminu, o którym mowa w § 4 ust. 8, Sprzedawca zapłaci karę umowną w wysokości 2.000,00 zł (słownie złotych: dwa tysiące 00/100) za każdy rozpoczęty dzień opóźnienia.
6. W przypadku opóźnienia Sprzedawcy w odbiorze Sprzętu IT wraz z Oprogramowaniem i Dokumentów z miejsca dostarczenia, w stosunku do terminu, o którym mowa w § 4 ust. 9, Sprzedawca zapłaci karę umowną w wysokości 2.000,00 zł (słownie złotych: dwa tysiące 00/100) za każdy rozpoczęty dzień kalendarzowy opóźnienia. W przypadku ponownej odmowy odbioru Sprzętu IT, o której mowa w § 4 ust. 9 Umowy, Kupujący ma prawo odstąpić od Umowy w terminie 30 dni od daty przekazania Sprzedawcy protokołu odmowy odbioru Sprzętu IT i żądać kary umownej w wysokości 20 % kwoty łącznego wynagrodzenia brutto określonego w § 7 ust. 1 Umowy, z zachowaniem prawa do kary umownej określonej w zdaniu poprzednim, naliczonej do dnia odstąpienia.
7. W przypadku opóźnienia Sprzedawcy w dostarczeniu Kupującemu Dokumentacji powykonawczej w stosunku do terminu o którym mowa w § 4 ust. 10 Sprzedawca zapłaci karę umowną w wysokości 2.000,00 zł (słownie złotych: dwa tysiące 00/100) za każdy rozpoczęty dzień kalendarzowy opóźnienia.
8. Jeżeli na skutek niewykonania lub nienależytego wykonania Umowy powstanie szkoda przewyższająca zastrzeżoną karę umowną, bądź szkoda powstanie z innych przyczyn niż te, dla których zastrzeżono karę, Kupującemu przysługuje prawo do dochodzenia odszkodowania uzupełniającego na zasadach ogólnych Kodeksu cywilnego.
9. Kary umowne płatne są w terminie 14 dni od daty otrzymania wezwania. Niezależnie od powyższego kary umowne mogą być potrącane z wynagrodzenia należnego Sprzedawcy lub z zabezpieczenia należytego wykonania Umowy.

§ 9. Prawa autorskie

1. Sprzedawca zapewnia, że korzystanie przez Kupującego z Dokumentacji powykonawczej nie będzie naruszało praw osób trzecich. Na podstawie Umowy Sprzedawca przeniesie na Kupującego autorskie prawa majątkowe w zakresie i w sposób opisany poniżej.
2. Z dniem podpisania Protokołu odbioru Dokumentacji powykonawczej, o którym mowa w § 4 ust. 10 Umowy, Sprzedawca przenosi na Kupującego autorskie prawa majątkowe do Dokumentacji powykonawczej, na polach eksploatacji wskazanych w ust. 3, w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 pkt 2 Umowy.
3. Przeniesienie autorskich praw majątkowych do utworów, o których mowa w niniejszym paragrafie, obejmuje następujące pola eksploatacji:
 - 1) w zakresie utwalania i wielokrotniania utworu – wytwarzanie każdą techniką egzemplarzy utworów, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;
 - 2) w zakresie obrotu oryginałem oraz egzemplarzami, na których utwory utwalono – wprowadzanie do obrotu, użyczenie oraz najem oryginału oraz egzemplarzy;
 - 3) w zakresie rozpowszechniania utworów w sposób inny niż określony w pkt. 2 – publiczne wykonanie, wystawienie, wyświetlanie, odtwarzanie oraz nadawanie i reemitowanie, a także publiczne udostępnianie utworów w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i w czasie przez siebie wybranym;
 - 4) dowolne przetwarzanie utworów, w tym łączenie z innymi utworami;
 - 5) zezwolenie na wykonywanie zależnych praw autorskich poprzez rozporządzenie i korzystanie na wszystkich polach eksploatacji wymienionych w pkt. 1-4.
4. Z dniem dokonania przez Kupującego odbioru Dokumentacji powykonawczej, Kupujący nabywa własność nośników, na których utwory te utwalono, w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 pkt 2 Umowy.

§ 10. Wady prawne

1. Sprzedawca gwarantuje, że Sprzęt IT, Oprogramowanie, Dokumenty oraz Dokumentacja powykonawcza nie naruszają praw własności intelektualnej ani innych praw osób Trzecich.
2. W przypadku wystąpienia osób trzecich wobec Kupującego z roszczeniami opartymi na twierdzeniu, iż używany przez Kupującego Sprzęt IT, Oprogramowanie, Dokumenty lub Dokumentacja powykonawcza naruszają jakiegokolwiek prawa, o których mowa w ust. 1, Kupującemu przysługują wszystkie niżej wymienione uprawnienia, które ma prawo zrealizować według swojego wyboru (łącznie lub osobno):
 - 1) prawo odstąpienia od Umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach z wyłączeniem zapłaty na rzecz Sprzedawcy jakichkolwiek kosztów, odszkodowań itp.,
 - 2) prawo żądania zapłaty przez Sprzedawcę kary umownej w wysokości 20 % łącznego wynagrodzenia brutto określonego w § 7 ust. 1 Umowy oraz prawo żądania odszkodowania uzupełniającego na zasadach ogólnych Kodeksu cywilnego.
3. W przypadku wytoczenia przeciwko Kupującemu powództwa opartego na twierdzeniu opisanym w ust. 2, Sprzedawca zobowiązuje się zapewnić Kupującemu na swój koszt ochronę sądową oraz ponieść konsekwencje zapadłego wyroku sądowego.

§ 11. Zabezpieczenie należytego wykonania Umowy (dalej: „ZNWU”)

1. Sprzedawca złożył u Kupującego ZNWU w jednej z form, o których mowa w art. 148 ust. 1 ustawy Prawo zamówień publicznych, w wysokości zł (słownie złotych: XX/100).
2. ZNWU dotyczy pokrycia ewentualnych roszczeń wynikających z niewykonania lub nienależytego wykonania Umowy.
3. ZNWU zostanie zwolnione (zwrócone):
 - 1) w wysokości 70% zabezpieczenia w terminie 30 dni od dnia podpisania bez zastrzeżeń Protokołu odbioru, o którym mowa w § 4 ust. 7 Umowy,
 - 2) w wysokości 30 % zabezpieczenia w terminie 15 dni po upływie okresu Serwisu gwarancyjnego i rękojmi.
4. W przypadku zmiany formy ZNWU w trakcie trwania Umowy obowiązować będą poniższe zasady.
5. ZNWU w formie pieniężnej Sprzedawca wpłaca przelewem na rachunek bankowy wskazany przez Kupującego.
6. ZNWU wnoszone w formie gwarancji bankowej lub ubezpieczeniowej może być wystawione przez bank albo ubezpieczyciela. Bank lub ubezpieczyciel zapłaci, na rzecz Kupującego w terminie 30 dni od pisemnego żądania kwotę zł (słownie złotych: XX/100), na pierwsze wezwanie Kupującego, bez odwołania, bez warunku, niezależnie od kwestionowania czy zastrzeżeń Sprzedawcy i bez dochodzenia czy wezwanie Kupującego jest uzasadnione czy nie.
7. ZNWU wnoszone w formie poręczenia ma być wystawione przez bank, spółdzielczą kasę oszczędnościowo-kredytową lub podmiot, o którym mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości, który poręczy należyte wykonanie Umowy do wysokości zł (słownie złotych: XX/100).
8. W przypadku, gdy ZNWU, o którym mowa w ust. 1 będzie wnoszone w formie: poręczenia, bankowej lub ubezpieczeniowej gwarancji, Kupujący zastrzega sobie prawo do akceptacji projektu tych dokumentów.
9. ZNWU wniesione w formie pieniężnej podlega zwrotowi wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszty prowadzenia rachunku bankowego oraz prowizji bankowej za przelew pieniędzy na rachunek Sprzedawcy.
10. ZNWU w formie innej niż pieniężna Sprzedawca złoży u Kupującego w Kancelarii Główniej, Warszawa ul. Poleczki 33, z dopiskiem „Dla Departamentu Informatyki”.

§ 12. Odstąpienie od Umowy

1. Strony mogą odstąpić od Umowy w przypadkach przewidzianych obowiązującymi przepisami, a także w przypadku zaistnienia okoliczności, o których mowa w Umowie.
2. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy lub dalsze wykonywanie umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, Kupujący może odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach. W takim wypadku Sprzedawca może żądać jedynie wynagrodzenia należnego z tytułu wykonania części Umowy.
3. Przy wykonaniu Umowy Sprzedawca bez zgody Kupującego nie ma prawa do korzystania w jakimkolwiek charakterze z osób zatrudnionych u Kupującego, pod rygorem odstąpienia od Umowy przez Kupującego z winy Sprzedawcy w terminie 30 dni od powzięcia wiadomości o zaistnieniu takiego faktu oraz żądania zapłaty kary umownej, o której mowa w ust. 4.
4. W wyniku wystąpienia okoliczności, o której mowa w ust. 3 Sprzedawca jest zobowiązany do zapłaty w terminie 14 dni od wezwania przez Kupującego kary umownej w wysokości 20.000,00 zł (słownie złotych: dwadzieścia tysięcy 00/100). Jeżeli szkoda poniesiona przez Kupującego jest wyższa od zastrzeżonej wyżej kary umownej, Kupujący może dochodzić odszkodowania uzupełniającego od Sprzedawcy na zasadach ogólnych Kodeksu cywilnego.
5. Wszelkie zmiany treści Umowy wymagają formy pisemnej pod rygorem nieważności, za wyjątkiem tych, dla których w Umowie zastrzeżono inną formę.

§ 13. Zawiadomienia

1. Wszelkie zawiadomienia wymienione w Umowie, niezależnie od nazwy, pod którą występują, dla swojej skuteczności Strony muszą przekazać osobiście za potwierdzeniem odbioru lub pocztą poleconą za zwrotnym poświadczaniem ich odbioru i będą uważane za skutecznie doręczone w dniu ich odbioru, z zastrzeżeniem § 6 ust. 6 Umowy.

2. Zawiadomienia, zapytania, informacje nie wymienione w postanowieniach Umowy mogą być przesyłane telefaksem, doręczane osobiście, przesyłane kurierem lub listem, pod warunkiem ich potwierdzenia przez drugą Stronę.
3. Zawiadomienia będą wysyłane na adresy Stron wskazane w komparycji Umowy. Każda ze Stron zobowiązana jest do informowania drugiej Strony o każdej zmianie adresu. Jeżeli Strona nie powiadomiła o zmianie adresu, zawiadomienia wysłane na ostatni znany adres Strony uznają za doręczone. Powiadomienie o powyższych zmianach nie stanowi zmiany Umowy wymagającej sporządzenia aneksu.

§ 14. Poufność, bezpieczeństwo informacji i zasady przetwarzania danych osobowych

1. Wszelkie wiadomości dotyczące Stron Umowy oraz warunków Umowy, w których posiadanie weszła druga Strona przy zawieraniu i wykonywaniu Umowy mają charakter poufny. Każda ze Stron zobowiązuje się nie ujawniać ich osobom trzecim, także po zakończeniu Umowy, wyjąwszy przypadki przewidziane prawem.
2. Sprzedawca zobowiązuje się do zapoznania się i przestrzegania przyjętych u Kupującego zasad bezpieczeństwa informacji, których treść została określona w Załączniku nr 6 (Regulamin bezpieczeństwa fizycznego i środowiskowego) i nr 12 (Regulamin eksploatacji systemów teleinformatycznych) do Zarządzenia nr 78/2019 w sprawie wprowadzenia Polityki bezpieczeństwa informacji w ARiMR, które stanowią Załącznik nr 5a do Umowy.
3. Sprzedawca potwierdza fakt zapoznania się, w zakresie dotyczącym Umowy, z Załącznikami nr 6 i nr 12 do Zarządzenia, o którym mowa w ust. 2 podpisując oświadczenie. Wzór oświadczenia stanowi Załącznik nr 5b do Umowy.
4. Sprzedawca zobowiązuje się do przestrzegania przy wykonywaniu Umowy przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2) oraz przepisów krajowych wydanych w związku z ogólnym rozporządzeniem o ochronie danych, zwanym dalej: „RODO”.
5. Sprzedawca pisemnie zobowiąże pracowników i osoby trzecie realizujące zobowiązania określone w Umowie do przestrzegania przepisów, o których mowa w ust. 2 i 4.
6. Sprzedawca oświadcza, że zapoznał się z klauzulą informacyjną w zakresie przetwarzania danych osobowych, stanowiącą Załącznik nr 6a do Umowy.
7. Sprzedawca zobowiązuje się do złożenia oświadczenia o wypełnieniu obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane bezpośrednio lub pośrednio pozyskał w celu zawarcia oraz wykonania Umowy zgodnie z wzorem oświadczenia stanowiącym Załącznik nr 6b do Umowy.

