25 lat
Agencja Restrukturyzacji
i Modernizacji Rolnictwa
Al. Jana Pawła II 70, 00-175 Warszawa

Zamawiający:

Agencja Restrukturyzacji i Modernizacji Rolnictwa
Al. Jana Pawła II 70
00-175 Warszawa

Adres biura:

ul. Poleczki 33
02-822 Warszawa

numer referencyjny sprawy: DPiZP.2610.26.2019

Specyfikacja Istotnych Warunków Zamówienia

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

na:
zakup wsparcia dla systemu Cisco Unifield Communications Manager wraz z infrastrukturą sprzętową: 2 szt. serwerów oraz 4000 szt. telefonów IP

wszczętym na podstawie ustawy z dnia 29 stycznia 2004 r.
- Prawo zamówień publicznych (tj.: Dz. U. z 2018 r. poz. 1986 z późn. zm.)

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 „Załóż konto", następnie należy wypełnić formularze i postępować zgodnie z poleceniami wyświetlającymi się na ekranie monitora. W przypadku Wykonawców niezalogowanych w celu złożenia oferty niezbędne jest podanie adresu e-mail (na który wysłane będzie potwierdzenie złożenia oferty), nr NIP oraz nazwy firmy, 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 z późn. zm.; 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:

   48510000 - Pakiety oprogramowania komunikacyjnego

   Dodatkowe kody:

   32550000 - Sprzęt telefoniczny

   50334140 - Usługi w zakresie napraw i konserwacji zestawów telefonicznych

2. Przedmiotem zamówienia jest

   a) zakup wraz z dostawą fabrycznie nowych, nienoszących śladów uprzedniego używania urządzeń 2 szt. serwerów i 4000 szt. telefonów IP do posiadanego przez Kupującego systemu CUCM /Cisco Unified Communications Manager/ (zwanych dalej „Sprzęt IT"), spełniających co najmniej parametry i funkcjonalności określone w Załączniku nr 1a do wzoru umowy wraz z załącznikami, stanowiącej Załącznik nr 6 do Specyfikacji Istotnych Warunków Zamówienia (dalej: „SIWZ"), wraz z niezbędnym Oprogramowaniem;

   b) wykonanie Wdrożenia Sprzętu IT, zgodnie z zasadami określonymi we wzorze umowy wraz z załącznikami, stanowiącej Załącznik nr 6 do SIWZ;

   c) wykonanie dokumentacji powykonawczej i dostarczenie jej w formie papierowej i elektronicznej do akceptacji i odbioru Kupującemu;

   d) świadczenie serwisu gwarancyjnego dla Sprzętu IT (usługa wsparcia), z czasem naprawy 6 godzin, przez okres minimum 36 miesięcy na warunkach opisanych we wzorze umowy wraz z załącznikami, stanowiącej Załącznik nr 6 do 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 6) i 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 przedmiotu zamówienia w następujących terminach:

a) Termin dostarczenia sprzętu IT: 15 dni roboczych.
b) Termin wdrożenia i dostarczenia dokumentacji powykonawczej: 15 dni roboczych licząc od dnia podpisania protokołu odbioru sprzętu.
c) Serwis gwarancyjny: 36 m-cy od dnia podpisania protokołu odbioru.

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 i technicznej:

   1.2.1. Zamawiający uzna, że Wykonawca spełnia warunek udziału we wskazanym zakresie, jeżeli Wykonawca wykaże, że: wykonał, w okresie ostatnich trzech (3) lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, a w przypadku świadczeń okresowych lub ciągłych również realizuje, co najmniej **jedno zamówienie** polegające na dostawie i wdrożeniu systemu telefonii IP, o wartości zamówienia co najmniej 1.000.000,00 zł brutto (słownie: jeden milion 00/100).

   UWAGA:

   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. Zamawiający uzna, że Wykonawca spełnia warunek udziału we wskazanym zakresie, jeżeli Wykonawca dysponuje co najmniej **1 osobą** posiadająca specjalistyczne kwalifikacje potwierdzone certyfikatem CCIE Collaboration/Voice lub równoważnym certyfikatem, o minimum **2-letnim doświadczeniu** zawodowym w zakresie wskazanego certyfikatu.

Przez certyfikat równoważny Zamawiający rozumie, że Wykonawca wykaże certyfikat, który:

1) jest analogiczny co do zakresu z przykładowymi certyfikatami wskazanymi z nazwy, co jest rozumiane jako:
   a) analogiczna dziedzina merytoryczna,
   b) analogiczny stopień poziomu kompetencji,
   c) analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu,
2) potwierdzony jest egzaminem (dotyczy przypadku gdy przykładowy certyfikat podany z nazwy musi być potwierdzony egzaminem).

UWAGA

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 2019 r. poz. 243 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 2019 r. poz. 498),
      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 2016 r. 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 pieniądz opatrzone kwalifikowanym podpisem elektronicznym osób upoważnionych do jego wystawienia (wystawców dokumentu). W przypadku wniesienia wadium w innej formie niż pieniądz, 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 umocowaną osobę. 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.

IV.2 Oświadczenie w formie Jednolitego Europejskiego Dokumentu Zamówienia.

1. Wykonawca wypełnia JEDZ, tworząc dokument w postaci elektronicznej. Wykonawca może korzystać z narzędzia ESPD lub innych dostępnych narzędzi lub oprogramowania, które umożliwiają wypełnienie JEDZ i utworzenie dokumentu w postaci elektronicznej.
   1.1. Zamawiający udostępnia Wykonawcom plik, w formacie xml, wygenerowany z narzędzia ESPD, który stanowi Załącznik nr 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 1.4. 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 2019 r. poz. 1170 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.

      Wzór oświadczenia w zakresie pkt 2.1.5. – 2.1.9. stanowi **Załącznik nr 2 do SIWZ**.

   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, w szczególności odpowiedzialnych za świadczenie usług, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami. Wzór oświadczenia stanowi **załącznik nr 5 do SIWZ.**
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 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,
      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. ze zm.),
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.2610.26.2019**, 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 przekaże 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. Pani Kinga Henzel, tel.: +48 22 595 00 66 w godz. 9.00 – 15.00.
   8.2. Pan Zbigniew Antonik, tel.: +48 22 595 00 62 w godz. 9.00 – 15.00.

Rozdział VI. Wymagania dotyczące wadium.

1. Wykonawca zobowiązany jest wnieść wadium w wysokości: **40.000,00 zł** (słownie: czterdzieści tysięcy złotych 00/100).
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 2019 r., poz. 310 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 wsparcia dla systemu Cisco Unifield Communications Manager wraz z infrastrukturą sprzętową: 2 szt. serwerów oraz 4000 szt. telefonów IP".
4. W przypadku wnoszenia wadium w innej formie niż pieniądz 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 wniesie wadium lub wniesie 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 2019 r. poz. 1010), 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 2019 r. poz. 162).
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.

1. 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: https://platformazakupowa.pl/pn/arimr.
2. Termin składania ofert upływa w dniu **21.10.2019 r.. o godzinie 10:00** 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.
3. Otwarcie ofert odbędzie się w dniu **21.10.2019 r. o godzinie 10:15** w biurze Zamawiającego, pod adresem ul. Poleczki 33, 02-822 Warszawa.
4. 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.

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

Rozdział X. Opis sposobu obliczenia ceny.

1. Wykonawca zobowiązany jest do wyliczenia i podania cen netto, brutto, łącznej ceny ofertowej netto, należnego podatku od towarów i usług VAT oraz łącznej ceny ofertowej brutto, w sposób określony w Formularzu Ofertowym stanowiącym Załącznik nr 1 do SIWZ.
2. Ceny określone w Formularzu Ofertowym powinny zawierać wszystkie koszty związane z wykonaniem przedmiotu zamówienia. Podane ceny nie podlegają zmianom przez okres obowiązywania umowy, z zastrzeżeniem postanowień Rozdziału XIV pkt 4 niniejszej SIWZ.
3. Ceny określone w formularzu ofertowym muszą być podane i wyliczone w zaokrągleniu do dwóch miejsc po przecinku (wg zasady zaokrąglenia: poniżej 5 należy końcówkę pominąć, powyżej i równe 5 należy zaokrąglić w górę).
4. Wszystkie ceny podane w Formularzu Ofertowym powinny być wyrażone w złotych polskich.
5. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający 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.

1. Przy wyborze oferty najkorzystniejszej Zamawiający będzie się kierował poniższym kryterium:

1) kryterium „cena" (Pc) – 60 %, wg poniższego wzoru

$$Pc = \frac{C_{min.}}{C_b} \text{ x 60 pkt}$$

gdzie:
Pc – ilość punktów oferty badanej w kryterium cena
$C_{min.}$ – cena najniższa spośród ważnych ofert
C_b – cena oferty badanej

2) kryterium „termin dostarczenia Sprzętu IT" (Ps) – waga 20 %, wg poniższej zasady:

Lp.	Termin dostarczenia Sprzętu IT – w Dniach Roboczych.	Ilość punktów
1	15	0
2	14-11	5
5	10 i mniej	20

Uwagi:
a) Maksymalny termin dostarczenia Sprzętu IT wynosi 15 Dni Roboczych.
b) Jeżeli Wykonawca zaoferuje termin dostarczenia Sprzętu IT dłuższy niż 15 Dni Roboczych – oferta takiego Wykonawcy zostanie odrzucona jako niezgodna z treścią SIWZ.
c) W przypadku braku wskazania terminu, o którym mowa powyżej, Zamawiający uzna, że Wykonawca zaoferował maksymalny termin dostarczenia Sprzętu IT tj. 15 Dni Roboczych i taki Wykonawca otrzyma 0 pkt.

3) **kryterium „termin przeprowadzenia Wdrożenia", (Pw) – waga 20 %, wg poniższej zasady:**

Lp.	Termin przeprowadzenia Wdrożenia – w Dniach Roboczych	Ilość punktów
1	15	0
2	14-11	5
4	10 i mniej	20

Uwagi:

a) *Maksymalny termin przeprowadzenia Wdrożenia wynosi 15 Dni Roboczych.*
b) *Jeżeli Wykonawca zaoferuje termin przeprowadzenia Wdrożenia dłuższy niż 15 Dni Roboczych – oferta takiego Wykonawcy zostanie odrzucona jako niezgodna z treścią SIWZ.*
c) *W przypadku braku wskazania terminu, o którym mowa powyżej, Zamawiający uzna, że Wykonawca zaoferował maksymalny termin przeprowadzenia Wdrożenia tj. 15 Dni Roboczych i taki Wykonawca otrzyma 0 pkt.*

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

P = Pc + Ps + Pw

gdzie:
P – ilość punktów oferty w łącznym kryterium oceny ofert,
Pc – ilość punktów oferty w kryterium „**cena**",
Ps – ilość punktów oferty w kryterium „**termin dostarczenia Sprzętu IT**,
Pw – ilość punktów oferty w kryterium „**termin przeprowadzenia wdrożenia**",

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 pieniądz, Zamawiający zastrzega sobie prawo do akceptacji projektu ww. dokumentów.
6. Zabezpieczenia w innej formie niż pieniądz, Wykonawca złoży u Zamawiającego w Kancelarii Głównej, mieszczącej się w Warszawie przy ul. Poleczki 33, z adnotacją „dla Departamentu Informatyki".
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 negocjacjom.
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).

ZASTĘPCA PREZESA

Zatwierdzam SIWZ wraz z załącznikami:

Warszawa, 19 .09.2019 r. Sebastian Jaworski

podpis Zamawiającego

Załącznik nr 1 do SIWZ wzór Formularza Ofertowego

Formularz Ofertowy
DPiZP.2610.26.2019

Ja(my) niżej podpisany(-i) .....

Działając w imieniu i na rzecz .....

.....

W odpowiedzi na ogłoszone postępowanie prowadzone w trybie przetargu nieograniczonego na „zakup wsparcia dla systemu Cisco Unifield Communications Manager wraz z infrastrukturą sprzętową: 2 szt. serwerów oraz 4000 szt. telefonów IP", zgodnie z wymaganiami określonymi w specyfikacji istotnych warunków zamówienia i wzorze Umowy wraz z załącznikami, oferuję(-emy) realizację przedmiotu zamówienia za cenę:

Lp.	Sprzęt IT	liczba	Parametry i wymagania minimalne:	Parametr oferowany – wypełnia Wykonawca
1.	Telefon IP	4 000 szt.	1. przełącznik port 10/100/1000 RJ-45 Ethernet 1 Gbps (IEEE 802.3) do podłączenia komputera; 2. port o prędkości portu 1 Gbps (IEEE 802.3) do sieci LAN; 3. wyświetlacz monochromatyczny LCD w 4bitowej skali szarości; 4. obsługujący min. 4 linie; 5. obsługiwane protokoły sygnalizacyjne: SCCP (Call Manager) / SIP; 6. gniazdo słuchawki nagłownej: RJ-9; 7. szerokopasmowe audio: obsługa kodeka G.722 zgodny z TIA 920, możliwość obsługi zestawu nagłownego i głośnika; 8. obsługiwane kodeki: G.711a, G.711u, G.729a, G.729ab, G.722 oraz kodeki kompresji audio iLBC; 9. głośnik: Full-duplex z funkcją korekcji szumów; 10. ilość klawiszy funkcyjnych min. 4; 11. obsługa QoS: DSCP oraz standardów 802.1.Q/p 12. fabrycznie zainstalowany certyfikat X.509v3, szyfrowanie AES-128, obsługa EAPOL pass-through 13. zgodność ze standardem PoE IEEE 802.3af (Class I); 14. posiada wsparcie producenta systemu CUCM min. dla wersji 12.5.	
2.	Serwer	2 szt.	1. zasoby dyskowe na min. 24 dyskach 300GB 6Gb SAS 10K RPM SFF HDD/hot plug/drive sled mounted; 2. kontroler modularny min. 12Gbps SAS 1GB FBWC Cache module (Raid 0/1/5/6); 3. zdublowany zestaw wentylatorów w układzie chłodzącym serwera; 4. min. dwa zasilacze AC 230V hot swap; 5. min. dwa gniazda CPU; 6. min. dwa procesory CPU 2.6 GHz 6132/140W 14C/18MB Cache/DDR4 2666 MHz; 7. pamięć RAM – min. 192GB w formie układów 16GB DDR4-2666-MHz RDIMM/PC4-21300/single rank/x4/1.2v; 8. wirtualizacja systemu zunifikowanej komunikacji musi być wspierana przez producenta rozwiązania pod względem technicznym; 9. w celu integracji z inną infrastrukturą serwerową, platforma wirtualizacyjna serwerów komunikacyjnych powinna mieć możliwość zarządzania przez centralny system zarządzania środowiskiem zwirtualizowanym np. VMWare vCenter lub równoważny; 10. posiada wsparcie producenta systemu CUCM min. dla wersji 12.5.	

L.p.	Przedmiot	Cena jednostkowa netto w zł	Ilość	Cena netto w zł	Podatek VAT		Cena brutto w zł
					%	zł	
a	b	c	d	e = c x d	f	g = e x f	f = e + g
1	Telefon IP fabrycznie nowy: Marka ..... Model ..... O parametrach technicznych wg Tabeli powyżej		4000 szt.				
2	Serwer fabrycznie nowy: Marka ..... Model ..... O parametrach technicznych wg Tabeli powyżej		2 szt.				
3	Oprogramowanie Webex		10 szt./licencji				
4	Oprogramowanie Enhanced		500 szt./licencji				
5	Aktualizacja (upgrade) do wersji Cisco UCM 12.5 lub wyższej		licencja na klaster 2 serwerów				
6	Wdrożenie i Dokumentacja powykonawcza		1				
7	Serwis gwarancyjny 1 rok		3				
Łącznie cena ofertowa					X		

Słownie zł cena ofertowa netto: .....

Słownie zł cena ofertowa brutto: .....

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. **Oferujemy termin dostarczenia Sprzętu IT w ciągu .... Dni Roboczych**
   - *Maksymalny termin dostarczenia Sprzętu IT wynosi 15 Dni Roboczych.*
   - *Jeżeli Wykonawca zaoferuje termin dostarczenia Sprzętu IT dłuższy niż 15 Dni Roboczych – oferta takiego Wykonawcy zostanie odrzucona jako niezgodna z treścią SIWZ.*
   - *W przypadku braku wskazania terminu, o którym mowa powyżej, Zamawiający uzna, że Wykonawca zaoferował maksymalny termin dostarczenia Sprzętu IT tj. 15 Dni Roboczych i taki Wykonawca otrzyma 0 pkt.*
4. **Oferujemy termin przeprowadzenia Wdrożenia w ciągu ..... Dni roboczych**
   - *Maksymalny termin przeprowadzenia Wdrożenia wynosi 15 Dni Roboczych.*
   - *Jeżeli Wykonawca zaoferuje termin przeprowadzenia Wdrożenia dłuższy niż 15 Dni Roboczych – oferta takiego Wykonawcy zostanie odrzucona jako niezgodna z treścią SIWZ.*
   - *W przypadku braku wskazania terminu, o którym mowa powyżej, Zamawiający uzna, że Wykonawca zaoferował maksymalny termin przeprowadzenia Wdrożenia tj. 15 Dni Roboczych i taki Wykonawca otrzyma 0 pkt.*
5. Uważamy się za związanych niniejszą ofertą na okres wskazany w SIWZ.
6. Wadium w wysokości **40.000,00 zł** (słownie: czterdzieści tysięcy złotych zero groszy) wnieśliśmy przed upływem terminu składania ofert.
7. Wadium wniesione w formie pieniądza należy zwrócić na rachunek bankowy nr .....prowadzony w banku ....., natomiast w przypadku wniesienia wadium w innej formie (gwarancji lub poręczenia) na adres .....
8. Zobowiązujemy się do wniesienia przed podpisaniem umowy zabezpieczenia należytego wykonania umowy w wysokości **5 %** ceny całkowitej podanej w ofercie.
9. W przypadku przyznania nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.

