30 lat
Agencja Restrukturyzacji
i Modernizacji Rolnictwa

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

Specyfikacja Warunków Zamówienia

w postępowaniu o udzielenie zamówienia publicznego
o wartości mniejszej niż progi unijne
prowadzonym w trybie podstawowym

na:

„Przeprowadzenie badania sprawozdania finansowego ARiMR za lata 2024-2025"

numer referencyjny sprawy: DPiZP.2619.7.2024

wszczętym na podstawie ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2023 poz. 1605 ze zm.)

Informacje dotyczące prowadzonego postępowania o udzielenie zamówienia publicznego

A. Dane Zamawiającego

1. Zamawiającym jest:
   Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie (adres: Al. Jana Pawła II 70, 00-175 Warszawa); adres do korespondencji: ul. Poleczki 33, 02-822 Warszawa, tel. 22 595 06 11, adres e-mail: zamowieniapubliczne@arimr.gov.pl;
   REGON: 010613083;
   NIP: 526-19-33-940.
2. Adres strony internetowej prowadzonego postępowania o udzielenie zamówienia publicznego (dalej: *„postępowanie"*): https://platformazakupowa.pl/pn/arimr.
3. Niniejsze postępowanie prowadzone jest w trybie podstawowym na podstawie przepisów ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2023 poz. 1605 ze zm.).; dalej: *„ustawa"*.

B. Pozostałe informacje dotyczące prowadzonego postępowania

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

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

Rozdział I. Przedmiot zamówienia

I.1. Opis przedmiotu zamówienia

1. Kod Wspólnego Słownika Zamówień (CPV).
   1.1. Główny kod: 79212100-4 – [Usługi audytu finansowego].
2. Przedmiot zamówienia jest usługa polegająca na:
   2.1. Przeprowadzeniu przez Wykonawcę badania sprawozdania finansowego Agencji Restrukturyzacji i Modernizacji Rolnictwa (ARiMR) dalej zwanej: „Zamawiającym" za lata 2024 -2025, zgodnie z postanowieniami projektowanych postanowień umowy (dalej: ppu), których wzór stanowi załącznik nr 9 do Specyfikacji Warunków Zamówienia (dalej: „SWZ").
   2.2. Przeprowadzeniu badania sprawozdania finansowego ARiMR za lata 2024, 2025 obejmującego sprawozdania finansowe działalności krajowej, SAPARD, SPO „Restrukturyzacja i modernizacja sektora żywnościowego oraz rozwój obszarów wiejskich 2004-2006", SPO „Rybołówstwo i przetwórstwo ryb 2004-2006", Programu Operacyjnego „Zrównoważony rozwój sektora rybołówstwa i nadbrzeżnych obszarów rybackich 2007-2013", Programu Operacyjnego „Rybactwo i Morze" na lata 2014-2020, Programu Rozwoju Obszarów Wiejskich na lata 2007-2013, Programu Rozwoju Obszarów Wiejskich na lata 2014-2020, Programów dotyczących Wspólnej Polityki Rolnej, Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury na lata 2021–2027, Planu Strategicznego dla Wspólnej Polityki Rolnej w ramach EFRROW na lata 2023-2027 oraz Krajowego Planu Odbudowy i Zwiększania Odporności w ramach agencji płatniczej sporządzonych według stanu na dzień 31.12.2024 r., 31.12.2025 r. oraz stanowiących ich podstawę ksiąg rachunkowych ARiMR.
   2.3. Przeprowadzeniu badania ksiąg rachunkowych ARiMR stanowiących podstawę sporządzenia sprawozdań finansowych za lata 2024, 2025.
   W zakresie działalności krajowej księgowanie dokumentów odbywa się w Centrali i 16 Oddziałach Regionalnych Zamawiającego. Dokumenty źródłowe księgowane przez Centralę ARiMR są przechowywane w Centrali ARiMR, natomiast dokumenty księgowane przez Oddziały Regionalne ARiMR są przechowywane w poszczególnych Oddziałach Regionalnych.
   W zakresie działalności unijnej księgi rachunkowe Zamawiającego prowadzone są w siedzibie Centrali ARiMR w pełnym zakresie. W 16 Oddziałach Regionalnych ARiMR prowadzona jest ewidencja księgowa zdarzeń gospodarczych w zakresie należności (rejestrowanie i rozliczanie należności w Module Należności e-BS UE) wraz z procesem windykacji należności powstałych z tytułu udzielonej pomocy z programów unijnych. W 16 Oddziałach Regionalnych ARiMR prowadzone są czynności związane z generowaniem w Module Należności e-BS UE i wysyłaniem do beneficjentów upomnień, generowaniem w Module Należności e-BS UE i wysyłaniem tytułów wykonawczych, kierowanych do urzędów skarbowych.

3. Zamawiający wymaga, aby badania sprawozdań finansowych zostało przeprowadzone zgodnie z:

   3.1. ustawą z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120 z późn. zm.);
   3.2. ustawą z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym (Dz. U. z 2023 r. poz. 1015 z późn. zm.) z uwzględnieniem bieżących zmian w przepisach prawnych;
   3.3. Krajowymi Standardami Rewizji Finansowej w brzmieniu Międzynarodowych Standardów Badań przyjętych uchwałą Nr 3430/52a/2019 Krajowej Rady Biegłych Rewidentów z dnia 21 marca 2019 r. w sprawie krajowych standardów badania oraz innych dokumentów (z późn. zm.);
   3.4. Zasadami etyki zawodowej biegłych rewidentów, które stanowi Międzynarodowy Kodeks etyki zawodowych księgowych wprowadzony uchwałą Nr 3431/52a/2019 Krajowej Rady Biegłych Rewidentów z dnia 25 marca 2019 r. w sprawie zasad etyki biegłych rewidentów.

I.2. Opis części zamówienia

1. Zamawiający nie dopuszcza składania przez Wykonawcę ofert częściowych w rozumieniu art. 7 pkt 15 ustawy.
2. Zamawiający wskazuje powody niedokonania podziału zamówienia na części:

W przypadku niniejszego postępowania Zamawiający odstąpił od podziału na części, ponieważ uznał, że specyfika przedmiotu zamówienia wymaga realizacji zamówienia przez jeden podmiot. Badanie sprawozdania finansowego polega na wykonaniu szeregu czynności ściśle ze sobą powiązanych, w wyniku których sporządzone zostanie sprawozdanie niezależnego biegłego rewidenta z badania rocznego sprawozdania finansowego dla Ministra Rolnictwa i Rozwoju Wsi oraz Prezesa Agencji Restrukturyzacji i Modernizacji Rolnictwa. Celem badania sprawozdania finansowego jest sprawdzenie, czy rzetelnie i jasno przedstawia ono sytuację majątkową i finansową oraz wynik finansowy jednostki dlatego też nie możliwym jest wydzielenie części zamówienia i przekazania jej do realizacji innym podmiotom, gdyż biegły rewident dokonuje oceny całościowej opartej o własną weryfikację. Nie możliwy jest również podział zamówienia i wskazania jako części zamówienia badania na poszczególne lata. Zgodnie z art. 66 ust. 5 ustawy z dnia 29 września 1994 r. o rachunkowości "w przypadku badania ustawowego w rozumieniu art. 2 pkt 1 ustawy o biegłych rewidentach, pierwsza umowa o badanie sprawozdania finansowego jest zawierana z firmą audytorską na okres nie krótszy niż dwa lata z możliwością przedłużenia na kolejne co najmniej dwuletnie okresy."

ARiMR jest państwową osobą prawną działającą na podstawie Ustawy z dnia 9 maja 2008 r. o Agencji Restrukturyzacji i Modernizacji Rolnictwa (Dz. U. z 2023 r. poz. 1199). Zgodnie z art. 64 ust. 1 pkt 4) ustawy o rachunkowości sprawozdania finansowe ARiMR podlegają obowiązkowemu badaniu i obejmują: sprawozdania finansowe działalności krajowej, SAPARD, SPO „Restrukturyzacja i modernizacja sektora żywnościowego oraz rozwój obszarów wiejskich 2004-2006", SPO „Rybołówstwo i przetwórstwo ryb 2004-2006", Programu Operacyjnego „Zrównoważony rozwój sektora rybołówstwa i nadbrzeżnych obszarów rybackich 2007-2013", Programu Operacyjnego „Rybactwo i Morze" na lata 2014-2020, Programu Rozwoju Obszarów Wiejskich na lata 2007-2013, Programu Rozwoju Obszarów Wiejskich na lata 2014-2020, Programów dotyczących Wspólnej Polityki Rolnej, Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury na lata 2021–2027, Planu Strategicznego dla Wspólnej Polityki Rolnej w ramach EFRROW na lata 2023-2027 oraz Krajowego Planu Odbudowy i Zwiększania Odporności w ramach agencji płatniczej. Centrala i Odziały Regionalne ARiMR posiadają jeden (ten sam) REGON i NIP, i nie stanowią odrębnych podmiotów prawa. Zgodnie z art. 21 ust. 7b. ustawy o ARiMR wyboru firmy audytorskiej uprawnionej do badania rocznego sprawozdania finansowego ARiMR dokonuje Minister właściwy do spraw rozwoju wsi.

I.3. Powierzenie Podwykonawcy wykonania części zamówienia

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

I.4. Pozostałe istotne elementy związane z przedmiotem zamówienia

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

Rozdział II. Termin wykonania zamówienia

1. Zamawiający wymaga realizacji zamówienia tj. badania sprawozdań finansowych za lata: 2024, 2025 oraz ksiąg rachunkowych, o których mowa w § 1 ust. 1 ppu w terminach:

   1.1. za rok 2024 – do dnia 25.04.2025 r. i udokumentowane przekazaniem sprawozdania z badania, sporządzonego w formie elektronicznej, przy czym przez zakończenie badania rozumie się wydanie sprawozdania z badania.
   1.2. za rok 2025 – do dnia 24.04.2026 r. i udokumentowane przekazaniem sprawozdania z badania, sporządzonego w formie elektronicznej, przy czym przez zakończenie badania rozumie się wydanie sprawozdania z badania.

2. Szczegółowe terminy realizacji zobowiązań umownych zostały określone przez Zamawiającego w ppu stanowiących Załącznik nr 9 do SWZ.

Rozdział III. Podstawy wykluczenia oraz warunki udziału w postępowaniu

1. O zamówienie objęte niniejszym postępowaniem mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu z postępowania na podstawie przesłanek wskazanych w Rozdz. III.1. SWZ oraz spełniają warunki udziału w postępowaniu opisane w Rozdz. III.2. SWZ.
2. Wykonawca jest zobowiązany wykazać, że spełnia warunki udziału w postępowaniu i nie podlega wykluczeniu z postępowania. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia brak podstaw wykluczenia, o których mowa w Rozdz. III.1. SWZ musi wykazać każdy Wykonawca z osobna.

III.1. Podstawy wykluczenia

1. Z postępowania, na podstawie art. 108 ust. 1 ustawy, Zamawiający wykluczy Wykonawcę:
   1.1. będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
      1.1.1. udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
      1.1.2. handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
      1.1.3. o którym mowa w art. 228–230a, art. 250a Kodeksu karnego, w art. 46–48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2020 r. poz. 1133 oraz z 2021 r. poz. 2142) lub w art. 54 ust. 1–4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2022 r. poz. 463),
      1.1.4. finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
      1.1.5. o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,

1.1.6. powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej,

1.1.7. przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,

1.1.8. o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej

– lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

1.2. jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1.1.;

1.3. wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że Wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

1.4. wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;

1.5. jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności, jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;

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

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

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

3. Z postępowania, na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2023 r. poz. 129; dalej „ustawa o szczególnych rozwiązaniach") Zamawiający wykluczy:

3.1. Wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy o szczególnych rozwiązaniach;

3.2. Wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593, 655, 835, 2180 i 2185.). jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy o szczególnych rozwiązaniach;

3.3. Wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120 z późn. zm) jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy o szczególnych rozwiązaniach.

III.2. Warunki udziału w postępowaniu

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

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

(a) wykonał w okresie ostatnich (5) pięciu lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, co najmniej 3 (trzy) usługi polegające na wykonaniu badania sprawozdania finansowego i badaniu ksiąg rachunkowych jednostek sektora finansów publicznych realizujących zadania z krajowych środków budżetowych i środków pomocowych Unii Europejskiej o sumie bilansowej nie mniejszej niż 100 000 000,00 złotych (słownie: sto milionów złotych zero groszy) dla każdej usługi.

UWAGA 1

- *Jeżeli wartość usługi wskazanej w wykazie jest podana w walucie innej niż PLN, Wykonawca zobowiązany jest, na potrzeby niniejszego postępowania, dokonać przeliczenia jej wartości na PLN wg średniego kursu NBP (www.nbp.pl tabela A – tabela kursów średnich walut obcych) z dnia zakończenia usługi o zakresie jak wyżej wraz z podaniem kursu oraz daty jego obowiązywania (zgodnie z tabelą A – tabela kursów średnich walut obcych) wg których dokonano przeliczenia; w przypadku usług nadal realizowanych - wg tabeli kursów średnich walut obcych z dnia rozpoczęcia realizacji danej usługi.*
- *Zamawiający dopuszcza realizację więcej niż 1 usługi w ramach jednego zamówienia/umowy.*
- *Okresy wyrażone w latach lub miesiącach, o których mowa powyżej, liczy się wstecz od dnia, w którym upływa termin składania ofert w postępowaniu.*

UWAGA 2

W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z Wykonawców, którzy wykonają usługi, do realizacji których te zdolności są wymagane. W takiej sytuacji Wykonawca składa wraz z ofertą oświadczenie w zakresie wskazania, które usługi wykonają poszczególni Wykonawcy (członkowie konsorcjum). Wzór oświadczenia stanowi Załącznik nr 6 do SWZ – „oświadczenie o podziale obowiązków w trakcie realizacji zamówienia".