§ 15. Postanowienia końcowe

1. W sprawach nieuregulowanych Umową mają zastosowanie przepisy Kodeksu cywilnego, ustawy Prawo zamówień publicznych oraz ustawy o prawie autorskim i prawach pokrewnych.
2. Ewentualne spory mogące wyniknąć na tle wykonania Umowy rozstrzygać będzie sąd powszechny właściwy dla siedziby Kupującego.
3. Sprzedawca nie może bez zgody Kupującego przenieść praw wynikających z Umowy na osoby trzecie.
4. Załączniki wymienione w Umowie stanowią jej integralną część.
Poniżej przedstawiono spis załączników:
 - 1) Załącznik nr 1 – Specyfikacja Sprzętu IT i Oprogramowania oraz zasady Wdrożenia;
 - 2) Załącznik nr 2a – Protokół odbioru Sprzętu IT, Oprogramowania i Dokumentów (wzór);
 - 3) Załącznik nr 2b – Protokół Wdrożenia (wzór);
 - 4) Załącznik nr 3 – Protokół odbioru Dokumentacji powykonawczej (wzór);
 - 5) Załącznik nr 4a – Protokół odbioru Serwisu gwarancyjnego / usunięcia wady (wzór);
 - 6) Załącznik nr 4b – Protokół odbioru konsultacji (wzór);
 - 7) Załącznik nr 5a – Oświadczenie o zapoznaniu się z treścią Załączników nr 6 i 12 do Zarządzenia Prezesa ARiMR nr 78/2019 z dnia 3 czerwca 2019 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji w ARiMR
 - 8) Załącznik nr 5b – Treść Załączników nr 6 i 12 do Polityki bezpieczeństwa informacji w ARiMR wprowadzonej Zarządzeniem Prezesa ARiMR nr 78/2019 z dnia 3 czerwca 2019 r. w sprawie wprowadzenia;
 - 9) Załącznik nr 6a – Klauzula informacyjna dotycząca przetwarzania danych osobowych;
 - 10) Załącznik nr 6b – Oświadczenie o wypełnieniu obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO (wzór);
 - 11) Załącznik nr 7 – Formularz ofertowy.
 - 12) Załącznik nr 8 – Wykaz osób.
5. Umowę sporządzono w 4 jednobrzmiących egzemplarzach, w tym jeden dla Sprzedawcy i trzy dla Kupującego.

Sprzedawca

Kupujący

Specyfikacja Sprzętu IT i Oprogramowania oraz zasady Wdrożenia**I. Sprzęt IT (Load Balancer) – 2 szt., wymagania minimalne i parametry techniczne:**

1. Sprzęt IT musi być dedykowaną platformą sprzętową typu appliance.
2. Sprzęt IT musi realizować następujące funkcje:
 - f) rozkład ruchu pomiędzy serwerami aplikacji Web;
 - g) selektywny http caching;
 - h) selektywna kompresja danych;
 - i) terminowanie sesji SSL;
 - j) optymalizacja i akceleracja aplikacji.
3. Wszystkie wymienione funkcje muszą być dostępne w obrębie jednego Sprzętu IT.
4. Sprzęt IT musi posiadać następujące metody równoważenia obciążenia:
 - i) cykliczna;
 - j) ważona;
 - k) najmniejsza liczba połączeń;
 - l) najszybsza odpowiedź serwera;
 - m) najmniejsza liczba połączeń i najszybsza odpowiedź serwera;
 - n) najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie;
 - o) dynamicznie ważona oparta na SNMP/WMI;
 - p) definiowana na podstawie grupy priorytetów dla serwerów;
5. Sprzęt IT musi posiadać wbudowany w system operacyjny język skryptowy, posiadający następujące cechy:
 - d) analiza, zmiana oraz zastępowanie parametrów w nagłówku http oraz w zawartości pakietów;
 - e) obsługa protokołów: http, tcp, xml, rtsp, sip;
 - f) musi posiadać funkcję inspekcji protokołów LDAP oraz RADIUS.
6. Język skryptowy musi bazować na języku programowania Tool Command Language lub równoważnym, z własnymi komendami.
7. Musi istnieć możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego.
8. Producent Sprzęt IT musi dostarczyć darmową, specjalizowaną aplikację do analizy poprawności składni skryptów pisanych przy wykorzystaniu języka skryptowego opisanego w pkt. 6. Aplikacja musi posiadać wbudowane szablony skryptów oraz funkcję automatycznego uzupełniania wpisywanych komend lub posiadać mechanizm analizy poprawności składni skryptów w graficznym interfejsie zarządzania.
9. Rozwiązanie musi pracować w trybie pełnego proxy.
10. Praca w trybie pełnego proxy nie może powodować degradacji wydajności rozwiązania.
11. Rozwiązanie musi posiadać programowalny interfejs API do integracji z zewnętrznymi systemami oraz automatyzacji wykonywania operacji.
12. Funkcjonalność lokalnego równoważenia obciążenia:
 - f) wspierane mechanizmy równoważenia obciążenia: round robin, ważona, dynamicznie ważona (na podstawie SNMP/WMI), najmniejsza liczba połączeń, najszybsza odpowiedź, observer, predictive, grupy priorytetów, możliwość modyfikacji za pomocą języka skryptowego;
 - g) buforowanie połączeń TCP w przypadku osiągnięcia zadanej ilości sesji dla danego serwera;
 - h) obsługiwane mechanizmy monitorowania stanu serwerów: ICMP, echo (port 7/TCP), TCP, TCP half-open, UDP, SSL, http/https, LDAP, zapytania do baz MS SQL i Oracle, FTP, SIP, SMB/CIFS, RADIUS, SIP, POP3, IMAP, SMTP, SNMP, SOAP, sprawdzanie odpowiedzi w oparciu o wyrażenia regularne. Dodatkowo musi istnieć możliwość wykorzystania skryptów do tworzenia złożonych monitorów sprawdzających aktywność usług;
 - i) obsługiwane mechanizmy przywiązywania sesji: cookie (hash, rewrite, custom, insert, passive), adres źródłowy, adres docelowy, SSL ID, RDP login name, JSESSIONID, SIP call ID;
 - j) wsparcie dla usług warstw 4-7: inspekcja warstwy 7, wstrzykiwanie nagłówków http, ukrywanie zasobów, zmiana odpowiedzi serwera, zaszyfrowane cookies, przepisywanie odpowiedzi, ochrona przed atakami DoS/DDoS i SYN Flood, multipleksacja zapytań HTTP, kompresja i cache'owanie http.
13. Optymalizacja i akceleracja aplikacji:
 - f) Sprzęt IT musi optymalizować protokół TCP i posiadać predefiniowane profile dla następujących charakterystyk sieci:
 - i. LAN;
 - ii. WAN;
 - iii. urządzeń mobilnych;
 - g) Sprzęt IT powinno implementować TCP proxy z mechanizmem zamykania okna w stronę serwera www w przypadku zbyt wolnego odbierania danych przez zdalnego klienta;
 - h) Sprzęt IT musi mieć możliwość włączenia ignorowania nagłówków przeglądarki dotyczących cachowania (Cache-control);
 - i) Sprzęt IT musi wspierać multipleksację wielu zapytań http w tej samej sesji TCP;
 - j) Sprzęt IT musi umożliwiać kompresję zwracanej zawartości http. Użycie kompresji powinno być zależne od:
 - v. listy dozwolonych URI;
 - vi. listy wykluczonych URI;
 - vii. listy kompresowalnych Content-Type;
 - viii. listy wykluczonych Content-Type.
14. Sprzęt IT musi posiadać następujące interfejsy administracyjne:
 - d) GUI przy wykorzystaniu protokołu https;
 - e) zarządzanie poprzez SSH;
 - f) zarządzanie poprzez API REST.

15. Autoryzacja administratorów Sprzętu IT musi bazować na rolach użytkowników.
16. Sprzęt IT musi posiadać funkcje przywiązywania sesji (*Session persistence*) przy wykorzystaniu następujących atrybutów:
 - h) Cookie (hash, rewrite, custom, insert, passive);
 - i) adres źródła;
 - j) SIP call ID;
 - k) identyfikator sesji SSL;
 - l) Microsoft Terminal Services (RDP) – nazwa użytkownika;
 - m) adres docelowy;
 - n) tworzone przez administratora przy wykorzystaniu języka skryptowego z pkt. 5.
17. Sprzęt IT musi posiadać funkcję definiowania maksymalnej ilości obsługiwanych przez dany serwer połączeń, w przypadku przekroczenia zdefiniowanej wartości musi istnieć możliwość wystania klientowi strony błędu lub przekierowania klienta na inny serwer.
18. Sprzęt IT musi zapewniać możliwość klonowania puli serwerów umożliwiając wysyłanie kopii ruchu do zewnętrznych systemów monitoringu lub urządzeń typu IDS/IPS.
19. Sprzęt IT musi zapewniać obsługę certyfikatów z kluczami typu ECDSA wykorzystującymi krzywe eliptyczne (ECC) zarówno od strony klienta, jak i od strony puli serwerów.
20. Sprzętowe wsparcie dla algorytmów AES, AES-GCM, RSA, DSA, DH, ECDSA, ECDH, SHA2. Wsparcie dla Perfect Forward Secrecy.
21. Dla protokołu TLS 1.2 wymagana jest obsługa AES-GCM zarówno od strony klienta, jak i od strony puli serwerów.
22. Wsparcie dla protokołu TLS 1.3.
23. Sprzęt IT musi zapewniać obsługę certyfikatów podpisanych funkcją skrótu SHA-2 zarówno od strony klienta, jak i od strony puli serwerów.
24. Sprzęt IT musi obsługiwać sieci VLAN w standardzie 802.1q.
25. Sprzęt IT musi obsługiwać agregację linków w standardzie 802.3ad (LACP).
26. Sprzęt IT musi obsługiwać Jumbo Frames.
27. Sprzęt IT musi posiadać funkcjonalność bramy VXLAN oraz NVGRE.
28. Sprzęt IT musi świadczyć następujące usługi w warstwach 4-7:
 - h) inspekcja warstwy aplikacji, w tym inspekcja nagłówka http;
 - i) ukrywanie zasobów;
 - j) zmiana odpowiedzi serwera;
 - k) przepisywanie odpowiedzi (*response rewriting*);
 - l) ochrona przed atakami typu DoS/DDoS;
 - m) ochrona przed atakami typu SYN Flood;
 - n) multipleksowanie połączeń http.
29. Sprzęt IT musi posiadać następujące funkcje zarządzania siecią:
 - i) obsługa protokołu SNMP v1/v2c/v3;
 - j) możliwość budowania własnych zdarzeń SNMP z własnymi numerami OID;
 - k) zewnętrzny syslog;
 - l) zbieranie danych i ich wyświetlanie;
 - m) zbieranie danych zgodnie z ustawieniami administratora;
 - n) osobna brama domyślna dla interfejsu zarządzającego;
 - o) zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy);
 - p) dedykowany podsystem monitorowania stanu pracy Sprzętu IT (*always on management*) z funkcjami restartu, wstrzymania oraz sprzętowego resetu Sprzętu IT.
30. Sprzęt IT musi posiadać funkcję integracji z zewnętrznymi serwerami uwierzytelnienia użytkowników LDAP, RADIUS, TACACS.
31. Sprzęt IT musi posiadać funkcję definiowania i edycji szablonów konfiguracji aplikacji. Szablony powinny służyć do optymalizacji procesu wdrażania Sprzętu IT zarówno dla znanych aplikacji biznesowych, jak i własnych aplikacji klienta. W ramach opisanych szablonów musi istnieć możliwość automatycznej kontroli poszczególnych elementów konfiguracji szablonu i zabezpieczenie ich przed modyfikacją i usunięciem.
32. Sprzęt IT musi posiadać moduł analizy ruchu http. Moduł powinien zbierać następujące metryki:
 - i) czas odpowiedzi per serwer;
 - j) czas odpowiedzi per URI;
 - k) ilość sesji użytkownika;
 - l) przepustowość;
 - m) adres źródła;
 - n) kraj;
 - o) User Agent (wykorzystywana przez klienta aplikacja);
 - p) metoda dostępu.
33. Sprzęt IT musi posiadać funkcję walidacji certyfikatów klientów łączących się przy wykorzystaniu protokołu SSL.
34. Sprzęt IT musi oferować podział na tzw. partycje administracyjne. Zdefiniowany użytkownik może zarządzać konfiguracją tylko i wyłącznie wewnątrz swojej partycji.
35. Sprzęt IT musi oferować wsparcie dla tzw. domen routingu (*Virtual Routing and Forwarding*). Rozwiązanie takie oferuje separację ruchu sieciowego do różnych aplikacji. Musi umożliwiać poprawnie działanie rozwiązania, kiedy podłączone VLANy do Sprzętu IT mają takie same podsieci i adresy IP.
36. Sprzęt IT musi oferować stworzenie minimum 10 partycji administracyjnych oraz 100 jednoczesnych domen routingu. Partycje administracyjne i domeny routingu muszą być dostępne również, jeżeli Sprzęt IT pracuje w formie klastra.
37. Rozwiązanie musi być dostarczone w formie klastra wysokiej dostępności (HA) złożonego z dwóch urządzeń tego samego typu pracujących w trybie *active – standby* z możliwością realizacji trybu *active-active* oraz rozbudowy do klastra N+1.
38. Sprzęt IT musi umożliwiać podział urządzenia na wirtualne części, przy czym każda taka część musi pracować logicznie jako niezależne urządzenie z niezależnym oprogramowaniem (każda część może posiadać inną wersję oprogramowania oraz osobną tablicę routingu). Sprzęt IT musi umożliwić podział na minimum 8 wirtualnych części.