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

    * w przypadku *niewypełnienia Zamawiający uzna, że Wykonawca nie zamierza powierzyć wykonania żadnej części zamówienia podwykonawcom.*
11. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na poniższy adres: ..... Dane kontaktowe: imię i nazwisko ....., nr tel. ....., nr faks ....., adres e-mail: .....
12. Dokumenty wymienione od strony ..... do strony ..... stanowią tajemnicę przedsiębiorstwa i nie mogą być ujawnione pozostałym 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.
13. Oferta została złożona na _____ stronach kolejno ponumerowanych od nr_____ do nr _____.
14. 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/usługi, 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) żadnej z ww. treści oświadczenia i niewypełnienia powyższego pola oznaczonego: *„należy wskazać nazwę (rodzaj) towaru/usługi, których dostawa/świadczenie będzie prowadzić do jego powstania oraz ich wartość bez kwoty podatku od towarów i usług"* – Zamawiający uzna, że wybór przedmiotowej oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego
15. 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).*

    *** 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.).*

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

Załącznik nr 2 do SIWZ wzór Oświadczenia o braku podstaw wykluczenia

Oświadczenie o braku podstaw wykluczenia

DPIZP.2610.26.2019

Ja(my) niżej podpisany(-i) .....
działając w imieniu i na rzecz .....
.....
[*Firma, adres siedziby Wykonawcy*]

Przystępując do udziału w postępowaniu o zamówienie publiczne na „zakup wsparcia dla systemu Cisco Unifield Communications Manager wraz z infrastrukturą sprzętową: 2 szt. serwerów oraz 4000 szt. telefonów IP" 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) niezalegamy 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

Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej

DPIZP.2610.26.2019

Ja(my) niżej podpisany(-i) .....
działając w imieniu i na rzecz .....
.....
[*Firma, adres siedziby Wykonawcy*]

Przystępując do udziału w postępowaniu o zamówienie publiczne na „zakup wsparcia dla systemu Cisco Unifield Communications Manager wraz z infrastrukturą sprzętową: 2 szt. serwerów oraz 4000 szt. telefonów IP"

1) Oświadczamy, że nie należymy do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (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 (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]

Oświadczenie – Wykaz dostaw
DPIZP.2610.26.2019

Ja(my) niżej podpisany(-i) .....
działając w imieniu i na rzecz .....
.....
[*Firma, adres siedziby Wykonawcy*]

Przystępując do udziału w postępowaniu o zamówienie publiczne na „zakup wsparcia dla systemu Cisco Unifield Communications Manager wraz z infrastrukturą sprzętową: 2 szt. serwerów oraz 4000 szt. telefonów IP", 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 spełniania 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: **jedno zamówienie** polegające na dostawie i wdrożeniu systemu telefonii IP, o wartości zamówienia co najmniej 1.000.000,00 zł brutto (słownie: jeden milion 00/100))	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*)	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								

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 spełniania warunku udziału;*
2. *Dla wykazania spełniania 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]

Oświadczenie – Wykaz osób, skierowanych do realizacji zamówienia
DPIZP.2610.26.2019

Ja(my) niżej podpisany(-i) .....
działając w imieniu i na rzecz .....
.....
[*Firma, adres siedziby Wykonawcy*]

Przystępując do udziału w postępowaniu o zamówienie publiczne na „zakup wsparcia dla systemu Cisco Unifield Communications Manager wraz z infrastrukturą sprzętową: 2 szt. serwerów oraz 4000 szt. telefonów IP", składamy wykaz osób, które będą uczestniczyć w wykonaniu zamówienia zgodnie z § 3 ust. 5 wzoru Umowy stanowiącego Załącznik nr 6 do SIWZ, które posiadają niżej opisane doświadczenie:

Wymagane w SIWZ [§ 3 pkt 1) wzoru Umowy]	Imię i nazwisko oraz opis posiadanego certyfikatu
Osoba wyznaczona do realizacji zamówienia posiadająca: • specjalistyczne kwalifikacje i minimum roczne doświadczenie w zakresie objętym przedmiotem zamówienia; • certyfikat CCIE Collaboration/Voice wystawionym przez Producenta lub równoważnym. *<u>Uwaga</u>:* *Przez certyfikat równoważny Zamawiający rozumie, że Wykonawca wykaże certyfikat, który:* *1) jest analogiczny co do zakresu z przykładowymi certyfikatami wskazanymi z nazwy, co jest rozumiane jako:* a) *analogiczna dziedzina merytoryczna,* b) *analogiczny stopień poziomu kompetencji,* c) *analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu,* *2) potwierdzony jest egzaminem (dotyczy przypadku gdy przykładowy certyfikat podany z nazwy musi być potwierdzony egzaminem).*	..... *(imię i nazwisko)* Posiada certyfikat, tj.: ..... *(nazwa certyfikatu)* Wydany przez: ..... nr ..... *(o ile dotyczy)* ważny do ..... *(o ile dotyczy)* **Doświadczenie**: ..... *(w latach)*

Załącznik nr 6 do SIWZ wzór Umowy

Wzór Umowy

Umowa nr _____ /DI/2019/2610

zawarta w dniu _____ _____ 2019 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 2018 r. poz. 1986 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, serwery (2 szt.) oraz telefony IP (4000 szt.) do rozbudowy i modernizacji posiadanego przez Kupującego zunifikowanego systemu komunikacji CUCM (*Cisco Unified Communications Manager*), szczegółowo opisane w Załączniku nr 1a do Umowy;
4) **Oprogramowanie** – programy dostarczone przez Sprzedawcę, z których Kupujący korzysta na podstawie Licencji udzielonych przez producenta, niezbędne do 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 i Oprogramowania;
7) **Wdrożenie** – czynności wykonywane przez Sprzedawcę, mające na celu przeprowadzenie migracji i uruchomienie dostarczonego Sprzętu IT, instalacje Oprogramowania oraz przeniesienie konfiguracji z posiadanych i użytkowanych przez Kupującego urządzeń na Sprzęt IT – szczegółowo opisane w Załączniku nr 1a do Umowy;
8) **Dokumentacja powykonawcza** – dokumentacja techniczna zawierająca schemat fizyczny i logiczny podłączenia Sprzętu IT, konfigurację Sprzętu IT oraz opis zastosowanych rozwiązań i technologii;
9) **Dokumenty** - instrukcje eksploatacyjne, instrukcje obsługi Sprzętu IT oraz dokumenty licencyjne dla Oprogramowania;
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 i ul. Poleczki 33, 02-822 Warszawa;
11) **Lokalizacja** – Biuro Centrali ARiMR, Oddziały Regionalne i Biura Powiatowe Kupującego, których adresy zostały wymienione w Załączniku nr 1b do Umowy;
12) **Dni Robocze** – dni w godzinach pracy 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 do Lokalizacji fabrycznie nowy, nienoszący śladów uprzedniego używania Sprzęt IT wraz z Oprogramowaniem, zgodnie ze specyfikacją stanowiącą Załącznik nr 1a i 1b 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 36 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. Sprzedawca będzie przyjmował zgłoszenia serwisowe, w ramach Serwisu gwarancyjnego zgodnie z § 6 Umowy, 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.

§ 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 CCIE Collaboration/Voice. W ramach Wdrożenia wymagane będzie przeniesienie funkcjonalności z urządzeń posiadanych przez Kupującego, zgodnie z Załącznikiem nr 1a do Umowy.
6. W terminie do 2 Dni Roboczych po podpisaniu przez upoważnionych przedstawicieli Stron Umowy, Kupujący przekaże Sprzedawcy aktualną konfigurację urządzeń, o których mowa w ust. 5 oraz zapisy konfiguracji do przeniesienia z urządzeń posiadanych przez Kupującego, zgodnie z Załącznikiem nr 1 do Umowy.

§ 4. Terminy i odbiory

1. W terminie:
   1) ..... Dni Roboczych od dnia zawarcia Umowy nastąpi dostarczenie Sprzętu IT do Lokalizacji wskazanych w Załączniku nr 1b do Umowy, dostarczenie Sprzętu IT z Oprogramowaniem, Dokumentów *(termin zostanie wpisany po wyborze oferty najkorzystniejszej, zależnie od ilości dni wskazanych przez Wykonawcę w pkt 3 Formularza Ofertowego. Maksymalny termin to 15 Dni Roboczych)*;
   2) ..... Dni Roboczych od dnia zakończenia czynności określonych w ust. 1 Sprzedawca wykona Wdrożenie w lokalizacjach COPD *(termin zostanie wpisany po wyborze oferty najkorzystniejszej, zależnie od ilości dni wskazanych w pkt 4 Formularza Ofertowego. Maksymalny termin to 15 Dni Roboczych).*
2. Sprzedawca powiadomi, w formie pisemnej, Kupującego o terminie dostarczenia Sprzętu IT w poszczególnych Lokalizacjach oraz Sprzętu IT wraz z Oprogramowaniem, i Dokumentów oraz o terminie rozpoczęcia Wdrożenia w lokalizacjach COPD, z wyprzedzeniem co najmniej 2 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 w Lokalizacjach oraz odbiór Sprzętu IT, Oprogramowania i Dokumentów w lokalizacjach COPD 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 1a i nr 7 do Umowy;
   2) podłączy Sprzęt IT do sieci zasilającej i zainstaluje Oprogramowanie;
   3) usunie z miejsca dostarczenia i zutylizuje wszelkie opakowania, pozostałe po dostarczeniu i zainstalowaniu Sprzętu IT;
   4) wykona Wdrożenie, zgodnie z ust. 7.
6. Potwierdzeniem odbioru przez Kupującego Sprzętu IT w poszczególnych Lokalizacjach będzie każdorazowo Protokół odbioru Sprzętu IT podpisany w każdej Lokalizacji Kupującego bez żadnych zastrzeżeń przez upoważnionych przedstawicieli Stron, którego wzór stanowi Załącznik nr 2a do Umowy.
7. W ramach Wdrożenia Sprzedawca w obecności pracownika Kupującego wykona czynności wskazane w Załączniku nr 1a do Umowy, co zostanie potwierdzone podpisaniem przez upoważnionych przedstawicieli Stron Protokołem odbioru końcowego Wdrożenia, którego wzór stanowi Załącznik nr 2b do Umowy.
8. Po dokonaniu przez upoważnionych przedstawicieli Kupującego bez zastrzeżeń odbioru Sprzętu IT wraz z Oprogramowaniem, Dokumentów oraz Wdrożenia w ostatniej lokalizacji COPD, upoważnieni przedstawiciele Stron podpiszą Protokół odbioru końcowego, którego wzór stanowi Załącznik nr 2b do Umowy.
9. W przypadku stwierdzenia podczas odbioru, że:
   1) Sprzęt IT lub Oprogramowanie są niezgodne z Załącznikiem nr 1a-1b 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 przekaże 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.

10. W przypadku stwierdzenia podczas powtórnej procedury czynności odbioru którejkolwiek z okoliczności wskazanych w ust. 9, Kupujący odmówi odbioru przedmiotu Umowy i jednocześnie przekaże Sprzedawcy protokół przedstawiający powód odmowy odbioru Sprzętu IT wraz z Oprogramowaniem, Dokumentów wraz z Wdrożeniem. W sytuacji odmowy odbioru Sprzętu IT wraz z Oprogramowaniem i Dokumentów Sprzedawca ma obowiązek odbioru dostarczonego Sprzętu IT wraz z Oprogramowaniem Dokumentów z miejsca dostarczenia w terminie 3 Dni Roboczych od daty przekazania Sprzedawcy protokołu przedstawiającego powody odmowy odbioru Sprzętu IT.
11. W terminie do 15 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 do Umowy. Kupujący zastrzega sobie prawo zgłaszania uwag do Dokumentacji powykonawczej. Sprzedawca zobowiązany jest uwzględnić uwagi Kupującego lub zgłosić zastrzeżenia w terminie 5 Dni Roboczych od dnia otrzymania uwag od Kupującego.
12. 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 jakiejkolwiek 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 36 miesięcy od dnia podpisania Protokołu odbioru Dokumentacji powykonawczej, o którym mowa w § 4 ust. 11 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 Lokalizacjach oraz w lokalizacji COPD, w których 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 1a i 7 do Umowy. Dostarczenie zastępcze wymaga zgody Kupującego.
6. Sprzedawca będzie przyjmował zgłoszenia serwisowe Kupującego od osób wskazanych w § 3 ust. 2 Umowy, 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. Usunięcie wady lub wymiana Sprzętu IT zostaną potwierdzone Protokołem odbioru usunięcia wady podpisanym przez upoważnionych przedstawicieli Stron, sporządzonym według wzoru stanowiącego Załącznik nr 4 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 1a 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 adresu Lokalizacji lub lokalizacji COPD (w obrębie Warszawy). W przypadku zmiany lokalizacji COPD Kupujący odinstaluje, przewiezie, dokona instalacji i uruchomi Sprzęt IT z Oprogramowaniem 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 adresu Lokalizacji lub 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 lub lokalizacji COPD, Sprzedawca świadczyć będzie zobowiązania wynikające z Umowy dla zmienionej Lokalizacji lub 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 udoskonaleń 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 istnieją;
    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 .....,XX zł (słownie złotych ..... XX/100), powiększone o należny VAT co daje kwotę brutto .....,XX zł (słownie złotych: ..... XX/100), z czego:
    1) wynagrodzenie za sprzedaż i dostarczenie Sprzętu IT wraz z Oprogramowaniem wynosi netto .....,XX zł (słownie złotych ..... XX/100), powiększone o należny VAT co daje kwotę brutto .....,XX zł (słownie złotych: ..... XX/100),
    2) wynagrodzenie za Wdrożenie i Dokumentację powykonawczą wynosi netto .....,XX zł (słownie złotych: ..... XX/100), powiększone o należny VAT co daje kwotę brutto ..... zł (słownie złotych: ..... XX/100),
    3) wynagrodzenie za Serwis gwarancyjny wynosi netto .....,XX zł (słownie złotych ..... XX/100), powiększone o należny VAT 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. 11 Umowy, stanowiącym podstawę wystawienia faktury VAT;
    2) w ust. 1 pkt 3 płatne jest każdorazowo w terminie do 28 dni licząc od daty otrzymania przez Kupującego prawidłowo wystawionej faktury oraz podpisanego bez zastrzeżeń przez upoważnionych przedstawicieli Stron protokołu odbioru, o którym mowa w § 6 ust. 6, w trzech równych częściach, przy czym Sprzedawca wystawi fakturę obejmującą pierwszą cześć wynagrodzenia 10 miesięcy po podpisaniu ww. protokołu odbioru Wdrożenia, fakturę obejmującą drugą cześć wynagrodzenia – po upływie roku od dokonania przez Kupującego płatności pierwszej faktury, jednak nie później niż 1.12.2021 r. oraz fakturę obejmującą trzecią cześć wynagrodzenia – po upływie roku od dokonania przez Kupującego płatności drugiej faktury, jednak nie później niż 1.12.2022 r.
3. Wynagrodzenie, o którym mowa w ust. 1, wyczerpuje wszelkie roszczenia finansowe Sprzedawcy z tytułu wykonania Umowy, w tym uwzględnia obsługę zgłoszeń serwisowych, 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. 11 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, o którym mowa w § 6 ust. 6 Umowy spowodują naliczenie ponownego, 28-dniowego terminu płatności od dostarczenia prawidłowo wystawionej faktury VAT lub podpisanego Protokołu odbioru Serwisu gwarancyjnego / usunięcia wady.
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 wysłania 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 pkt. 1 lub pkt 2 lub § 4 ust. 2 Umowy Kupującemu przysługuje kara umowna w wysokości 3000,00 zł (słownie złotych: trzy 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 przesłanki uprawniającej do odstąpienia) oraz zażądać kary umownej w wysokości 10 % 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 rękojmi, w stosunku do terminów, o którym mowa w § 6 ust. 4 lub 5 Umowy, Kupującemu przysługuje kara umowna w wysokości 0,2 % 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 0,01 % 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 wyznaczania dodatkowego terminu na usunięcie wad oraz żądać kary umownej w wysokości 10 % 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. 9, Sprzedawca zapłaci karę umowną w wysokości 3000,00 zł (słownie złotych: trzy 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 1000,00 zł (słownie złotych: tysiąc 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 10 % 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. 11 Sprzedawca zapłaci karę umowną w wysokości 2000,00 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. 11 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 utrwalania i zwielokrotniania utworu – wytwarzanie każdą techniką egzemplarzy utworów, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;
   2) w zakresie obrotu oryginałem oraz egzemplarzami, na których utwory utrwalono – wprowadzanie do obrotu, użyczanie oraz najem oryginału oraz egzemplarzy;
   3) w zakresie rozpowszechniania utworów w sposób inny niż określony w pkt. 2 – publiczne wykonanie, wystawienie, wyświetlanie, odtwarzanie oraz nadawanie i reemitowanie, a także publiczne udostępnianie utworów w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i w czasie przez siebie wybranym;
   4) dowolne przetwarzanie utworów, w tym łączenie z innymi utworami;
   5) zezwalanie na wykonywanie zależnych praw autorskich poprzez rozporządzanie 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 utrwalono, 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 jakiekolwiek 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 10 % 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 ……,XX 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 Dokumentacji powykonawczej, o którym mowa w § 4 ust. 11 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 obowiązywać 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 ……,XX 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 ……,XX 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 Głównej, 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. 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 poświadczeniem 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 1a – Specyfikacja Sprzętu IT i Oprogramowania oraz zasady Wdrożenia;
   2) Załącznik nr 1b – Wykaz Lokalizacji Kupującego;
   3) Załącznik nr 2a – Protokół odbioru Sprzętu IT w Lokalizacjach (wzór);
   4) Załącznik nr 2b – Protokół odbioru końcowego Sprzętu IT / Wdrożenia (wzór);
   5) Załącznik nr 3 – Protokół odbioru Dokumentacji powykonawczej (wzór);
   6) Załącznik nr 4 – Protokół odbioru Serwisu gwarancyjnego / usunięcia wady (wzór);
   7) Załącznik nr 5a – 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;
   8) Załącznik nr 5b – 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;
   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.
5. Umowę sporządzono w 4 jednobrzmiących egzemplarzach, w tym jeden dla Sprzedawcy i trzy dla Kupującego.

Sprzedawca **Kupujący**

....

Załącznik nr 1a do Umowy nr ____/DI/2019/2610 z dnia _____ 2019 r.