1.1.1. **dysponuje następującymi osobami,** które zostaną skierowane przez Wykonawcę do realizacji zamówienia, legitymującymi się odpowiednimi kwalifikacjami zawodowymi, wykształceniem i doświadczeniem umożliwiającymi realizację zamówienia na odpowiednim poziomie jakości, w tym co najmniej **1 (jedną) osobą, posiadającą uprawnienia biegłego rewidenta** zgodnie z ustawą z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym (Dz. U. z 2022 r. poz. 1302).

UWAGA 3

- *Zamawiający wymaga, aby świadczenie usług objętych przedmiotem zamówienia odbywało się co najmniej przez osoby wykazane przez Wykonawcę na potwierdzenie spełniania opisanego przez Zamawiającego warunku udziału w postępowaniu w zakresie osób skierowanych do realizacji zamówienia.*
- *W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia powyższy warunek musi spełniać co najmniej jeden Wykonawca lub wszyscy Wykonawcy łącznie.*

1.2. **Uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej.** Zamawiający uzna, że Wykonawca spełnia warunek udziału we wskazanym zakresie, jeżeli Wykonawca wykaże, że posiada uprawnienia do prowadzenia działalności zawodowej, wynikające z ustawy z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym (Dz. U. z 2022 r. poz. 1302) - tj. posiada wpis na listę firm audytorskich, prowadzoną przez Polską Agencję Nadzoru Audytowego.

1.3. **Sytuacji finansowej lub ekonomicznej.** Zamawiający uzna, że Wykonawca spełnia warunek udziału we wskazanym zakresie, jeżeli Wykonawca wykaże, że posiada ubezpieczenie od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na sumę gwarancyjną nie niższą niż równowartość 400 tys. EURO (słownie: czterysta tysięcy euro);

UWAGA 4

W odniesieniu do ww. warunku udziału w postępowaniu Wykonawcy wspólnie ubiegający się o udzielenie zamówienia składają wraz z ofertą oświadczenie w zakresie wskazania, które usługi wykonają poszczególni Wykonawcy (członkowie konsorcjum). Wzór oświadczenia stanowi Załącznik nr 6 do SWZ.

UWAGA 5

W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia uprawnienie musi mieć ten z Wykonawców, który będzie wykonywał czynności, do których zgodnie z przepisami wymagane jest posiadanie takiego uprawnienia.

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

Rozdział IV. Zawartość ofert, wykaz podmiotowych środków dowodowych

1. W zakresie nieuregulowanym postanowieniami SWZ zastosowanie mają przepisy rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie rodzajów podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od Wykonawcy (Dz. U. z 2020 r. poz. 2415; dalej: *„Rozporządzenie w sprawie rodzajów podmiotowych środków dowodowych"*).
2. Jeżeli Wykonawca nie złożył oświadczenia, o którym mowa w art. 125 ust. 1 ustawy, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu lub są one niekompletne lub zawierają błędy, Zamawiający wzywa Wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w terminie przez siebie wskazanym, chyba że:
   2.1. oferta Wykonawcy podlega odrzuceniu bez względu na ich złożenie, uzupełnienie lub poprawienie lub

2.2. zachodzą przesłanki unieważnienia postępowania.

IV.1. Zawartość ofert

1. Ofertę należy złożyć, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym przez osoby upoważnione do tych czynności. Wykonawca składa ofertę na Formularzu Ofertowym wg Załącznika nr 1 do SWZ **za pośrednictwem Platformy Zakupowej**.
2. Wykonawca obowiązany jest złożyć wraz z ofertą następujące dokumenty:
   2.1. Odpis lub informację z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru, w celu potwierdzenia, że osoba działająca w imieniu Wykonawcy jest umocowana do jego reprezentowania.
   2.2. Pełnomocnictwo lub inny dokument potwierdzający umocowanie osoby działającej w imieniu Wykonawcy do jego reprezentowania, jeżeli oferta nie została podpisana przez osoby upoważnione do tych czynności dokumentem rejestracyjnym.
   2.3. Dowód wniesienia wadium. Jeżeli Wykonawca wnosi wadium w formie gwarancji lub poręczenia Wykonawca przekazuje Zamawiającemu oryginał gwarancji lub poręczenia, w postaci elektronicznej. W przypadku wniesienia wadium w innej formie niż pieniądz, powinno ono obowiązywać przez cały okres związania ofertą.
   2.4. Zobowiązanie podmiotów udostępniających zasoby do oddania Wykonawcy do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie będzie dysponował niezbędnymi zasobami, jeżeli Wykonawca powołuje się na zasoby innych podmiotów. Zobowiązanie winno być podpisane przez osobę upoważnioną do reprezentacji podmiotu udostępniającego zasoby. Zapisy pkt 2.1. i 2.2. oraz Rozdz. IV.4 SWZ stosuje się odpowiednio.
   2.5. Aktualne na dzień składania ofert:
      2.5.1. Oświadczenie o braku podstaw wykluczenia. Wzór oświadczenia stanowi Załącznik nr 2 do SWZ,
      2.5.2. Oświadczenie Wykonawcy, w zakresie braku podstaw wykluczenia na podstawie art. 7 ustawy o szczególnych rozwiązaniach Wzór oświadczenia stanowi Załącznik nr 2a do SWZ,
      2.5.3. Oświadczenie o spełnianiu warunków udziału w postępowaniu. Wzór oświadczenia stanowi Załącznik nr 3 do SWZ.
   2.6. Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia w zakresie wskazania, które usługi wykonają poszczególni Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (członkowie konsorcjum). Wzór oświadczenia stanowi Załącznik nr 6 do SWZ – „oświadczenie o podziale obowiązków w trakcie realizacji zamówienia"

IV.2 Wykaz podmiotowych środków dowodowych

Zamawiający przed wyborem najkorzystniejszej oferty wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia za pośrednictwem Platformy Zakupowej, w wyznaczonym terminie, nie krótszym niż 5 dni od dnia wezwania, aktualnych na dzień złożenia podmiotowych środków dowodowych, w formie elektronicznej podpisanych kwalifikowanym podpisem elektronicznym, w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym przez osoby upoważnione do tych czynności, w poniższym zakresie:

1. braku podstaw wykluczenia Wykonawcy z postępowania o udzielenie zamówienia:
   1.1. odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
   1.2. oświadczenia Wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy, w zakresie podstaw wykluczenia z postępowania wskazanych przez zamawiającego, o których mowa w:
      1.2.1. art. 108 ust. 1 pkt 3 ustawy,
      1.2.2. art. 108 ust. 1 pkt 4 ustawy, dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego,
      1.2.3. art. 108 ust. 1 pkt 5 ustawy, dotyczących zawarcia z innymi Wykonawcami porozumienia mającego na celu zakłócenie konkurencji,
      1.2.4. art. 108 ust. 1 pkt 6 ustawy
      - sporządzone według wzoru, który stanowi Załącznik nr 4 do SWZ.
   1.3. oświadczenia Wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r. poz. 275), z innym Wykonawcą, który złożył odrębną ofertę, ofertę częściową, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej. Wzór oświadczenia stanowi Załącznik nr 5 do SWZ.
2. potwierdzenia spełniania warunków udziału w postępowaniu dotyczących zdolności zawodowej:
   2.1. wykazu usług wykonanych, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których usługi zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te usługi zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego usługi zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli

Wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów - oświadczenie Wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy. Wzór oświadczenia stanowi Załącznik nr 7 do SWZ;

2.2. wykazu osób, skierowanych przez Wykonawcę do realizacji zamówienia publicznego, w szczególności odpowiedzialnych za świadczenie usług, kontrolę jakości lub kierowanie robotami budowlanymi, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami. Wzór oświadczenia stanowi Załącznik nr 8 do SWZ;

3. potwierdzenia spełniania warunków udziału w postępowaniu dotyczących uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej:
   3.1. zaświadczenie Polskiej Agencji Nadzoru Audytowego lub innego dokumentu potwierdzającego, że Wykonawca jest wpisany na listę podmiotów uprawionych do badania sprawozdań finansowych prowadzona przez Polską Agencję Nadzoru Audytowego, zgodnie z ustawą z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym (Dz. U. z 2022 r. poz. 1302).

4. potwierdzenia spełniania warunków udziału w postępowaniu dotyczących sytuacji finansowej lub ekonomicznej:
   4.1. dokument potwierdzający, że Wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na sumę gwarancyjną określoną przez Zamawiającego.

IV.3. Podmiotowe środki dowodowe składane przez Wykonawców mających siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej

1. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast odpisu albo informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, o których mowa IV.2 pkt 1.1 SWZ – składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury.
2. Dokument lub dokumenty, o którym mowa w pkt 1 powinny być wystawione nie wcześniej niż 3 miesiące przed ich złożeniem.
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 odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument miał dotyczyć, nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy lub miejsce zamieszkania osoby, której dokument miał dotyczyć . Postanowienie pkt 2 stosuje się.

IV.4. Zasady i warunki korzystania przez Wykonawcę ze zdolności lub sytuacji innych podmiotów

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
2. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających **zasoby, składa, wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby** do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
3. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w pkt 2, potwierdza, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
   3.1. zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
   3.2. sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
   3.3. czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje usługi, których wskazane zdolności dotyczą.
4. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają usługi, do realizacji których te zdolności są wymagane.

5. Zamawiający żąda od Wykonawcy, który polega na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 118 ustawy, przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych w Rozdz. IV.2 pkt 1.1. i 1.2. SWZ. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia także oświadczenie podmiotu udostępniającego zasoby, potwierdzające spełnianie warunków udziału w postępowaniu w zakresie, w jakim Wykonawca powołuje się na jego zasoby, wymienione w Rozdz. IV.1. pkt 2.5.2. Postanowienia Rozdz. IV.2. SWZ stosuje się odpowiednio.

IV.5. Klauzule informacyjne w zakresie danych osobowych

W związku z treścią 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 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35), dalej: „RODO" Zamawiający informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w toku postępowania jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, al. Jana Pawła II 70, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazanych w pkt 1.
3. Pani/Pana dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu przeprowadzenia niniejszego postępowania o udzielenie zamówienia publicznego.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
   4.1. osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 2 ustawy,
   4.2. organy kontrolne,
   4.3. osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902 tj.),
   4.4. podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa.
5. Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do przeprowadzenia niniejszego postępowania. Ponadto, zgodnie z art. 78 ust. 1 ustawy przechowywane będą przez okres 4 lat od dnia zakończenia niniejszego postępowania. Okres przechowywania danych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora. Ponadto, okres przechowywania danych może zostać przedłużony na okres 5 lat, na potrzeby archiwizacji.
6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych.
7. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
8. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego, a konsekwencje niepodania określonych danych wynikają z ustawy.

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

1. Komunikacja między Zamawiającym, a Wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują wyłącznie za pośrednictwem Platformy Zakupowej, z zachowaniem postaci elektronicznej stosownie do obowiązujących w tym zakresie przepisów prawa. Za datę wpływu oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się ich datę wczytania do Platformy Zakupowej.
2. Postępowanie prowadzone jest pod numerem referencyjnym sprawy: **DPiZP.2619.7.2024**, Wykonawcy powinni we wszelkich kontaktach z Zamawiającym powoływać się na wskazany numer referencyjny.
3. Wykonawcy powinni kierować do Zamawiającego wszelką korespondencję z zachowaniem zasad opisanych w pkt 1, za pośrednictwem Platformy Zakupowej.
4. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SWZ. Wniosek należy przesłać za pośrednictwem Platformy Zakupowej.
5. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert. Treść pytań (bez ujawnienia źródła zapytania) wraz z wyjaśnieniami bądź informacje o dokonaniu zmiany treści SWZ, Zamawiający przekaże (opublikuje) Wykonawcom za pośrednictwem Platformy Zakupowej.
6. Jeżeli wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego po upływie terminu, o którym mowa w pkt 5 Zamawiający nie ma obowiązku udzielania wyjaśnień treści SWZ.
7. W uzasadnionym przypadku Zamawiający może przed terminem składania ofert zmienić treść dokumentów składających się na niniejszą SWZ.

8. Zamawiający nie zamierza zwoływać zebrania Wykonawców.
9. Osobami uprawnionymi ze strony Zamawiającego do kontaktów z Wykonawcami są:
   9.1. Pani Agnieszka Skarżyńska, tel.: +48 22 595 00 65 w godz. 9.00 – 15.00.
   9.2. Pani Kinga Henzel, tel.: +48 22 595 00 66 w godz. 9.00 – 15.00.