39. Klaster wysokiej dostępności musi zapewniać kopiowanie informacji o sesji SSL i stanu sesji TCP pomiędzy urządzeniami, aby uniknąć ponownej negocjacji po przetączeniu ruchu.
40. Klaster wysokiej dostępności musi zapewniać synchronizację:
 - d) konfiguracji;
 - e) stanu połączeń;
 - f) przywiązywania sesji (*Session persistence*).
41. Wykrycie awarii Sprzętu IT w klastrze odbywać się musi przy użyciu weryfikacji stanu pracy Sprzętu IT poprzez analizę aktywności w sieci (*Network failover*).
42. Sprzęt IT musi być dostarczony z 4 sztukami licencji testowych do wykorzystania w środowiskach testowo-deweloperskich.
43. Licencje testowe muszą być rozwiązaniem wirtualnym działającym w następujących środowiskach:
 - a) VMware ESXi 5.5 U3, 6.0 U2, 6.5;
 - b) Microsoft Hyper-V dla Windows 2008 R2 SP1, Windows 2012, Windows 2012 R2 RTM i Update 1, Windows Server 2016;
 - c) Linux KVM dla CentOS/RHEL od 6.3, Ubuntu od 14.04, Debian od 7.1;
 - d) Microsoft Azure.
44. Licencje testowe muszą zawierać w sobie wszystkie wyspecyfikowane wyżej funkcjonalności z wyłączeniem subskrypcji dla serwisu reputacyjnego i z kampaniami oraz wymagań wydajnościowych.
45. Sprzęt IT w postaci jednego urządzenia musi spełniać wymogi przedstawione w Tabeli 1 (poniżej).

Tabela 1. Wymagania minimalne dla pojedynczego Sprzętu IT:

Lp.	Parametr:	Minimalne wartości parametru:
1	Pamięć	48 GB
2	Dysk twardy	jeden dysk SSD o pojemności 480 GB
3	Przepływność dla warstwy 4	60 Gbps
4	Przepływność dla warstwy 7	35 Gbps
5	Przepływność wewnętrznej magistrali	640 Gbps
6	Ilość jednocześnie obsługiwanych połączeń	40 000 000
7	Ilość transakcji SSL na sekundę dla klucza o długości 2048	35 000
8	Ilość transakcji SSL na sekundę dla szyfrowania ECC (ECDHE-ECDSA-AES128-SHA256)	20 000
9	Przepływność ruchu szyfrowanego	20 Gbps
10	Ilość połączeń na sekundę w warstwie 4	800 000
11	Kompresja sprzętowa	20 Gbps
12	Sprzętowa ochrona DDoS	50 000 000 SYN cookies na sekundę
13	Gęstość interfejsów	8 interfejsów z możliwością obsadzenia wkładkami SFP (T, SX lub LX) lub SFP+ 10G (SR lub LR). 4 interfejsy z możliwością obsadzenia wkładkami 40Gb QSFP+. oddzielny interfejs zarządzania, port konsolowy, interfejs szeregowy failover, port USB. 2 wkładki QSFP+ 40Gb. 2 wkładki QSFP+ 40Gb do switcha Cisco Nexus 6004, do którego zostanie podłączony Sprzęt IT. Wymagane jest dostarczenie odpowiednich kabli transmisyjnych w ilości 2 sztuk dla każdego Sprzętu IT w celu połączenia z dostarczonymi wkładkami do switchy Cisco Nexus 6004. Dostarczone wkładki muszą być oficjalnie wspierane przez producentów zarówno Sprzętu IT jak i urządzenia, do którego zostaną podłączone. Dostarczone wkładki nie mogą nieść ze sobą ryzyka odmowy świadczenia gwarancji, serwisu bądź pomocy technicznej przez producenta. Dostarczone wkładki muszą być objęte takimi samymi świadczeniami serwisowo-gwarancyjnymi jak Sprzęt IT oraz pochodzić z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej.
14	Zarządzanie	Panel i wyświetlacz LCD z funkcjami: ustawienia adresu IP na potrzeby zarządzania, ustawienia parametrów portu szeregowego, wyświetlania podstawowych alarmów, możliwości restartu Sprzętu IT, wyświetlania informacji o Sprzęcie IT. Funkcjonalność „Always On Management”.
15	Obudowa	Przeznaczona do montażu w szafie rack 19", wysokość nie większa niż 2U.
16	Zasilanie	2 redundantne zasilacze - prąd zmienny 230V AC.
17	Wymagana certyfikacja	EN 300 386 V1.6.1 (2012) EN 55032:2012 Class A EN 61000-3-2:2014 EN 61000-3-3:2013 EN 55024:2010 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
18	MTBF	69 000 godzin

II. W ramach Wdrożenia Sprzedawca wykona następujące czynności:

- 1) przygotuje konfigurację Sprzętu IT (konfiguracja klastra rozciągniętego na dwie lokalizacje);
- 2) zainstaluje oraz skonfiguruje Sprzęt IT i Oprogramowanie w COPD, w wskazanym przez Kupującego miejscu, przy czym Wdrożenie obejmuje dostawę i montaż wkładek oraz kabli logicznych i zasilających;
- 3) dokona przeniesienia z 4 szt. urządzeń F5 BIG IP wszystkich funkcjonalności zaimplementowanych na Sprzęt IT;
- 4) uruchomi Sprzęt IT oraz przedstawi, na życzenie Kupującego, wskazane przez Kupującego funkcjonalności Sprzętu IT i Oprogramowania, o których mowa w niniejszym Załączniku oraz w Załączniku nr 7 do Umowy;
- 5) uruchomi Sprzęt IT produkcyjnie z funkcjonalnościami wskazanymi przez Kupującego;
- 6) dokona instruktażu obsługi wdrożonych Sprzętu IT dla 10 pracowników Kupującego, przy czym czas trwania instruktażu wyniesie do 5 Dni Roboczych.

Załącznik nr 2b do Umowy nr ____/DI/20.../2610 z dnia _____ 20.... r.

Protokół odbioru Wdrożenia
(wzór)

Zgodnie z Umową nr/DI/2019/2610 zawartą w dniu 2019 r. pomiędzy Agencją Restrukturyzacji i Modernizacji Rolnictwa (Kupujący) a, Kupujący potwierdza, że Sprzedawca wykonał Wdrożenie zgodnie z Umową:

Lp.	Wdrożenie	Liczba	Numer seryjny/wersja*
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Upoważnieni przedstawiciele Kupującego i Sprzedawcy złożonymi pod niniejszym protokołem podpisami zgodnie oświadczają, że:

1. Dostarczony Sprzęt IT wraz z Oprogramowaniem jest fabrycznie nowy i nie nosi śladów uszkodzeń zewnętrznych oraz uprzedniego użytkowania. Liczba oraz rodzaj dostarczonego Sprzętu IT wraz z Oprogramowaniem jest zgodny z Umową.
2. Dostarczony Sprzęt IT oraz Oprogramowanie są wolne od oprogramowania szkodliwego i szpiegującego, a także są zabezpieczone przed nieautoryzowanym dostępem.
3. Wraz ze Sprzętem IT dostarczone wszystkie wymagane Dokumenty (instrukcje eksploatacyjne, instrukcje obsługi Sprzętu IT oraz dokumenty licencyjne dla Oprogramowania).
4. Dokonano usunięcia i utylizacji wszelkich opakowań pozostałych po rozpakowaniu Sprzętu IT.
5. Wykonano Wdrożenie prawidłowo, zgodnie z Umową.
6. Numery seryjne Sprzętu IT zostały przekazane Kupującemu w wersji elektronicznej – MS Excel.

Uwagi i zastrzeżenia:

Kupujący (upoważniony przedstawiciel)			Sprzedawca (upoważniony przedstawiciel)
.....		
.....		

....., dnia 2019 roku

Załącznik nr 3 do Umowy nr ____/DI/20..../2610 z dnia _____ 20..... r.

Protokół odbioru Dokumentacji powykonawczej
(wzór)

Dane dokumentu

Nazwa projektu + Lokalizacja Kierownik Sprzedawcy:	Numer wersji dokumentu: Data wersji dokumentu:
---	---

UWAGI:

1.
2.
3.
4.
5.
6.
7.

Kupujący odbiera / nie odbiera*
Dokumentację *

Kupujący (upoważniony przedstawiciel)		Sprzedawca (upoważniony przedstawiciel)	
Imię i nazwisko:		Imię i nazwisko:	
Stanowisko:		Stanowisko:	
Data:		Data:	
Podpis:		Podpis:	

* - niewłaściwe skreślić.

Załącznik nr 4a do Umowy nr ____/DI/20..../2610 z dnia _____ 20..... r.

Protokół odbioru Serwisu gwarancyjnego / usunięcia wady *
(wzór)

1. Imiona i nazwiska osób dokonujących czynności odbioru:

2. Wyszczególnienie odbieranych czynności w ramach Serwisu gwarancyjnego / usuniętych wad*:

3. Data podpisania protokołu: r.

4. Podpisy

Sprzedawca
(upoważniony przedstawiciel)

Kupujący
(upoważniony przedstawiciel)

.....

.....

.....

.....

* - niepotrzebne skreślić.

Załącznik nr 4b do umowy nr _____/DI/20..../2610 z dnia _____.20.... r.

Protokół odbioru konsultacji
(wzór)

1. Opis konsultacji w kwartale _____

2. Ilość wykorzystanych godzin _____

3. Uwagi/zastrzeżenia

4. Podpisy

Sprzedawca
(upoważniony przedstawiciel)

Kupujący
(upoważniony przedstawiciel)

.....

.....

.....

.....

Warszawa, dnia _____ r.

Załącznik nr 5a do Umowy nr ____/DI/20.../2610 z dnia _____ 20... r.

Oświadczenie
o zapoznaniu się z treścią Zarządzenia Prezesa ARiMR
nr 78/2019 w sprawie wprowadzenia Polityki bezpieczeństwa informacji w ARiMR

Sprzedawca oświadcza, że w dniu ____ _____ 20... r. w siedzibie Agencji Restrukturyzacji i Modernizacji Rolnictwa w Warszawie, ul. Poleczki 33 zapoznał się z treścią Załączników nr 6 i 12 Polityki bezpieczeństwa informacji w ARiMR wprowadzonej Zarządzeniem Prezesa ARiMR nr 78/2019 z dnia 3 czerwca 2019 r. i zobowiązuje się do przestrzegania ich postanowień podczas realizacji Umowy.

.....
(podpis i pieczęć osoby (osób) upoważnionej
do reprezentowania Sprzedawcy)

Warszawa., dn.20... r.

Załącznik nr 5b do Umowy nr ____/DI/20.../2610 z dnia _____ 20.... r.

Treść Załączników nr 6 i 12 do Zarządzenia Prezesa ARiMR nr 78/2019
z dnia 3 czerwca 2019 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji w ARiMR

Organizacja bezpieczeństwa fizycznego i środowiskowego

1. Działaniami w zakresie zapewniania bezpieczeństwa fizycznego i środowiskowego w Agencji bezpośrednio kierują: Administrator Zabezpieczeń Fizycznych w zakresie ochrony osób i mienia oraz administrator obiektu, w zakresie bezpieczeństwa środowiskowego, a w szczególności prawa budowlanego i ochrony przeciwpożarowej.
2. Administrator Zabezpieczeń Fizycznych sprawuje nadzór funkcjonalny nad działaniami realizowanymi przez agencje ochrony zabezpieczające obiekty Agencji.
3. Dyrektor komórki właściwej ds. bezpieczeństwa informacji w Centrali ARiMR a Inspektor Bezpieczeństwa Informacji w Oddziale Regionalnym lub Administrator Zabezpieczeń Fizycznych przynajmniej raz w roku organizuje szkolenie pracowników w zakresie ochrony osób i mienia Agencji.