Specyfikacja Sprzętu IT i Oprogramowania oraz zasady Wdrożenia

Lp.	Sprzęt IT	Liczba	Parametry i wymagania minimalne	Oprogramowanie	Zasady Wdrożenia
1	Telefon IP	4 000 szt.	1. przełącznik port 10/100/1000 RJ-45 Ethernet 1 Gbps (IEEE 802.3) do podłączenia komputera; 2. port o prędkości portu 1 Gbps (IEEE 802.3) do sieci LAN; 3. wyświetlacz monochromatyczny LCD w 4bitowej skali szarości; 4. obsługujący min. 4 linie; 5. obsługiwane protokoły sygnalizacyjne: SCCP (Call Manager) / SIP; 6. gniazdo słuchawki nagłownej: RJ-9; 7. szerokopasmowe audio: obsługa kodeka G.722 zgodny z TIA 920, możliwość obsługi zestawu nagłownego i głośnika; 8. obsługiwane kodeki: G.711a, G.711u, G.729a, G.729ab, G.722 oraz kodeki kompresji audio iLBC; 9. głośnik: Full-duplex z funkcją korekcji szumów; 10. ilość klawiszy funkcyjnych min. 4; 11. obsługa QoS: DSCP oraz standardów 802.1.Q/p 12. fabrycznie zainstalowany certyfikat X.509v3, szyfrowanie AES-128, obsługa EAPOL pass-through 13. zgodność ze standardem PoE IEEE 802.3af (Class I); 14. posiada wsparcie producenta systemu CUCM min. dla wersji 12.5.	Webex – 10 szt.(licencji) Enhanced – 500 szt.(licencji) aktualizacja (upgrade): Cisco UCM 12.5 – licencja na klaster 2 serwerów;	1.dostarczenie Sprzętu IT (telefonów IP) do Lokalizacji Kupującego zgodnie z wykazem określonym w Załączniku nr 1b do Umowy. 2.uruchomienie Sprzętu IT (telefonów IP) i sprawdzenie poprawności działania - nie ma konieczności obecności w miejscu funkcjonowania telefonów IP i ich fizycznego podłączania. 3.przeprowadzenie migracji systemu Cisco Unified Call Manager do wersji 12.5, z obecnej platformy sprzętowej na nowe urządzenia dostarczone w ramach Umowy. 4.przeprowadzenie analizy istniejącego środowiska UC i przygotowanie szczegółowego planu migracji; 5.przeprowadzenie inwentaryzacji telefonów IP i wskazanie które z nich nie są lub nie będą wspierane przez producenta w najnowszej (na dzień migracji systemu) wersji oprogramowania Cisco CUCM; 6.migracja wyżej opisanego środowiska Unified Communication (wraz z zainstalowanymi aplikacjami firm trzecich wspomagających system CUCM). Skalowanie platformy powinno być zgodne z wytycznymi producenta zawartymi w dokumentacji technicznej; 7.przeprowadzenie migracji użytkowników i telefonów IP oraz skonfigurowanie nowych telefonów IP w CUCM. Nie ma konieczności obecności w miejscu funkcjonowania telefonów IP i ich fizycznego podłączania; 8.uaktualnienie Oprogramowania telefonów IP do najnowszego wspieranego przez producenta Device Pack'a dla wersji UCM z pkt. 4 powyżej; 9.przeprowadzenie migracji istniejącego środowiska UC na nowe serwery; 10. przeprowadzenie testów powdrożeniowych; 11. wykonanie Dokumentacji powykonawczej i uaktualnienie dokumentacji technicznej systemu CUCM.
2	Serwer	2 szt.	1. zasoby dyskowe na min. 24 dyskach 300GB 6Gb SAS 10K RPM SFF HDD/hot plug/drive sled mounted; 2. kontroler modularny min. 12Gbps SAS 1GB FBWC Cache module (Raid 0/1/5/6); 3. zdublowany zestaw wentylatorów w układzie chłodzącym serwera; 4. min. dwa zasilacze AC 230V hot swap; 5. min. dwa gniazda CPU; 6. min. dwa procesory CPU 2.6 GHz 6132/140W 14C/18MB Cache/DDR4 2666 MHz; 7. pamięć RAM – min. 192GB w formie układów 16GB DDR4-2666-MHz RDIMM/PC4-21300/single rank/x4/1.2v; 8. wirtualizacja systemu zunifikowanej komunikacji musi być wspierana przez producenta rozwiązania pod względem technicznym; 9. w celu integracji z inną infrastrukturą serwerową, platforma wirtualizacyjna serwerów komunikacyjnych powinna mieć możliwość zarządzania przez centralny system zarządzania środowiskiem zwirtualizowanym np. VMWare vCenter lub równoważny; 10. posiada wsparcie producenta systemu CUCM min. dla wersji 12.5.		

Aktualny stan infrastruktury Kupującego dla platformy Cisco Unified Communication:

Kupujący posiada system Cisco Unified Communication składający się z:

1) klastra 7 serwerów Cisco Unified Communication Manager w wersji 10.5.2 na 4 fizycznych maszynach;
2) serwera Cisco Unified Communciation Manager IM&P w wersji 10.5.2;
3) serwera Cisco Unity Connection w wersji 10.5.2;
4) serwera PLM;
5) dwóch serwerów Cisco UCCX w wersji 10.6.1 działających w układzie HA.

Aktualna ilość skonfigurowanych w systemie urządzeń (telefonów IP) wynosi 10 000.

System Unified Communication został zintegrowany z następującymi aplikacjami zewnętrznymi zainstalowanymi (wymagane zapewnienie ciągłości działania po aktualizacji):

1) Aspiria TiM,
2) TRX,
3) Intelix Billing Online,
4) Genesis Contact Center.

Kupujący posiada obecnie następujące licencje, które Sprzedawca przeniesie na migrowany system:

1) CUWL Professional - 100 szt.
2) Enhanced - 9248 szt.
3) Essential – 3 szt.
4) CUWL Professional Messaging - 100 szt.

Wszystkie aplikacje Unified Communication zainstalowane zostały w środowisku wirtualnym na 4 serwerach Cisco UCS C240 rozłożonych w 3 lokalizacjach. W środowisku Unified Communication wykorzystywane są następujące urządzenia końcowe firmy Cisco (stan obecny, który może ulec zmianie):
7910 – 6 szt., 7911 – 417 szt., 7912 – 3769 szt., 7940 – 184 szt., 7960 – 459 szt., 7962 – 341 szt., 6941 – 465 szt., 8811 – 3538 szt., 9951 – 108 szt., 7970 – 1 szt., 7961 – 1 szt., 7942 – 24 szt., 8865 – 46 szt., 8945 – 9 szt.

Styk do operatora zapewniają dwa redundantne łącza SIP Trunk zastawione za pomocą urządzeń Cisco CUBE.
System Cisco Unified Contact Center Express obsługuje obecnie zapowiedzi IVR dla 16 Oddziałów Regionalnych Kupującego oraz 2 drzewa IVR na potrzeby wewnętrznego oraz zewnętrznego helpdesk.
W systemie skonfigurowano 200 agentów korzystających rotacyjnie z portalu Cisco Finesse. Agenci korzystają ze wszystkich wyżej wymienionych typów urządzeń oraz z softphonów serwera Cisco Jabber.

Załącznik nr 1b do Umowy nr _____/DI/2019/2610 z dnia _____ 2019 r.

Wykaz Lokalizacji Kupującego

Symbol	Województwo	Powiat	Nazwa	Kod pocztowy	Miejscowość	Adres	Liczba Sprzętu IT (telefonów IP)
P001	dolnośląskie	bolesławiecki	Bolesławieckie Biuro Powiatowe ARiMR	59-700	Bolesławiec	ul. Komuny Paryskiej 38	5
P002	dolnośląskie	dzierżoniowski	Dzierżoniowskie Biuro Powiatowe ARiMR	58-200	Dzierżoniów	ul. Bat. Chłopskich 19	2
P003	dolnośląskie	głogowski	Głogowskie Biuro Powiatowe ARiMR	67-200	Głogów	ul. Sikorskiego 40	2
P004	dolnośląskie	górowski	Górowskie Biuro Powiatowe ARiMR	56-200	Góra	ul. Armii Polskiej 8	1
P005	dolnośląskie	jaworski	Jaworskie Biuro Powiatowe ARiMR	59-400	Jawor	ul. Starojaworska 91	5
P006	dolnośląskie	jeleniogórski	Jeleniogórskie Biuro Powiatowe ARiMR	58-500	Jelenia Góra	ul. Morcinka 33A	5
P007	dolnośląskie	kamiennogórski	Kamiennogórskie Biuro Powiatowe ARiMR	58-400	Kamienna Góra	ul. Papieża Jana Pawła II 11a	3
P008	dolnośląskie	kłodzki	Kłodzkie Biuro Powiatowe ARiMR	57-300	Kłodzko	ul. Grunwaldzka 2	7
P009	dolnośląskie	legnicki	Legnickie Biuro Powiatowe ARiMR	59-220	Legnica	ul. Bydgoska 18	6
P010	dolnośląskie	lubański	Lubańskie Biuro Powiatowe ARiMR	59-800	Lubań	ul. Karola Miarki 1	5
P011	dolnośląskie	lubiński	Lubińskie Biuro Powiatowe ARiMR	59-305	Rudna	ul. Ścinawska 19	7
P012	dolnośląskie	lwówecki	Lwóweckie Biuro Powiatowe ARiMR	59-620	Gryfów Śląski	Ubocze 300	4
P013	dolnośląskie	milicki	Milickie Biuro Powiatowe ARiMR	56-300	Milicz, Sławoszowice	ul. Kolejowa 28B	4
P014	dolnośląskie	oleśnicki	Oleśnickie Biuro Powiatowe ARiMR	56-500	Syców	ul. Ogrodowa 10	4
P015	dolnośląskie	oławski	Oławskie Biuro Powiatowe ARiMR	55-200	Oława	ul. Nowodojazdowa 9	1
P016	dolnośląskie	polkowicki	Polkowickie Biuro Powiatowe ARiMR	59-100	Polkowice	ul. Spółdzielcza 2	2
P017	dolnośląskie	strzeliński	Strzelińskie Biuro Powiatowe ARiMR	57-100	Strzelin	ul. Kamienna 10	4
P018	dolnośląskie	średzki	Średzkie Biuro Powiatowe ARiMR	55-300	Środa Śląska	ul. Wawrzyńca Korwina 2	3
P019	dolnośląskie	świdnicki	Świdnickie Biuro Powiatowe ARiMR	58-100	Świdnica	ul. Saperów 25B	5
P020	dolnośląskie	trzebnicki	Trzebnickie Biuro Powiatowe ARiMR	55-100	Trzebnica	ul. Milicka 23	7
P021	dolnośląskie	wałbrzyski	Wałbrzyskie Biuro Powiatowe ARiMR	58-300	Wałbrzych	ul. Uczniowska 21	3
P022	dolnośląskie	wołowski	Wołowskie Biuro Powiatowe ARiMR	56-100	Wołów	ul. Zaułek Zielony 20	2
P023	dolnośląskie	wrocławski	Wrocławskie Biuro Powiatowe ARiMR	50-452	Wrocław	ul. Komuny Paryskiej 72	11
P024	dolnośląskie	ząbkowicki	Ząbkowickie Biuro Powiatowe ARiMR	57-200	Ząbkowice Śląskie	ul. Staszica 18	6
P025	dolnośląskie	zgorzelecki	Zgorzeleckie Biuro Powiatowe ARiMR	59-900	Zgorzelec	ul. Bohaterów II AWP 8	3
P026	dolnośląskie	złotoryjski	Złotoryjskie Biuro Powiatowe ARiMR	59-524	Pielgrzymka	ul. Pielgrzymka 109A/1	1
OR01	**dolnośląskie**		Dolnośląski Oddział Regionalny ARiMR	52-438	Wrocław	ul. Giełdowa 8	31
P027	kujawsko-pomorskie	aleksandrowski	Aleksandrowskie Biuro Powiatowe ARiMR	87-700	Aleksandrów Kujawski	ul. Wyspiańskiego 4	8
P028	kujawsko-pomorskie	brodnicki	Brodnickie Biuro Powiatowe ARiMR	87-300	Brodnica	ul. Wczasowa 46	9
P029	kujawsko-pomorskie	bydgoski	Bydgoskie Biuro Powiatowe ARiMR	85-240	Bydgoszcz	ul. Kraszewskiego 1	8
P030	kujawsko-pomorskie	chełmiński	Chełmińskie Biuro Powiatowe ARiMR	86-212	Stolno	Grubno 56	5
P031	kujawsko-pomorskie	golubsko-dobrzyński	Golubsko-Dobrzyńskie Biuro Pow. ARiMR	87-400	Golub-Dobrzyń	ul. J.G. Koppa 1B	8
P032	kujawsko-pomorskie	grudziądzki	Grudziądzkie Biuro Powiatowe ARiMR	86-300	Grudziądz	ul. Piłsudskiego 51/53	6
P033	kujawsko-pomorskie	inowrocławski	Inowrocławskie Biuro Powiatowe ARiMR	88-100	Inowrocław	ul. Toruńska 25	8
P034	kujawsko-pomorskie	lipnowski	Lipnowskie Biuro Powiatowe ARiMR	87-630	Skępe	ul. Wymyślińska 2	8
P035	kujawsko-pomorskie	mogileński	Mogileńskie Biuro Powiatowe ARiMR	88-300	Mogilno	ul. Piłsudskiego 3	6
P036	kujawsko-pomorskie	nakielski	Nakielskie Biuro Powiatowe ARiMR	89-100	Nakło nad Notecią	ul. Strażacka 4	7
P037	kujawsko-pomorskie	radziejowski	Radziejowskie Biuro Powiatowe ARiMR	88-200	Radziejów	Przemystka 23	9
P038	kujawsko-pomorskie	rypiński	Rypińskie Biuro Powiatowe ARiMR	87-500	Rypin	ul. Nowy Rynek 5	8
P039	kujawsko-pomorskie	sępoleński	Sępoleńskie Biuro Powiatowe ARiMR	89-400	Sępólno Krajeńskie	ul. Przemysłowa 2	6
P040	kujawsko-pomorskie	świecki	Świeckie Biuro Powiatowe ARiMR	86-100	Świecie	ul. Witosa 5	9
P041	kujawsko-pomorskie	toruński	Toruńskie Biuro Powiatowe ARiMR	87-100	Toruń	ul. Rejtana 2-4	8
P042	kujawsko-pomorskie	tucholski	Tucholskie Biuro Powiatowe ARiMR	89-500	Tuchola	ul. Przemysłowa 1	8
P043	kujawsko-pomorskie	wąbrzeski	Wąbrzeskie Biuro Powiatowe ARiMR	87-200	Wąbrzeźno	ul. Wolności 27A	5
P044	kujawsko-pomorskie	włocławski	Włocławskie Biuro Powiatowe ARiMR	87-800	Włocławek	ul. Ogniowa 7 A	16
P045	kujawsko-pomorskie	żniński	Żnińskie Biuro Powiatowe ARiMR	88-400	Żnin	ul. 700-lecia 32	6

Symbol	Województwo	Powiat	Nazwa	Kod pocztowy	Miejscowość	Adres	Liczba Sprzętu IT (telefonów IP)
OR02	**kujawsko-pomorskie**		Kujawsko-Pomorski Oddział Regionalny	87-100	Toruń	ul. Dąbrowskiego 4	73
P046	lubelskie	bialski	Bialskie Biuro Powiatowe ARiMR	21-500	Biała Podlaska	ul. Piłsudskiego 38	53
P047	lubelskie	biłgorajski	Biłgorajskie Biuro Powiatowe ARiMR	23-400	Biłgoraj	ul. Gen. Bora Komorowskiego 3	39
P048	lubelskie	chełmski	Chełmskie Biuro Powiatowe ARiMR	22-100	Chełm	Pl. Niepodległości 1	36
P049	lubelskie	hrubieszowski	Hrubieszowskie Biuro Powiatowe ARiMR	22-500	Hrubieszów	ul. Nowa 16	23
P050	lubelskie	janowski	Janowskie Biuro Powiatowe ARiMR	23-300	Janów Lubelski	ul. Ulanowska 61	23
P051	lubelskie	krasnystawski	Krasnostawskie Biuro Powiatowe ARiMR	22-300	Krasnystaw	ul. Browarna 1	23
P052	lubelskie	kraśnicki	Kraśnickie Biuro Powiatowe ARiMR	23-210	Kraśnik	ul. Słowackiego 7	36
P053	lubelskie	lubartowski	Lubartowskie Biuro Powiatowe ARiMR	21-100	Lubartów	ul. 1 Maja 82	33
P054	lubelskie	lubelski	Lubelskie Biuro Powiatowe ARiMR	21-003	Elizówka	Elizówka 65C k/Lublina	7
P055	lubelskie	łęczyński	Łęczyńskie Biuro Powiatowe ARiMR	21-010	Łęczna	ul. Krasnystawska 54	12
P056	lubelskie	łukowski	Łukowskie Biuro Powiatowe ARiMR	21-400	Łuków	ul. Przemysłowa 15	37
P057	lubelskie	opolski	Opolskie Biuro Powiatowe ARiMR (	24-300	Opole Lubelskie	Al. 600-lecia 8	17
P058	lubelskie	parczewski	Parczewskie Biuro Powiatowe ARiMR	21-200	Parczew	ul. Nowa 35	13
P059	lubelskie	puławski	Puławskie Biuro Powiatowe ARiMR	24-100	Puławy	ul. Czartoryskich 8	24
P060	lubelskie	radzyński	Radzyńskie Biuro Powiatowe ARiMR	21-300	Radzyń Podlaski	ul. Chomiczewskiego 5	19
P061	lubelskie	rycki	Ryckie Biuro Powiatowe ARiMR	08-500	Ryki	ul. Wyczółkowskiego 10A	18
P062	lubelskie	świdnicki	Świdnickie Biuro Powiatowe ARiMR	21-050	Piaski	ul. Lubelska 80	11
P063	lubelskie	tomaszowski	Tomaszowskie Biuro Powiatowe ARiMR	22-600	Tomaszów Lubelski	ul. Ściegiennego 57	27
P064	lubelskie	włodawski	Włodawskie Biuro Powiatowe ARiMR	22-200	Włodawa	ul. Piłsudskiego 66	22
P065	lubelskie	zamojski	Zamojskie Biuro Powiatowe ARiMR	22-400	Zamość	ul. Szczebrzeska 71	53
OR03	**lubelskie**		Lubelski Oddział Regionalny ARiMR	21-003	Elizówka	Elizówka 65 k/Lublina	207
P066	lubuskie	gorzowski	Gorzowskie Biuro Powiatowe ARiMR	66-400	Gorzów Wlkp.	ul. Myśliborska 30A	2
P067	lubuskie	krośnieński	Krośnieńskie Biuro Powiatowe ARiMR	66-600	Krosno Odrzańskie	Pl. B. Prusa 4	1
P068	lubuskie	międzyrzecki	Międzyrzeckie Biuro Powiatowe ARiMR	66-300	Międzyrzecz	ul. Reymonta 5	1
P069	lubuskie	nowosolski	Nowosolskie Biuro Powiatowe ARiMR	67-120	Kożuchów	ul. Szprotawska 10	0
P070	lubuskie	słubicki	Słubickie Biuro Powiatowe ARiMR	69-100	Słubice	ul. Transportowa 8	0
P071	lubuskie	strzelecko-drezdenecki	Strzelecko-Drezdeneckie Biuro Pow.	66-500	Strzelce Krajeńskie	Al. Piastów 13	0
P072	lubuskie	sulęciński	Sulęcińskie Biuro Powiatowe ARiMR	69-200	Sulęcin	ul. Lipowa 18D	1
P073	lubuskie	świebodziński	Świebodzińskie Biuro Powiatowe ARiMR	66-200	Świebodzin	ul. Rynkowa 2	0
P074	lubuskie	wschowski	Wschowskie Biuro Powiatowe ARiMR	67-400	Wschowa	ul. Kazimierza Wielkiego 6	0
P075	lubuskie	zielonogórski	Zielonogórskie Biuro Powiatowe ARiMR	65-120	Zielona Góra	Al. Zjednoczenia 104	0
P076	lubuskie	żagański	Żagańskie Biuro Powiatowe ARiMR	67-300	Szprotawa	ul. Niepodległości 15	0
P077	lubuskie	żarski	Żarskie Biuro Powiatowe ARiMR	68-300	Lubsko	ul. XX-lecia 3B	2
OR04	**lubuskie**		Lubuski Oddział Regionalny ARiMR	65-120	Zielona Góra	Al. Zjednoczenia 104	11
P078	łódzkie	bełchatowski	Bełchatowskie Biuro Powiatowe ARiMR	97-400	Bełchatów	ul. 1 Maja 9	3
P079	łódzkie	brzeziński	Brzezińskie Biuro Powiatowe ARiMR	95-063	Rogów	ul. Wojska Polskiego 9	4
P080	łódzkie	kutnowski	Kutnowskie Biuro Powiatowe ARiMR	99-300	Kutno	ul. Łąkoszyńska 127	7
P081	łódzkie	łaski	Łaskie Biuro Powiatowe ARiMR	98-100	Łask	ul. Narutowicza 17	9
P082	łódzkie	łęczycki	Łęczyckie Biuro Powiatowe ARiMR	99-100	Łęczyca	ul. Zachodnia 8	8
P083	łódzkie	łowicki	Łowickie Biuro Powiatowe ARiMR	99-400	Łowicz	ul. Świętojańska 5/7	6
P084	łódzkie	łódzki wschodni	Łódzkie Wschodnie Biuro Powiat. ARiMR	95-040	Koluszki	ul. 11 Listopada 65	2
P085	łódzkie	opoczyński	Opoczyńskie Biuro Powiatowe ARiMR	26-300	Opoczno	ul. Piotrkowska 49	10
P086	łódzkie	pabianicki	Pabianickie Biuro Powiatowe ARiMR	95-200	Pabianice	ul. Zamkowa 6	6
P087	łódzkie	pajęczański	Pajęczańskie Biuro Powiatowe ARiMR	98-330	Pajęczno	ul. 17 Stycznia 15	5
P088	łódzkie	piotrkowski	Piotrkowskie Biuro Powiatowe ARiMR	97-300	Piotrków Trybunalski	ul. Kostromska 63	13
P089	łódzkie	poddębicki	Poddębickie Biuro Powiatowe ARiMR	99-200	Bałdrzychów	Bałdrzychów 80A	9
P090	łódzkie	radomszczański	Radomszczańskie Biuro Powiatowe	97-500	Radomsko	ul. Wyszyńskiego 142	2
P091	łódzkie	rawski	Rawskie Biuro Powiatowe ARiMR	96-200	Rawa Mazowiecka	ul. J. Sobieskiego 1	9
P092	łódzkie	sieradzki	Sieradzkie Biuro Powiatowe ARiMR	98-200	Sieradz	ul. Warneńczyka 1	15