Rozdział VI. Wymagania dotyczące wadium

1. Wykonawca zobowiązany jest wnieść **wadium w wysokości 2000,00 zł** (słownie: dwa tysiące złotych 00/100).
2. Wadium może być wniesione w:
   2.1. pieniądzu;
   2.2. gwarancjach bankowych;
   2.3. gwarancjach ubezpieczeniowych;
   2.4. poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2023 r. poz. 462).
3. Wadium w formie pieniądza należy wnieść przelewem na rachunek bankowy Zamawiającego prowadzony w Banku Gospodarstwa Krajowego III Oddział w Warszawie numer rachunku – 45 1130 1062 8000 0000 0002 8175, z dopiskiem na przelewie: **„wadium w postępowaniu na Przeprowadzenie badania sprawozdania finansowego ARiMR za lata 2024-2025".**
4. W przypadku wnoszenia wadium w innej formie gwarancji lub poręczenia, o których mowa w pkt 2.2.-2.4., Wykonawca przekazuje Zamawiającemu oryginał gwarancji lub poręczenia, w postaci elektronicznej poprzez wczytanie na Platformie Zakupowej. Wadium powinno być oznaczone w następujący sposób: WADIUM – numer referencyjny sprawy, nazwa postępowania lub w inny sposób umożliwiający identyfikację postępowania, którego dotyczy.
5. Dokument wadialny (gwarancja lub poręczenie) musi wyraźnie wskazywać na wszystkie okoliczności jego utraty określone w art. 98 ust. 6 ustawy.
6. Z treści gwarancji/poręczenia powinno wynikać bezwarunkowe, na każde pisemne żądanie zgłoszone przez Zamawiającego, zobowiązanie Gwaranta do wypłaty Zamawiającemu pełnej kwoty wadium w okolicznościach określonych w art. 98 ust. 6 ustawy.
7. Oferta Wykonawcy, który nie wniósł wadium lub wniósł w sposób nieprawidłowy lub nie utrzymywał wadium nieprzerwanie do upływu terminu związania ofertą lub złożył wniosek o zwrot wadium w przypadku, o którym mowa w art. 98 ust. 2 pkt 3 ustawy zostanie odrzucona.
8. W przypadku wniesienia wadium i niezłożenia oferty, Wykonawca jest zobowiązany złożyć do Zamawiającego wniosek o zwrot wadium.

Rozdział VII. Termin związania ofertą

Wykonawcy pozostają związani złożoną ofertą **do dnia 27.07.2024 r.** Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

Rozdział VIII Opis sposobu przygotowywania ofert

VIII.1. Przygotowanie ofert

1. Ofertę należy złożyć pod rygorem nieważności w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym przez osoby upoważnione do tych czynności. Wykonawca składa ofertę na Formularzu Ofertowym (wg Załącznika nr 1 do SWZ).
2. Treść złożonej oferty musi być zgodna z warunkami zamówienia. Wykonawca ma prawo złożyć tylko jedną ofertę. Oferta powinna być sporządzona w języku polskim, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym. Ofertę należy złożyć wyłącznie za pośrednictwem Platformy Zakupowej.
3. Oferta powinna zawierać jedną, jednoznacznie opisaną propozycję.
4. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.
5. Zamawiający informuje, iż zgodnie z art. 74 ust. 1 i 2 ustawy oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu niezwłocznie po otwarciu ofert, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeśli Wykonawca nie później niż w terminie składania ofert zastrzegł, że nie mogą one być udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji określonych w art. 222 ust. 5 ustawy, tj. nazw albo imion i nazwisk oraz siedzib lub miejsc prowadzonej działalności gospodarczej albo miejsc zamieszkania Wykonawców, których oferty zostały otwarte, cen lub kosztów zawartych w ofertach.
   Uwaga:
   Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), które Wykonawca zamierza zastrzec jako tajemnicę przedsiębiorstwa, muszą zostać odpowiednio oznaczone a następnie załączone na Platformie Zakupowej w osobnym pliku w miejscu właściwym dla Informacji stanowiących tajemnicę przedsiębiorstwa.
6. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia, w takim przypadku:
   6.1. oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia musi być podpisana w taki sposób, by prawnie zobowiązywała wszystkich Wykonawców występujących wspólnie,

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

VIII.2. Forma dokumentów składanych w postępowaniu

1. Wszystkie dokumenty wchodzące w skład oferty oraz składane w trakcie postępowania należy złożyć na Platformie Zakupowej
   w postaci elektronicznej, podpisane kwalifikowanym podpisem elektronicznym, wystawionym przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne – podpis elektroniczny spełniający wymogi bezpieczeństwa określone w ustawie z dnia 5 września 2016 r. – o usługach zaufania oraz identyfikacji elektronicznej (tj. Dz. U. z 2021 r. poz. 1797), podpisem zaufanym lub osobistym.
2. Dokumenty i oświadczenia wchodzące w skład oferty oraz składane w trakcie postępowania, sporządzone w językach obcych muszą być złożone wraz z tłumaczeniami na język polski.
3. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, w tym dokumenty, o których mowa w art. 94 ust. 2 ustawy, lub dokumenty potwierdzające umocowanie do reprezentowania odpowiednio Wykonawcy, Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, podmiotu udostępniającego zasoby na zasadach określonych w art. 118 ustawy lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach, zwane dalej *„dokumentami potwierdzającymi umocowanie do reprezentowania"*, zostały wystawione przez upoważnione podmioty inne niż Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, zwane dalej *„upoważnionymi podmiotami"*, jako dokument elektroniczny, przekazuje się ten dokument.
4. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, w tym dokumenty, o których mowa w art. 94 ust. 2 ustawy, lub dokumenty potwierdzające umocowanie do reprezentowania, zostały wystawione przez upoważnione podmioty jako dokument w postaci papierowej, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
5. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt 4, dokonuje w przypadku:
   5.1. podmiotowych środków dowodowych oraz dokumentów potwierdzających umocowanie do reprezentowania – odpowiednio Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych lub dokumentów potwierdzających umocowanie do reprezentowania, które każdego z nich dotyczą;
   5.2. innych dokumentów, w tym dokumentów, o których mowa w art. 94 ust. 2 ustawy – odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia, w zakresie dokumentów, które każdego z nich dotyczą.
6. Podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, dokumenty, o których mowa w art. 94 ust. 2 ustawy, niewystawione przez upoważnione podmioty, oraz pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
7. W przypadku gdy podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, dokumenty, o których mowa w art. 94 ust. 2 ustawy, niewystawione przez upoważnione podmioty lub pełnomocnictwo, zostały sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
8. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt 7, dokonuje w przypadku:
   8.1. podmiotowych środków dowodowych – odpowiednio Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych, które każdego z nich dotyczą;
   8.2. zobowiązania podmiotu udostępniającego zasoby – odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia;
   8.3. pełnomocnictwa – mocodawca.
9. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt 4 i 7, może dokonać również notariusz.

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

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

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

1. Ofertę pod rygorem nieważności należy złożyć w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym. Oferta musi zostać podpisana przez osoby upoważnione do tych czynności. Ofertę należy złożyć na Platformie Zakupowej udostępnionej przez Zamawiającego na stronie internetowej: https://platformazakupowa.pl/pn/arimr.
2. Termin składania ofert upływa w dniu **28.06.2024 r. o godzinie 10.00.**
3. Otwarcie ofert odbędzie się w dniu **28.06.2024r. o godzinie 11.00.**
4. Zamawiający nie bierze odpowiedzialności za nieprawidłowe złożenie oferty wynikające z niezastosowania się przez Wykonawcę do wymagań niniejszej SWZ.

IX.2. Warunki zmiany i wycofania złożonej oferty

1. Wykonawca posiadający konto na Platformie Zakupowej, za jej pośrednictwem może przed upływem terminu składania ofert samodzielnie zmienić lub wycofać ofertę.
2. Wykonawca nieposiadający 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 Operatora 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 ceny ofertowej netto, należnego podatku od towarów i usług VAT oraz ceny ofertowej brutto, w sposób określony w Formularzu Ofertowym stanowiącym Załącznik nr 1 do SWZ.
2. W Formularzu Ofertowym Wykonawca zobowiązany jest podać łączną cenę za realizację całego zamówienia wraz z podziałem ceny za poszczególne badania sprawozdania finansowego:
   2.1. za wykonanie badania sprawozdania finansowego ARiMR za rok 2024 (za okres od 1 stycznia do 31 grudnia 2024 r.);
   2.2. za wykonanie badania sprawozdania finansowego ARiMR za rok 2025 (za okres od 1 stycznia do 31 grudnia 2025r.)
3. Ceny określone w Formularzu Ofertowym powinny zawierać wszystkie koszty związane z wykonaniem przedmiotu zamówienia. Podane ceny nie podlegają zmianom przez okres obowiązywania umowy, z zastrzeżeniem postanowień Rozdz. XIV pkt 4 niniejszej SWZ.
4. 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).
5. Wszystkie ceny podane w Formularzu Ofertowym powinny być wyrażone w złotych polskich.
6. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający dla celów zastosowania kryterium ceny lub kosztu doliczy do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć. Wykonawca, składając ofertę, obowiązany jest do poinformowania Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku, wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.

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

1. Przy wyborze oferty najkorzystniejszej Zamawiający będzie się kierował poniższymi kryteriami:
   1.1. kryterium **cena (P_C)** – waga **100% (100,00 pkt)**, wg poniższego wzoru:

$$P_C = \frac{C_{min.}}{C_b} \text{ x } 100{,}00 \text{ pkt},$$

gdzie:

P_C – ilość punktów oferty badanej w kryterium cena

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

C_b – cena oferty badanej.

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

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

Rozdział XIV. Informacje dotyczące umowy w sprawie zamówienia publicznego

1. Zawarcie umowy nastąpi wg treści projektowanych postanowień umowy w sprawie zamówienia publicznego, stanowiących Załącznik nr 9 do niniejszej SWZ.
2. Postanowienia ustalone w projektowanych postanowieniach umowy nie podlegają negocjacjom.
3. Przyjęcie niniejszych projektowanych postanowień umowy stanowi jeden z istotnych warunków przyjęcia oferty.
4. Zamawiający dopuszcza zmiany postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy. Warunki zmian zostały opisane przez Zamawiającego w projektowanych postanowieniach umowy wraz z załącznikami, stanowiących Załącznik nr 9 do SWZ.
5. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza zobowiązany będzie do udzielenia Zamawiającemu wszelkich informacji oraz złożenia oświadczeń i dokumentów niezbędnych do ustalenia czy:
   5.1. aktualne pozostaje niepodleganie wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 7 ustawy o szczególnych rozwiązaniach.

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

1. Wykonawcom, którzy mają lub mieli interes w uzyskaniu danego zamówienia oraz ponieśli lub mogą ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy przysługują środki ochrony prawnej określone w dziale IX ustawy.
2. Odwołanie przysługuje na:
   2.1. niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienia umowy;

2.2. zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której zamawiający był obowiązany na podstawie ustawy.

3. Odwołanie winno zawierać informacje określone w art. 516 ust. 1 ustawy, w szczególności wskazanie czynności lub zaniechania czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy.
4. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej. Pisma w postępowaniu odwoławczym wnosi się w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej, z tym że odwołanie i przystąpienie do postępowania odwoławczego, wniesione w postaci elektronicznej, wymagają opatrzenia podpisem zaufanym.
5. Odwołujący przekazuje Zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, że Zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przekazanie odpowiednio odwołania albo jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
6. Odwołanie wnosi się w terminie:
   6.1 5 (pięciu) dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przesłane przy użyciu środków komunikacji elektronicznej;
   6.2 10 (dziesięciu) dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przekazane w inny sposób niż określony w pkt 6.1.;
7. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie lub wobec treści dokumentów zamówienia wnosi się w terminie:
   7.1. 5 (pięciu) dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub dokumentów zamówienia na stronie internetowej.
8. Odwołanie w przypadkach innych niż określone w pkt 6 i 7 wnosi się w terminie:
   8.1. 5 (pięciu) dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.