Spis treści:

§ 1. Organizacja bezpieczeństwa fizycznego i środowiskowego	2
§ 2. Podstawowe zasady bezpieczeństwa fizycznego i środowiskowego	2
§ 3. Zapewnianie bezpieczeństwa fizycznego i środowiskowego	3
§ 4. Zarządzanie kluczami	4
§ 5. Zarządzanie uprawnieniami w systemie kontroli dostępu	5
§ 6. Pomieszczenia i zasoby chronione	6
§ 7. Bezpieczeństwo środowiskowe	7
§ 8. Wymagania dla systemów wspomagających	8
§ 9. Eksploatacja technicznych systemów zabezpieczeń oraz systemów wspomagających	8
§ 10. Eksploatacja zabezpieczeń mechanicznych	10
§ 11. Eksploatacja zabezpieczeń techniczno-budowlanych	11
§ 12. Eksploatacja systemów okablowania zasilającego i teleinformatycznego w zakresie konstrukcyjno-mechanicznym	12
§ 13. Eksploatacja elektronicznych systemów zabezpieczeń	13
§ 14. Systemy wspomagające oświetlenie	15
§ 15. Systemy transmisji sygnałów alarmowych do centrów monitoringu	15
§ 16. Rejestrowanie i przechowywanie informacji w elektronicznych systemach zabezpieczeń	15
§ 17. Prowadzenie dokumentacji związanej z technicznymi systemami zabezpieczeń	16
§ 18. Zarządzanie zapisami pochodzącymi z elektronicznych systemów zabezpieczeń	16
Załącznik nr 1 do Regulaminu bezpieczeństwa fizycznego i środowiskowego – Wzór rejestru wejścia/wyjścia do strefy bezpieczeństwa	17
Załącznik nr 2 do Regulaminu – Wzór rejestru wejścia/wyjścia gości do strefy administracyjnej	18

§ 2.**Podstawowe zasady bezpieczeństwa fizycznego i środowiskowego**

1. Środki bezpieczeństwa fizycznego dotyczą:
 - 1) rozmieszczenia i granic stref bezpieczeństwa,
 - 2) konstrukcji budowlanych wyznaczających granice stref bezpieczeństwa,
 - 3) sposobu zabezpieczenia wejścia do obiektu oraz do stref bezpieczeństwa,
 - 4) stosowania bezpośredniej ochrony fizycznej,
 - 5) stosowania systemu sygnalizacji napadu i włamania,
 - 6) stosowania systemu monitoringu wizyjnego,
 - 7) stosowania mechanicznych zabezpieczeń technicznych,
 - 8) dostępu do obszarów bezpiecznych oraz wykonywanie prac w obszarach bezpiecznych.
2. Bezpieczeństwo środowiskowe obejmuje:
 - 1) stosowanie urządzeń ochrony przeciwpożarowej,
 - 2) zabezpieczenie przed zalaniem wodą,
 - 3) zapewnienie właściwych warunków pracy w zakresie temperatury i wilgotności powietrza,
 - 4) stosowanie środków ochrony odgromowej na liniach telekomunikacyjnych,
 - 5) stosowanie zabezpieczeń przeciwprzepięciowych
3. Zakres stosowania środków bezpieczeństwa fizycznego i środowiskowego wynika z przeprowadzonego i udokumentowanego szacowania ryzyka.
4. Szacowanie ryzyka i określanie wymagań bezpieczeństwa przeprowadza się w oparciu o:
 - 1) charakterystykę obiektu i pełnione przez niego funkcje, w szczególności rodzaj umieszczonych w nim zasobów podlegających ochronie (ludzie, dokumentacja, sprzęt komputerowy, itp.),
 - 2) określenie kategorii potencjalnych zagrożeń obiektu,
 - 3) opis topografii, konstrukcji obiektu i architektury, najbliższego otoczenia (zabezpieczenia budowlane i mechaniczne, ogrodzenie, bramy, furty, oświetlenie, miejsca do parkowania, drogi komunikacyjne i ewakuacyjne, inne budowle i elementy towarzyszące), odnotowane w przeszłości czyny przestępcze (rodzaj i typ czynu przestępczego, działania zewnętrzne, wewnętrzne, data, rozmiary, wartości szkody, wynik śledztwa),
 - 4)

- 5) aktualny stan bezpieczeństwa obiektu.
- 6) opis i ocene funkcjonalności i poprawności zamstalowanych technicznych systemów zabezpieczenia, ich poprawności eksploatacji i aktualny stan techniczny (poziom technologiczny, sprawność, dokumentacja, serwisowanie).
- 7) aktualny stan ochrony fizycznej obiektu.
- 8) opis stosowanych procedur i rozwiązań organizacyjnych.
- 9) wnioski co do odpowiedności (w stosunku do rodzaju i stopnia zagrożeń) kompletności i poprawności zastosowanych zabezpieczeń (mechanicznych, technicznych i proceduralno – organizacyjnych).
- 10) propozycje doskonalenia systemów oraz procedur ochrony obiektu.

§ 3.

Zapewnianie bezpieczeństwa fizycznego i środowiskowego

1. Dyrektor komórki właściwej ds. bezpieczeństwa informacji, dyrektorzy oddziałów regionalnych, kierownicy biur powiatowych ustalają podział powierzchni biurowych zajmowanych przez komórki i jednostki organizacyjne Agencji na:
 - 1) strefy administracyjne, do których dostęp posiadają wszyscy pracownicy Agencji,
 - 2) strefy bezpieczeństwa, do których dostęp jest ograniczony do osób posiadających specjalne prawa dostępu.
 - 3) strefy obsługi klienta, do której dostęp posiadają beneficjenci ARiMR, goście i inni interesanci.
2. Ochrona stref administracyjnych i stref bezpieczeństwa sprawowana jest na zasadach określonych w:
 - 1) przepisach o ochronie osób i mienia,
 - 2) planie ochrony obiektu (jeżeli został opracowany),
 - 3) niniejszym Regulaminie.
3. Na granicy strefy administracyjnej odbywa się kontrola ruchu osobowego i materiałowego. Wejścia gości do strefy administracyjnej jest rejestrowane. Wzór rejestru wejść stanowi załącznik nr 2 do niniejszego Regulaminu.
4. Strefa bezpieczeństwa powinna być ustalona na obszarze wydzielonym solidnymi konstrukcjami budowlanymi. Za solidne konstrukcje budowlane uznaje się łukcie, których ściany zewnętrzne i stropy budynków, w których zlokalizowane są strefy bezpieczeństwa, posiadają klasę odporności włamaniowej równowaznej murowi o grubości 25 cm wykonanemu z pełnej cegły. Natomiast pomieszczenia stref bezpieczeństwa powinny mieć ściany o odporności włamaniowej równowaznej murowi o grubości 12,5 cm. Zasady organizacji strefy bezpieczeństwa kancelarii niejawniej w ARiMR określają odrębne regulacje.
5. Wszystkie osoby przebywające w strefie administracyjnej muszą posiadać identyfikatory noszone w widocznym miejscu. Pracownicy Agencji posiadają identyfikatory zawierające: zdjęcie, imię i nazwisko, symbol lub nazwę jednostki organizacyjnej lub komórki organizacyjnej. Goście posiadają identyfikatory z napisem „Gość” i numerem identyfikatora.
6. Goście mogą poruszać się w obrębie strefy administracyjnej wyłącznie w asyście pracownika odpowiedzialnego za ich przyjęcie. Pracownik ten przed wprowadzeniem gości do strefy administracyjnej winien dopilnować pobrania przez nich w strefie obsługi klienta lub na stanowisku recepcyjnym identyfikatorów, o których mowa w ust. 5.

7. W jednostkach organizacyjnych, w których odbywa się masowa obsługa interesantów dopuszcza się wydzielenie z części strefy administracyjnej strefy obsługi klienta, w której goście – interesanci mogą przebywać bez identyfikatorów. Strefa obsługi klienta musi być oddzielona od pozostałych części strefy administracyjnej kontrolowanymi przejściami.

8. W przypadku stosowania systemu kontroli dostępu musi być to system z klasą dostępu B. Dla stref administracyjnych i bezpieczeństwa wymagana jest klasa rozpoznania 2 na wejściu i klasa rozpoznania 0 na wyjściu.

9. Klasa dostępu B oznacza, że w systemie możliwe jest przyznawanie dostępu w określonych godzinach oraz, że transakcje uzyskania dostępu są rejestrowane. Klasa rozpoznania 0 oznacza, że dostęp uzyskiwany jest bez sprawdzania tożsamości (np. wyjście po naciśnięciu przycisku). Klasa rozpoznania 2 oznacza, że dostęp uzyskiwany jest po sprawdzeniu tożsamości na podstawie danych zawartych na identyfikatorze lub na podstawie danych biometrycznych. (Według Polskiej Normy PN-EN 50133-1 - „Systemy alarmowe. Systemy kontroli dostępu. Wymagania systemowe”).

10. Wszystkie drzwi z kontrolą dostępu muszą być zaopatrzone w urządzenia samozamykające.

11. Kontrolę ruchu osobowego i materiałowego na granicy strefy administracyjnej może sprawować pracownik ze strefy obsługi klienta lub stanowiska recepcyjnego, który wydaje identyfikatory gościom.

12. Pomieszczenia biurowe w strefie administracyjnej posiadają zamki klasy 0. Pomieszczenia w strefach bezpieczeństwa powinny posiadać zamki klasy C lub klasy 7 zabezpieczenia (wg normy PN-EN 12209:2005) oraz drzwi antywłamaniowe klasy C (wg normy PN-EN 14351-1) lub drzwi o odporności co najmniej klasy 4 (wg normy PN-EN 1627:2011), z odpornością ognową co najmniej 60 minut.

13. Wejście oraz wyjście ze stref bezpieczeństwa jest rejestrowane. Rejestruje się tożsamość osób, cel pobytu oraz czas ich wejścia i wyjścia. Wzór rejestru stanowi załącznik nr 1 do niniejszego Regulaminu.

§ 4.

Zarządzanie kluczami

1. Klucze od pomieszczeń przechowywane są u ochrony obiektu, z tym, że klucze do pomieszczeń w strefach bezpieczeństwa muszą być zdawane na przechowanie w zaplombowanych pojemnikach.
2. Jeżeli obiekt nie posiada stałej ochrony po godzinach pracy, to klucze od pomieszczeń biurowych muszą być zdawane przez wyznaczonych pracowników Agencji w zaplombowanej kasecie pracownikowi firmy realizującej ochronę obiektu na zasadzie monitoringu, a następnego dnia roboczego pobierane z tej firmy. Przyjęcie kluczy przez pracownika firmy sprawującej monitoring jest równoznaczne z przyjęciem obiektu pod ochronę. Szczegółowe zasady takiej procedury określa umowa pomiędzy Agencją a firmą sprawującą ochronę. W przypadku braku możliwości obecności pracownika Agencji w celu zabezpieczenia ich w zaplombowanej kasecie, a następnego dnia roboczego pracownik ten zobowiązany jest wydać klucze upoważnionym pracownikom. Dopuszcza się, w biurach powiatowych Agencji, irwalne wydanie kluczy zewnętrznym do obiektu osobom funkcyjnym posiadającym indywidualny kod dostępu do Systemu Sygnalizacji Włamania i Napadu (SSWiN), w takim przypadku jeden z kluczy musi być zdeponowany w jednostce monitorującej obiekt, klucze

wewnętrzne mogą być przechowywane w skrytce wewnętrznej obiektu, osoba otwierająca obiekt odpowiedzialna jest za wydanie kluczy, osoba zamykająca obiekt odpowiedzialna jest za przyjęcie do skrytki wszystkich kluczy wewnętrznych.

3. Klucze wydaje się na podstawie rejestru osób upoważnionych do ich pobierania. Fakt wydania kluczy i przyjęcia ich na przechowanie musi być odnotowany. Rejestr wydawania i zdawania kluczy prowadzony jest w formie papierowej w książce wydawania kluczy lub w formie elektronicznej w dedykowanym systemie elektromechanicznego depozytora kluczy. Wzór książki wydawania i zdawania kluczy stosowany w jednostce organizacyjnej określa Administrator Zabezpieczeń Fizycznych danej jednostki w porozumieniu z Inspektorem Bezpieczeństwa Informacji. Prowadzony rejestr musi określać:

- nr pomieszczenia / nr klucza,
- dokładną godzinę pobrania / zdania,
- imię i nazwisko osoby pobierającej / zdającej bądź jej identyfikator (w systemie elektronicznego depozytora),
- czytelny podpis osoby pobierającej / zdającej oraz przyjmującej klucz na przechowanie (w przypadku rejestru w formie papierowej).

4. Za przyznanie i odebranie prawa do pobierania kluczy do konkretnego pomieszczenia odpowiedzialny jest:

- 1) w Centrali – dyrektor komórki organizacyjnej, któremu podlega dane pomieszczenie,
- 2) w oddziale regionalnym – kierownicy biur w stosunku do pomieszczeń zajmowanych przez pracowników biura lub kierownik biura oddziału regionalnego w stosunku do pozostałych pomieszczeń oddziału,
- 3) w biurze powiatowym – kierownik biura powiatowego.