Symbol	Województwo	Powiat	Nazwa	Kod pocztowy	Miejscowość	Adres	Liczba Sprzętu IT (telefonów IP)
P093	łódzkie	skierniewicki	Skierniewickie Biuro Powiatowe ARiMR	96-100	Skierniewice	ul. Lelewela 5	4
P094	łódzkie	tomaszowski	Tomaszowskie Biuro Powiatowe ARiMR	97-200	Tomaszów Mazowieck	ul. Spalska 103/105	5
P095	łódzkie	wieluński	Wieluńskie Biuro Powiatowe ARiMR	98-300	Wieluń	ul. Sieradzka 70	7
P096	łódzkie	wieruszowski	Wieruszowskie Biuro Powiatowe ARiMR	98-400	Wieruszów	ul. Kępińska 1	7
P097	łódzkie	zduńskowolski	Zduńskowolskie Biuro Powiatowe ARiMR	98-220	Zduńska Wola	Plac Wolności 20	4
P098	łódzkie	zgierski	Zgierskie Biuro Powiatowe ARiMR	95-070	Aleksandrów Łódzki	ul. Piotra Ściegiennego 4	3
OR05	**łódzkie**		Łódzki Oddział Regionalny ARiMR	92-202	Łódź	Al. Piłsudskiego nr 84	73
P099	małopolskie	bocheński	Bocheńskie Biuro Powiatowe ARiMR	32-700	Bochnia	ul. Windakiewicza 9/1	8
P100	małopolskie	brzeski	Brzeskie Biuro Powiatowe ARiMR	32-800	Brzesko	ul. Szczepanowska 23	6
P101	małopolskie	chrzanowski	Chrzanowskie Biuro Powiatowe ARiMR	32-500	Chrzanów	ul. Fabryczna 16	2
P102	małopolskie	dąbrowski	Dąbrowskie Biuro Powiatowe ARiMR	33-200	Dąbrowa Tarnowska	ul. J. Piłsudskiego 33	13
P103	małopolskie	gorlicki	Gorlickie Biuro Powiatowe ARiMR	38-300	Gorlice	ul. Wincentego Pola 2	12
P104	małopolskie	krakowski	Krakowskie Biuro Powiatowe ARiMR	31-481	Kraków	ul. Promienistych 1	0
P105	małopolskie	limanowski	Limanowskie Biuro Powiatowe ARiMR	34-600	Limanowa	ul. Piłsudskiego 6	8
P106	małopolskie	miechowski	Miechowskie Biuro Powiatowe ARiMR	32-200	Miechów	ul. M. Konopnickiej 23A	12
P107	małopolskie	myślenicki	Myślenickie Biuro Powiatowe ARiMR	32-400	Myślenice	ul. Słowackiego 100A	11
P108	małopolskie	nowosądecki	Nowosądeckie Biuro Powiatowe ARiMR	33-300	Nowy Sącz	Kraszewskiego 44	14
P109	małopolskie	nowotarski	Nowotarskie Biuro Powiatowe ARiMR	34-400	Nowy Targ	ul. Składowa 7	16
P110	małopolskie	olkuski	Olkuskie Biuro Powiatowe ARiMR	32-300	Olkusz	ul. Bylicy 1	10
P111	małopolskie	oświęcimski	Oświęcimskie Biuro Powiatowe ARiMR	32-602	Oświęcim	ul. Wyspiańskiego 10	6
P112	małopolskie	proszowicki	Proszowickie Biuro Powiatowe ARiMR	32-100	Proszowice	ul. Krakowska 32	10
P113	małopolskie	suski	Suskie Biuro Powiatowe ARiMR	34-200	Sucha Beskidzka	ul. Adama Mickiewicza 19	10
P114	małopolskie	tarnowski	Tarnowskie Biuro Powiatowe ARiMR	33-100	Tarnów	ul. Krakowska 134	19
P115	małopolskie	tatrzański	Tatrzańskie Biuro Powiatowe ARiMR	34-500	Zakopane	ul. Do Samków 29	8
P116	małopolskie	wadowicki	Wadowickie Biuro Powiatowe ARiMR	34-100	Wadowice	ul. Mickiewicza 36	8
P117	małopolskie	wielicki	Wielickie Biuro Powiatowe ARiMR	32-005	Niepołomice	ul. 3 Maja 2	4
OR06	**małopolskie**		Małopolski Oddział Regionalny ARiMR	31-481	Kraków	ul. Promienistych 1	81
P118	mazowieckie	białobrzeski	Białobrzeskie Biuro Powiatowe ARiMR	26-800	Białobrzegi	ul. Składowa 5	1
P119	mazowieckie	ciechanowski	Ciechanowskie Biuro Powiatowe ARiMR	06-400	Ciechanów	ul. 17 Stycznia 60	6
P120	mazowieckie	garwoliński	Garwolińskie Biuro Powiatowe ARiMR	08-400	Garwolin	Miętne, ul. Garwolińska 3	10
P121	mazowieckie	gostyniński	Gostynińskie Biuro Powiatowe ARiMR	09-500	Gostynin	ul. Dybanka 4	0
P122	mazowieckie	grodziski	Grodziskie Biuro Powiatowe ARiMR	05-825	Grodzisk Mazowiecki	ul. Cegielniana 1	7
P123	mazowieckie	grójecki	Grójeckie Biuro Powiatowe ARiMR	05-600	Grójec	ul. Sportowa 7	0
P124	mazowieckie	kozienicki	Kozienickie Biuro Powiatowe ARiMR	26-900	Kozienice	ul. Warszawska 72	3
P125	mazowieckie	legionowski	Legionowskie Biuro Powiatowe ARiMR	05-120	Legionowo	ul. Gen. Wł. Sikorskiego 11	0
P126	mazowieckie	lipski	Lipskie Biuro Powiatowe ARiMR	27-300	Lipsko	ul. Iłżecka 1	7
P127	mazowieckie	łosicki	Łosickie Biuro Powiatowe ARiMR	08-200	Łosice	ul. Narutowicza 6	4
P128	mazowieckie	makowski	Makowskie Biuro Powiatowe ARiMR	06-200	Maków Mazowiecki	Oś. Bazar 15	7
P129	mazowieckie	miński	Mińskie Biuro Powiatowe ARiMR	05-300	Mińsk Mazowiecki	ul. Konstytucji 3 Maja 12	6
P130	mazowieckie	mławski	Mławskie Biuro Powiatowe ARiMR	06-500	Mława	ul. Joachima Lelewela 4	3
P131	mazowieckie	nowodworski	Nowodworskie Biuro Powiatowe ARiMR	05-180	Pomiechówek	ul. Ogrodnicza 6	5
P132	mazowieckie	ostrołęcki	Ostrołęckie Biuro Powiatowe ARiMR	07-410	Ostrołęka	ul. Kościuszki 17	7
P133	mazowieckie	ostrowski	Ostrowskie Biuro Powiatowe ARiMR	07-300	Ostrów Mazowiecka	ul. Różańska 9	8
P134	mazowieckie	otwocki	Otwockie Biuro Powiatowe ARiMR	05-400	Otwock	ul. Legionów 2	6
P135	mazowieckie	piaseczyński	Piaseczyńskie Biuro Powiatowe ARiMR	05-530	Góra Kalwaria	ul. Rybie 8	2
P136	mazowieckie	płocki	Płockie Biuro Powiatowe ARiMR	09-407	Płock	al. Józefa Piłsudskiego 35	15
P137	mazowieckie	płoński	Płońskie Biuro Powiatowe ARiMR	09-100	Płońsk	ul. Sienkiewicza 11	6
P138	mazowieckie	pruszkowski	Pruszkowskie Biuro Powiatowe ARiMR	05-820	Piastów	ul. Harcerska 30	1
P139	mazowieckie	przasnyski	Przasnyskie Biuro Powiatowe ARiMR	06-300	Przasnysz	ul. Szpitalna 10A	4
P140	mazowieckie	przysuski	Przysuskie Biuro Powiatowe ARiMR	26-400	Przysucha	ul. Szkolna 7	2

Symbol	Województwo	Powiat	Nazwa	Kod pocztowy	Miejscowość	Adres	Liczba Sprzętu IT (telefonów IP)
P141	mazowieckie	pułtuski	Pułtuskie Biuro Powiatowe ARiMR	06-120	Winnica	Golądkowo 41J	2
P142	mazowieckie	radomski	Radomskie Biuro Powiatowe ARiMR	26-600	Radom	ul. Lubelska 65	3
P143	mazowieckie	siedlecki	Siedleckie Biuro Powiatowe ARiMR	08-110	Siedlce	ul. Warszawska 133	20
P144	mazowieckie	sierpecki	Sierpeckie Biuro Powiatowe ARiMR	09-200	Sierpc	ul. Kopernika 8	2
P145	mazowieckie	sochaczewski	Sochaczewskie Biuro Powiatowe ARiMR	96-500	Sochaczew	ul. Łąkowa 22	7
P146	mazowieckie	sokołowski	Sokołowskie Biuro Powiatowe ARiMR	08-300	Sokołów Podlaski	ul. Oleksiaka Wichury 3	3
P147	mazowieckie	szydłowiecki	Szydłowieckie Biuro Powiatowe ARiMR	26-500	Szydłowiec	ul. Wschodnia 68	1
P149	mazowieckie	warszawski	Warszawskie Zachodnie Biuro Pow.	05-082	Wojcieszyn	Wojcieszyn, ul. Trakt Królewski 91	4
P150	mazowieckie	węgrowski	Węgrowskie Biuro Powiatowe ARiMR	07-100	Węgrów	ul. Podlaska 1	7
P151	mazowieckie	wołomiński	Wołomińskie Biuro Powiatowe ARiMR	05-250	Radzymin	ul. Komunalna 2	4
P152	mazowieckie	wyszkowski	Wyszkowskie Biuro Powiatowe ARiMR	07-200	Wyszków	ul. I Armii Wojska Polskiego 54	8
P153	mazowieckie	zwoleński	Zwoleńskie Biuro Powiatowe ARiMR	26-700	Zwoleń	ul. Targowa 54	2
P154	mazowieckie	żuromiński	Żuromińskie Biuro Powiatowe ARiMR	09-310	Zielona	ul. 1 Maja 8D	3
P155	mazowieckie	żyrardowski	Żyrardowskie Biuro Powiatowe ARiMR	96-300	Żyrardów	ul. Piaskowa 21/23	3
OR07	**mazowieckie**		Mazowiecki Oddział Regionalny ARiMR	00-175	Warszawa	Al. Jana Pawła II nr 70	166
P156	opolskie	brzeski	Brzeskie Biuro Powiatowe ARiMR	49-340	Lewin Brzeski	ul. Moniuszki 14	3
P157	opolskie	głubczycki	Głubczyckie Biuro Powiatowe ARiMR	48-100	Głubczyce	ul. Powstańców 4	0
P158	opolskie	kędzierzyńsko-	Kędzierzyńsko-Kozielskie B. Pow. ARiMR	47-260	Polska Cerekiew	ul. Rynek 2	4
P159	opolskie	kluczborski	Kluczborskie Biuro Powiatowe ARiMR	46-200	Kluczbork	ul. Waryńskiego 7	4
P160	opolskie	krapkowicki	Krapkowickie Biuro Powiatowe ARiMR	47-303	Krapkowice	ul. Kilińskiego 1	2
P161	opolskie	namysłowski	Namysłowskie Biuro Powiatowe ARiMR	46-100	Namysłów	ul. J. Piłsudskiego 3	3
P162	opolskie	nyski	Nyskie Biuro Powiatowe ARiMR	48-300	Nysa	ul. Marcinkowskiego 2-4	13
P163	opolskie	oleski	Oleskie Biuro Powiatowe ARiMR	46-300	Olesno	ul. Powstańców Śląskich 14	8
P164	opolskie	opolski	Opolskie Biuro Powiatowe ARiMR	45-323	Opole	ul. Zielonogórska 3	5
P165	opolskie	prudnicki	Prudnickie Biuro Powiatowe ARiMR	48-210	Biała	ul. Kościuszki 24	1
P166	opolskie	strzelecki	Strzeleckie Biuro Powiatowe ARiMR	47-100	Strzelce Opolskie	ul. 1 Maja 59	7
OR08	**opolskie**		Opolski Oddział Regionalny ARiMR	45-836	Opole	ul. Wrocławska 170 G	49
P167	podkarpackie	bieszczadzki	Bieszczadzkie Biuro Powiatowe ARiMR	38-700	Ustrzyki Dolne	ul. Rynek 6	5
P168	podkarpackie	brzozowski	Brzozowskie Biuro Powiatowe ARiMR	36-200	Brzozów	ul. 3 Maja 1	4
P169	podkarpackie	dębicki	Dębickie Biuro Powiatowe ARiMR	39-200	Dębica	ul. Kolejowa 36	7
P170	podkarpackie	jarosławski	Jarosławskie Biuro Powiatowe ARiMR	37-500	Jarosław	ul. Grunwaldzka 7	12
P171	podkarpackie	jasielski	Jasielskie Biuro Powiatowe ARiMR	38-200	Jasło	ul. Słowackiego 6	7
P172	podkarpackie	kolbuszowski	Kolbuszowskie Biuro Powiatowe ARiMR	36-100	Kolbuszowa	ul. Towarowa 4	7
P173	podkarpackie	krośnieński	Krośnieńskie Biuro Powiatowe ARiMR	38-400	Krosno	ul. Żwirki i Wigury 9	5
P174	podkarpackie	leski	Leskie Biuro Powiatowe ARiMR	38-600	Lesko	ul. Moniuszki 6	7
P175	podkarpackie	leżajski	Leżajskie Biuro Powiatowe ARiMR	37-300	Leżajsk	ul. Mickiewicza 20	1
P176	podkarpackie	lubaczowski	Lubaczowskie Biuro Powiatowe ARiMR	37-600	Lubaczów	ul. Mazury 3	9
P177	podkarpackie	łańcucki	Łańcuckie Biuro Powiatowe ARiMR	37-100	Łańcut	ul. Traugutta 20	6
P178	podkarpackie	mielecki	Mieleckie Biuro Powiatowe ARiMR	39-300	Mielec	ul. Sienkiewicza 1	9
P179	podkarpackie	niżański	Niżańskie Biuro Powiatowe ARiMR	37-400	Nisko	ul. Rzeszowska 42	6
P180	podkarpackie	przemyski	Przemyskie Biuro Powiatowe ARiMR	37-700	Przemyśl	ul. Grunwaldzka 58	4
P181	podkarpackie	przeworski	Przeworskie Biuro Powiatowe ARiMR	37-200	Przeworsk	ul. Budowlanych 1	7
P182	podkarpackie	ropczycko-sędziszowski	Ropczycko-Sędziszowskie B. Pow. ARiMR	39-100	Ropczyce	ul. Barbary 4	5
P183	podkarpackie	rzeszowski	Rzeszowskie Biuro Powiatowe ARiMR	35-233	Rzeszów	ul. Lubelska 46	14
P184	podkarpackie	sanocki	Sanockie Biuro Powiatowe ARiMR	38-500	Sanok	ul. Mickiewicza 29	5
P185	podkarpackie	stalowowolski	Stalowowolskie Biuro Powiatowe ARiMR	37-450	Stalowa Wola	ul. Dmowskiego 10	4
P186	podkarpackie	strzyżowski	Strzyżowskie Biuro Powiatowe ARiMR	38-100	Strzyżów	ul. 1 Maja 38	6
P187	podkarpackie	tarnobrzeski	Tarnobrzeskie Biuro Powiatowe ARiMR	39-400	Tarnobrzeg	ul. 1 Maja 4A	8
OR09	**podkarpackie**		Podkarpacki Oddział Regionalny ARiMR	35-310	Rzeszów	Al. Tadeusza Rejtana 36	55
P188	podlaskie	augustowski	Augustowskie Biuro Powiatowe ARiMR	16-300	Augustów	ul. Przemysłowa 6	11