Załączniki do SWZ:

1. Załącznik nr 1 – Wzór Formularza Ofertowego
2. Załącznik nr 2 – Wzór Oświadczenia własnego oraz Oświadczenia o braku podstaw wykluczenia
3. Załącznik nr 2a – Wzór Oświadczenia o braku podstaw wykluczenia – art. 7 ustawy o szczególnych rozwiązaniach
4. Załącznik nr 3 – Wzór Oświadczenia dotyczącego spełniania warunków udziału w postępowaniu
5. Załącznik nr 4 – Wzór Oświadczenia o braku podstaw wykluczenia
6. Załącznik nr 5 – Wzór Oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej
7. Załącznik nr 6 – Wzór Oświadczenia o podziale obowiązków w trakcie realizacji zamówienia
8. Załącznik nr 7 – Wzór Oświadczenia – Wykaz usług
9. Załącznik nr 8 – Wzór Oświadczenia – Wykaz osób
10. Załącznik nr 9 – Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do umowy w sprawie zamówienia publicznego

PREZES

Wojciech Legawiec

Zatwierdzam SWZ wraz z załącznikami: Warszawa, 13. 06..2024 r. .....

podpis Zamawiającego

Załącznik nr 1 do SWZ – wzór Formularza Ofertowego

Formularz Ofertowy
DPiZP.2619.7.2024

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

W odpowiedzi na ogłoszone postępowanie prowadzone w trybie podstawowym na **„Przeprowadzenie badania sprawozdania finansowego ARiMR za lata 2024 -2025"**, zgodnie z wymaganiami określonymi w specyfikacji warunków zamówienia i projektowanych postanowieniach umowy wraz z załącznikami, oferuję(-emy) realizację przedmiotu zamówienia, za cenę:

Lp.	Przedmiot zamówienia	Cena ofertowa netto [PLN]	Podatek VAT		Cena ofertowa brutto [PLN]
			(%)	PLN	
[a]	[b]	[c]	[d]	[e]=[c]x[d]	[f]=[c]+[e]
1.	Przeprowadzenie badania sprawozdania finansowego i ksiąg rachunkowych za rok 2024				
2	Przeprowadzenie badania sprawozdania finansowego i ksiąg rachunkowych za rok 2025				
	SUMA		X		

Łączna cena ofertowa (wartość wynagrodzenia) netto zł (słownie) _____

Łączna cena ofertowa (wartość wynagrodzenia) brutto zł (słownie) _____

Oświadczamy, że:

1. Zapoznaliśmy się z treścią specyfikacji warunków zamówienia (SWZ), w tym projektowanych postanowień umowy i nie wnosimy do nich zastrzeżeń oraz przyjmujemy warunki w nich zawarte.
2. Realizację przedmiotu zamówienia wykonamy w terminach określonych w Rozdz. II SWZ oraz projektowanych postanowieniach umowy.
3. W cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia.
4. Uważamy się za związanych niniejszą ofertą do terminu określonego w SWZ.
5. Wadium w wysokości **2000,00 zł** (słownie dwa tysiące złotych 00/100) wnieśliśmy przed upływem terminu składania ofert.
6. Wadium wniesione w formie pieniądza należy zwrócić na rachunek bankowy nr .....prowadzony w banku ..... Oświadczenie o zwolnieniu wadium wniesionego w innej formie niż pieniądz należy przekazać gwarantowi/poręczycielowi na następujący adres e-mail.....
7. Zobowiązujemy się do wniesienia przed podpisaniem umowy zabezpieczenia należytego wykonania umowy w wysokości **2 %** ceny całkowitej podanej w ofercie.
8. W przypadku udzielenia nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.
9. Podwykonawcom zamierzamy powierzyć wykonanie następującej(-ych) części zamówienia (należy podać zakres prac oraz nazwę Podwykonawcy, jeśli jest już znany):
   9.1. .....[1]

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

UWAGA:

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

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

10. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na poniższy adres e-mail: .....
    Dane kontaktowe: imię i nazwisko ....., nr tel. ....., adres e-mail: .....
11. Dokumenty wymienione od strony ..... do strony ..... stanowią tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2021 r. poz. 1913) i nie mogą być ujawnione pozostałym uczestnikom postępowania.

    UWAGA:

    Zamawiający przypomina, że stosownie do treści:
    - *art. 18 ust. 3 ustawy Wykonawca winien nie później niż w terminie składania dokumentów wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa*
    - *Rozdz. VIII.1. pkt 5 SWZ wszelkie informacje stanowiące tajemnicę przedsiębiorstwa muszą zostać odpowiednio oznaczone a następnie załączone na Platformie Zakupowej w osobnym pliku w miejscu właściwym dla Informacji stanowiących tajemnicę przedsiębiorstwa.*
12. Wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO)[2] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.[3]

    [2] *rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35).*

    [3] *w przypadku, gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie ma obowiązku składać (w takim przypadku Wykonawca może usunąć treści oświadczenia np. przez jego wykreślenie, przekreślenie, itp.).*
13. Jednocześnie, zgodnie z treścią art. 225 ust. 2 ustawy oświadczam, że wybór niniejszej oferty:
    13.1. **nie będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego[4]
    13.2. **będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, w związku z tym:[4]

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

    [5] *W pkt 13.2.1. należy wskazać: nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego, wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku, stawkę podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.*
14. Zgodnie z Rozdz. IV.1. SWZ do oferty zostają załączone dokumenty:
    14.1. .....
    14.2. .....
    14.3. .....
    14.4. .....
    14.5. .....

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

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

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

Oświadczenie własne oraz Oświadczenie o braku podstaw wykluczenia
DPIZP.2619.7.2024

Przystępując do udziału w postępowaniu o zamówienie publiczne na **„Przeprowadzenie badania sprawozdania finansowego ARiMR za lata 2024 -2025"** składam oświadczenia:

CZĘŚĆ A – Oświadczenie własne Wykonawcy.
Wykonawca oświadcza, że jest:[1]
1. Mikroprzedsiębiorstwem: tak/nie[2]
2. Małym przedsiębiorstwem: tak/nie[2]
3. Średnim przedsiębiorstwem: tak/nie[2]

Uwaga
[1] *Zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.Urz. L 124 z 20.5.2003, s. 36). Te informacje są wymagane wyłącznie do wypełnienia ogłoszenia o udzieleniu zamówienia (do celów statystycznych).*
Mikroprzedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EUR.
Małe przedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR.
Średnie przedsiębiorstwa: przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami i które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów EUR lub roczna suma bilansowa nie przekracza 43 milionów EUR.
[2] ***niepotrzebne skreślić.***

CZĘŚĆ B – Oświadczenie Wykonawcy dotyczące przesłanek wykluczenia z postępowania, o którym mowa w art. 125 ust. 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2023 poz. 1605 ze zm.; dalej: *„ustawa"*)
Oświadczam(-y), że:
1. nie podlegam(-y) wykluczeniu z postępowania na podstawie art. 108 ust 1 pkt 1-6 ustawy,
2. nie podlegam(-y) wykluczeniu z postępowania na podstawie art. 109 ust. 1 pkt 4 ustawy.
3. Oświadczam(-y), że zachodzą w stosunku do mnie (nas) podstawy wykluczenia z postępowania na podstawie art. ..... ustawy (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2, 5 lub art. 109 ust. 1 pkt 4 ustawy). Jednocześnie oświadczam(-y), że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy podjąłem(-ęliśmy) następujące środki naprawcze: .....[3]

Uwaga
[3] *Wykonawca wypełnia pkt 3. wyłącznie w przypadku, gdy go dotyczy*

CZĘŚĆ C – Oświadczenie Wykonawcy dotyczące informacji podanych w CZĘŚCI B
Oświadczam(-y), że wszystkie informacje podane w oświadczeniach w CZĘŚCI B są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

Załącznik nr 2a do SWZ – wzór Oświadczenia o braku podstaw wykluczenia na podstawie art. 7 ustawy o szczególnych rozwiązaniach

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

Oświadczenie braku podstaw wykluczenia na podstawie art. 7 ustawy o szczególnych rozwiązaniach

DPiZP.2619.7.2024

Przystępując do udziału w postępowaniu o zamówienie publiczne na **„Przeprowadzenie badania sprawozdania finansowego ARiMR za lata 2024 -2025"** oświadczam(-y), że na dzień złożenia niniejszego oświadczenia nie podlegam(-y) wykluczeniu na podstawie na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t.j. Dz.U. z 2023 poz. 129 ze zm.) tj.:

1) Nie jestem wykonawcą wymienionym w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanym na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającą o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy o szczególnych rozwiązaniach;

2) Nie jestem wykonawcą, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593, 655, 835, 2180 i 2185) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy o szczególnych rozwiązaniach;

3) Nie jestem wykonawcą, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120 z późn. zm.) jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy o szczególnych rozwiązaniach.

*Niepotrzebne skreślić

Załącznik nr 3 do SWZ – wzór Oświadczenia dotyczącego spełniania warunków udziału w postępowaniu

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

Oświadczenie dotyczące spełniania warunków udziału w postępowaniu, o którym mowa w art. 125 ust. 1 z dnia 11 września 2019 r. – Prawo zamówień publicznych
DPIZP.2619.7.2024

CZĘŚĆ A
Przystępując do udziału w postępowaniu o zamówienie publiczne na **„Przeprowadzenie badania sprawozdania finansowego ARiMR za lata 2024 -2025"** oświadczam(-y), że spełniam(-y) warunki udziału w postępowaniu określone przez Zamawiającego w Rozdziale III.2. SWZ.

CZĘŚĆ B - informacja w związku z poleganiem na zasobach innych podmiotów[1]:
Oświadczam(-y), że w celu wykazania spełniania warunków udziału w ww. postępowaniu, określonych przez Zamawiającego w Rozdziale III pkt 1.2 SWZ, polegam(-y) na zasobach następującego/ych podmiotu/ów[2]:

1. ..... *(podać firmę i adres podmiotu)*, w następującym zakresie: ..... *(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu);*
2. ..... *(podać firmę i adres podmiotu)*, w następującym zakresie: ..... *(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu).*

Uwaga:
[1] *Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia, wraz z oświadczeniem własnym, także oświadczenie podmiotu udostępniającego zasoby, potwierdzające spełnianie warunków udziału w postępowaniu w zakresie, w jakim Wykonawca powołuje się na jego zasoby.*
[2] *Wymienić wszystkie inne podmioty i dla każdego odrębnie wymienić zasoby, które udostępnia on Wykonawcy.*

CZĘŚĆ C – Oświadczenie Wykonawcy dotyczące informacji podanych w CZĘŚCI A oraz CZĘŚCI B
Oświadczam(-y), że wszystkie informacje podane w oświadczeniach w CZĘŚCI A oraz CZĘŚCI B są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

Załącznik nr 4 do SWZ – wzór Oświadczenia o braku podstaw wykluczenia

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

Oświadczenie o braku podstaw wykluczenia

DPIZP.2619.7.2024

Przystępując do udziału w postępowaniu o zamówienie publiczne na **„Przeprowadzenie badania sprawozdania finansowego ARiMR za lata 2024 -2025"** oświadczam(-y), że na dzień złożenia niniejszego oświadczenia aktualne pozostają informacje zawarte w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy, tj. nie podlegam(-y) wykluczeniu na podstawie:

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

Załącznik nr 5 do SWZ – wzór Oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej
DPIZP.2619.7.2024

Przystępując do udziału w postępowaniu o zamówienie publiczne na „**Przeprowadzenie badania sprawozdania finansowego ARiMR za lata 2024 -2025**" oświadczam(-y), że:

1. **nie należę(-ymy) do grupy kapitałowej** w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j.: Dz. U. z 2023 r., poz. 1689 ze zm.) **z żadnym z Wykonawców, którzy złożyli odrębną ofertę w przedmiotowym postępowaniu** o udzielenie zamówienia publicznego[1].
2. **należę(-ymy) do grupy kapitałowej** w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j.: Dz. U. z 2023 r., poz. 1689 ze zm) **z następującymi Wykonawcami, którzy złożyli odrębną ofertę w przedmiotowym postępowaniu** o udzielenie zamówienia publicznego[1]:

Lp.	Nazwa podmiotu	Siedziba
1		
(...)		

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

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

UWAGA:
[1] niepotrzebne skreślić

Załącznik nr 6 do SWZ – wzór Oświadczenia o podziale obowiązków w trakcie realizacji zamówienia

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

DPIZP.2619.7.2024

Działając w imieniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia: .....[1], przystępując do udziału w postępowaniu o zamówienie publiczne na **„Przeprowadzenie badania sprawozdania finansowego ARiMR za lata 2024 -2025"** oświadczam(-y), że wyszczególnione poniżej dostawy/usługi zostaną zrealizowane zgodnie z poniższym:

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

UWAGA:

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

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

Załącznik nr 7 do SWZ – wzór Oświadczenia – Wykaz usług
[warunek udziału w postępowaniu]

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

Oświadczenie – Wykaz usług
DPIZP.2619.7.2024

Przystępując do udziału w postępowaniu o zamówienie publiczne na **„Przeprowadzenie badania sprawozdania finansowego ARiMR za lata 2024 -2025”,** składam(-y) wykaz usług wykonanych (wykonywanych) w okresie ostatnich pięciu lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, na potwierdzenie spełniania warunku udziału w postępowaniu, o którym mowa w Rozdz. III.2. pkt 1.1.1. SWZ.