5. Za organizację wydawania kluczy do pomieszczeń odpowiada administrator obiektu lub Administrator Zabezpieczeń Fizycznych. Organizacja wydawania kluczy musi być uzgodniona z:

- 1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa informacji,
- 2) w oddziale regionalnym i biurach powiatowych - Inspektorem Bezpieczeństwa Informacji.

6. Klucze do szaf i mebli biurowych, w których przechowywane są dokumenty zawierające informacje wrażliwe, nie mogą po zakończeniu pracy pozostawać w zamkach. Za organizację przechowywania takich kluczy odpowiada Administrator Zabezpieczeń Fizycznych, w uzgodnieniu z:

- 1) w Centrali Agencji – dyrektorem komórki organizacyjnej, któremu podlega pomieszczenie z szafami i meblami biurowymi zawierającymi informacje wrażliwe,
- 2) w oddziale regionalnym i biurze powiatowym – kierownikiem komórki organizacyjnej, któremu podlega pomieszczenie z szafami i meblami biurowymi zawierającymi informacje wrażliwe.

7. Zasady organizacji przechowywania kluczy do szaf, sejfów i mebli biurowych, w których przechowuje się informacje niejawne określają odrębne regulacje.

§ 5.

Zarządzanie uprawnieniami w systemie kontroli dostępu

1. W przypadku zastosowania systemu kontroli dostępu uprawnienia są jednoznacznie powiązane z urządzeniami aktywującymi przejsięcie, które pełnią także rolę identyfikatorów.

5

2. Wstęp do poszczególnych stref, o których mowa w § 3 ust. 1 jest ograniczony tylko do tych osób, które uzyskały stosowne uprawnienia.

3. Uprawnienia przyznawane są zgodnie z profilem dostępu (zakresem odpowiedzialności i uprawnień) na danym stanowisku pracy. Uprawnienia dostępu są nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzebą wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień do pomieszczeń będzie kwalifikowane jako incydent związany z naruszeniem bezpieczeństwa informacji.

4. Za przyznawanie, zmianę oraz odbieranie uprawnień dostępu do stref bezpieczeństwa odpowiedzialny jest:

- 1) w Centrali Agencji - dyrektor komórki organizacyjnej, któremu podlega dane pomieszczenie,
- 2) w oddziale regionalnym i biurze powiatowym - kierownik biura oddziału regionalnego w stosunku do pomieszczeń oddziału regionalnego lub kierownik biura powiatowego w stosunku do pomieszczeń tego biura.

5. Przyznawanie, zmiana oraz odbieranie uprawnień jest realizowane w systemie kontroli dostępu przez Administratora Zabezpieczeń Fizycznych.

6. Administrator Zabezpieczeń Fizycznych jest obowiązany bezzwłocznie zablokować uprawnienia dostępu w przypadku:

- 1) zgłoszenia przez pracownika Agencji utraty lub podejrzenia utraty urządzenia aktywującego przejsięcie,
- 2) zgłoszenia telefonicznego, za pośrednictwem faksu lub poczty elektronicznej, potwierdzonego bezzwłocznie pisemnym wnioskiem bezpośredniego przełożonego pracownika.

7. Ponowne nadanie uprawnień dostępu w przypadku zaistnienia okoliczności opisanych w ust. 6 pkt 1) odbywa się zgodnie z zasadami określonymi w ust. 4 i 5.

8. Uprawnienia dostępu są regularnie przeglądane zgodnie z zasadami opisanymi w Regulaminie nadzoru.

§ 6.

Pomieszczenia i zasoby chronione

1. Wnoszenie i wynoszenie do i ze stref bezpieczeństwa komputerowych nośników danych może mieć miejsce tylko w przypadkach wynikających z procedur eksploatacji zainstalowanego tam sprzętu teleinformatycznego.

2. Strefy bezpieczeństwa powinny być chronione systemem sygnalizacji włamania i napadu.

3. W uzasadnionych przypadkach, zarówno strefy administracyjne jak i strefy bezpieczeństwa, powinny być poddane monitoringowi wizyjnemu.

4. Strefy bezpieczeństwa nie posiadają oznakowania wewnątrz lub na zewnątrz, które wskazywałyby na to, że znajdują się w nich szczególnie chronione zasoby.

5. W strefach bezpieczeństwa dopuszcza się przebywanie osób bez uprawnień dostępu do tych stref tylko w wyjątkowych przypadkach, za zezwoleniem:

- 1) dla pomieszczeń BP - kierownika biura powiatowego,
- 2) dla pomieszczeń OR - kierownika Biura OR,
- 3) dla pomieszczeń Centrali.

6

a) dyrektora komórki właściwej ds. informatyki dla pomieszczeń serwerowni, węzłów teletechnicznych i biblioteki kodów źródłowych.

b) dyrektora komórki właściwej ds. organizacyjno-gospodarczych dla pomieszczeń archiwum zakładowego.

c) Pełnomocnika ds. Ochrony. Informacji Niejawnych w przypadku strefy bezpieczeństwa, w której przetwarzane są informacje niejawne.

6. Proby osoby, która nie posiada uprawnień do przebywania w strefie bezpieczeństwa jest rejestrowany. Za prowadzenie rejestru odpowiedzialne są osoby wskazane w ust. 5, a wpisy dokonywane są pod nadzorem osoby uprawnionej do przebywania w danej strefie.

7. Serwery, aktywne i pasywne urządzenia sieci teleinformatycznej, centrale telefoniczne i archiwa muszą być umieszczone w strefach bezpieczeństwa.

8. Zasoby, którym nadano status zasobu kluczowego podlegają szczególnej ochronie i są dodatkowo zabezpieczane przed pożarem i zalaniem.

9. Rozmieszczenie sprzętu służącego do przetwarzania informacji, zarówno w obszarach bezpieczeństwa, jak i w pozostałych pomieszczeniach, poprzedzone jest udokumentowanym szacowaniem ryzyk związanych z systemami zabezpieczeń technicznych oraz systemami wspomagającymi (wentylacyjno-klimatyzacyjnymi, zasilającymi, wodno-kanalizacyjnymi, grzewczymi).

§ 7.

Bezpieczeństwo środowiskowe

1. Przy planowaniu zabezpieczeń technicznych i organizacyjnych, ich rodzaju i siły, bierze się pod uwagę ryzyka związane z występującymi lokalnie zagrożeniami, takimi jak pożar, zalanie, trzęsienie ziemi, wybuch, wyładowania atmosferyczne, niepokojące społeczne i inne formy naturalnych lub spowodowanych przez działania umyślnie bądź błędz człowieka katastrof. Ponadto analizie jest poddawany wpływ sąsiedziwa innych obiektów lub lokalnych instalacji i dróg (np. pożar w sąsiednim budynku, woda przeciekająca przez dach, powódź, bliska katastrofa komunikacyjna, eksplozja, zamieszki uliczne).

2. Pomieszczenia, w których zlokalizowane są zasoby kluczowe, wyposaża się w:

- 1) system sygnalizujący wystąpienie pożaru,
- 2) system klimatyzacji w serwerowniach.

3. Nie prowadzi się instalacji wodnych przez pomieszczenia, w których zlokalizowane są zasoby kluczowe do przetwarzania informacji (serwery, centra danych).

4. Urządzenia zapewniające bezpieczeństwo środowiskowe poddawane są regularnej kontroli zgodnie z obowiązującymi przepisami prawa, normami oraz zaleceniami producentów.

5. Na wypadek zagrożenia pożarem dla każdej z lokalizacji jednostek organizacyjnych Agencji opracowuje się instrukcję przeciwpożarowe. Ciągi komunikacyjne obiektów muszą być zaopatrzone w tabliczki informujące o kierunku ewakuacji i w miarę potrzeby wyposażone w oświetlenie awaryjne.

6. W przypadku, jeśli ktoreś z wymagań w zakresie bezpieczeństwa środowiskowego nie może być z przyczyn obiektywnych spełnione, Administrator Zabezpieczeń Fizycznych sporządza protokół opisujący rodzaj odstępstwa, ryzyko wynikające z odstępstwa, zastosowane środki ochrony doróżnej lub zamiennej, plan dojścia do rozwiązania docelowego.

7

7. Parametry środowiska, w którym pracuje sprzęt systemu teleinformatycznego zaliczany do zasobów kluczowych, tj. temperatura, jest monitorowana w celu natychmiastowego wykrycia odchylen, które mogłyby mieć negatywne skutki dla tego sprzętu.

8. Budynek, w którym znajdują się systemy teleinformatyczne wskazane w ust. 7 wyposażony jest, zgodnie z przepisami ppoz., w samoczynnie złączające się oświetlenie awaryjne (bezpieczeństwa i ewakuacyjne).

9. Oświetlenie bezpieczeństwa, stosowane jest w pomieszczeniach, w których nawet krótkotrwale wyłączenie oświetlenia podstawowego może spowodować zagrożenie zdrowia i życia podczas ewakuacji.

10. W przypadku, gdy oświetlenie bezpieczeństwa działa, co najmniej przez 2 godziny, nie ma potrzeby stosowania oświetlenia ewakuacyjnego.

§ 8.

Wymagania dla systemów wspomagających

1. Jeżeli jest to możliwe, należy projektować nadmiarową, modułową klimatyzację tak, aby w przypadku awarii lub przeglądu serwisowego jednego modułu pozostałe były w stanie zapewnić wymagane parametry środowiskowe, w szczególności środowiska eksploatacyjnego w serwerowniach.

2. Rozmieszczenie w obiekcie kanałów oraz czerpni należy zaprojektować uwzględniając ryzyko takich zdarzeń, jak przedostanie się przez nie do pomieszczeń chronionych wody, środków niebezpiecznych czy też zwierząt.

3. W przypadku prowadzenia instalacji wodno-kanalizacyjnych i grzewczych w sąsiedztwie (również nad lub bezpośrednio pod pomieszczeniem) serwerowni i pomieszczeń, w których usytuowano infrastrukturę techniczną służącą do przetwarzania w krytycznych systemach Agencji, należy wdrożyć systemy zapewniające wykrycie i alarmowanie w przypadku zalania pomieszczenia oraz zainstalować środki umożliwiający szybkie usunięcie wody (cieczy).

4. Przy ocenie sprawności instalacji wodno – kanalizacyjnej i grzewczej należy uwzględnić jej współdziałanie z innymi systemami wspomagającymi, takimi jak system klimatyzacyjny - wentylacyjny oraz w szczególności system przeciwpożarowy.

§ 9.

Eksploatacja technicznych systemów zabezpieczeń oraz systemów wspomagających

1. Systemy zabezpieczenia technicznego Agencji muszą spełniać następujące funkcje:

- 1) zabezpieczenia budowlane i zabezpieczenia mechaniczne muszą zagwarantować uniemożliwienie dostępu osobom niepowołanym do chronionych pomieszczeń i urządzeń oraz zabezpieczyć osoby i mienie przed potencjalnymi zagrożeniami,
- 2) system sygnalizacji napadu i włamania (SSW/IN) musi zapewnić skuteczne przekazanie sygnału o realnym zagrożeniu do wskazanych osób, miejsc i urządzeń,
- 3) system monitorowania w przypadku wystąpienia alarmu musi zapewnić podjęcie odpowiednich działań stosownych do zaistniałego zdarzenia,

8

4) system monitoringu (CCTV) musi zapewnić, poprzez rozmieszczone kamery, rozpoznanie rodzaju zagrożenia i śledzenie rozwoju sytuacji, prowadzenie obserwacji obrazu z kilku kamer oraz automatyczną jednoczesną rejestrację tych obrazów,

5) system kontroli dostępu (SKD) musi zabezpieczyć chronione pomieszczenie (grupe pomieszczeń) lub wydzieloną strefę przed dostępem do nich osób nieuprawnionych.

2. Wszystkie systemy zabezpieczeń podlegają regularnym przeglądom dokonywanym przez Administratora Zabezpieczeń Fizycznych lub pod jego nadzorem przez osoby posiadające odpowiednie uprawnienia. Przegląd polega na sprawdzeniu poprawności działania danego systemu zgodnie z dokumentacją techniczno-eksploatacyjną systemu. Przeglądy każdego systemu zabezpieczeń wykonywane są zgodnie z harmonogramem ustalonym przez Administratora Zabezpieczeń Fizycznych w porozumieniu z:

- 1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa,
- 2) w oddziale regionalnym i biurach powiatowych - Inspektorem Bezpieczeństwa Informacji.

3. Przeglądy dokonywane przez Administratora Zabezpieczeń Fizycznych co 6 miesięcy obejmują dodatkowo sprawdzenie stanu technicznego nośników elektronicznych SKD (identyfikatorów) przeznaczonych dla gości, jeśli mają zastosowanie w danej jednostce organizacyjnej.