Symbol	Województwo	Powiat	Nazwa	Kod pocztowy	Miejscowość	Adres	Liczba Sprzętu IT (telefonów IP)
P189	podlaskie	białostocki	Białostockie Biuro Powiatowe ARiMR	15-427	Białystok	ul. Lipowa 32A	59
P190	podlaskie	bielski	Bielskie Biuro Powiatowe ARiMR	17-100	Bielsk Podlaski	ul. Białowieska 113D	15
P191	podlaskie	grajewski	Grajewskie Biuro Powiatowe ARiMR	19-203	Grajewo	ul. Fabryczna 4	15
P192	podlaskie	hajnowski	Hajnowskie Biuro Powiatowe ARiMR	17-200	Hajnówka	ul. J. Piłsudskiego 10	10
P193	podlaskie	kolneński	Kolneńskie Biuro Powiatowe ARiMR	18-500	Kolno	ul. 11 Listopada 1	10
P194	podlaskie	łomżyński	Łomżyńskie Biuro Powiatowe ARiMR	18-400	Łomża	ul. Nowa 2	2
P195	podlaskie	moniecki	Monieckie Biuro Powiatowe ARiMR	19-100	Mońki	ul. Białostocka 51	13
P196	podlaskie	sejneński	Sejneńskie Biuro Powiatowe ARiMR	16-500	Sejny	ul. Zawadzkiego 3	10
P197	podlaskie	siemiatycki	Siemiatyckie Biuro Powiatowe ARiMR	17-300	Siemiatycze	ul. Ks. Ściegiennego 1	10
P198	podlaskie	sokólski	Sokólskie Biuro Powiatowe ARiMR	16-100	Sokółka	ul. Piłsudskiego 8	18
P199	podlaskie	suwalski	Suwalskie Biuro Powiatowe ARiMR	16-400	Suwałki	ul. Sportowa 22	23
P200	podlaskie	wysokomazowiecki	Wysokomazowieckie Biuro Powiatowe	18-200	Wysokie Mazowieckie	ul. Ludowa 7	9
P201	podlaskie	zambrowski	Zambrowskie Biuro Powiatowe ARiMR	18-300	Zambrów	Al. Wojska Polskiego 27	13
OR10	**podlaskie**		Podlaski Oddział Regionalny ARiMR	18-400	Łomża	ul. Nowa 2	87
P202	pomorskie	bytowski	Bytowskie Biuro Powiatowe ARiMR	77-100	Bytów	ul. Miastecka 2	5
P203	pomorskie	chojnicki	Chojnickie Biuro Powiatowe ARiMR	89-604	Chojnice	ul. Kościerska 10	3
P204	pomorskie	człuchowski	Człuchowskie Biuro Powiatowe ARiMR	77-300	Człuchów	ul. Słowackiego 5	2
P205	pomorskie	gdański	Gdańskie Biuro Powiatowe ARiMR	83-000	Pruszcz Gdański	ul. Sikorskiego 2A	1
P206	pomorskie	kartuski	Kartuskie Biuro Powiatowe ARiMR	83-300	Kartuzy	ul. Kolejowa 15/17	6
P207	pomorskie	kościerski	Kościerskie Biuro Powiatowe ARiMR	83-400	Kościerzyna	ul. Przemysłowa 7B	4
P208	pomorskie	kwidzyński	Kwidzyńskie Biuro Powiatowe ARiMR	82-500	Kwidzyn	ul. Słowiańska 13A	3
P209	pomorskie	lęborski	Lęborskie Biuro Powiatowe ARiMR	84-300	Lębork	Plac Pokoju 9	2
P210	pomorskie	malborski	Malborskie Biuro Powiatowe ARiMR	82-220	Stare Pole	ul. Marynarki Wojennej 21	3
P211	pomorskie	nowodworski	Nowodworskie Biuro Powiatowe ARiMR	82-100	Nowy Dwór Gdański	ul. Kanałowa 2	0
P212	pomorskie	pucki	Puckie Biuro Powiatowe ARiMR	84-100	Puck	ul. Kolejowa 7	4
P213	pomorskie	słupski	Słupskie Biuro Powiatowe ARiMR	76-200	Słupsk	ul. Jana Pawła II 1	6
P214	pomorskie	starogardzki	Starogardzkie Biuro Powiatowe ARiMR	83-200	Starogard Gdański	ul. Kościuszki 18	3
P215	pomorskie	sztumski	Sztumskie Biuro Powiatowe ARiMR	82-400	Sztum	ul. Sienkiewicza 68	3
P216	pomorskie	tczewski	Tczewskie Biuro Powiatowe ARiMR	83-110	Tczew	ul. Kołłątaja 9	4
P217	pomorskie	wejherowski	Wejherowskie Biuro Powiatowe ARiMR	84-200	Wejherowo	ul. Sikorskiego 60	5
OR11	**pomorskie**		Pomorski Oddział Regionalny ARiMR	81-332	Gdynia	ul. Kołłątaja 1	85
P218	śląskie	będziński	Będzińskie Biuro Powiatowe ARiMR	42-500	Będzin	ul. Krasickiego 17	8
P219	śląskie	bielski	Bielskie Biuro Powiatowe ARiMR	43-300	Bielsko-Biała	ul. Gen. M. Boruty-Spiechowicza	5
P220	śląskie	bieruńsko-lędziński	Bieruńsko-Lędzińskie Biuro Powiat.	43-155	Bieruń	ul. Turystyczna 1	7
P221	śląskie	cieszyński	Cieszyńskie Biuro Powiatowe ARiMR	43-430	Skoczów	Międzyświeć, ul. Cieszyńska 85	4
P222	śląskie	częstochowski	Częstochowskie Biuro Powiatowe ARiMR	42-200	Częstochowa	ul. Tkacka 5	18
P223	śląskie	gliwicki	Gliwickie Biuro Powiatowe ARiMR	44-120	Pyskowice	ul. Kopernika 2	8
P224	śląskie	kłobucki	Kłobuckie Biuro Powiatowe ARiMR	42-100	Kłobuck	ul. Wojska Polskiego 2	16
P225	śląskie	lubliniecki	Lublinieckie Biuro Powiatowe ARiMR	42-700	Lubliniec	ul. Spokojna 2	7
P226	śląskie	mikołowski	Mikołowskie Biuro Powiatowe ARiMR	43-190	Mikołów	ul. Wyszyńskiego 13	5
P227	śląskie	myszkowski	Myszkowskie Biuro Powiatowe ARiMR	42-300	Myszków	ul. Pułaskiego 6	7
P228	śląskie	pszczyński	Pszczyńskie Biuro Powiatowe ARiMR	43-200	Pszczyna	ul. Szymanowskiego 23	8
P229	śląskie	raciborski	Raciborskie Biuro Powiatowe ARiMR	47-400	Racibórz	ul. Leśmiana 4	7
P230	śląskie	rybnicki	Rybnickie Biuro Powiatowe ARiMR	44-200	Rybnik	ul. Białych 7	3
P231	śląskie	tarnogórski	Tarnogórskie Biuro Powiatowe ARiMR	42-622	Nakło Śląskie	ul. G. Morcinka 9	10
P232	śląskie	wodzisławski	Wodzisławskie Biuro Powiatowe ARiMR	44-330	Jastrzębie Zdrój	ul. Czecha 8B	4
P233	śląskie	zawierciański	Zawierciańskie Biuro Powiatowe ARiMR	42-400	Zawiercie	ul. Obrońców Poczty Gdańskiej 95	8
P234	śląskie	żywiecki	Żywieckie Biuro Powiatowe ARiMR	34-300	Żywiec	ul. Ks. Pr. Stanisława Słonki 24	11
OR12	**śląskie**		Śląski Oddział Regionalny ARiMR	42-200	Częstochowa	ul. Sobieskiego 7	47
P235	świętokrzyskie	buski	Buskie Biuro Powiatowe ARiMR	28-100	Busko-Zdrój	Al. Mickiewicza 27	17

Symbol	Województwo	Powiat	Nazwa	Kod pocztowy	Miejscowość	Adres	Liczba Sprzętu IT (telefonów IP)
P236	świętokrzyskie	jędrzejowski	Jędrzejowskie Biuro Powiatowe ARiMR	28-300	Jędrzejów	ul. Reymonta 12	20
P237	świętokrzyskie	kazimierski	Kazimierskie Biuro Powiatowe ARiMR	28-500	Kazimierza Wielka	ul. 1-go Maja 14	14
P238	świętokrzyskie	kielecki	Kieleckie Biuro Powiatowe ARiMR	25-565	Kielce	ul. Magazynowa 4	36
P239	świętokrzyskie	konecki	Koneckie Biuro Powiatowe ARiMR	26-200	Końskie	ul. Staszica 2	6
P240	świętokrzyskie	opatowski	Opatowskie Biuro Powiatowe ARiMR	27-500	Opatów	ul. Sempołowskiej 3	14
P241	świętokrzyskie	ostrowiecki	Ostrowieckie Biuro Powiatowe ARiMR	27-400	Ostrowiec Świętokrzys	ul. Focha 12	9
P242	świętokrzyskie	pińczowski	Pińczowskie Biuro Powiatowe ARiMR	28-400	Pińczów	ul. Batalionów Chłopskich 3	12
P243	świętokrzyskie	sandomierski	Sandomierskie Biuro Powiatowe ARiMR	27-600	Sandomierz	ul. Mokoszyńska 8	17
P244	świętokrzyskie	skarżyski	Skarżyskie Biuro Powiatowe ARiMR	26-110	Skarżysko Kamienna	ul. Żeromskiego 48	3
P245	świętokrzyskie	starachowicki	Starachowickie Biuro Powiatowe ARiMR	27-200	Starachowice	ul. Kościelna 30	13
P246	świętokrzyskie	staszowski	Staszowskie Biuro Powiatowe ARiMR	28-200	Staszów	ul. Towarowa 30	15
P247	świętokrzyskie	włoszczowski	Włoszczowskie Biuro Powiatowe ARiMR	29-100	Włoszczowa	ul. Wiśniowa 23	10
OR13	**świętokrzyskie**		Świętokrzyski Oddział Regionalny ARiMR	25-414	Kielce	ul. Warszawska 430	78
P248	warmińsko-mazurskie	bartoszycki	Bartoszyckie Biuro Powiatowe ARiMR	11-200	Bartoszyce	ul. Kętrzyńska 43	13
P249	warmińsko-mazurskie	braniewski	Braniewskie Biuro Powiatowe ARiMR	14-500	Braniewo	ul. Bł. Reginy Protman 2	10
P250	warmińsko-mazurskie	działdowski	Działdowskie Biuro Powiatowe ARiMR	13-200	Działdowo	ul. Gen. Hallera 28A	11
P251	warmińsko-mazurskie	elbląski	Elbląskie Biuro Powiatowe ARiMR	82-300	Elbląg	ul. Grunwaldzka 2	15
P252	warmińsko-mazurskie	ełcki	Ełckie Biuro Powiatowe ARiMR	19-300	Ełk	ul. Toruńska 6 A	14
P253	warmińsko-mazurskie	giżycki	Giżyckie Biuro Powiatowe ARiMR	11-500	Giżycko	Pl. Grunwaldzki 9	11
P254	warmińsko-mazurskie	gołdapski	Gołdapskie Biuro Powiatowe ARiMR	19-500	Gołdap	ul. Konstytucji 3 Maja 3	12
P255	warmińsko-mazurskie	iławski	Iławskie Biuro Powiatowe ARiMR	14-200	Iława	ul. Lubawska 3	17
P256	warmińsko-mazurskie	kętrzyński	Kętrzyńskie Biuro Powiatowe ARiMR	11-400	Kętrzyn	ul. Mazurska 18	14
P257	warmińsko-mazurskie	lidzbarski	Lidzbarskie Biuro Powiatowe ARiMR	11-100	Lidzbark Warmiński	ul. Bartoszycka 9	13
P258	warmińsko-mazurskie	mrągowski	Mrągowskie Biuro Powiatowe ARiMR	11-700	Mrągowo	ul. Lubelska 5	9
P259	warmińsko-mazurskie	nidzicki	Nidzickie Biuro Powiatowe ARiMR	13-100	Nidzica	ul. Traugutta 4	13
P260	warmińsko-mazurskie	nowomiejski	Nowomiejskie Biuro Powiatowe ARiMR	13-300	Nowe Miasto	ul. Działyńskich 1B	13
P261	warmińsko-mazurskie	olecki	Oleckie Biuro Powiatowe ARiMR	19-400	Olecko	ul. Gołdapska 23	14
P262	warmińsko-mazurskie	olsztyński	Olsztyńskie Biuro Powiatowe ARiMR	10-417	Olsztyn	Towarowa 20	0
P263	warmińsko-mazurskie	ostródzki	Ostródzkie Biuro Powiatowe ARiMR	14-100	Ostróda	ul. Grunwaldzka 43a	14
P264	warmińsko-mazurskie	piski	Piskie Biuro Powiatowe ARiMR	12-200	Pisz	ul. 1 Maja 4C	13
P265	warmińsko-mazurskie	szczycieński	Szczycieńskie Biuro Powiatowe ARiMR	12-100	Szczytno	ul. Lipperta 10	9
P266	warmińsko-mazurskie	węgorzewski	Węgorzewskie Biuro Powiatowe ARiMR	11-600	Węgorzewo	ul. Jaracza 1	11
OR14	**warmińsko-mazurskie**		Warmińsko-Mazurski Oddział Reg. ARiMR	10-038	Olsztyn	ul. Św. Wojciecha 2	54
P267	wielkopolskie	chodzieski	Chodzieskie Biuro Powiatowe ARiMR	64-830	Margonin	ul. Kościelna 17	4
P268	wielkopolskie	czarnkowsko-trzcianeck	Czarnkowsko-Trzcianeckie B. Pow.	64-700	Czarnków	ul. Kościuszki 88	11
P269	wielkopolskie	gnieźnieński	Gnieźnieńskie Biuro Powiatowe ARiMR	62-200	Gniezno	ul. Roosevelta 114	12
P270	wielkopolskie	gostyński	Gostyńskie Biuro Powiatowe ARiMR	63-800	Gostyń	ul. Wrocławska 140A	15
P271	wielkopolskie	grodziski	Grodziskie Biuro Powiatowe ARiMR	62-065	Grodzisk Wlkp.	ul. Przemysłowa 12	9
P272	wielkopolskie	jarociński	Jarocińskie Biuro Powiatowe ARiMR	63-200	Jarocin	ul. St. Moniuszki 29A	11
P273	wielkopolskie	kaliski	Kaliskie Biuro Powiatowe ARiMR	62-800	Kalisz	ul. Zacisze 2	24
P274	wielkopolskie	kępiński	Kępińskie Biuro Powiatowe ARiMR	63-600	Kępno	ul. Przemysłowa 1A	9
P275	wielkopolskie	kolski	Kolskie Biuro Powiatowe ARiMR	62-600	Koło	ul. Bolesława Prusa 8	23
P276	wielkopolskie	koniński	Konińskie Biuro Powiatowe ARiMR	62-510	Konin	ul. Hurtowa 1	34
P277	wielkopolskie	kościański	Kościańskie Biuro Powiatowe ARiMR	64-000	Kościan	ul. Bernardyńska 2	9
P278	wielkopolskie	krotoszyński	Krotoszyńskie Biuro Powiatowe ARiMR	63-700	Krotoszyn	ul. Fabryczna 4B	12
P279	wielkopolskie	leszczyński	Leszczyńskie Biuro Powiatowe ARiMR	64-100	Leszno	ul. Kurpińskiego 6	11
P280	wielkopolskie	międzychodzki	Międzychodzkie Biuro Powiatowe ARiMR	64-400	Międzychód	ul. Sikorskiego 22A	3
P281	wielkopolskie	nowotomyski	Nowotomyskie Biuro Powiatowe ARiMR	64-300	Nowy Tomyśl	ul. Emilii Sczanieckiej 2	8
P282	wielkopolskie	obornicki	Obornickie Biuro Powiatowe ARiMR	64-610	Rogoźno	ul. Boguniewska 38	8
P283	wielkopolskie	ostrowski	Ostrowskie Biuro Powiatowe ARiMR	63-400	Ostrów Wlkp.	ul. Staroprzygodzka 117	14