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

Uwaga do kol. [7]:
1. *Do wykazu należy dołączyć dowody potwierdzające, że powyższe usługi zostały wykonane lub są wykonywane należycie, tj.:*
   - 1.1. *referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonywane lub są wykonywane należycie, z tym, że w odniesieniu do nadal wykonywanych usług okresowych lub ciągłych referencje bądź inne dokumenty powinny być wydane nie wcześniej niż 3 m-ce przed upływem terminu składania ofert;*
   - 1.2. *oświadczenie Wykonawcy - jeżeli z uzasadnionych przyczyn o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać dokumentów, o którym mowa wyżej w pkt 1.1;*
2. *Należy wpisać nazwę dowodu (dokumentu) potwierdzającego, że usługi zostały wykonane lub są wykonywane należycie (podać numer strony);*

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 Rozdz. III.2. pkt 1.1.1.SWZ, Wykonawca może polegać na zasobach innego podmiotu, na zasadach określonych w art. 118 Ustawy. W tym celu Wykonawca składa dokumenty i oświadczenia zgodnie z zasadami określonymi w Rozdz. IV.4. SWZ.*

Załącznik nr 8 do SWZ – wzór Oświadczenia — Wykaz osób
[warunek udziału w postępowaniu]

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

Oświadczenie – Wykaz osób
skierowanych przez Wykonawcę do realizacji zamówienia publicznego
DPiZP.2619.7.2024

Przystępując do udziału w postępowaniu o zamówienie publiczne na **„Przeprowadzenie badania sprawozdania finansowego ARiMR za lata 2024 -2025”,** składam(-y) wykaz osób, które skieruję(-emy) do realizacji niniejszego zamówienia, na potwierdzenie spełniania warunku udziału w postępowaniu, o którym mowa w Rozdz. III.2. pkt 1.1.2. SWZ:

Nazwisko i imię osoby, która będzie skierowana do realizacji zamówienia publicznego, w szczególności odpowiedzialna za świadczenie usług, według wymagań wskazanych w Rozdziale III.2, pkt 1.1.2.1 SWZ	**Zakres wykonywanych czynności**	**Czy ta osoba jest biegłym rewidentem, uprawnionym do badania sprawozdań finansowych, wpisanym do rejestru biegłych rewidentów, o którym mowa w ustawie z dnia**	**Dysponujemy osobą na podstawie art. 118 ustawy Pzp**
1. ..... (imię i nazwisko)	Biegły rewident	tak/nie* *niewłaściwe skreślić	tak/nie* **niewłaściwe skreślić*

Załącznik nr 9 do SWZ – projektowane postanowienia umowy

UMOWA nr ...../DK/202../.....

zawarta w dniu..... 202.. r. w Warszawie pomiędzy:

Agencją Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie i adresem przy Al. Jana Pawła II nr 70, 00-175 Warszawa, REGON Nr 010613083, zarejestrowanym podatnikiem podatku od towarów i usług, NIP 526-19-33-940, zwaną dalej „**ARiMR**" lub „Zamawiającym" reprezentowaną przez:

Pana Wojciecha Legawca – Prezesa Agencji Restrukturyzacji i Modernizacji Rolnictwa,
a
..... z siedzibą w ..... i adresem: ....., wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla ..... pod Nr KRS ....., REGON: ....., NIP: ....., o kapitale zakładowym w wysokości ..... zł, zwaną dalej: **„Wykonawcą"**, reprezentowaną przez:

.....

zwanych łącznie „Stronami"

zgodnie z dyspozycją przepisu art. 66 ust. 5 ustawy z dnia 29 września 1994 r. o rachunkowości, w rezultacie wyboru oferty w postępowaniu o udzielenie zamówienia w trybie podstawowym, zgodnie z art. 275 pkt. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605 z późn. zm.) została zawarta umowa, zwana dalej „umową" o następującej treści:

§ 1.

1. Na podstawie niniejszej umowy ARiMR zleca a Wykonawca przyjmuje do realizacji przeprowadzenie badania sprawozdania finansowego ARiMR, za lata: 2024, 2025 obejmującego sprawozdania finansowe: działalności krajowej, SAPARD, SPO „Restrukturyzacja i modernizacja sektora żywnościowego oraz rozwój obszarów wiejskich 2004-2006", SPO „Rybołówstwo i przetwórstwo ryb 2004-2006", Programu Operacyjnego „Zrównoważony rozwój sektora rybołówstwa i nadbrzeżnych obszarów rybackich 2007-2013", Programu Operacyjnego „Rybactwo i Morze" na lata 2014-2020, Programu Rozwoju Obszarów Wiejskich na lata 2007-2013, Programu Rozwoju Obszarów Wiejskich na lata 2014-2020, Programów dotyczących Wspólnej Polityki Rolnej, Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury na lata 2021–2027, Planu Strategicznego dla Wspólnej Polityki Rolnej w ramach EFRROW na lata 2023-2027 oraz Krajowego Planu Odbudowy i Zwiększania Odporności w ramach agencji płatniczej sporządzonych według stanu na dzień 31.12.2024 r., 31.12.2025 r. oraz stanowiących ich podstawę ksiąg rachunkowych ARiMR.
2. Badanie sprawozdań finansowych zostanie przeprowadzone zgodnie z:
   1) ustawą z dnia 29.09.1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120 z późn. zm.);
   2) ustawą z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym (Dz. U. z 2023 r. poz. 1015 z późn. zm.) z uwzględnieniem bieżących zmian w przepisach prawnych;
   3) Krajowymi Standardami Rewizji Finansowej w brzmieniu Międzynarodowych Standardów Badań;
   4) kodeksem etyki zawodowych księgowych Międzynarodowej Federacji Księgowych IFAC.
3. Wyniki badania sprawozdań finansowych zostaną wyrażone przez Wykonawcę w postaci sprawozdania z badania, o tym czy sprawozdanie finansowe jest prawidłowe oraz rzetelnie i jasno przedstawia sytuację majątkową i finansową jak też wynik finansowy ARiMR. Sprawozdanie z badania powinno w szczególności odpowiadać wymogom określonym w art. 83 ustawy z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym, z zastrzeżeniem § 7 umowy.
4. Oferta Wykonawcy stanowi integralną część umowy jako załącznik nr 2 do umowy.

§ 2.

Badanie sprawozdań finansowych za lata: 2024, 2025 oraz ksiąg rachunkowych, o których mowa w § 1 ust. 1 umowy zostanie przeprowadzone w terminach:
1) za rok 2024 – do dnia 25.04.2025 r. i udokumentowane przekazaniem sprawozdania z badania, sporządzonego w formie elektronicznej, przy czym przez zakończenie badania rozumie się wydanie sprawozdania z badania,
2) za rok 2025 – do dnia 24.04.2026 r. i udokumentowane przekazaniem sprawozdania z badania, sporządzonego w formie elektronicznej, przy czym przez zakończenie badania rozumie się wydanie sprawozdania z badania.

§ 3.

1. Wykonawca zobowiązuje się wykonać wynikające z niniejszej umowy zobowiązania z należytą starannością zawodową oraz zobowiązuje się do zachowania w tajemnicy wszelkich informacji finansowych, danych i dokumentów, w których posiadanie wszedł w związku z realizacją niniejszej umowy, przy czym obowiązek zachowania tajemnicy nie jest ograniczony w czasie.
2. Wykonawca zobowiązany jest do posiadania – przez cały okres obowiązywania umowy – ważnego ubezpieczenia od odpowiedzialności cywilnej podmiotów uprawnionych do badania sprawozdań finansowych, zgodnie z ustawą z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz o nadzorze publicznym (Dz. U. z 2023 r. poz. 1015 z późn. zm). Minimalna suma gwarancyjna przedmiotowego ubezpieczenia odpowiedzialności cywilnej powinna być zgodna z wymogami rozporządzenia Ministra Rozwoju i Finansów z dnia 7 listopada 2017 r. w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej firmy audytorskiej (Dz. U. z 2017 r., poz. 2074).
3. Dokumentacja rewizyjna (zwana „dokumentacją") z badania sprawozdań finansowych będzie przechowywana przez Wykonawcę i ARiMR przez 5 lat od daty przekazania sprawozdania z badania.
4. Wykonawca zobowiązuje się do przestrzegania przy wykonywaniu umowy przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35), zwanego dalej: „RODO", oraz przepisów krajowych wydanych w związku z tym rozporządzeniem.
5. Wykonawca pisemnie zobowiąże pracowników i osoby trzecie realizujące zobowiązania określone w umowie do przestrzegania przepisów, o których mowa w ust. 4.
6. Wykonawca zobowiązuje się do zapoznania się i przestrzegania przyjętych u Zamawiającego zasad bezpieczeństwa informacji, których treść została określona w Załączniku nr 5 „Regulamin użytkownika" i nr 12 (Regulamin eksploatacji systemów teleinformatycznych (ICT)) do Polityki bezpieczeństwa informacji w ARiMR stanowiącej Załącznik do Zarządzenia nr 7/2019 Prezesa Agencji Restrukturyzacji i Modernizacji Rolnictwa w sprawie wprowadzenia Polityki bezpieczeństwa w Agencji Restrukturyzacji i Modernizacji Rolnictwa (z późn. zm.), zwanej dalej: „Polityka bezpieczeństwa informacji w ARiMR"
7. Wykonawca pisemnie zobowiąże pracowników i osoby trzecie realizujące zobowiązania określone w Umowie do przestrzegania przepisów, o których mowa w ust. 6.
8. Wykonawca oświadcza, że zapoznał się z klauzulami informacyjnymi w zakresie przetwarzania danych osobowych, stanowiącymi Załączniki nr 3, 5 i 6 do Umowy (o ile znajdują zastosowanie), a także poinformował podwykonawców i osoby wyznaczone do kontaktów roboczych oraz odpowiedzialne za koordynację i realizację Umowy o treści Załącznika nr 7 (o ile znajduje zastosowanie).
9. Wykonawca zobowiązuje się do złożenia oświadczenia o wypełnieniu obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane bezpośrednio lub pośrednio pozyskał w celu zawarcia oraz wykonania Umowy, zgodnie z wzorem oświadczenia stanowiącym Załącznik nr 4 do Umowy.
10. Za każdy stwierdzony przypadek naruszenia obowiązków, o których mowa w § 3 ust. 1 – 2,4 - 7 Zamawiającemu przysługuje względem Wykonawcy kara umowna w wysokości 1 % wartości brutto przedmiotu umowy wskazanej w § 6 ust. 1.W przypadku powstania szkody przenoszącej wysokość zastrzeżonej kary umownej, Zamawiający może również dochodzić odszkodowania na zasadach ogólnych.
11. Jeżeli nieprawidłowości wskazane w ust. 1-2, 4-7 zostaną ponownie stwierdzone, Zamawiającemu, niezależnie od dochodzenia kary umownej i odszkodowania na zasadach ogólnych, przysługuje uprawnienie do wypowiedzenia umowy ze skutkiem natychmiastowym.
12. W przypadku naliczenia kary umownej, Zamawiający może według własnego wyboru:
    1) potrącać karę umowną z łącznego wynagrodzenia za wykonanie umowy, o którym mowa w § 6 Umowy,
    2) wezwać Wykonawcę do zapłaty kary umownej w terminie 14 dni od dnia doręczenia pisemnego wezwania do jej zapłaty.

§ 4.

ARiMR zobowiązuje się:

1) udostępnić Wykonawcy sprawozdania finansowe, księgi rachunkowe, a także inne dokumenty wymagane przez biegłych rewidentów;
2) udzielić Wykonawcy wyczerpujących wyjaśnień i informacji niezbędnych do przeprowadzenia badania sprawozdań finansowych;
3) udzielić Wykonawcy niezbędnych informacji dotyczących spraw przygotowanych do postępowania sądowego oraz znajdujących się w toku tego postępowania;
4) do terminowego sporządzenia oświadczeń na temat kompletności ujęcia danych w księgach rachunkowych, ujawnienia wszelkich zobowiązań warunkowych oraz zdarzeń jakie nastąpiły po dacie bilansu, a także innych zdarzeń, rzutujących na rzetelność oraz prawidłowość sprawozdań finansowych i ksiąg rachunkowych, których drogą badania sprawozdań finansowych nie da się ustalić;

i informuje, że księgowanie dokumentów w zakresie działalności krajowej odbywa się w Centrali ARiMR i 16 Oddziałach Regionalnych. Dokumenty źródłowe gromadzone są w Centrali w zakresie dokumentów źródłowych księgowanych przez Centralę i w 16 Oddziałach Regionalnych w zakresie dokumentów źródłowych księgowanych przez Oddziały Regionalne.

§ 5.

Podstawę przyjęcia przez ARiMR sprawozdania z badania stanowić będzie każdorazowo protokół zdawczo – odbiorczy podpisany przez Wykonawcę i ARiMR bez zastrzeżeń po przeprowadzeniu przez Wykonawcę badania sprawozdań finansowych oraz ksiąg rachunkowych, w terminach określonych w §2 pkt 1 - 2 umowy, z zastrzeżeniem § 7 umowy.

§ 6.

1. Łączne wynagrodzenie Wykonawcy z tytułu przeprowadzenia badania sprawozdania finansowego i ksiąg rachunkowych, o których mowa w § 1 ust. 1 umowy, strony ustalają na kwotę ..... netto zł (słownie złotych: .....) plus należny podatek od towarów i usług VAT w wysokości ..... zł, co daje łącznie kwotę wynagrodzenia brutto ..... zł (słownie złotych: .....).
2. Wynagrodzenie, o którym mowa w ust. 1 płatne będzie odpowiednio:
   2.1. Za przeprowadzenie badania sprawozdania finansowego za rok 2024 oraz stanowiących ich podstawę ksiąg rachunkowych, zgodnie z terminami wymienionymi w § 2 pkt 1 umowy w kwocie ..... zł netto (słownie złotych: .....) plus należny podatek VAT w wysokości ..... zł, co daje kwotę wynagrodzenia brutto ..... zł (słownie złotych: .....).
   2.2. Za przeprowadzenie badania sprawozdania finansowego za rok 2025 oraz stanowiących ich podstawę ksiąg rachunkowych, zgodnie z terminami wymienionymi w § 2 pkt 2 umowy w kwocie ..... zł netto (słownie złotych: .....) plus należny podatek VAT w wysokości ..... zł, co daje kwotę wynagrodzenia brutto ..... zł (słownie złotych: .....).
3. Wynagrodzenie płatne będzie na podstawie faktur VAT wystawianych przez Wykonawcę. Podstawą do wystawienia faktury będzie podpisany bez zastrzeżeń przez Wykonawcę i ARiMR protokół zdawczo-odbiorczy, o którym mowa w § 5 umowy, potwierdzający przyjęcie przez ARiMR sprawozdania z badania, a w sytuacji określonej w § 7 również uzasadnienia. Wzór protokołu zdawczo-odbiorczego stanowi nr 1 do umowy.
4. Zapłata wynagrodzenia zostanie dokonana przelewem na rachunek bankowy Wykonawcy na numer konta wskazany na fakturze VAT w terminie 21 dni, licząc od daty otrzymania przez ARiMR prawidłowo wystawionej faktury VAT łącznie z podpisanym przez Wykonawcę i ARiMR bez zastrzeżeń protokołem zdawczo-odbiorczym.
5. Za termin zapłaty wynagrodzenia strony uznają dzień potwierdzenia przez bank realizujący płatność otrzymania od ARiMR dyspozycji przelewu płatności.
6. Błędnie wystawiona faktura VAT lub brak podpisanego przez strony protokołu zdawczo-odbiorczego, spowodują naliczenie ponownego, 21-dniowego terminu płatności od momentu dostarczenia poprawionych lub brakujących dokumentów.
7. Wynagrodzenie, o którym mowa w ust. 1 powyżej wyczerpuje wszelkie roszczenia finansowe Wykonawcy z tytułu realizacji umowy.
8. Jeżeli w trakcie realizacji umowy nastąpi zmiana:
   1) stawki podatku od towarów i usług oraz podatku akcyzowego,
   2) wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej, ustalonych na podstawie ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę,
   3) zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub ubezpieczenie zdrowotne,
   4) zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych (Dz. U. z 2024 r. poz. 427),