4. Przeglądy systemów zabezpieczeń poza ustalonym harmonogramem przeprowadzane są każdorazowo w przypadku wystąpienia incydentów zagrażających lub mogących powodować zagrożenie dla bezpieczeństwa osób i mienia (np. katastrofa budowlana w sąsiedztwie obiektu, pożar, kolizja drogową powodująca szczególne zagrożenie w pobliżu budynku, pożar, roboty budowlane w sąsiednich budynkach, ewakuacja osób i mienia z budynku, interwencja służb ratunkowych mająca wpływ na stan techniczny obiektu, wystąpienie anomalii pogodowych, itp.).

5. Administrator Zabezpieczeń Fizycznych odnotowuje przeprowadzenie przeglądu w dzienniku przeglądów prowadzonym dla każdego z funkcjonujących w Agencji systemów zabezpieczeń. Dziennik przeglądu zawiera następujące informacje:

- 1) datę i czas przeglądu,
- 2) dane personalne wykonującego przegląd,
- 3) wynik przeglądu,
- 4) dane personalne osoby nadzorującej/kontrolującej,
- 5) uwagi z przeglądu.

Dopuszcza się prowadzenie dziennika w systemie elektronicznym lub wersji elektronicznej umieszczonej na serwerze plików (fileservet).

6. Administrator Zabezpieczeń Fizycznych nadzoruje i dokumentuje bieżące prace konserwacyjne, w tym wymianę lub prostą naprawę elementów każdego z systemów zabezpieczeń, które nie wymagają posiadania stosownych uprawnień specjalistycznych. Pozostałe prace konserwacyjne wykonują pracownicy podmiotów zewnętrznych posiadający stosowne uprawnienia. Prace konserwacyjne polegają na wykonaniu niezbędnych czynności mających na celu utrzymanie systemu w sprawności techniczno-użytkowej zgodnie z dokumentacją techniczno-eksploatacyjną systemu. Prace konserwacyjne dla wszystkich systemów zabezpieczenia przeprowadzane są nie rzadziej niż raz na 12 miesięcy.

7. Administrator Zabezpieczeń Fizycznych nadzoruje i dokumentuje prace serwisowe przeprowadzane przez uprawnionych pracowników podmiotów zewnętrznych. Prace serwisowe

polegają na wykonaniu niezbędnych czynności mających na celu przywrócenie sprawności techniczno-użytkowej systemu zgodnie z dokumentacją techniczno-eksploatacyjną systemu.

8. Wymiany lub naprawy o wysokim poziomie technicznym dokonuje podmiot zewnętrzny posiadający stosowne uprawnienia producenta, dystrybutora wyrobu lub specjalistyczne urządzenia do naprawy lub wymiany.

9. Dla każdego systemu alarmowego oraz dla każdego innego systemu technicznego zabezpieczenia funkcjonującego w Agencji jest założony dziennik/system rejestrowania zawierający:

- 1) rejestr wyposażenia,
- 2) rejestr zdarzeń,
- 3) rejestr prac konserwacyjnych,
- 4) rejestr prac serwisowych.

§ 10.

Eksploatacja zabezpieczeń mechanicznych

1. Do zabezpieczeń mechanicznych zalicza się: kraty, żaluzje, okiennice, folie antywłamaniowe, zamki w drzwiach (w szczególności te, do których bezpośredni dostęp mają osoby postronne), inne zabezpieczenia otworów okiennych, włazów, kanałów wentylacyjnych, rygle, klodki, zamki, zasuwę z blokadą mechaniczną.

2. Zabezpieczenia mechaniczne muszą być zamontowane przez uprawniony podmiot zgodnie z warunkami technicznymi wynikającymi z certyfikatu lub aprobaty technicznej

3. Zabezpieczenia mechaniczne podlegają przeglądom przeprowadzanym przez Administratora Zabezpieczeń Fizycznych, zgodnie z harmonogramem - dotyczy tylko tych zabezpieczeń, które są dostępne dla osób postronnych i nie ma możliwości realizacji nadzoru przez inne systemy zabezpieczeń. Harmonogram przeglądów jest ustalany przez Administratora Zabezpieczeń Fizycznych w porozumieniu z:

- 1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa,
- 2) w oddziale regionalnym i biurach powiatowych - osobami pełniącymi funkcję Inspektora Bezpieczeństwa Informacji.

4. Przeglądy polegają na sprawdzeniu stanu technicznego elementów zabezpieczenia mechanicznego, przeprowadzanych w następujący sposób:

- 1) w przypadku krat, żaluzji, okiennic i innych zabezpieczeń otworów okiennych, włazów, kanałów wentylacyjnych:
 - a) sprawdzenie mocowań do murów (np. poprzez poruszenie elementów zabezpieczenia w pionie i poziomie i obserwacji reakcji elementów mocujących),
 - b) sprawdzenie istnienia odszalceń mechanicznych na poszczególnych elementach, przy zastosowaniu metody porównawczej z opisem w dokumentacji technicznej,
 - c) sprawdzenie występowania śladów po próbach penetracji lub usunięcia zabezpieczenia np. w postaci opilków, śladów tyłku, rysach na elementach zabezpieczeń, itp.,
 - d) sprawdzić stan powłok lakierowanych i zabezpieczeń antykorozyjnych elementów narażonych na bezpośrednie działanie czynników atmosferycznych lub innych szkodliwych czynników dla mechanizmów klodki, zamków, rygli (szczególnie kurz, pył).

- 3) sprawdzenie występowania śladów po próbach penetracji lub usunięcia zabezpieczenia np. w postaci opilków, śladów tynku, rysach na elementach zabezpieczeń, rdzy, itp.,
 - 4) sprawdzenie mechanizmów ryglowych (zamek, rygiel, itp.),
 - 5) porównanie położenia elementów ruchomych z opisem w dokumentacji technicznej.
4. Przynajmniej dwa razy do roku Administrator Zabezpieczeń Fizycznych dokonuje oceny stanu powłoki lakierniczej, śladów korozji elementów zabezpieczeń techniczno-budowlanych narazonych na bezpośrednie działanie czynników atmosferycznych lub innych czynników środowiskowych.
 5. Wymiana/naprawa zabezpieczeń dokonywana jest pod nadzorem administratora obiektu w porozumieniu z Administratorem Zabezpieczeń Fizycznych.

§ 12.

Eksploatacja systemów okablowania zasilającego i teleinformatycznego w zakresie konstrukcyjno-mechanicznym

1. W skład systemów okablowania w zakresie konstrukcyjno-mechanicznym wchodzi: trakty kablowe (listwy PCV, szyny, przepusty), osłony włazów i studzienek, szafy dystrybucyjne, tablice, krosownice.
2. Systemy okablowania znajdujące się w obszarze dostępnym publicznie podlegają przeglądowi przeprowadzanym przez Administratora Zabezpieczeń Fizycznych oraz Administratora Systemu. Harmonogram przeglądów jest ustalany przez Administratora Zabezpieczeń Fizycznych w porozumieniu z:
 - 1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa,
 - 2) w oddziale regionalnym i biurach powiatowych – osobami pełniącymi funkcję Inspektora Bezpieczeństwa Informacji.
3. Przeglądy polegają na sprawdzeniu stanu technicznego (konstrukcyjno-mechanicznego) elementów systemu okablowania z dokumentacją techniczną.
4. Przeglądy zabezpieczeń elektronicznych systemów okablowania polegają na sprawdzeniu poprawności funkcjonowania np. systemów sygnalizacji włamania zastosowanych do zabezpieczenia szaf dystrybucyjnych, krosownic lub innych zabezpieczeń.
5. Przeglądy przeprowadzane lub nadzorowane przez Administratora Zabezpieczeń Fizycznych powinny obejmować sprawdzenie:
 - 1) ciągłości struktury (mocowanie listew) traktów kablowych w miejscach ogólnie dostępnych – np. narazonych na uszkodzenia mechaniczne spowodowane przez przenoszenie przedmiotów o dużych gabarytach (burko, szafa), nuch osobowy,
 - 2) stanu powłoki lakierniczej, śladów korozji elementów narazonych na bezpośrednie działanie czynników atmosferycznych lub innych szkodliwych czynników dla obudów, osłon lub innych zabezpieczeń systemów okablowania,
 - 3) czy występują ślady po próbach penetracji lub usunięcia zabezpieczenia, np. w postaci opilków, śladów tynku, rysach na elementach zabezpieczeń, itp.
6. Przeglądy prowadzone lub nadzorowane przez Administratora Systemu powinny obejmować sprawdzenie:

- 2) w przypadku klodek i zamków - sprawdzenie działania kluczy: zapasowych oraz mechanizmu ryglującego przez otwarcie i zamknięcie klodek i zamków, przegrod mechanicznych i budowlanych.
- 3) w przypadku rygli i zasuw z blokadą mechaniczną - porównanie położenia elementów ruchomych z opisem w dokumentacji technicznej.
5. Przynajmniej dwa razy do roku Administrator Zabezpieczeń Fizycznych dokonuje oceny stanu powłoki lakierniczej, śladów korozji elementów narazonych na bezpośrednie działanie czynników atmosferycznych lub innych szkodliwych czynników dla mechanizmów.
6. Wycołane z użycia elementy zabezpieczeń mechanicznych zawierające informacje o kodzie zamków (klucze, wkładki, karty elektroniczne) niszczone są mechanicznie.
7. Zakup zamków (mechanizmów zamkowych) i wkładek dokonywany jest w sposób określony jako „zakup z polką”.
8. Dla stref bezpieczeństwa każda faza procesu wymiany mechanizmów zamkowych, w tym zakup i transport, montaż zamków (mechanizmów zamkowych) i wkładek wykonywany jest co najmniej przez dwie osoby (w tym przez Administratora Zabezpieczeń Fizycznych sprawującego bezpośredni nadzór).
9. Wycołanie elementu zabezpieczenia mechanicznego przeprowadza się po uzyskaniu informacji od dystrybutora/producenta wyrobu o konieczności jego wymiany lub po uzyskaniu informacji o pojawieniu się metod/narzędzi powodujących przełamanie zabezpieczenia lub obniżenie jego właściwości.
10. Z zastrzeżeniem ust. 8, koniec okresu ważności certyfikatu lub świadectwa kwalifikacyjnego nie stanowi przyczyny demontażu elementu zabezpieczenia.

§ 11.

Eksploatacja zabezpieczeń techniczno-budowlanych

1. Do zabezpieczeń techniczno-budowlanych zalicza się drzwi, śluzi, ściany, stropy, ogrodzenia (wykoneane z różnych materiałów), furtki, bramy, zapory, szlabany, kołowroty (w szczególności te, do których bezpośrednio dostęp mają osoby postronne).
2. Zabezpieczenia techniczno-budowlane podlegają przeglądowi przeprowadzanym przez Administratora Zabezpieczeń Fizycznych, zgodnie z harmonogramem - dotyczy tylko tych zabezpieczeń, które są dostępne dla osób postronnych i nie ma możliwości realizacji nadzoru przez inne systemy zabezpieczeń. Harmonogram przeglądów jest ustalany przez Administratora Zabezpieczeń Fizycznych w porozumieniu z:
 - 1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa,
 - 2) w oddziale regionalnym i biurach powiatowych – osobami pełniącymi funkcję Inspektora Bezpieczeństwa Informacji.
3. Przeglądy polegają na sprawdzeniu stanu technicznego elementów zabezpieczeń techniczno-budowlanych, przeprowadzanych w następujący sposób:
 - 1) sprawdzenie mocowań elementów ruchomych i elementów umocowanych na stałe do podłoża (np. poprzez poruszenie elementów konstrukcji zabezpieczenia i obserwacji reakcji elementów mocujących),
 - 2) sprawdzenie istnienia odkształceń mechanicznych na poszczególnych elementach, przy zastosowaniu metody porównawczej z opisem w dokumentacji technicznej.

- 1) przestrzegania zasad ochrony okablowania oraz punktów połączeń okablowania (inspekcja pod kątem podłączonych nieautoryzowanych urządzeń przechwytyjących, rejestrujących, transmityjących i zniekształcających sygnał transmisyjny),
- 2) zamknięcia szaf, tablic, osłon włazów i studzienek należących do Agencji,
- 3) zgodności stanu faktycznego z dokumentacją techniczną okablowania,
- 4) stanu technicznego instalacji poprzez wykonanie pomiarów okablowania.

§ 13.