Symbol	Województwo	Powiat	Nazwa	Kod pocztowy	Miejscowość	Adres	Liczba Sprzętu IT (telefonów IP)
P284	wielkopolskie	ostrzeszowski	Ostrzeszowskie Biuro Powiatowe ARiMR	63-500	Ostrzeszów	ul. Kościuszki 25	10
P285	wielkopolskie	pilski	Pilskie Biuro Powiatowe ARiMR	64-920	Piła	ul. Wojska Polskiego 49B	11
P286	wielkopolskie	pleszewski	Pleszewskie Biuro Powiatowe ARiMR	63-300	Pleszew	ul. Ogrodowa 13	12
P287	wielkopolskie	poznański	Poznańskie Biuro Powiatowe ARiMR	60-479	Poznań	ul. Strzeszyńska 29	18
P288	wielkopolskie	rawicki	Rawickie Biuro Powiatowe ARiMR	63-910	Miejska Górka	ul. Paderewskiego 20	11
P289	wielkopolskie	słupecki	Słupeckie Biuro Powiatowe ARiMR	62-400	Słupca	Al. Tysiąclecia 60	16
P290	wielkopolskie	szamotulski	Szamotulskie Biuro Powiatowe ARiMR	64-500	Szamotuły	ul. B. Chrobrego 8A	10
P291	wielkopolskie	średzki	Średzkie Biuro Powiatowe ARiMR	63-000	Środa Wlkp.	ul. Kilińskiego 1	6
P292	wielkopolskie	śremski	Śremskie Biuro Powiatowe ARiMR	63-100	Śrem	ul. Gostyńska 1	7
P293	wielkopolskie	turecki	Tureckie Biuro Powiatowe ARiMR	62-700	Turek	ul. Komunalna 2	15
P294	wielkopolskie	wągrowiecki	Wągrowieckie Biuro Powiatowe ARiMR	62-100	Wągrowiec	ul. Grunwaldzka 30	13
P295	wielkopolskie	wolsztyński	Wolsztyńskie Biuro Powiatowe ARiMR	64-200	Wolsztyn	ul. Przemysłowa 7	13
P296	wielkopolskie	wrzesiński	Wrzesińskie Biuro Powiatowe ARiMR	62-300	Września	ul. Sikorskiego 34	7
P297	wielkopolskie	złotowski	Złotowskie Biuro Powiatowe ARiMR	77-400	Złotów	ul. 8 Marca 5	7
OR15	**wielkopolskie**		Wielkopolski Oddział Regionalny ARiMR	60-479	Poznań	ul. Strzeszyńska 36	23
P298	zachodniopomorskie	białogardzki	Białogardzkie Biuro Powiatowe ARiMR	78-200	Białogard	ul. Królowej Jadwigi 9	4
P299	zachodniopomorskie	choszczeński	Choszczeńskie Biuro Powiatowe ARiMR	73-201	Choszczno	ul. Dąbrowszczaków 29	3
P300	zachodniopomorskie	drawski	Drawskie Biuro Powiatowe ARiMR	78-520	Złocieniec	ul. Drawska 13	4
P301	zachodniopomorskie	goleniowski	Goleniowskie Biuro Powiatowe ARiMR	72-200	Nowogard	ul. Batalionów Chłopskich 3	8
P302	zachodniopomorskie	gryficki	Gryfickie Biuro Powiatowe ARiMR	72-300	Gryfice	Ościęcin 1	3
P303	zachodniopomorskie	gryfiński	Gryfińskie Biuro Powiatowe ARiMR	74-110	Banie	ul. Targowa 19	4
P304	zachodniopomorskie	kamieński	Kamieńskie Biuro Powiatowe ARiMR	72-410	Golczewo	ul. Witosa 9	2
P305	zachodniopomorskie	kołobrzeski	Kołobrzeskie Biuro Powiatowe ARiMR	78-123	Siemyśl	ul. Kołobrzeska 14	5
P306	zachodniopomorskie	koszaliński	Koszalińskie Biuro Powiatowe ARiMR	75-845	Koszalin	ul. Słowiańska 15A	7
P307	zachodniopomorskie	łobeski	Łobeskie Biuro Powiatowe ARiMR	73-150	Łobez	Pl. Spółdzielców 2	6
P308	zachodniopomorskie	myśliborski	Myśliborskie Biuro Powiatowe ARiMR	74-400	Dębno	ul. Baczewskiego 22	5
P309	zachodniopomorskie	policki	Policki Biuro Powiatowe ARiMR	71-005	Szczecin	ul. Husarów 4A	7
P310	zachodniopomorskie	pyrzycki	Pyrzyckie Biuro Powiatowe ARiMR	74-200	Pyrzyce	ul. 1 Maja 7	5
P311	zachodniopomorskie	sławieński	Sławieńskie Biuro Powiatowe ARiMR	76-150	Darłowo	ul. Powstańców Warszawskich 17	3
P312	zachodniopomorskie	stargardzki	Stargardzkie Biuro Powiatowe ARiMR	73-110	Stargard	ul. Bogusława IV 10	6
P313	zachodniopomorskie	szczecinecki	Szczecineckie Biuro Powiatowe ARiMR	78-400	Szczecinek	ul. Limanowskiego 8	8
P314	zachodniopomorskie	świdwiński	Świdwińskie Biuro Powiatowe ARiMR	78-300	Świdwin	ul. Katowicka 1	5
P315	zachodniopomorskie	wałecki	Wałeckie Biuro Powiatowe ARiMR	78-650	Mirosławiec	ul. Kościuszki 16	2
OR16	**zachodniopomorskie**		Zachodniopomorski Oddział Regionalny	71-245	Szczecin	ul. Szafera 10	51
Central	**Centrala**		Centrala ARiMR	02-822	Warszawa	ul. Poleczki 33	78
						Razem:	4 000 szt.

Załącznik nr 2a do Umowy nr _____/DI/2019/2610 z dnia _____ 2019 r.

Protokół odbioru Sprzętu IT w Lokalizacjach
(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 dostarczył Sprzęt IT/Oprogramowanie z Umową:

Lp.	*Nazwa Sprzętu IT*	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 jest fabrycznie nowy i nie nosi śladów uszkodzeń zewnętrznych oraz uprzedniego używania. Liczba oraz rodzaj dostarczonego Sprzętu IT 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 dostarczono wszystkie wymagane Dokumenty (instrukcje eksploatacyjne, instrukcje obsługi Sprzętu IT).
4. Dokonano usunięcia i utylizacji wszelkich opakowań pozostałych po rozpakowaniu Sprzętu IT.
5. Numery seryjne Sprzętu IT zostały przekazane Kupującemu w wersji elektronicznej – MS Excel.

Uwagi i zastrzeżenia:

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

....., dnia ..... 2019 roku

* - niepotrzebne skreślić

Załącznik nr 2b do Umowy nr _____/DI/2019/2610 z dnia _____ 2019 r.

Protokół odbioru końcowego Sprzętu IT / 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 dostarczył Sprzęt IT/Oprogramowanie i wykonał Wdrożenie zgodnie z Umową:

Lp.	*Nazwa Sprzętu IT / Oprogramowania*	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 używania. 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 dostarczono 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

* - niepotrzebne skreślić

Załącznik nr 3 do Umowy nr _____/DI/2019/2610 z dnia _____ 2019 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 4 do Umowy nr _____/DI/2019/2610 z dnia _____ 2019 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

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

* - niepotrzebne skreślić.

Załącznik nr 5a do Umowy nr _____/DI/2019/2610 z dnia _____ 2019 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 ____ _____ 2019 r. w siedzibie Agencji Restrukturyzacji i Modernizacji Rolnictwa w Warszawie, ul. Poleczki 33 zapoznał 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 i zobowiązuje się do przestrzegania ich postanowień podczas realizacji Umowy.

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

Warszawa., dn. . . . . .2019 r.

Załącznik nr 5b do Umowy nr _____/DI/2019/2610 z dnia _____ 2019 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

Załącznik nr 6a do umowy nr _____/DI/2019/2610 z dnia _____.2019 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 udzieli 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/2019/2610 z dnia _____.2019 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 ....., Wydział .....Gospodarczy 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 RODO[1] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu zawarcia oraz wykonania Umowy[2].

(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/2019/2610 z dnia _____ 2019 r.

Formularz ofertowy

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.

REGULAMIN BEZPIECZEŃSTWA FIZYCZNEGO I ŚRODOWISKOWEGO

Spis treści:

§ 1.

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.

§ 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),
   4) odnotowane w przeszłości czyny przestępcze (rodzaj i typ czynu przestępczego, działania zewnętrzne, wewnętrzne, data, rozmiary, wartość szkody, wynik śledztwa),

5) aktualny stan bezpieczeństwa obiektu,
6) opis i ocenę funkcjonalności i poprawności zainstalowanych 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 odpowiedniości (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 takie, których ściany zewnętrzne i stropy budynków, w których zlokalizowane są strefy bezpieczeństwa, posiadają klasę odporności włamaniowej równoważnej murowi o grubości 25 cm wykonanemu z pełnej cegły. Natomiast pomieszczenia stref bezpieczeństwa powinny mieć ściany o odporności włamaniowej równoważnej murowi o grubości 12,5 cm. Zasady organizacji strefy bezpieczeństwa kancelarii niejawnej 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 ogniową 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 firmy monitorującej, klucze muszą być zdawane wyznaczonemu pracownikowi Agencji w celu zabezpieczenia ich w zaplombowanej kasetce, a następnego dnia roboczego pracownik ten zobowiązany jest wydać klucze upoważnionym pracownikom. Dopuszcza się, w biurach powiatowych Agencji, trwałe wydanie kluczy zewnętrznych 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 wewnątrz 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 przejście, które pełnią także role identyfikatorów.

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 zgodne 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 przejście,
   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:

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. Pobyt 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 bezpiecznych, 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, niepokoje społeczne i inne formy naturalnych lub spowodowanych przez działania umyślne bądź błędy człowieka katastrof. Ponadto analizie jest poddawany wpływ sąsiedztwa 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 instrukcje 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 któreś 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 doraźnej lub zamiennej, plan dojścia do rozwiązania docelowego.

7. Parametry środowiska, w którym pracuje sprzęt systemu teleinformatycznego zaliczany do zasobów kluczowych, tj. temperatura, jest monitorowana w celu natychmiastowego wykrycia odchyleń, 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 ppoż., w samoczynnie załączające się oświetlenie awaryjne (bezpieczeństwa i ewakuacyjne).
9. Oświetlenie bezpieczeństwa stosowane jest w pomieszczeniach, w których nawet krótkotrwałe 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 umożliwiające szybkie usunięcie wody (cieczy).
4. Przy ocenie sprawności instalacji wodno – kanalizacyjnej i grzewczej należy uwzględnić jej współdziałanie z innymi systemami wspomagającymi, takimi jak system klimatyzacyjno - 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 (SSWiN) 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,

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 (grupę 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, tąpnięcie, kolizja drogowa 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 (fileserver).
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 technologicznym 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 zabezpieczeń 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, kłódki, zamki, zasuwy 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 odkształceń 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 opiłków, śladów tynku, rysach na elementach zabezpieczeń, itp.,
      d) sprawdzić stan powłok lakierniczych i zabezpieczeń antykorozyjnych elementów narażonych na bezpośrednie działanie czynników atmosferycznych lub innych szkodliwych czynników dla mechanizmów kłódek, zamków, rygli (szczególnie kurz, pył),

2) w przypadku kłódek i zamków - sprawdzenie działania kluczy zapasowych oraz mechanizmu ryglującego przez otwarcie i zamknięcie kłódek i zamków, przegród 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 narażonych na bezpośrednie działanie czynników atmosferycznych lub innych szkodliwych czynników dla mechanizmów.

6. Wycofane 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 określany jako „zakup z półki".

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. Wycofanie 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, śluzy, ściany, stropy, ogrodzenia (wykonane 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,

   3) sprawdzenie występowania śladów po próbach penetracji lub usunięcia zabezpieczenia np. w postaci opiłków, śladów tynku, rysach na elementach zabezpieczeń, rdzy, itp.,
   4) sprawdzenie mechanizmów ryglowych (zamków, rygli, 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 narażonych 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 wchodzą: trakty kablowe (listwy PCV, szyny, rury, przepusty), osłony włazów i studzienek, szafy dystrybucyjne, tablice, krosownice.

2. Systemy okablowania znajdujące się w obszarze dostępnym publicznie podlegają przeglądom 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. narażonych na uszkodzenia mechaniczne spowodowane przez przenoszenie przedmiotów o dużych gabarytach (biurko, szafa), ruch osobowy,
   2) stanu powłoki lakierniczej, śladów korozji elementów narażonych 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 opiłków, śladów tynku, rysach na elementach zabezpieczeń, itp.

6. Przeglądy prowadzone lub nadzorowane przez Administratora Systemu powinny obejmować sprawdzenie:

1) przestrzegania zasad ochrony okablowania oraz punktów połączeń okablowania (inspekcja pod kątem podłączonych nieautoryzowanych urządzeń przechwytujących, rejestrujących, transmitujących 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 podczerwienią 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 strefowych poprzez załączanie i rozłączanie systemu wprowadzając odpowiedni kod,
   4) ilości i rozmieszczenia klawiatur strefowych 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 (uchwytów, ścian); szczególnie dotyczy to stref ogólnego i ograniczonego dostępu oraz znajdujących się poza pomieszczeniami Agencji (płaszczyzna 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 czytnikami działającymi jednostronnie, w tym działania przycisków ewakuacyjnych w przypadku, gdy SKD nie współpracuje z systemem ppoż.,

   3) działania czytników systemu z odpowiednią kartą dostępu,
   4) mocowania czytników, samozamykaczy, zamków elektromagnetycznych drzwi i przejść, w tym istnienia śladów prób penetracji (rysy, wgniecenia, próby podważania, demontażu),
   5) ilości i rozmieszczenia czytników 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 przeszłym.
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 „pozostawaniem" obrazu na ekranie po odłączeniu źródła sygnału),
   3) sprawdzenie jakości zarejestrowanego obrazu z kamer rejestrujących punkty newralgiczne (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 przeciwśnieżne, jeśli zostały zainstalowane),
   7) sprawdzenie działania głowic obrotowych i funkcji „zoom" (optyczny i elektroniczny),
   8) sprawdzenie mocowania reflektorów podczerwieni i oświetlenia sztucznego związanego z CCTV (np. halogeny włączane automatycznie – z czasowym wyłącznikiem).

§ 14.

Systemy wspomagające oświetlenie

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 uziemienia,
   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/wyłączania, lub
   2) przed zapełnieniem pamięci systemu powodującej nadpisywanie danych (wg danych w dokumentacji techniczno-eksploatacyjnej systemu),

   nie rzadziej jednak niż raz 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.

Załącznik nr 1 do Regulaminu bezpieczeństwa fizycznego i środowiskowego – Wzór rejestru wejścia/wyjścia do strefy bezpieczeństwa

Rejestr osób przebywających w strefie bezpieczeństwa BP…./OR….

Lp.	Imię i nazwisko osoby otwierającej	Imię i nazwisko osoby wchodzącej	Data i godzina wejścia	Data i godzina wyjścia	Cel wejścia

Załącznik nr 2 do Regulaminu bezpieczeństwa fizycznego i środowiskowego – Wzór rejestru wejścia/wyjścia gości do strefy administracyjnej

Rejestr gości przebywających w strefie Administracyjnej Centrali/BP…./OR….

Lp.	Czas wejścia	Imię i nazwisko gościa	Rodzaj dokumentu tożsamości	Nr dokumentu tożsamości	Imię i nazwisko osoby wizytowanej	Nr identyfikatora	Czas wyjścia

REGULAMIN EKSPLOATACJI SYSTEMÓW TELEINFORMATYCZNYCH

Spis treści:

§ 1.

Definicje

Użyte w regulaminie określenia oznaczają:

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

18) przywilej – specjalne uprawnienie posiadające wyższe od podstawowych prawa dostępu w systemie lub aplikacji, dostępne jedynie dla wybranych pracowników, w szczególności uprawnienie administracyjne.

Rozdział 1.
Podstawowe zasady eksploatacji systemów teleinformatycznych

§ 2.

Podział obowiązków w eksploatacji

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

§ 3.

Monitorowanie pojemności i wydajności systemów

1. Administrator Systemu jest odpowiedzialny za prognozowanie wymagań dotyczących pojemności oraz wydajności kluczowych elementów systemów teleinformatycznych w celu ograniczenia ryzyka przeciążenia systemu.
2. Wymagania dotyczące pojemności nowych systemów, wynikające z rzeczywistych potrzeb Agencji, są definiowane i zatwierdzane przed dokonaniem zakupu, zaakceptowaniem i wdrożeniem tych systemów, zgodnie z Regulaminem rozwoju aplikacji, stanowiącym załącznik nr 11 do Polityki.
3. Administrator Systemu prowadzi monitorowanie eksploatowanych systemów teleinformatycznych, przez gromadzenie informacji dotyczących krytycznych elementów i parametrów systemów:
    1) infrastruktury sieciowej, w zakresie przepustowości i obciążenia łączy (interfejsów) oraz procesorów urządzeń sieciowych,

2) serwerów usług wewnętrznych Agencji (serwery plików, wydruków, faksów, itp.), w zakresie obciążenia procesora, zajętości pamięci dyskowej, przyrostu danych w okresie miesiąca,

3) serwerów aplikacyjnych i baz danych, w zakresie obciążenia procesora, zajętości pamięci dyskowej, przyrostu danych w okresie miesiąca.

4. Raz w roku oraz po wprowadzeniu istotnej zmiany do systemu Administrator Systemu przekazuje Komitetowi informację z monitorowania pojemności i wydajności systemów.

5. W sytuacji, w której analiza pojemności lub wydajności systemów wykazuje wzrost ryzyka niespełnienia celów statutowych Agencji, Administrator Systemu niezwłocznie przekazuje te informacje Przewodniczącemu Komitetu oraz dyrektorowi komórki właściwej ds. bezpieczeństwa informacji.

§ 4.

Ochrona przed szkodliwym oprogramowaniem

1. Stacje robocze i serwery w Agencji są objęte ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory (firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie teleinformatycznym Agencji.

2. Użytkowane poza systemem Agencji wymienne nośniki komputerowe, przed rozpoczęciem pracy z tymi nośnikami w systemach teleinformatycznych Agencji, są sprawdzane za pomocą aktualnego oprogramowania antywirusowego.

3. W systemach Agencji wdrożono scentralizowany system antywirusowy.

4. Aktualizacja baz wirusów odbywa się automatycznie, przynajmniej raz dziennie.

5. Po każdej naprawie i konserwacji urządzenia a przed ponownym włączeniem do systemu teleinformatycznego Agencji zawartość stałych nośników komputerowych jest sprawdzana za pomocą aktualnego oprogramowania antywirusowego zawierającego najnowsze bazy antywirusowe.

6. W przypadku, gdy stacje robocze oraz serwery nie są objęte ochroną w czasie rzeczywistym Administrator Systemu, co najmniej raz w tygodniu dokonuje rutynowej kontroli pod kątem obecności złośliwego oprogramowania, przy czym kontrola może być realizowana w sposób:

   1) automatyczny, zgodnie z harmonogramem zdefiniowanym w scentralizowanym systemie zarządzającym,
   2) automatyczny, zgodnie z harmonogramem zdefiniowanym w każdym systemie teleinformatycznym osobno,
   3) ręczny na żądanie, centralnie lub w każdym systemie teleinformatycznym osobno.

7. Działania Administratora Systemu są dokumentowane stosownymi zapisami w Dzienniku pracy systemu, którego wzór zamieszczono w załączniku nr 3 do niniejszego Regulaminu.

§ 5.