   a zmiany te będą miały wpływ na koszty wykonania umowy – zastosowanie mają zasady wprowadzania zmian wysokości wynagrodzenia należnego Wykonawcy określone w ust. 9 – 16 poniżej.
9. Zmiana wysokości wynagrodzenia wymaga zmiany umowy w drodze aneksu.
10. Wykonawca najpóźniej w terminie 30 dni od dnia wejścia w życie przepisów wprowadzających zmiany, o których mowa w ust. 8 uprawniony jest do wystąpienia do ARiMR z pisemnym wnioskiem o dokonanie zmiany umowy w zakresie wysokości wynagrodzenia wraz z jej uzasadnieniem oraz dokumentami niezbędnymi do oceny przez ARiMR, czy zmiany, o których mowa w ust. 8 mają wpływ na koszty wykonania umowy przez Wykonawcę oraz w jakim stopniu zmiany tych kosztów uzasadniają zmianę wysokości wynagrodzenia Wykonawcy określonego w niniejszej umowie, a w szczególności:
    1) szczegółową kalkulację proponowanej zmienionej wysokości wynagrodzenia Wykonawcy oraz wykazanie adekwatności propozycji do zmiany wysokości kosztów wykonania umowy przez Wykonawcę,
    2) przyjęte przez Wykonawcę zasady kalkulacji wysokości kosztów wykonania umowy oraz założenia 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.
11. W terminie 30 dni od otrzymania wniosku, o którym mowa w ust 10, ARiMR może zwrócić się do Wykonawcy o jego uzupełnienie lub przekazanie dodatkowych wyjaśnień lub dokumentów (np. zażądać: oryginałów do wglądu, przekazania kopii dokumentów potwierdzonych za zgodność z oryginałami).

12. ARiMR w terminie 30 dni od dnia otrzymania kompletnego wniosku zajmie w stosunku do niego pisemne stanowisko. Za dzień przekazania stanowiska uznaje się dzień jego wysłania na adres właściwy dla doręczeń pism dla Wykonawcy.
13. ARiMR najpóźniej w terminie 30 dni od dnia wejścia w życie przepisów wprowadzających zmiany, o których mowa w ust. 8 może przekazać Wykonawcy pisemny wniosek o dokonanie zmiany umowy. Wniosek powinien zawierać co najmniej propozycję zmiany umowy w zakresie wysokości wynagrodzenia oraz powołanie zmian przepisów.
14. Przed przekazaniem wniosku, o którym mowa w ust.13, ARiMR może zwrócić się do Wykonawcy o złożenie wyjaśnień lub dokumentów (oryginałów do wglądu lub kopii potwierdzonych za zgodność z oryginałem) niezbędnych do oceny przez ARiMR czy zmiany, o których mowa w ust. 8, mają wpływ na koszty wykonania umowy przez Wykonawcę oraz w jakim stopniu zmiany tych kosztów uzasadniają zmianę wysokości wynagrodzenia. Rodzaj i zakres tych informacji określi ARiMR. Postanowienia ust. 11-12 stosuje się odpowiednio, z tym, że Wykonawca jest zobowiązany w każdym przypadku do zajęcia pisemnego stanowiska w terminie 30 dni od dnia otrzymania wniosku od ARiMR.
15. W przypadku niewykonania lub nienależytego wykonania przez Wykonawcę zobowiązania określonego w ust. 14 w terminie określonym w ust. 14. Wykonawca zapłaci na rzecz ARiMR karę umowną w wysokości 0,2 % łącznej kwoty wynagrodzenia brutto, określonego w § 6 ust. 1 umowy za każdy rozpoczęty dzień zwłoki. Jeżeli w terminie określonym w ust. 14 Wykonawca nie przedłoży wyjaśnień lub dokumentów, o których mowa w ust. 14 lub przedłożone przez Wykonawcę wyjaśnienia lub dokumenty będą niewystraczające do dokonania przez ARiMR oceny, w której mowa w ust. 14 – ARiMR wyznaczy Wykonawcy dodatkowy termin, nie dłuższy niż 10 dni, na dostarczenie lub uzupełnienie wyjaśnień lub dokumentów. W przypadku bezskutecznego upływu terminu wyznaczonego zgodnie ze zdaniem drugim, ARiMR uprawniony będzie do wypowiedzenia umowy z zachowaniem miesięcznego terminu wypowiedzenia.
16. Jeżeli w trakcie procedury opisanej w ust. 10-15 zostanie wykazane, że zmiany, o których mowa w ust. 8 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. 8.
17. Zasady zmiany wynagrodzenia określone w ust. 8-16 powyżej mają odpowiednie zastosowanie do zmiany wysokości wynagrodzenia w przypadku zmiany średniorocznego wskaźnika cen towarów i usług konsumpcyjnych ogółem ogłaszanego w komunikacie Prezesa Głównego Urzędu Statystycznego na podstawie przepisów ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (dalej: „wskaźnik"), z zastrzeżeniem następujących zasad:
    1) zmiana wynagrodzenia jest możliwa, gdy wskaźnik w stosunku do roku poprzedniego będzie wyższy niż 101,5 albo będzie niższy niż 98,5 (tj. wzrost poziomu cen o 1,5 % albo spadek poziomu cen o 1,5 %);
    2) zmiana wynagrodzenia obowiązuje w stosunku do wynagrodzenia, które stanie się należne dopiero po dniu podpisania aneksu do umowy (w formie pisemnej pod rygorem nieważności), tym samym zmiana nie dotyczy wynagrodzenia ustalonego (wystawienie faktury) lub rozliczonego przed dokonaniem zmiany umowy;
    3) zmiana wynagrodzenia możliwa jest najwcześniej po upływie 6 miesięcy od zawarcia umowy, chyba że data zawarcia umowy przypada po upływie 180 dni od daty złożenia oferty przez Wykonawcę, wówczas:
        a) zmiana wynagrodzenia możliwa jest po upływie 6 miesięcy od dnia otwarcia oferty Wykonawcy,
        b) wartość zmiany wskaźnika zostanie ustalona nie względem roku poprzedniego, a względem roku, w którym doszło do otwarcia oferty Wykonawcy;
    4) zmiany wynagrodzenia zgodnie z zasadami określonymi w niniejszym ustępie są możliwe do wysokości nieprzekraczającej łącznie 5% wartości wynagrodzenia określonego w § 6 ust. 1 umowy;
    5) uprawnienie do wnioskowania o waloryzację wynagrodzenia zastrzeżone jest dla obu Stron umowy.
18. Wykonawca, którego wynagrodzenie zostało zmienione w związku ze zmianą wskaźnika, o którym mowa w ust. 17, zobowiązany jest do zmiany wynagrodzenia przysługującego podwykonawcy, z którym zawarł umowę, w zakresie odpowiadającym zmianom cen materiałów lub kosztów dotyczących zobowiązania podwykonawcy. Wykonawca złoży oświadczenie w formie pisemnej, w którym potwierdzi fakt, iż dokonał zmiany wynagrodzenia należnego podwykonawcy oraz wskaże jego kwotą oraz datę zapłaty na rzecz podwykonawcy zmienionego wynagrodzenia. Przedmiotowe oświadczenie stanowić będzie załącznik do faktur wystawianych ARiMR z tytułu zmienionego wynagrodzenia za realizację umowy.
19. W przypadku niezgodności, w dniu realizacji płatności, numeru rachunku bankowego wskazanego przez Wykonawcę na fakturze z numerem rachunku bankowego zamieszczonym w wykazie podmiotów, o których mowa w art. 96b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2024 r., poz. 361 z późn. zm.), Strony ustalają, że realizacja płatności nastąpi w trybie art. 108a ww. ustawy.

§ 7.

W przypadku wyrażenia przez Wykonawcę opinii zawierającej istotne zastrzeżenia, co do prawidłowości oraz rzetelności sprawozdania finansowego, albo wyrażenia opinii negatywnej, ARiMR zostanie wydane uzasadnienie.

§ 8.

Wykonawca nie ma prawa bez pisemnej zgody ARiMR do korzystania przy wykonywaniu umowy z osób zatrudnionych w ARiMR, pod rygorem odstąpienia od umowy przez ARiMR w terminie 14 dni od dnia stwierdzenia przez ARiMR powyższej przesłanki oraz żądania zapłaty kary umownej w wysokości ... % łącznej kwoty wynagrodzenia brutto, określonego w § 6 ust. 1 umowy, a także żądania odszkodowania uzupełniającego na zasadach ogólnych Kodeksu Cywilnego.

§ 9.

Wykonawca ma prawo udostępnić rezultaty badania sprawozdań finansowych ARiMR wyłącznie organom upoważnionym przepisami prawa do wglądu w tego rodzaju dokumenty.

§ 10.

1. W przypadku stwierdzenia przez ARiMR nieprawidłowości w przeprowadzeniu przez Wykonawcę chociażby jednego z badań sprawozdań finansowych oraz stanowiących ich podstawę ksiąg rachunkowych, ARiMR wyznaczy Wykonawcy 7-dniowy termin celem usunięcia stwierdzonych nieprawidłowości, licząc od dnia otrzymania zgłoszenia, z zastrzeżeniem że po bezskutecznym upływie tego terminu ARiMR przysługuje kara umowna w wysokości 0,5 % przypadającej za dany rok części wynagrodzenia brutto, o którym mowa w § 6 ust. 2 umowy za każdy rozpoczęty dzień zwłoki.
2. Wykonawca zobowiązany jest do zapłaty na rzecz ARiMR kary umownej za każdy dzień zwłoki w przeprowadzeniu któregokolwiek z badań sprawozdań finansowych lub stanowiących ich podstawę ksiąg rachunkowych, w stosunku do terminów określonych w § 2 pkt 1 – 2 umowy – w wysokości 0,5% przypadającej za dany rok części wynagrodzenia brutto, o którym mowa w § 6 ust. 2 umowy za każdy rozpoczęty dzień zwłoki.
3. Jeżeli zwłoka Wykonawcy, o której mowa w ust. 1 lub ust. 2 wyniesie 14 dni, ARiMR po bezskutecznym upływie tego terminu może w terminie 14 dni odstąpić od umowy w całości lub części oraz zażądać z tego tytułu kary umownej w wysokości 20 % łącznej kwoty wynagrodzenia brutto, określonego w § 6 ust. 1 umowy, z zachowaniem prawa do kary umownej, o której mowa odpowiednio w ust. 1 lub 2 umowy, liczonej do dnia odstąpienia od umowy.
4. W przypadku braku zapłaty lub nieterminowej zapłaty wynagrodzenia należnego podwykonawcom z tytułu zmiany wysokości wynagrodzenia, w zakresie odpowiadającym zmianom wskaźnika dotyczących zobowiązania podwykonawcy, ARiMR przysługiwać będzie od Wykonawcy kara umowna w wysokości 0,5 % za każdy rozpoczęty dzień zwłoki.
5. W przypadku wystąpienia okoliczności uzasadniających zapłatę przez Wykonawcę kar umownych, ARiMR może według własnego wyboru potrącać kary umowne z wynagrodzenia należnego Wykonawcy za wykonanie umowy, wezwać Wykonawcę do zapłaty kar umownych w terminie 14 dni od daty otrzymania pisemnego wezwania do ich zapłaty lub potrącać z zabezpieczenia należytego wykonania umowy.
6. Jeżeli na skutek niewykonania lub nienależytego wykonania umowy powstanie szkoda przewyższająca zastrzeżoną karę umowną ARiMR oprócz tej kary przysługuje prawo do dochodzenia odszkodowania uzupełniającego. Jeżeli szkoda powstanie z innych przyczyn niż te, ze względu na które zastrzeżono karę umowną, ARiMR przysługuje prawo do dochodzenia odszkodowania na zasadach ogólnych Kodeksu Cywilnego.
7. Łączna wysokość kar umownych, których mogą dochodzić strony zostaje określona w wysokości nie większej niż 50 % łącznej kwoty wynagrodzenia brutto, określonego w § 6 ust. 1 umowy.

§ 11.