Eksploatacja elektronicznych systemów zabezpieczeń

1. Do elektronicznych systemów zabezpieczeń zalicza się systemy sygnalizacji włamania i napadu (SSWiN), systemy kontroli dostępu (SKD), systemy telewizji dozorowej (CCTV) oraz inne systemy współdziałające z elektronicznymi systemami zabezpieczeniowymi, np. system oświetlenia podczernienia dla systemu CCTV.
2. Elektroniczne systemy zabezpieczeniowe i systemy współdziałające podlegają przeglądom przeprowadzanym przez Administratora Zabezpieczeń Fizycznych zgodnie z harmonogramem i zakresem konserwacji systemu przeprowadzanej przez pracownika podmiotu zewnętrznego, posiadającego licencję pracownika zabezpieczenia technicznego.
3. Przeglądy SSWiN są przeprowadzane przez Administratora Zabezpieczeń Fizycznych i obejmują, w zależności od zastosowanego rozwiązania technicznego, sprawdzenie:
 - 1) trybu pracy urządzeń wg wskazań paneli sterujących poprzez porównanie z dokumentacją techniczno-eksploatacyjną systemu,
 - 2) działania przycisków sygnalizacji napadu/przycisków wezwania pomocy,
 - 3) działania poszczególnych klawiatur sterowych poprzez załączenie i rozłączenie systemu wprowadzając odpowiedni kod,
 - 4) ilości i rozmieszczenia klawiatur sterowych zgodnie z danymi w dzienniku systemu.
4. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują:
 - 1) sprawdzenie prawidłowości funkcjonowania systemu SSWiN w zakresie określonym w dokumentacji technicznej,
 - 2) sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego; (wymiana akumulatorów zgodnie z harmonogramem załączonym do dokumentacji technicznej systemu),
 - 3) sprawdzenie poprawności działania akustycznych lub optycznych sygnalizatorów alarmowych,
 - 4) sprawdzenie czujników systemu,
 - 5) sprawdzenie mocowania czujek do podłoża (uchwyty, ściany), szczególnie dotyczy to stref ogólnego i ograniczonego dostępu oraz znajdujących się poza pomieszczeniami Agencji (plaszczyna ścian, ogrodzenia).
5. Przeglądy SKD są przeprowadzane przez Administratora Zabezpieczeń Fizycznych i obejmują, w zależności od zastosowanego rozwiązania technicznego, sprawdzenie:
 - 1) trybu pracy urządzeń wg wskazań paneli sterujących bądź aplikacji zarządzającej, poprzez porównanie z dokumentacją systemu,
 - 2) działania przycisków otwierających wyjścia z czynnikiem działającym jednostronnie, w tym działania przycisków ewakuacyjnych w przypadku, gdy SKD nie współpracuje z systemem ppoż..

- 3) działania czynników systemu z odpowiednią kartą dostępu,
- 4) mocowania czynników, samozamykaczy, zamków elektromagnetycznych drzwi i przejeść, w tym istnienia śladów prób penetracji (rysy, wgniecenia, próby podważania, demontażu),
- 5) ilości i rozmieszczenia czynników zgodnie z danymi w dzienniku systemu,
- 6) limitu użytkowników systemu.

6. Przeglądy dokonywane przez Administratora Zabezpieczeń Fizycznych co 6 miesięcy obejmują dodatkowo sprawdzenie stanu technicznego nośników elektronicznych SKD (identyfikatorów) przeznaczonych dla gości, jeśli mają zastosowanie w danej jednostce organizacyjnej.

7. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują sprawdzenie:

- 1) prawidłowości funkcjonowania systemu SKD w zakresie określonym w dokumentacji technicznej,
 - 2) ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego, w tym wymiana akumulatorów zgodnie z harmonogramem załączonym do dokumentacji technicznej systemu,
 - 3) działania części elektromechanicznych (elektrozaczepów, trzymaczy elektromagnetycznych, śluz, tripodów itp.).
8. Przeglądy CCTV są przeprowadzane przez Administratora Zabezpieczeń Fizycznych i obejmują sprawdzenie:
- 1) trybu pracy urządzeń rejestrujących poprzez porównanie z dokumentacją techniczno-eksploatacyjną na podstawie wskazań paneli sterujących informujących o trybie pracy urządzeń,
 - 2) jakości obrazu i pola obserwacji na monitorach poprzez porównanie z opisem oraz zdjęciem obrazu wykonanym w trybie dziennym i nocnym,
 - 3) wymiany nośników w urządzeniu rejestrującym zgodnie z dokumentacją techniczną systemu,
 - 4) poprawności pracy urządzeń rejestrujących poprzez nagranie i odtworzenie przebiegu zdarzeń w trybie czasu rzeczywistego oraz losowo wybranego zdarzenia w czasie przesyłnym.

9. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują:

- 1) sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego,
- 2) wyłączenie monitora i sprawdzenie „poświaty” (efekt „wypalania się” kineskopu objawiający się „pozostawieniem” obrazu na ekranie po odłączeniu źródła sygnału),
- 3) sprawdzenie jakości zarejestrowanego obrazu z kamer rejestrujących punkty neuralgiczne szczególnie z kamer zewnętrznych, rejestracja wykonana w godzinach nocnych),
- 4) sprawdzenie zapisu z wewnętrznych pamięci kamer (jeśli kamery posiadają taką pamięć),
- 5) sprawdzenie mocowania kamer zewnętrznych, jeśli są narażone na działania czynników atmosferycznych i innych np. konary drzew,
- 6) sprawdzenie działania wycieraczek, obwodów: grzałek (elementy przeciwmroźne, jeśli zostały zainstalowane),
- 7) sprawdzenie działania głowic obrotowych i funkcji „zoom” (optyczny i elektroniczny),
- 8) sprawdzenie mocowania reflektorów podczernieni i oświetlenia sztucznego związanego z CCTV (np. halogeny włączane automatycznie – z czasowym wyłącznikiem).

§ 14.

Systemy wspomagające oświadczenie

1. Przeglądy systemu są przeprowadzane przez Administratora Zabezpieczeń Fizycznych zgodnie z harmonogramem i obejmują sprawdzenie systemów sterujących (włączających i wyłączających oświetlenie). Harmonogram przeglądów jest ustalany przez Administratora Zabezpieczeń Fizycznych w porozumieniu z:
 - 1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa,
 - 2) w oddziale regionalnym i biurach powiatowych – osobami pełniącymi funkcję Inspektora Bezpieczeństwa Informacji.

2. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują:

- 1) sprawdzenie zasilania podstawowego i awaryjnego,
- 2) sprawdzenie innych elementów, zgodnie z dokumentacją systemu.

§ 15.

Systemy transmisji sygnałów alarmowych do centrów monitoringu

1. Przeglądy systemu transmisji sygnałów alarmowych do centrów monitoringu są przeprowadzane przez podmiot zewnętrzny zgodnie z harmonogramem i obejmują sprawdzenie trybu pracy urządzenia wg wskazań paneli sterujących poprzez porównanie z dokumentacją systemu.

2. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują:

- 1) sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego (wymiana akumulatorów zgodnie z harmonogramem załączonym do dokumentacji technicznej systemu),
- 2) sprawdzenie systemu anten, masztów, stanu uzziemienia,
- 3) sprawdzenie/potwierdzenie prawidłowego działania systemu/systemów w centrum monitoringu.

§ 16.

Rejestrowanie i przechowywanie informacji w elektronicznych systemach zabezpieczeń

1. Zdarzenia rejestrowane w elektronicznych systemach zabezpieczeniowych podlegają regularnym przeglądom przeprowadzanym przez Administratora Zabezpieczeń Fizycznych.

2. Częstość przeglądu zapisów wyznacza się na podstawie pojemności pamięci zdarzeń danego systemu:

- 1) przed czynnością włączenia/wyłączenia dla systemów, których pamięć zdarzeń jest kasowana podczas włączania/wyłączenia, lub
- 2) przed zapelnieniem pamięci systemu powodującej nadpisywanie danych (wg danych w dokumentacji techniczno-eksploatacyjnej systemu),
nie rzadziej jednak niż raz w 6 miesięcy.

3. Zapisy w systemach telewizji dozorowej (CCTV), kontroli dostępu (SKD) sygnalizacji włamania i napadu (SSWiN) oraz w dziennikach/rejestrach wejścia/wyjścia podlegają wyrywkowej kontroli korelacji rejestrowanych zdarzeń dokonywanej przez Administratora Zabezpieczeń Fizycznych.

4. W przypadku wystąpienia incydentu naruszenia bezpieczeństwa lub podejrzenia wystąpienia, którego okoliczności mogą być wyjaśnione dzięki zapisom z rejestrów elektronicznych systemów zabezpieczeń, Administrator Zabezpieczeń Fizycznych zapewnia utrwalenie zapisów z tych rejestrów elektronicznych systemów zabezpieczeń zgodnie z Regulaminem zarządzania incydentami.

§ 17.

Prowadzenie dokumentacji związanej z technicznymi systemami zabezpieczeń

1. Administrator Zabezpieczeń Fizycznych jest odpowiedzialny za prowadzenie wszelkich ewidencji, wykazów uprawnień, rejestrów, w tym rejestrów elektronicznych systemów zabezpieczeń.

2. Wszelka dokumentacja wskazana w ust. 1 jest klasyfikowana jako informacja wrażliwa.

3. Administrator Zabezpieczeń Fizycznych jest odpowiedzialny za aktualność i kompletność dokumentacji technicznych własnych systemów zabezpieczeń (tzn. dokumentacji powykonawczej, zmian w tej dokumentacji, aktualnych plików konfiguracyjnych systemów i urządzeń).

§ 18.

Zarządzanie zapisami pochodzącymi z elektronicznych systemów zabezpieczeń

1. Administrator Zabezpieczeń Fizycznych jest odpowiedzialny za utrzymanie rejestrów elektronicznych własnych systemów zabezpieczeń (SKD, SSWiN, CCTV), Okres przechowywania zapisów pochodzących z elektronicznych systemów zabezpieczeń powinien wynosić co najmniej 14 dni.

2. W przypadku powierzenia utrzymania rejestrów systemów kontroli dostępu, sygnalizacji napadu i włamania lub telewizji dozorowej podmiotowi zewnętrznemu, umowa z usługodawcą musi zapewniać Agencji skuteczną kontrolę nad zapisami przez umieszczenie w niej:

- 1) warunków i czasu przechowywania rejestrów (min. 14 dni),
- 2) wymagań bezpieczeństwa w odniesieniu do rejestrów,
- 3) zasad dostępu Agencji do przechowywanych zapisów, w tym uzyskania kopii stanowiących materiał dowodowy, jeśli zachodzi taka potrzeba,
- 4) sposobów komunikowania się Agencji z usługodawcą, w tym potwierdzania dostarczenia kopii rejestrów w trybie awaryjnym,
- 5) zakres odpowiedzialności usługodawcy za utratę lub uszkodzenie rejestrów.

3. W przypadku stwierdzenia incydentu naruszenia bezpieczeństwa informacji Administrator Zabezpieczeń Fizycznych wykonuje kopie rejestrów elektronicznych systemów zabezpieczeń dla celów dowodowych.

REGULAMIN EKSPLOATACJI SYSTEMÓW TELEINFORMATYCZNYCH

Świadczenie usług informatycznych przez podmioty zewnętrzne.....	14
Rozdział 4. Zarządzanie zmianami w systemach teleinformatycznych Agencji	15
Odbiór systemu teleinformatycznego	15
Kontrola zmian w eksploatacji.....	16
Bezpieczeństwo dokumentacji systemu.....	17
Rozdział 5. Zarządzanie wymiennymi nośnikami komputerowymi.....	17
Użytkowanie nośników.....	17
Wycofanie z eksploatacji nośników komputerowych.....	18
Rozdział 6. Bezpieczeństwo wymiany danych	18
Bezpieczeństwo serwisów intranetowych i ekstranetowych.....	18
Bezpieczeństwo wyniany poczty elektronicznej wewnętrznej i zewnętrznej.....	19
Rozdział 7 Konserwacja i naprawa sprzętu	19
Konserwacja i naprawa sprzętu.....	19
Zabezpieczenie sprzętu poza siedzibą.....	20
Rozdział 8. Zarządzanie dostępem do systemów teleinformatycznych.....	20
Rejestrowanie użytkowników i przypisanie praw dostępu.....	20
Zarządzanie przywilejami.....	21
Zarządzanie hasłami użytkowników.....	21
Zasady dostępu do plików i katalogów.....	23
Rozdział 9. Zasady monitorowania systemów i ich użycia.....	23
Mechanizmy monitorowania systemów.....	23
Dziennik pracy systemu.....	24
Synchronizacja zegarów.....	25
Bezpieczeństwo okablowania.....	26
Eksploatacja urządzeń zasilających.....	26
Załącznik nr 1 do Regulaminu eksploatacji systemów teleinformatycznych - Rejestr kopii zapasowych.....	28
Załącznik nr 2 do Regulaminu eksploatacji systemów teleinformatycznych - Ewidencja bezpiecznych kopert.....	29
Załącznik nr 3 do Regulaminu eksploatacji systemów teleinformatycznych - Dziennik pracy systemu	30
Załącznik nr 4 do Regulaminu eksploatacji systemów teleinformatycznych - Wniosek dotyczący użytkownika programu narzędziowego.....	31