Kontrola licencjonowanego oprogramowania

1. Dla wszystkich systemów i aplikacji użytkowanych w Agencji Administrator Systemu prowadzi spisy licencjonowanego oprogramowania zawierające:

   1) nośniki instalacyjne (i ich kopie, przechowywane w innej lokalizacji),
   2) licencje wraz z okresami ich ważności,
   3) kopie dowodów zakupu licencji,
   4) miejsce zainstalowania,
   5) dane dotyczące użytkownika/Właściciela Procesu/Właściciela Zasobu.

2. Standardowa konfiguracja stacji użytkownika określona jest w Regulaminie standaryzacji stacji roboczych, zatwierdzonym przez Komitet.

3. Za utrzymanie standardu stacji roboczych odpowiada komórka właściwa ds. informatyki.

4. Przeglądy licencjonowanego oprogramowania mogą być przeprowadzane w trybie doraźnym lub w terminie ustalonym w harmonogramie przeglądów, zatwierdzanym przez Prezesa Agencji.

5. Spis licencjonowanego oprogramowania jest sprawdzany przez dyrektora komórki właściwej ds. bezpieczeństwa informacji pod kątem kompletności ewidencji.

6. Okresowo, nie rzadziej niż raz w roku, stacje robocze i udostępnione udziały sieciowe użytkowników są sprawdzane przez Administratora Systemu pod kątem obecności nieautoryzowanego oprogramowania.

7. Przesłanką do podjęcia przeglądu doraźnego jest:

   1) żądanie kierownika komórki organizacyjnej, Właściciela Procesu/Właściciela Zasobu, dyrektora komórki właściwej ds. bezpieczeństwa informacji, Komitetu lub uprawnionych organów ścigania, w związku z informacją o popełnieniu lub podejrzeniu popełnienia czynu niedozwolonego przez pracownika,

   2) otrzymanie zgłoszenia od pracownika o pojawieniu się lub podejrzeniu pojawienia się w systemie teleinformatycznym nieautoryzowanego oprogramowania.

8. Do przeprowadzenia przeglądu zgodności zainstalowanego oprogramowania z posiadanymi licencjami, a także zgodności z konfiguracją standardową, Administrator Systemu może stosować narzędzia programowe umożliwiające m.in.:

   1) automatyczne sprawdzanie stacji roboczych i serwerów,

   2) centralne zarządzanie spisem licencjonowanego oprogramowania,

   3) automatyczne ostrzeganie przed przekroczeniem liczby licencji.

9. Nieautoryzowane oprogramowanie jest niezwłocznie usuwane z systemu teleinformatycznego, a informacje o przypadkach używania nieautoryzowanego oprogramowania są przedstawiane przez Administratora Systemu Komitetowi z rekomendacją podjęcia odpowiednich działań.

§ 6.

Zarządzanie kopiami zapasowymi i archiwalnymi

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

12. Miejsce przechowywania kopii jest zabezpieczone przed nieuprawnionym dostępem oraz skutkami zdarzeń takich, jak pożar, zalanie, oddziaływanie silnego pola elektromagnetycznego, promieniowanie, zanieczyszczenie środowiska na takim poziomie, jak jest zabezpieczony system, z którego kopia zapasowa została wykonana.
13. Kopie są przechowywane w bezpiecznej odległości (w innej lokalizacji) od miejsca, w którym jest prowadzona eksploatacja systemów. Proces przekazywania nośników zawierających kopie zapasowe i archiwalne do innej lokalizacji jest udokumentowany.
14. Regularnie, co najmniej raz w roku, Administrator Systemu w porozumieniu z Właścicielem Procesu/Właścicielem Zasobu przeprowadza testowe sprawdzenie odtworzenia systemu, aplikacji, bazy danych lub dokumentów z kopii. Testowe odtworzenie podlega udokumentowaniu w dzienniku pracy systemu.
15. W przypadku, gdy okres trwałości zapisu na nośniku elektronicznym lub magnetycznym jest krótszy od wymaganego okresu przechowywania wynikającego z uwarunkowań prawnych dane z nośników są przenoszone na inny nośnik.
16. Kopię na inny nośnik wykonuje Administrator Systemu. Nośnik, z którego przeniesiono zapis, jest niszczony zgodnie z zasadami obowiązującymi w Agencji, a całość operacji przeniesienia jest dokumentowana.
17. Po upływie wymaganego okresu przechowywania kopie archiwalne są niszczone zgodnie z zasadami obowiązującymi w Agencji.
18. Usługi transportowania lub przechowywania kopii zapasowych lub archiwalnych mogą być powierzone podmiotowi zewnętrznemu.
19. Umowa z podmiotem zewnętrznym na transportowanie lub przechowywanie kopii zapasowych lub archiwalnych powinna zawierać:
   1) wymagania bezpieczeństwa transportowania (przechowywania) kopii zapasowych,
   2) tryb przekazywania (odbierania) kopii zapasowych lub archiwalnych:
      a) zwykły (rotacja kopii zapasowych),
      b) awaryjny (w celu użycia kopii zapasowej lub archiwalnej),
   3) sposoby komunikowania się Agencji z usługodawcą, w tym potwierdzania dostarczenia kopii zapasowych w trybie awaryjnym,
   4) zakres odpowiedzialności usługodawcy za utratę lub uszkodzenie kopii zapasowych lub archiwalnych.

§ 7.

Zarządzanie poprawkami technicznymi

1. Zarządzanie poprawkami ma na celu eliminowanie lub ograniczanie zidentyfikowanych podatności systemów teleinformatycznych.
2. Administrator Systemu zobowiązany jest do monitorowania pojawiania się poprawek do poszczególnych usług sieciowych, systemów operacyjnych i aplikacji ARiMR.
3. Administrator Systemu obowiązany jest do wprowadzania poprawek w oparciu informacje uzyskane od producentów urządzeń sieciowych, systemów operacyjnych i apli-

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) rozdzielenia środowisk produkcyjnych od testowych.
2. Podsieci logiczne VLAN wewnątrz sieci Agencji tworzy się dla elementów systemu o różnych wymaganiach bezpieczeństwa. Każda z takich podsieci stanowi odrębną strefę bezpieczeństwa, do której dostęp musi być kontrolowany z wykorzystaniem zapory ogniowej zapewniającej realizację ścisłej kontroli oraz selektywnego dostępu do wybranych usług i systemów w danej strefie.
3. Ruch między podsieciami jest kontrolowany za pomocą reguł filtrujących wprowadzonych w urządzeniach sieciowych oraz serwerach.
4. W Agencji wdrożono mechanizmy kontroli rutingu w sieciach oparte na zdefiniowaniu możliwych tras pakietów w sieci.

5. Sygnatury systemów wykrywania i przeciwdziałania włamaniom podlegają regularnej aktualizacji.
6. Komunikacja systemów zewnętrznych z systemami Agencji musi być realizowana poprzez routery dostępowe przyłączone w jednej ze stref zapory ogniowej – strefy dostępowej dedykowanej dla komunikacji z systemami zewnętrznymi.
7. Do realizacji połączeń z systemami zewnętrznymi wymagane jest wykorzystanie łączy dedykowanych. W szczególnych przypadkach oraz do celów testowych zezwala się na dostęp do systemów aplikacyjnych Agencji za pośrednictwem łączy wirtualnych realizowanych poprzez sieć publiczną z wykorzystaniem technologii VPN (połączenia terminowane w zaporze ogniowej lub koncentratorze VPN zlokalizowanym w strefie dostępowej).

§ 9.

Uwierzytelnianie węzłów

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

§ 10.

Ochrona urządzeń sieciowych

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

§ 11.

Bezpieczeństwo zdalnego dostępu do portów diagnostycznych i konfiguracyjnych

1. Ustawienia parametrów konfiguracyjnych oraz przeprowadzenie diagnostyki urządzeń systemu teleinformatycznego wykonuje się z lokalnej konsoli administracyjnej, wykorzystując do tego celu dedykowane konta administracyjne (lokalny dostęp administracyjny).
2. W szczególnych przypadkach przewidzianych umowami z podmiotami zewnętrznymi oraz sytuacjach awaryjnych, działania administracyjne można wykonywać w trybie zdalnego dostępu. Zdalny dostęp administracyjny jest realizowany wyłącznie ze stacji dedykowanych dla systemów administracyjnych.
3. Do nawiązywania zdalnych połączeń administracyjnych stosuje się:
   1) mechanizmy zapewniające uwierzytelnianie stacji i użytkownika,

2) szyfrowanie komunikacji z wykorzystaniem bezpiecznych protokołów, zapewniających poufność i integralność przesyłanych danych,

3) ograniczenie dostępu do określonej grupy adresacji oraz usług niezbędnych do realizacji powierzonych zadań.

4. Warunki techniczne zdalnego dostępu podlegają zatwierdzeniu przez Komitet.

§ 12.

Bezpieczeństwo dostępu do sieci publicznych (Internet)

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

Rozdział 3.
Bezpieczeństwo systemów operacyjnych

§ 13.

Ogólne mechanizmy bezpieczeństwa

1. W Agencji stosuje się następujące mechanizmy bezpieczeństwa systemów operacyjnych:
   1) uwierzytelnianie użytkowników, zgodnie z przyjętymi w Agencji zasadami kontroli dostępu,
   2) rejestrowanie nieudanych prób dostępu do systemu,
   3) rejestrowanie korzystania z przywilejów systemowych,
   4) generowanie alarmów w przypadku naruszenia reguł bezpieczeństwa systemu,

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

§ 14.

Identyfikacja i uwierzytelnianie użytkowników

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

§ 15.

System zarządzania hasłami

1. Ustawienia zasad zarządzania hasłami w systemach teleinformatycznych zapewniają:
   1) wymuszanie użycia indywidualnych haseł,
   2) wybór i zmianę haseł przez użytkowników,

3) potwierdzanie zmiany haseł dla uniknięcia błędów podczas ich wprowadzania,

4) wymuszenie wyboru haseł o odpowiedniej jakości, tj.: składających się co najmniej z 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne,

5) wymuszenie zmiany haseł z ustaloną częstotliwością, w przypadku systemów przetwarzających dane osobowe zmiana hasła następuje nie rzadziej niż co 30 dni,

6) wymuszenie zmiany haseł tymczasowych przy pierwszym rejestrowaniu się w systemie,

7) pamiętanie haseł przez system w celu zapobiegania ponownemu ich użyciu, minimalna liczba haseł pamiętanych przez system wynosi 5.

2. Hasła administracyjne mogą być w szczególnych sytuacjach stosowane dłużej niż zaznaczono to w ust. 1 pkt 5, jednak nie dłużej niż 6 miesięcy.

§ 16.

Użycie programów narzędziowych

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

§ 17.

Ograniczenia czasowe sesji połączeniowej

1. W celu wymuszenia ochrony urządzeń systemu teleinformatycznego stosuje się następujące mechanizmy włączane w przypadku stwierdzenia braku aktywności użytkownika:
   1) blokowanie lub wyłączanie stacji roboczej (sesji połączeniowej),
   2) powtarzanie identyfikacji i uwierzytelnianie użytkownika.
2. System operacyjny po ustalonym okresie bezczynności użytkownika, jednak nie dłużej niż 10 minut, przechodzi w stan nieaktywny, w którym blokowany jest dostęp do konsoli. Powrót do stanu aktywności wymaga podania hasła.
3. Dla zapewnienia bezpieczeństwa systemów teleinformatycznych Agencji stosuje się ograniczenia czasu pracy w systemach operacyjnych do godzin pracy Agencji.

4. O ograniczeniu czasu trwania połączenia decyduje Właściciel Procesu/Właściciel Zasobu odpowiedzialny za funkcjonowanie i bezpieczeństwo danego systemu teleinformatycznego.
5. W przypadku konieczności pracy w systemie w innym czasie niż wyżej określony, zgodę wydaje Właściciel Procesu/Właściciel Zasobu na wniosek kierownika komórki organizacyjnej, której pracownicy potrzebują dostępu do systemu poza ustalonymi godzinami pracy.

§ 18.

Eksploatacja aplikacji w systemach teleinformatycznych Agencji

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

§ 19.

Świadczenie usług informatycznych przez podmioty zewnętrzne

1. Dostęp podmiotu zewnętrznego do systemów Agencji wymaga przeprowadzenia udokumentowanego szacowania ryzyka.
2. Szacowanie ryzyka przeprowadza Właściciel Procesu/Właściciel Zasobu na podstawie informacji dostarczonych przez Administratora Systemu.
3. W szczególności, Właściciel Procesu/Właściciel Zasobu otrzymuje następujące informacje:
   1) podstawę udzielenia dostępu dla danego podmiotu zewnętrznego,
   2) zakres i sposób dostępu do sieci Agencji, w tym zakres przydzielanych uprawnień,
   3) proponowane rozwiązania techniczne i organizacyjne służące ograniczeniu ryzyka dla bezpieczeństwa systemów teleinformatycznych Agencji.
4. Zgodę na udzielenie dostępu podmiotowi zewnętrznemu wydaje Właściciel Procesu/Właściciel Zasobu, po zaakceptowaniu i wdrożeniu rozwiązań, o których mowa w ust. 3 pkt 3.
5. W umowie z podmiotem zewnętrznym dotyczącej utrzymania systemów teleinformatycznych Agencji uwzględnia się zapis zobowiązujący podmiot zewnętrzny do stosowania zasad i procedur wynikających z dokumentów polityki bezpieczeństwa informa-

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. Doraźne działania serwisowe podmiotów zewnętrznych (nie mające charakteru stałego utrzymania systemów teleinformatycznych) są dokumentowana przez Administratora Systemu w dzienniku pracy systemu. Zapis w dzienniku zawiera, co najmniej:
   1) dokładny czas rozpoczęcia i zakończenia działania serwisowego,
   2) identyfikacja osoby realizującej działania serwisowe po stronie podmiotu zewnętrznego oraz nadzorującej te działania po stronie Agencji,
   3) dokładny opis przeprowadzonych działań wraz ze wskazaniem statusu tych działań (wymagające kontynuacji, zakończone).
7. Doraźne działania serwisowe w systemie teleinformatycznym osób, nie będących uprawnionymi pracownikami Agencji dokonywane są w obecności Administratora Systemu.
8. Osobie reprezentującej podmiot zewnętrzny, wykonującej działania serwisowe, nie mogą zostać nadane uprawnienia administratora. Jeśli wyjątkowa sytuacja uzasadnia taką potrzebę, to nadanie uprawnienia wymaga zgody Właściciela Procesu/Właściciela Zasobu. Niezwłocznie po zakończeniu pracy uprawnienia administratora oraz jakiekolwiek inne uprawnienia nadane osobie reprezentującej podmiot zewnętrzny muszą zostać odebrane.
9. W przypadku dokonywania zmian konfiguracji (naprawy, rekonfiguracje) przez stronę trzecią Agencja zapewnia odpowiednie uprawnienia do użycia oprogramowania narzędziowego służącego do celów zarządzania konfiguracją.

Rozdział 4.
Zarządzanie zmianami w systemach teleinformatycznych Agencji

§ 20.

Odbiór systemu teleinformatycznego

1. Kryteria odbioru obejmują dostarczenie:
   1) w przypadku oprogramowania - dokumentacji technicznej, instrukcji dla administratora i użytkownika,
   2) w przypadku infrastruktury – dokumentacji powykonawczej obejmującej w szczególności schemat połączeń fizycznych i logicznych elementów infrastruktury.
2. Ponadto, kryteria odbioru obejmują:
   1) wymagania wydajnościowe i pojemnościowe systemu teleinformatycznego,
   2) dokumenty potwierdzające, że instalacja nowych systemów nie będzie miała negatywnego wpływu na istniejące systemy, szczególnie w chwilach największego obciążenia (jeżeli ma zastosowanie),
   3) dokumenty potwierdzające, że wpływ nowych systemów na bezpieczeństwo informacji został uwzględniony,

   4) szkolenia z zakresu posługiwania się i działania nowych systemów,
   5) w przypadku oprogramowania, odbiór obejmuje dodatkowo zapisy zawarte w § 7 Regulaminu rozwoju aplikacji.

§ 21.

Kontrola zmian w eksploatacji

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

5) harmonogramem wprowadzanych zmian,

6) wykonaniem kopii zapasowej z możliwością odtworzenia stanu poprzedniego na wypadek nieprzewidzianych zdarzeń (jeżeli ma zastosowanie),

7) przetestowaniem zmian.

7. Jeżeli zmiana ma charakter awaryjny, dokumentacja może być opracowana najpóźniej w przeciągu 7 dni od dokonania zmiany.

8. Zmiana mająca charakter awaryjny, którą trzeba wprowadzić bezzwłocznie w celu ograniczenia ryzyka poważnego zakłócenia działalności Agencji wymaga zgody Właściciela Procesu / Właściciela Zasobu.

9. Dokonywane zmiany: regularne, awaryjne i rutynowe podlegają rejestracji w Dzienniku pracy systemu prowadzonym przez Administratora Systemu.

10. Wpisu dokonuje osoba przeprowadzająca zmianę. Wpis zawiera w szczególności odnośniki do dokumentów określonych w ust. 6.

§ 22.

Bezpieczeństwo dokumentacji systemu

1. Dokumentacja powykonawcza infrastruktury oraz dokumentacja techniczna systemu podlega ochronie zgodnie z zasadami ochrony informacji wrażliwych przedstawionymi w Polityce.

2. Osobą odpowiedzialną za aktualność i kompletność dokumentacji jest dyrektor komórki właściwej ds. informatyki.

3. Dokumentacja systemów jest udostępniana na zasadzie „wiedzy koniecznej". Udostępnienie dokumentacji jest rejestrowane.

Rozdział 5.
Zarządzanie wymiennymi nośnikami komputerowymi

§ 23.

Użytkowanie nośników

1. Nośniki komputerowe są przechowywane i eksploatowane zgodnie z zaleceniami producenta, z uwzględnieniem wymagań w zakresie ochrony informacji, które są umieszczone na nośnikach.

2. Nośniki zawierające informacje wrażliwe przechowywane są w specjalnych, atestowanych szafach (np. S120 DIS) zlokalizowanych w strefie administracyjnej. Szafy do przechowywania nośników zapewniają ochronę przed:

   1) pożarem,

   2) eksplozją towarzyszącą pożarowi,

   3) działaniem gazów powstałych podczas pożaru,

   4) zalaniem,

   5) działaniem pola elektromagnetycznego.

3. Wymienne nośniki komputerowe takie, jak: przenośne dyski twarde, kamery taśmy magnetyczne, optyczne nośniki danych, pamięci typu flash, podlegają ewidencji prowadzonej przez Administratora Systemu. Rejestr wymiennych nośników komputerowych prowadzony jest w postaci papierowej lub elektronicznej.