1. W przypadku odstąpienia przez Wykonawcę od realizacji umowy, nie z winy ARiMR, ARiMR przysługuje prawo do naliczenia kary umownej w wysokości 20% łącznego wynagrodzenia brutto, o którym mowa w § 6 ust. 1 umowy.
2. Wykonawca zobowiązuje się do zapłacenia odszkodowania w przypadku powstania szkody związanej z koniecznością zapłacenia przez ARiMR kar i odsetek wynikających z negatywnej oceny wydanej przez inne jednostki kontrolujące obszar, który stanowił przedmiot niniejszej umowy.

§ 12.

1. Wykonawca złożył u ARiMR zabezpieczenie należytego wykonania umowy (dalej: „ZNWU") w jednej z form, o których mowa w art. 450 ust. 1 ustawy Prawo zamówień publicznych w wysokości _____ zł (słownie złotych: _____ XX/100).
2. ZNWU dotyczy pokrycia ewentualnych roszczeń wynikających z niewykonania lub nienależytego wykonania umowy.
3. ZNWU zostanie zwolnione (zwrócone) w wysokości 100 % zabezpieczenia w terminie 30 dni od wykonania umowy i uznania przez ARiMR Umowy za należycie wykonaną.
4. W przypadku zmiany formy ZNWU w trakcie trwania umowy obowiązywać będą poniższe zasady.
5. ZNWU w formie pieniężnej Wykonawca wpłaca przelewem na rachunek bankowy wskazany przez ARiMR.
6. ZNWU wnoszone w formie gwarancji bankowej lub ubezpieczeniowej może być wystawione przez bank albo ubezpieczyciela. Bank lub ubezpieczyciel zapłaci, na rzecz ARiMR w terminie 30 dni od pisemnego żądania kwotę _____,XX zł (słownie złotych: _____ _____ XX/100), na pierwsze wezwanie ARiMR, bez odwołania, bez warunku, niezależnie od kwestionowania czy zastrzeżeń Wykonawcy i bez dochodzenia czy wezwanie ARiMR 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 będzie wnoszone w formie: poręczenia, bankowej lub ubezpieczeniowej gwarancji, ARiMR zastrzega sobie prawo do akceptacji projektu tych dokumentów.

§ 13.

1. Wszelkie zawiadomienia wymienione lub nie wymienione w umowie, niezależnie od nazwy, pod którą występują, dla swojej skuteczności muszą być przekazywane w formie pisemnej osobiście za zwrotnym, pisemnym potwierdzeniem odbioru i będą uważane za skutecznie doręczone w dniu ich odbioru.
2. Zawiadomienia będą wysyłane na adresy podane przez strony. Każda ze stron zobowiązana jest do informowania drugiej strony o każdej zmianie podanego adresu w formie pisemnej. Jeżeli strona nie powiadomiła o zmianie adresu, zawiadomienia wysłane na ostatni znany adres, strony uznają za doręczone. Powiadomienia o powyższych zmianach nie stanowią zmiany umowy wymagającej sporządzenia aneksu.
3. Przekazywanie informacji, w ramach realizacji przedmiotowej umowy z zastosowaniem formy elektronicznej wymaga zaszyfrowania danych. Hasło do otwarcia pliku powinno być przesłane odrębnym kanałem informacyjnym. Dane przekazywane w postaci papierowej należy przesyłać listem poleconym za potwierdzeniem osobistego odbioru.

§ 14.

Wszelkie zmiany umowy wymagają dla swej ważności formy pisemnej.

§ 15.

W sprawach nie uregulowanych niniejszą umową mają zastosowanie powszechnie obowiązujące przepisy prawa, w tym w szczególności przepisy Kodeksu Cywilnego i ustawy prawo zamówień publicznych.

§ 16.

Wszelkie spory, jakie mogą wyniknąć między Wykonawcą a ARiMR na tle realizacji umowy rozstrzygane będą przez sąd powszechny właściwy dla siedziby ARiMR.

§ 17.

Umowę sporządzono w postaci elektronicznej i opatrzono kwalifikowanymi podpisami elektronicznymi przez upoważnionych przedstawicieli Stron.

§ 18.

Integralną część umowy stanowią następujące Załączniki:

1) Załącznik nr 1 Protokół zdawczo-odbiorczy,
2) Załącznik nr 2 Formularz cenowy
3) Załącznik nr 3 Klauzula informacyjna w zakresie przetwarzania danych osobowych, która znajdzie zastosowanie w przypadku bezpośredniego pozyskania danych drugiej strony umowy będącej osobą fizyczną
4) Załącznik nr 4 Oświadczenie o wypełnieniu obowiązków informacyjnych przewidzianych w art. 13 lub art.14 RODO
5) Załącznik nr 5 Klauzula informacyjna w zakresie przetwarzania danych osobowych, która znajdzie zastosowanie w przypadku pośredniego pozyskania danych: pełnomocników, prokurenta oraz reprezentantów drugiej strony umowy będącej spółką prawa handlowego,
6) Załącznik nr 6 Klauzula informacyjna w zakresie przetwarzania danych osobowych, która znajdzie zastosowanie w przypadku bezpośredniego pozyskania danych: pełnomocnika, prokurenta oraz reprezentantów drugiej strony umowy będącej spółką prawa handlowego,
7) Załącznik nr 7 Klauzula informacyjna w zakresie przetwarzania danych osobowych – dotyczy osób których dane Administrator pozyskuje w sposób pośredni, w szczególności podwykonawców oraz osób wyznaczonych do kontaktów roboczych oraz odpowiedzialnych za koordynację i realizację umowy,
8) Załącznik nr 8 - Załącznik nr 5 „Regulamin użytkownika" do Polityki bezpieczeństwa informacji w ARiMR,
9) Załącznik nr 9 - Załącznik nr 12 (Regulamin eksploatacji systemów teleinformatycznych (ICT)) do Polityki bezpieczeństwa informacji w ARiMR.

ARiMR **WYKONAWCA**

Załącznik nr 1 do Umowy Nr ...../DK/202../..... z dnia.....

PROTOKÓŁ ZDAWCZO – ODBIORCZY

Zgodnie z umową nr .....z dnia.....
Przekazujemy dokumentację z badania sprawozdania finansowego za rok ....., zawierającą:

1. sprawozdanie z badania,
2. fakturę nr.....
3. zgodnie z § 7 umowy uzasadnienie opinii zawierającej istotne zastrzeżenia (jeżeli występuje taka opinia)

Wykonawca ARiMR

....

Załącznik nr 2 do Umowy Nr ...../DK/202../.... z dnia.....

Formularz Ofertowy

Załącznik nr 3 do Umowy Nr ...../DK/202../.... z dnia.....

Klauzula informacyjna w zakresie przetwarzania 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, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35), dalej: „RODO", ARiMR informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: „Administrator") pozyskanych w związku z zawarciem umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II 70, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazany w pkt 1.
3. Dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. b i c RODO w zw. z art. 431 i nast. ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605 z późn. zm.), tj. w celu zawarcia oraz wykonania niniejszej umowy.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
   1) organy kontrolne,
   2) osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902),
   3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
   4) podmioty przetwarzające w imieniu Administratora na mocy zawartej umowy, m. in. dostawcy IT.
5. Pani/Pana dane osobowe będą przechowywane przez okres obowiązywania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa. Okres przechowywania danych zostanie 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 zostanie przedłużony o okres 5 lat, na potrzeby archiwizacji.
6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, usunięcia, prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych oraz prawo do przenoszenia danych, w przypadkach określonych w RODO.
7. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
8. Podanie przez Panią/Pana danych osobowych jest konieczne w celu określonym w pkt 3 powyżej, dla zawarcia i wykonania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa, a konsekwencją niepodania Pani/Pana danych osobowych będzie brak możliwości zawarcia umowy.

[1] Klauzula informacyjna w zakresie przetwarzania danych osobowych, która znajdzie zastosowanie w przypadku bezpośredniego pozyskania danych drugiej strony umowy będącej osobą fizyczną.

Załącznik nr 4 do Umowy Nr ...../DK/202../.... z dnia.....

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

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

_____ – _____;

oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[2] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu zawarcia oraz wykonania Umowy[3].

(podpisy)

.....

.....

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35).

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

Załącznik nr 5 do Umowy Nr ...../DK/202../.... z dnia.....

Klauzula informacyjna w zakresie przetwarzania danych osobowych[4]

W związku z treścią z art. 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35), dalej: „RODO", ARiMR informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: „Administrator") pozyskanych w związku z zawarciem umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II 70, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazany w pkt 1.
3. Dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w zw. z art. 431 i nast. Ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605 z późn. zm.) w zw. z art. 98 i nast. Ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2023 r. poz. 1610 z późn. zm.) oraz w zw. z ustawą z 15 września 2000 r. Kodeks spółek handlowych (Dz. U. z 2024 r. poz. 18 z późn. zm.), tj. w celu zawarcia oraz wykonania niniejszej umowy.
4. Administrator będzie przetwarzał następujące kategorie Pani/Pana danych: dane identyfikacyjne oraz dane kontaktowe.
5. Odbiorcami Pani/Pana danych osobowych mogą być:
   1) organy kontrolne,
   2) osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902),
   3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
   4) podmioty przetwarzające w imieniu Administratora na mocy zawartej umowy, m. in. Dostawcy IT.
6. Pani/Pana dane osobowe będą przechowywane przez okres obowiązywania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa. Okres przechowywania danych zostanie 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 zostanie przedłużony o okres 5 lat, na potrzeby archiwizacji.
7. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, usunięcia oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych, w przypadkach określonych w RODO.
8. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
9. Pani/Pana dane Administrator uzyskał od ..... *

*należy wskazać źródło pozyskania danych [np. firmę przedsiębiorcy, od którego Administrator pozyskał dane].

[4] Niniejsza klauzula znajdzie zastosowanie w przypadku pośredniego pozyskania danych: pełnomocników, prokurenta oraz reprezentantów drugiej strony umowy będącej spółką prawa handlowego.

Załącznik nr 6 do Umowy Nr ...../DK/202../.... Z dnia.....

Klauzula informacyjna w zakresie przetwarzania danych osobowych[5]

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, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35), dalej: „RODO", ARiMR informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: „Administrator") pozyskanych w związku z zawarciem umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II 70, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazany w pkt 1.
3. Dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w zw. z art. 431 i nast. Ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605 z późn. zm.) w zw. z art. 98 i nast. Ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2023 r. poz. 1610 z późn. zm.) oraz w zw. z ustawą z 15 września 2000 r. Kodeks spółek handlowych (Dz. U. z 2024 r. poz. 18 z późn. zm.), tj. w celu zawarcia oraz wykonania niniejszej umowy.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
   1) organy kontrolne,
   2) osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902),
   3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
   4) podmioty przetwarzające w imieniu Administratora na mocy zawartej umowy, m. in. Dostawcy IT.
5. Pani/Pana dane osobowe będą przechowywane przez okres obowiązywania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa. Okres przechowywania danych zostanie 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 zostanie przedłużony o okres 5 lat, na potrzeby archiwizacji.
6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, usunięcia oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych, w przypadkach określonych w RODO.
7. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
8. Podanie przez Panią/Pana danych osobowych jest konieczne w celu określonym w pkt 3 powyżej, dla zawarcia i wykonania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa, a konsekwencją niepodania Pani/Pana danych osobowych będzie brak możliwości zawarcia umowy.

[5] Niniejsza klauzula znajdzie zastosowanie w przypadku bezpośredniego pozyskania danych: pełnomocnika, prokurenta oraz reprezentantów drugiej strony umowy będącej spółką prawa handlowego.

Załącznik nr 7 do Umowy Nr ...../DK/202../.... Z dnia.....

Klauzula informacyjna w zakresie przetwarzania danych osobowych[6]

W związku z treścią z art. 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35), dalej: „RODO", ARiMR informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: „Administrator") pozyskanych w związku z zawarciem umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II 70, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazany w pkt 1.
3. Dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w zw. z art. 431 i nast. ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605 z późn. zm.), tj. w celu zawarcia oraz wykonania niniejszej umowy.
4. Administrator będzie przetwarzał następujące kategorie Pani/Pana danych: dane identyfikacyjne oraz dane kontaktowe.
5. Odbiorcami Pani/Pana danych osobowych mogą być:
   1) organy kontrolne,
   2) osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902),
   3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
   4) podmioty przetwarzające w imieniu Administratora na mocy zawartej umowy, m. in. dostawcy IT.
6. Pani/Pana dane osobowe będą przechowywane przez okres obowiązywania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa. Okres przechowywania danych zostanie 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 zostanie przedłużony o okres 5 lat, na potrzeby archiwizacji.
7. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, usunięcia oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych, w przypadkach określonych w RODO.
8. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
9. Pani/Pana dane Administrator uzyskał od ..... *

*należy wskazać źródło pozyskania danych [np. firmę przedsiębiorcy, od którego Administrator pozyskał dane].

[6] Niniejsza klauzula dotyczy osób, których dane Administrator pozyskuje w sposób pośredni, w szczególności podwykonawców oraz osób wyznaczonych do kontaktów roboczych oraz odpowiedzialnych za koordynację i realizację umowy.

Załącznik nr 8 do Umowy Nr ...../DK/202../.... z dnia.....

Załącznik nr 5 do Polityki bezpieczeństwa informacji w ARiMR

REGULAMIN UŻYTKOWNIKA

Spis treści:

2

§ 1.