Spis treści:

§ 1. Definicje.....	3
Rozdział 1. Podstawowe zasady eksploatacji systemów teleinformatycznych.....	4
Podział obowiązków w eksploatacji.....	4
Monitorowanie pojemności i wydajności systemów.....	4
Ochrona przed szkodliwym oprogramowaniem.....	5
Kontrola licencjonowanego oprogramowania.....	6
Zarządzanie kopiami zapasowymi i archiwalnymi.....	7
Zarządzanie poprawkami technicznymi.....	8
Rozdział 2. Zasady bezpieczeństwa sieci.....	9
Ogólne mechanizmy bezpieczeństwa sieci.....	9
Uwierzytelnianie węzłów.....	10
Ochrona urządzeń sieciowych.....	10
Bezpieczeństwo zdalnego dostępu do portów diagnostycznych i konfiguracyjnych.....	10
Bezpieczeństwo dostępu do sieci publicznych (Internet).....	11
Rozdział 3. Bezpieczeństwo systemów operacyjnych.....	11
Ogólne mechanizmy bezpieczeństwa.....	11
Identyfikacja i uwierzytelnianie użytkowników.....	12
System zarządzania hasłami.....	12
Użycie programów narzędziowych.....	13
Ograniczenia czasowe sesji połączeniowej.....	13
Eksploatacja aplikacji w systemach teleinformatycznych Agencji.....	14

§ 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 polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszonym sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej (PN-1-13335-1);
- 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 zapewniająca, 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 stosowanych 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 – uzgodniona i zaakceptowana wcześniej zmiana konfiguracji urządzeń lub sposobu/ zakresu świadczonych usług;
- 17) zmiana infrastruktury/ usługa awaryjna - zmianę podejmowaną w trybie nagłym wynikającą z konieczności usunięcia awarii lub błędów 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. Rola 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 zatwierdzone 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,

§ 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 standardyzacji 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 doraznym 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 doraznego jest:
 - 1) Ządanie 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 ostrzeżenie 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.

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 urządzeń 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

§ 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 zlecić 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 Księdze 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, zamieszanie 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. Kopie 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 o informacje uzyskane od producentów urządzeń sieciowych, systemów operacyjnych i aplikacji

kacji 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) rozdzielania 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 routingu 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 dostępne przyłączone w jednej ze stref zapory ogniowej – strefy dostępnej 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 zaporce ogniowej lub koncentratorze VPN zlokalizowanym w strefie dostępnej).

§ 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 podłączonego 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, zapewniającej 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 połączona do sieci ogólnodostępnych (np. sieć publiczna Internet) tylko na poziomie WANu 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. Architektury 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 uprawnień 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 hasel.

§ 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; odblokowanie 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 hasel,
 - 2) wybór i zmianę hasel przez użytkowników,

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 uprawnień 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 użytkowników 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 wymykających z dokumentów polityki bezpieczeństwa informacyjnego.

- 3) potwierdzenie zmiany hasel dla uniknięcia błędów podczas ich wprowadzania,
 - 4) wymuszenie wyboru hasel o odpowiedniej jakości, tj.: składających się co najmniej z 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne,
 - 5) wymuszenie zmiany hasel z ustaloną częstotliwością, w przypadku systemów przetwarzających dane osobowe zmiana hasła następuje nie rzadziej niż co 30 dni.
 - 6) wymuszenie zmiany hasel tymczasowych przy pierwszym rejestrowaniu się w systemie,
 - 7) pamiętanie hasel przez system w celu zapobiegania ponownemu ich użyciu, minimalna liczba hasel 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 wyłączenie 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.

cji 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. Doradne 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. Doradne 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 jakiegokolwiek 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, zatwierdzeniu, 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 sprawujących się do wprowadzenia nowego elementu infrastruktury, zmodyfikowania lub usunięcia istniejącego elementu infrastruktury, poprawiania błędów 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 zmiany Administrator Systemu (jeżeli działania te zostały na niego delegowane).

6. Każda zmiana regularna jest poprzedzona udokumentowanymi:

- 1) opisem zmiany,
- 2) opisem przyczyn zmiany (wraz z podaniem aktów prawnych uzasadniających zmianę - jeżeli ma zastosowanie),
- 3) opisem rodzaju wymaganych działań,
- 4) szacowaniem ryzyka potencjalnego wpływu zmian.

- 5) harmonogramem prowadzonych zmian.
- 6) wykonaniem kopii zapisowej z możliwością odwołania stanu poprzedniego na wypadek nieprzewidywanych zdarzeń (jeżeli ma zastosowanie),
- 7) przetestowaniu 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 bezwzględnie 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 wykonawcza 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 powstających podczas pożaru,
 - 4) zlaniami,
 - 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 jednoznaczna 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 informację,
 - 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 utracie, 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 świadczący 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. Wymoszenie 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 niezasyfrowanej.
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 Księżce Procedur KP-611-206-ARiMR.
6. Wymoszenie 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/odbięcia uprawnień pracownikom ARiMR zawartą w Księżce 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 prowadzi Właściciel Procesów/Właściciel 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 dokumentowe 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 Księżce 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 hasłami.

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 hasel przez osoby trzecie lub za pośrednictwem otwartych wiadomości poczty elektronicznej (nie dotyczy to hasel 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 hasel:

1) siły hasła (długość i złożoność hasel),

2) maksymalnego okresu ważności,

3) ograniczenia możliwości ponownego wykorzystania hasła (pamięć ostatnio używanych hasel).

7. Specjalne warunki przechowywania duplikatów hasel dotyczą:

1) elementów aktywnych sieci teleinformatycznej,

2) hasel 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 hasel w wersji elektronicznej poprzez zastosowanie oprogramowania typu „password manager” z bazą szyfrowaną algorytmem AES lub Twofish.

9. Do przechowywania hasła głównego do zaszyfrowanej bazy hasel, bądź innych hasel 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 hasel,

2) datę jej złożenia i podpis osoby składającej kopertę,

3) skróconą nazwę przynależności hasła.

11. Koperty z hasłami podlegają oznaczeniu zgodnie z załącznikiem nr 2 do niniejszego Regulaminu oraz ścisłej ewidencji prowadzonej przez Administratora Systemu.

12. Ewidencja hasel przechowywana jest w miejscu zabezpieczonym przed utratą i dostępem osób niepowołanych

13. Za aktualność przechowywanych hasel odpowiedzialny jest Administrator Systemu.

14. Awaryjne otwarcie bezpiecznej koperty oraz pobranie kopii hasła znajdującego się w kopercie wymaga uprzedniej 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 Proceasu/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 Proceasu/Właściciela Zasobu odpowiedzialnego 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 zapewniających 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 uruchomienie 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 podjęcie 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 podjęcie 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, takte jak:

§ 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, podlogach 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 umożliwiający 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).

26

- 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 szacowania 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.

25

- zastosowanie zasilaczy bezprzewodowych (UPS), zastosowanie awaryjnych agregatów prądotwórczych.
5. Konfiguracja zasilania gwarantowanego wynika z Planu Zapewnienia Ciągłości Działania Agencji.
 6. Dobór urządzeń podtrzymujących zasilanie pod względem wydajności mocy jest poprzedzane jest przeprowadzeniem udokumentowanego bilansu mocy.
 7. Każde urządzenie sieci teleinformatycznej jest opatrzone tabliczką, z której wynika skład dane urządzenie jest zasilane, zawierającą nazwę rozdzielni lub tablicy zabezpieczeń oraz nazwę pola w rozdzielni 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 bezprzewodowe, 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 użytkownika.
 13. Servisowanie 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 zapisanych

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

Lp.	Nazwa systemu lub aplikacji	Crystofitność wykonywania backupu	Ilość kopii zapisanych	Sposób wykonywania kopii	Okres przechowywania	Miejsce przechowywania kopii zapisanych	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 hasel, 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	Rezerwacje pracy (data, godzina)	4	Zakończenie pracy (data, godzina)	5	Nazwisko i imię osoby dokonującej wpisu	6	Konto, które zostało usztychowane do obsługi zdarzenia	7	Podpis działająca naprawcze	8
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, producent, dostawcy)	
O 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(c) identyfikator(y) (ID) użytkownik(ów)

.....

Poziom uprawnień (przywilejów)

.....

.....
(data i podpis Administratora Systemu)

Załącznik nr 6a do umowy nr _____/DI/20..../2610 z dnia _____, 20.... r.

Klauzula informacyjna dotycząca przetwarzania danych osobowych

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

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator danych) pozyskanych w związku z zawarciem Umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II, 00-175 Warszawa. Z Administratorem danych można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator danych wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora danych, wskazany w pkt 1.
3. Dane osobowe pozyskane przez Administratora danych przetwarzane będą na podstawie art. 6 ust. 1 lit. b RODO w celu zawarcia oraz wykonania Umowy.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
 - 1) organy kontrolne,
 - 2) osoby lub podmioty, którym Administrator danych udzielił informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2018 poz. 1330 z późn. zm.),
 - 3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
 - 4) podmioty przetwarzające dane osobowe w imieniu Administratora danych na mocy zawartych innych umów, m. in. dostawcy IT.
5. Pani/Pana dane osobowe będą przechowywane przez okres obowiązywania Umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa. Okres przechowywania danych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora danych. Ponadto, okres przechowywania danych może zostać przedłużony na okres 5 lat, na potrzeby archiwizacji.
6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych oraz prawo do przenoszenia Pani/Pana danych osobowych.
7. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
8. Podanie przez Panią/Pana danych osobowych jest konieczne w celu określonym w pkt 3 powyżej, dla zawarcia i wykonania Umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa, a konsekwencją niepodania Pani/Pana danych osobowych będzie brak możliwości zawarcia Umowy.

Załącznik nr 6b do umowy nr _____/DI/20..../2610 z dnia _____20.... r.

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

..... z siedzibą w i adresem ul., zarejestrowaną w rejestrze przedsiębiorców Krajowego Rejestru Sądowego prowadzonym przez Sąd Rejonowy, WydziałGospodarczy Krajowego Rejestru Sądowego pod numerem KRS, o numerze Regon, zarejestrowanym podatnikiem podatku od towarów i usług NIP, kapitał zakładowy zł, którą reprezentuje:

1.
2.

zwana „Sprzedawcą”

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO¹ wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu zawarcia oraz wykonania Umowy².

(podpisy)

1.
2.

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

² W przypadku, gdy Sprzedawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Sprzedawca nie składa.

Załącznik nr 7 do Umowy nr ____/DI/20..../2610 z dnia _____ 20..... r.

Formularz ofertowy

Załącznik nr 8 do Umowy nr ____/DI/20.../2610 z dnia _____ 20.... r.

Wykaz osób
(zgodny ze złożonym w postępowaniu)

Doświadczenie osób wyznaczonych do realizacji zamówienia, o których mowa w § 3 ust. 5 Umowy:

1. **osoba z co najmniej 12 miesięcznym doświadczeniem przy realizacji zamówień na dostawy urządzeń typu Load Balancer, wraz z wdrożeniem, posiadająca certyfikat F5 Certified Solutions Expert Security lub równoważny.**

UWAGA

Przez certyfikat równoważny, o którym mowa powyżej Zamawiający rozumie certyfikat, który:

- 3) jest analogiczny co do zakresu z przykładowym certyfikatem wskazanym z nazwy dla danej roli, co jest rozumiane jako:
 - d) analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat,
 - e) analogiczny stopień poziomu kompetencji,
 - f) analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu,
- 4) potwierdzony jest egzaminem (dotyczy tylko tych ról, których przykładowe certyfikaty muszą być potwierdzone egzaminem).

Załącznik nr 7 do SIWZ

Plik, w formacie xml, wygenerowany z narzędzia ESPD

Plik, w formacie xml, wygenerowany z narzędzia ESPD („ESPD”) znajduje się w odrębnym pliku o nazwie „Załącznik nr 7 do SIWZ ESPD”. Plik należy pobrać i zapisać na dysk komputera oraz wypełnić przy pomocy narzędzia udostępnionego przez Urząd Zamówień Publicznych pod adresem <https://espd.uzp.gov.pl> .

Po uruchomieniu wyżej wymienionej strony internetowej, należy wybrać „pl Polski”, a potem zaznaczyć „Jestem wykonawcą”. Następnie należy zaimportować „ESPD” wczytując plik będący Załącznikiem nr 7 do SIWZ. Po sporządzeniu JEDZ należy go podpisać przez osobę lub osoby uprawnione.

Aktualne na dzień składania ofert oświadczenie w formie jednolitego europejskiego dokumentu zamówienia należy złożyć w postaci elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym, za pomocą środka komunikacji elektronicznej tj. Platformę Zakupową.

Szczegółowy zakres wymagań określony został w Rozdziale IV.2 SIWZ.