4. Etykiety nośników informacji posiadają identyfikator lub numer umożliwiający ich jednoznaczną identyfikację (np.: nr seryjny, kod kreskowy, itp.). Na podstawie etykiety nośnika informacji i danych zawartych w ewidencji nośników możliwe jest ustalenie:

   1) numeru ewidencyjnego nośnika,

   2) typu nośnika,

   3) daty zapisu na nośniku (informacja nieobowiązkowa dla nośników wielokrotnego zapisu),

   4) nazwy komórki organizacyjnej składującej informacje,

   5) określenia rodzaju przechowywanej informacji (informacja nieobowiązkowa dla nośników wielokrotnego zapisu),

   6) imienia i nazwiska osoby dokonującej zapisu (w przypadku nośników wielokrotnego zapisu imię i nazwisko osoby, na stanie której jest dany nośnik).

5. Nośniki wymienne zawierające informacje wrażliwe przewożone są przez pracowników Agencji do innych lokalizacji w pojemniku zapewniającym ochronę nośników przed zagrożeniami wskazanymi w ust. 2.

§ 24.

Wycofanie z eksploatacji nośników komputerowych

1. Wycofanie z eksploatacji wymiennych nośników komputerowych, przekazanie do naprawy lub ponownego użycia jest poprzedzone archiwizacją, a następnie skutecznym usunięciem zapisanych danych.

2. Uszkodzone wymienne nośniki komputerowe zawierające informacje wrażliwe są niszczone w sposób uniemożliwiający odczytanie zapisanych na nich informacji.

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

Rozdział 6.
Bezpieczeństwo wymiany danych

§ 25.

Bezpieczeństwo serwisów intranetowych i ekstranetowych

1. Serwisy intranetowe i ekstranetowe są lokalizowane na serwerach, do których dostęp wymaga identyfikacji i uwierzytelnienia.

2. Udostępnienie informacji w serwisach intranetowych i ekstranetowych wymaga zatwierdzenia przez Właściciela Procesu/Właściciela Zasobu.

3. Dostęp do serwisów ekstranetowych posiadają wyłącznie pracownicy Agencji.

4. Dostęp do serwisów ekstranetowych mogą posiadać uprawnione z mocy prawa podmioty zewnętrzne współpracujące z Agencją.

§ 26.

Bezpieczeństwo wymiany poczty elektronicznej wewnętrznej i zewnętrznej

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

Rozdział 7.
Konserwacja i naprawy sprzętu

§ 27.

Konserwacja i naprawa sprzętu

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

§ 28.

Zabezpieczenie sprzętu poza siedzibą

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

Rozdział 8.
Zarządzanie dostępem do systemów teleinformatycznych

§ 29.

Rejestrowanie użytkowników i przypisanie praw dostępu

1. Użytkownik systemu teleinformatycznego jest jednoznacznie identyfikowany poprzez indywidualny identyfikator (nazwę) użytkownika.
2. Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego użytkownika (chyba, że z przyczyn technicznych nie ma możliwości stosowania osobistych identyfikatorów).
3. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.
4. Uprawnienia dostępu są nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzeby wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień administratora (przywilejów) będzie kwalifikowane jako incydent związany z bezpieczeństwem informacji.
5. Nadawanie uprawnień dostępu do systemu teleinformatycznego Agencji odbywa się zgodnie z procedurą nadawania/zmiany/odbierania uprawnień pracownikom ARiMR zawartą w Książce Procedur KP-611-101-ARiMR.
6. W przypadku konieczności natychmiastowego odebrania/ograniczenia praw dostępu dopuszcza się możliwość zastosowania uproszczonego trybu polegającego na przekazaniu stosownej informacji pocztą elektroniczną od bezpośredniego przełożonego do Administratora Systemu, która niezwłocznie jest potwierdzana w zwykłym trybie.
7. Rejestr użytkowników wraz z przyznanymi uprawnieniami do systemu lub aplikacji prowadzi Administrator Systemu. Rejestr publikowany jest w sieci wewnętrznej

na stronie intranetowej Agencji i aktualizowany nie rzadziej niż raz na miesiąc. Weryfikację aktualności tego rejestru prowadzą Właściciele Procesów/Właściciele Zasobów w odniesieniu do nadzorowanych przez siebie zasobów.

8. Prawa dostępu do wielu aktywów (plików, katalogów, aplikacji, stron internetowych) jednocześnie przydzielane są dla każdego z aktywów za osobną zgodą danego Właściciela Procesu/Właściciela Zasobu. W przypadku, gdy w Agencji wykorzystuje się domenowe mechanizmy zarządzania dostępem (usługi katalogowe, active directory, itp.) aktywa są grupowane, za uprzednią zgodą odpowiednich Właścicieli Procesów / Właścicieli Zasobów.
9. Administrator Systemu raz na miesiąc dokonuje przeglądu stanu aktywności kont użytkowników.
10. Konta nieużywane przez okres 30 dni są automatycznie blokowane.

§ 30.

Zarządzanie przywilejami

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

§ 31.

Zarządzanie hasłami użytkowników

1. Niedopuszczalne jest występowanie w systemie teleinformatycznym kont niezabezpieczonych hasłem.
2. Administrator Systemu, za pomocą ustawień systemowych, wymusza natychmiastową zmianę hasła początkowego, przydzielonego użytkownikowi, na nowe przez niego wybrane (o ile istnieją możliwości techniczne wymuszenia).
3. Zabronione jest przekazywanie haseł przez osoby trzecie lub za pośrednictwem otwartych wiadomości poczty elektronicznej (nie dotyczy to haseł tymczasowych do systemów wyposażonych w mechanizm wymuszający zmianę hasła przy pierwszej próbie uwierzytelnienia się w danym systemie).

4. Hasła tymczasowe, dostarczane w przypadku utraty hasła, są wydawane dopiero po pozytywnej weryfikacji tożsamości użytkownika.
5. Przy konfigurowaniu mechanizmów logowania do systemów uwzględnia się następujące zasady:
   1) użytkownik musi podać swój identyfikator oraz hasło,
   2) w polu logowania nie jest prezentowana ostatnio użyta nazwa użytkownika (o ile system to umożliwia),
   3) wpisywane hasło nie pojawia się w postaci jawnej na ekranie logowania,
   4) hasło przesyłane jest w postaci zaszyfrowanej (o ile system to umożliwia).
6. Systemy operacyjne i aplikacje spełniają wymagania dotyczące możliwości ustawienia następujących parametrów haseł:
   1) siły hasła (długość i złożoność haseł),
   2) maksymalnego okresu ważności,
   3) ograniczenia możliwości ponownego wykorzystania hasła (pamięć ostatnio używanych haseł).
7. Specjalne warunki przechowywania duplikatów haseł dotyczą:
   1) elementów aktywnych sieci teleinformatycznej,
   2) haseł administracyjnych do systemów, aplikacji i baz danych,
   3) konfiguracji komputerów, w tym hasła do BIOS.
8. Hasła administracyjne przechowuje się w postaci zaszyfrowanej. Dopuszcza się przechowywanie haseł w wersji elektronicznej poprzez zastosowanie oprogramowania typu „password manager" z bazą szyfrowaną algorytmem AES lub Twofish.
9. Do przechowywania hasła głównego do zaszyfrowanej bazy haseł, bądź innych haseł zapisanych na papierze, stosuje się wyłącznie koperty, które uniemożliwiają otwarcie bez uszkodzenia ich struktury (tzw. „koperty bezpieczne"). Koperty z hasłami przechowuje się w sejfie, w miejscu zapewniającym dostęp tylko osobom upoważnionym.
10. Dane umieszczone na bezpiecznej kopercie zawierają:
    1) numer koperty adekwatny do numeru ewidencyjnego podanego w książce ewidencji haseł,
    2) datę jej złożenia i podpis osoby składającej kopertę,
    3) skróconą nazwę przynależności hasła.
11. Koperty z hasłami podlegają oznaczaniu zgodnie z załącznikiem nr 2 do niniejszego Regulaminu oraz ścisłej ewidencji prowadzonej przez Administratora Systemu.
12. Ewidencja haseł przechowywana jest w miejscu zabezpieczonym przed utratą i dostępem osób niepowołanych.
13. Za aktualność przechowywanych haseł odpowiedzialny jest Administrator Systemu.
14. Awaryjne otwarcie bezpiecznej koperty oraz pobranie kopii hasła znajdującego się w kopercie wymaga uprzedniej pisemnej akceptacji Właściciela Procesu / Właściciela Zasobu lub osoby przez niego upoważnionej i jest udokumentowane w ewidencji kopert.

15. Po użyciu, hasło ulega zniszczeniu, a w to miejsce jest generowane nowe hasło, którego kopia jest przechowywana na identycznych zasadach jak w przypadku zniszczonego hasła.

§ 32.

Zasady dostępu do plików i katalogów

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

Rozdział 9.
Zasady monitorowania systemów i ich użycia

§ 33.

Mechanizmy monitorowania systemów

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

5. Serwery kontrolujące dostęp do Internetu tworzą zdalne pliki rejestrów lub mają wdrożony system przesyłania rejestrów zdarzeń na inne, wewnętrzne serwery.
6. W celu wykrywania incydentów związanych z bezpieczeństwem Administrator Systemu regularnie monitoruje zapisy dokonywane automatycznie przez systemy w rejestrach zdarzeń pod kątem właściwego wykorzystania systemu teleinformatycznego i zarządzania nim.
7. Systemy zapisu zdarzeń są zabezpieczone przed manipulacją i nieuprawnionymi zmianami.
8. W ramach weryfikacji zgodności systemów teleinformatycznych względem standardów bezpieczeństwa przeprowadzane są, na podstawie zatwierdzonego przez Prezesa Agencji harmonogramu oraz procedury KP-611-298-ARiMR, testy bezpieczeństwa systemów teleinformatycznych ARiMR.

§ 34.

Dziennik pracy systemu

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

1) czas rozpoczęcia i zakończenia pracy w systemie;

2) nazwisko osoby wykonującej wpis do dziennika,

3) identyfikator konta, z którego wykonano czynności (jeśli ma zastosowanie).

3. Administrator Systemu odnotowuje w dzienniku wszelkie dodatkowe informacje, które pozwolą zlokalizować przyczynę błędu:

   1) w przypadku awarii sprzętu lub usługi, w szczególności:

      a) powtórzenie błędu (np. analogiczny wcześniejszy zapis w dzienniku),

      b) objawy towarzyszące (np. komunikaty systemowe, logi połączeń),

      c) krytyczność awarii, zgodnie z klasyfikacją uzgodnioną z dostawcą usług (np. w umowie SLA),

   2) w przypadku awarii oprogramowania, w szczególności:

      a) powtórzenie błędu (np. analogiczny wcześniejszy zapis w dzienniku),

      b) zrzuty ekranów,

      c) konfiguracje oprogramowania i baz danych (np. otwarte pliki, zapisy w logach),

      d) krytyczność błędu, zgodnie z klasyfikacją uzgodnioną z dostawcą oprogramowania.

4. Lista działań wykonywanych przez administratorów podlegających bezwzględnemu odnotowywaniu w dziennikach może zostać poszerzona lub ograniczona dla danego systemu teleinformatycznego po ówczesnym przeprowadzeniu udokumentowanego szacowanie ryzyka i zatwierdzeniu przez Komitet.

5. Dzienniki mogą być prowadzone oddzielnie dla każdego serwera, urządzenia sieciowego, aplikacji.

6. Dzienniki prowadzone są przez administratora odpowiedzialnego za dany serwer, urządzenie sieciowe, aplikację.

7. Dzienniki systemowe lub ich części prowadzone są w formie elektronicznej lub papierowej.

8. Rejestracja błędów może być prowadzona poza dziennikiem administratora, w dedykowanym rejestrze.

§ 35.

Synchronizacja zegarów

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

2. Do synchronizacji czasu wykorzystuje się protokół NTP.

3. Źródłem synchronizacji powinien być zewnętrzny wzorzec czasu.

4. Stacje robocze synchronizują czas z kontrolerów domen.

§ 36.

Bezpieczeństwo okablowania

1. W Agencji przyjęto następujące zasady instalowania i ochrony okablowania:

   1) sposób instalacji okablowania uwzględnia ochronę okablowania przed nieautoryzowanym dostępem lub uszkodzeniem, poprzez prowadzenie kabli w rurach kablowych, listwach PCV, podłogach technologicznych,

   2) okablowanie, w miarę możliwości, nie jest prowadzone przez ogólnie dostępne strefy; w przypadku prowadzenia okablowania przez takie miejsca stosowane są środki uniemożliwiające bądź ograniczające dostęp do okablowania przez osoby nieupoważnione,

   3) przy projektowaniu przebiegu linii sieci teleinformatycznej poza strefami administracyjnymi wykorzystywane są w maksymalnym stopniu rozwiązania wykorzystujące technologie światłowodowe,

   4) w instalacji okablowania oddzielono kable zasilające od okablowania komunikacyjnego w celu unikania interferencji,

   5) w instalacji okablowania zastosowano jednoznaczne i wyraźne oznakowanie umożliwiające identyfikację kabli i sprzętu w celu zmniejszenia ryzyka błędów takich, jak niewłaściwe połączenie lub zastosowanie nieodpowiedniego kabla,

   6) kable komunikacyjne wyposażone są w zabezpieczenia odgromowe (jeżeli ma zastosowanie),

   7) prowadzi się kompletną i aktualną dokumentację połączeń fizycznych i logicznych w celu zmniejszenia prawdopodobieństwa błędów.

2. Pomieszczenia, w których znajdują się panele połączeniowe, węzły telekomunikacyjne i szafy dystrybucyjne objęte są systemem kontroli dostępu.

3. Niewykorzystywane segmenty sieci strukturalnej są odłączane od sieci teleinformatycznej.

4. W przypadku systemów wskazanych w procesie szacowania ryzyka jako kluczowe, są uwzględnione następujące zabezpieczenia obejmujące:

   1) stosowanie zapasowych (awaryjnych) dróg komunikacyjnych lub mediów transmisyjnych zapewniających odpowiedni poziom bezpieczeństwa,

   2) korzystanie z kabli światłowodowych.

5. Badanie właściwości transmisyjnych okablowania strukturalnego przeprowadzane jest przez Administratora Systemu nie rzadziej niż raz na 2 lata.

§ 37.

Eksploatacja urządzeń zasilających

1. Wszystkie urządzenia sieci teleinformatycznej są zasilane napięciem o parametrach zgodnych z wymaganiami producenta.

2. Urządzenia teleinformatyczne muszą być zasilane z wydzielonej instalacji elektrycznej.

3. Urządzenia sieci teleinformatycznej, od ciągłości pracy, których zależne jest realizowanie podstawowych zadań Agencji, muszą być zasilane z gwarantowanych źródeł.

4. Gwarantowane zasilanie uzyskiwane jest przez zastosowanie dywersyfikacji zewnętrznych źródeł energii elektrycznej z samoczynnym załączaniem rezerwy (SZR),

zastosowanie zasilaczy bezprzerwowych (UPS), zastosowanie awaryjnych agregatów prądotwórczych.

5. Konfiguracja zasilania gwarantowanego wynika z Planu Zapewnienia Ciągłości Działania Agencji.
6. Dobór urządzeń podtrzymujących zasilanie pod względem wydajności mocowej poprzedzane jest przeprowadzeniem udokumentowanego bilansu mocy.
7. Każde urządzenie sieci teleinformatycznej jest opatrzone tabliczką, z której wynika skąd dane urządzenie jest zasilane, zawierającą nazwę rozdzielnicy lub tablicy zabezpieczeń oraz nazwę pola w rozdzielnicy lub bezpiecznika na tablicy zabezpieczeń.
8. Stan zasilania zasobów sieci teleinformatycznej, którym nadano status zasobu kluczowego, jest na bieżąco monitorowany przez Administratora Systemu. Jakość zasilania pozostałych zasobów sieci teleinformatycznej musi być okresowo sprawdzana.
9. Zasilacze bezprzerwowe, zasilające kluczowe zasoby sieci teleinformatycznej, raportują stan swojej pracy (zasilanie z sieci, zasilanie z baterii) oraz parametry baterii (jej stopień naładowania i przewidziany czas pracy z baterii przy danym obciążeniu) systemom operacyjnym serwerów. W przypadku, gdy stopień naładowania baterii osiągnie w czasie pracy z baterii poziom, którego przekroczenie nie gwarantuje podtrzymania ciągłości pracy, system operacyjny wymusza automatyczne zamknięcie aplikacji i baz danych oraz kontrolowane wyłączenie serwera.
10. W przypadku, gdy automatyczne raportowanie nie jest technicznie możliwe Administrator Systemu dokonuje okresowych, raz na tydzień, oględzin polegających na sprawdzeniu wskazań paneli sterujących (według instrukcji techniczno-eksploatacyjnych). Oględziny muszą być odnotowywane w dzienniku pracy systemu.
11. Elementy systemu zasilania gwarantowanego podlegają okresowym przeglądom i konserwacjom w zakresie określonym przez producenta.
12. Akumulatory podlegają wymianie po okresach eksploatacji przewidzianych w instrukcjach użytkowania.
13. Serwisowanie urządzeń zasilających przeprowadzane jest wyłącznie przez autoryzowane podmioty zewnętrzne.
14. Przeglądy, konserwacje i serwisowanie podlega odnotowaniu w dzienniku pracy systemu.
15. Agregaty prądotwórcze są okresowo uruchamiane w okresach i zakresie przewidzianych przez ich producentów.

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

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

cd.:

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

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

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

Wzór etykiety na kopercie:

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

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

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

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

Część I

(Wypełnia kierownik komórki/jednostki organizacyjnej/Właściciel Zasobu)

1) Komórka organizacyjna:

.....

2) Nazwa programu narzędziowego, wersja i krótki opis

.....

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

3) Imiona i nazwiska użytkowników:

.....

.....

4) Uzasadnienie wniosku:

.....

.....

.....

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

Część II Ocena zasadności wniosku (w aspekcie bezpieczeństwa informacji i systemów teleinformatycznych)

(wypełnia dyrektor komórki właściwej ds. bezpieczeństwa informacji)

Decyzja pozytywna	☐	Decyzja negatywna	☐

Uzasadnienie:

.....

.....

.....

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

Część III Informacje o realizacji wniosku

(Wypełnia Administrator Systemu)

Identyfikator wniosku: .....

.....

.....

.....

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

.....

Poziom uprawnień (przywilejów) .....

.....

(data i podpis Administratora Systemu)