Definicje

Użyte w regulaminie określenia oznaczają:

1) dane uwierzytelniające – informacje wprowadzane do systemu, potwierdzające tożsamość użytkownika (np. hasła dostępu, kody zawarte w sprzętowych tokenach kryptograficznych);

2) hasło -ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie teleinformatycznym;

3) konto – część systemu teleinformatycznego (dane, oprogramowanie, zasoby sieciowe), które są powiązane z identyfikatorem użytkownika;

4) spam – niepożądaną przesyłkę poczty elektronicznej kierowaną do niezdefiniowanego adresata;

5) uwierzytelnianie - działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby/podmiotu;

6) urządzenie przenośne (mobilne) – urządzenie elektroniczne pozwalające na przetwarzanie, odbieranie oraz wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią takie jak laptop, notebook, netbook, palmtop, tablet, telefon komórkowy, smart-fon, MDA/PDA, pendrive, odtwarzacz mp3/4, aparat cyfrowy, czytnik kart pamięci, urządzenie do nawigacji GPS itp.

§ 2.

Szkolenia dla użytkowników systemów teleinformatycznych

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

2) zmian przepisów prawa oraz uregulowań wewnętrznych,

3) wystąpienia przypadków naruszenia bezpieczeństwa, słabości systemu lub zidentyfikowanych błędów systemów teleinformatycznych.

5. Okresowo (nie rzadziej niż raz na rok) przeprowadza się szkolenia doskonalące z zakresu bezpieczeństwa informacji. Szkolenia te obejmują zagadnienia ujęte w niniejszym Regulaminie, a w szczególności dotyczą:

1) zapoznania z obowiązującymi regulacjami prawnymi dotyczącymi ochrony informacji, w tym z obowiązującą w Agencji polityką bezpieczeństwa informacji oraz polityką systemu zarządzania bezpieczeństwem informacji,

2) przygotowania użytkowników do właściwego korzystania z powierzonych zasobów (instrukcje użytkowania sprzętu, systemów operacyjnych, aplikacji, itp.),

3) sposobu postępowania w przypadku zdarzenia związanego z naruszeniem bezpieczeństwa informacji,

4) sposobów postępowania w sytuacjach awaryjnych i kryzysowych.

6. Szkolenia doskonalące w zakresie obowiązujących w Agencji regulaminów związanych z bezpieczeństwem informacji mogą być przeprowadzane w zależności od zakresu obowiązków danego użytkownika przez:

1) Administratora Systemu,

2) Inspektora Bezpieczeństwa Informacji,

3) Administratora Zabezpieczeń Fizycznych,

4) Właściciela Procesu / Właściciela Zasobu,

5) Bezpośredniego przełożonego

W uzasadnionych przypadkach przedmiotowe szkolenie może zostać przeprowadzone w formie szkolenia e-learningowego.

7. Szkolenia doskonalące powinny kończyć się testem sprawdzającym zrozumienie przekazanych informacji adekwatnym do poziomu i zakresu prowadzonego szkolenia.

8. Uczestnictwo w szkoleniu stacjonarnym każdy użytkownik potwierdza podpisem na liście obecności. W przypadku szkoleń odbywających się w formie e-learning lista obecności tworzona jest na podstawie zalogowania użytkownika do szkolenia.

9. Szkolenia i egzaminy związane z użytkowaniem systemów teleinformatycznych są odnotowywane w Systemie e-szkoleń ARiMR.

10. Nieprzystąpienie do szkolenia, o którym mowa w ust. 5 lub niezaliczenie testu, o którym mowa w ust. 7, w terminie podstawowym i dodatkowym skutkuje blokadą dostępu do systemu teleinformatycznego Agencji, z wyłączeniem systemu e-szkoleń ARiMR na wniosek dyrektora komórki właściwej ds. bezpieczeństwa informacji.

11. Przywrócenie dostępu do systemu teleinformatycznego następuje na wniosek przełożonego użytkownika, zgodnie z procedurą zawartą w KP-611-101-ARiMR, po wcześniejszym odbyciu dodatkowego szkolenia doskonalącego i pozytywnym zaliczeniu testu.

§ 3.

Używanie autoryzowanych środków do przetwarzania informacji

1. Środki do przetwarzania informacji wykorzystywane w Agencji są przeznaczone wyłącz-nie do wykonywania zadań służbowych.

2. Każdy środek do przetwarzania informacji podlega inwentaryzacji i autoryzacji (dopuszczenie do pracy w systemie teleinformatycznym Agencji) zgodnie z zasadami określonymi w odrębnych dokumentach Agencji.

3. Wykorzystywanie środków do przetwarzania informacji, będących własnością Agencji, w celach niezwiązanych z powierzonymi obowiązkami wymaga uzgodnienia z bezpośrednim przełożonym i jeżeli zachodzi taka potrzeba wynikająca z zakresu ewentualnego wy-korzystania urządzeń, z Administratorem Systemu.

4. Zabrania się podłączania do sieci teleinformatycznej jakichkolwiek urządzeń nieposiadających autoryzacji.

5. Użytkownicy mogą korzystać ze stacji roboczych wyłącznie na stanowiskach im przydzielonych. Korzystanie z innego stanowiska komputerowego dopuszczalne jest jedynie za zgodą i na polecenie bezpośredniego przełożonego lub w przypadkach opisanych w Planach Zapewnienia Ciągłości Działania Agencji.

6. Użytkownik ponosi odpowiedzialność za powierzony sprzęt i oprogramowanie oraz sposób jego eksploatacji.

7. W przypadku korzystania ze stacji roboczej przez kilku użytkowników, kierownik komórki bądź jednostki organizacyjnej wyznacza osobę odpowiedzialną za sprzęt.

8. Użytkowników obowiązuje zakaz testowania lub podejmowania prób poznania metod zabezpieczenia systemów teleinformatycznych.

9. Użytkownicy nie mogą samodzielnie dokonywać jakiejkolwiek zmiany konfiguracji systemu teleinformatycznego.

10. Nośniki uszkodzone, wycofywane z eksploatacji lub przekazywane do ponownego użycia użytkownik przekazuje Administratorowi Systemu odpowiedzialnemu za przeprowadzenie zniszczenia lub trwałego skasowania danych, korzystając z następujących procedur:

1) programowego kasowania danych na dyskach twardych – zamieszczonej w Książce Procedur KP-611-204-ARiMR,

2) niszczenia zawartości komputerowych nośników magnetycznych – zamieszczonej w Książce Procedur KP-611-204-ARiMR,

3) niszczenia nośników optycznych – zamieszczonej w Książce Procedur KP-611-186-ARiMR.

11. Postanowienia ust. 10 nie ograniczają ani nie wykluczają stosowania obowiązujących w Agencji zasad dotyczących gospodarowania środkami trwałymi oraz wyposażeniem.

§ 4.

Wynoszenie mienia i korzystanie z urządzeń przenośnych

1. Komputery przenośne podlegają szczególnej ochronie polegającej na zabezpieczaniu dostępu do komputera hasłem (hasło na BIOS), zaszyfrowaniu dysku, zabezpieczeniu systemem antywirusowym. Ich używanie poza strefą administracyjną uzasadnia organizacja pracy oraz realizowane przez użytkownika zadania poza stałym miejscem wykonywania pracy.

2. Wynoszenie sprzętu komputerowego poza Agencję, w tym sposób programowego zabezpieczenia komputerów przenośnych, reguluje procedura wydawania zezwoleń na wynoszenie sprzętu komputerowego z ARiMR zawarta w Książce Procedur KP-611-206-ARiMR.

3. Na użytkowniku urządzenia przenośnego spoczywa obowiązek jego ochrony, w szczególności zabrania się pozostawiania bez opieki tego typu urządzenia w samochodach, prze-działach wagonów, salach konferencyjnych oraz innych miejscach, gdzie użytkownik nie ma możliwości sprawowania nad nimi skutecznego nadzoru.

4. Wszelkie informacje wrażliwe nie mogą być przechowywane w urządzeniach przenośnych, które pracują poza Agencją, jeśli pozostają w postaci niezaszyfrowanej.

5. Każdy użytkownik, któremu powierzono urządzenie przenośne, przed rozpoczęciem użytkowania go poza strefą administracyjną Agencji, obowiązany jest do wystąpienia do Administratora Systemu z wnioskiem o zapewnienie środków techniczno-organizacyjnych gwarantujących poufność i integralność przetwarzanych informacji. Do środków tych zalicza się zabezpieczenia kryptograficzne określone w Polityce kryptografii oraz ochronę antywirusową.

6. W przypadku utraty powierzonego urządzenia przenośnego używanego poza Agencją użytkownik niezwłocznie powiadamia o tym fakcie Help Desk ARiMR oraz bezpośredniego przełożonego, a w przypadku kradzieży niezwłocznie zgłasza ten fakt na policję. Ponadto o kradzieży informuje osobę wydającą zgodę na wyniesienie sprzętu.

§ 5.

Korzystanie z systemów teleinformatycznych Agencji oraz Internetu

1. Przydzielanie uprawnień do korzystania z systemów teleinformatycznych realizowane jest w oparciu o następujące zasady:

1) „minimalnych przywilejów" – każdy pracownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków,

2) „wiedzy koniecznej" – pracownicy posiadają wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań,

3) „domniemanej odmowy" – wszystkie działania, które nie są jawnie dozwolone są zabronione.

2. Każdy użytkownik otrzymuje prawa dostępu wyłącznie w zakresie niezbędnym do realizowania powierzonych zadań na danym stanowisku pracy.

3. Prawa dostępu są przydzielone po nadaniu użytkownikowi identyfikatora i hasła dostępu lub innych danych uwierzytelniających użytkownika.

4. Każdy użytkownik ma w systemie unikalny identyfikator.

5. Przed uzyskaniem dostępu do systemów teleinformatycznych Agencji użytkownik jest in-formowany przez bezpośredniego przełożonego o zakresie przyznawanych mu uprawnień.

6. Użytkownik ponosi odpowiedzialność za wszelkie czynności wykonane z użyciem jego identyfikatora i hasła.

7. Jeżeli w trakcie korzystania z zasobów systemu teleinformatycznego użytkownik stwierdzi, że posiadane uprawnienia wykraczają poza przyznane, zobowiązany jest niezwłocznie zgłosić ten fakt do Help Desk ARiMR. Niedokonanie zgłoszenia tego faktu może zostać potraktowane jako celowe i świadome naruszenie praw dostępu.

8. Po stwierdzeniu posiadania większych uprawnień zabronione jest ich testowanie i wykorzystywanie.

9. Każdorazowo w przypadku oddalenia się od stacji roboczej Użytkownik zobowiązany jest zablokować dostęp do systemu.

10. Na użytkowniku spoczywa obowiązek zabezpieczenia opracowywanych bądź tworzonych przez siebie danych przed utratą. Również wszelkie dane źródłowe, na których użytkownik wykonuje operacje, winny być zabezpieczone przed utratą i nieautoryzowanym użyciem bądź modyfikacją.

11. Użytkownik ma następujące możliwości zabezpieczenia danych (plików) przed utratą:

1) umieszczenie danych na serwerze plików (fileserver) – jest to zalecana forma zabezpieczenia danych,

2) sporządzenie kopii zapasowej na wymiennym nośniku komputerowym,

3) sporządzenie wydruków z wyniku pracy nad przetwarzanymi danymi.

12. Niedopuszczalne jest umieszczanie na serwerze plików danych niezwiązanych z wykonywanymi obowiązkami służbowymi.

13. W przypadku potrzeby zabezpieczenia plików o dużych rozmiarach należy skorzystać z procedury nagrywania danych na nośnikach optycznych zawartej w Książce Procedur KP-611-186-ARiMR - „Postępowanie z optycznymi nośnikami danych".

14. Zabronione jest:

1) umożliwianie dostępu do systemów teleinformatycznych osobom nieupoważnionym,

2) rejestrowanie się w systemie teleinformatycznym na identyfikatorze innego użytkownika,

3) korzystanie z konta innego użytkownika, chyba że część lub całość zasobów związanych z tym kontem są udostępniane zgodnie z zasadami obowiązującymi w Agencji,

4) przenoszenie informacji uzyskanych w związku z wykonywanymi zadaniami służbowymi na prywatne nośniki informacji, w szczególności pamięci typu pendrive i inne pamięci zewnętrzne,

5) dokonywanie prób sprawdzania, testowania i omijania zabezpieczeń systemów teleinformatycznych wewnętrznych jak również zewnętrznych, nie należących do Agencji,

6) udzielanie informacji o zasadach ochrony systemów teleinformatycznych Agencji, w tym o identyfikatorach używanych w tych systemach,

7) samowolne modyfikowanie ustawień związanych z bezpieczeństwem w systemach teleinformatycznych,

8) świadome niszczenie danych mających znaczenie archiwalne gromadzonych w systemach teleinformatycznych,

9) świadome wprowadzanie błędnych danych do systemów teleinformatycznych,

10) udostępnianie danych osobom nieupoważnionym,

11) włączanie urządzeń elektrycznych do wydzielonej instalacji elektrycznej przeznaczonej dla systemów teleinformatycznych,

12) przeglądanie stron internetowych o treściach pornograficznych, erotycznych, rasistowskich, użytkowanych przez grupy przestępcze i terrorystyczne,

13) pobieranie z Internetu, kopiowanie, instalowanie, przechowywanie lub rozpowszechnianie nieautoryzowanego przez Komitet oprogramowania i danych,

14) korzystanie z list i forów dyskusyjnych, gier internetowych oraz innych usług, nie-mających związku z wykonywaną pracą,

15) przechowywania plików danych outlook typu *.pst, *.ost na zasobie współdzielonym,

16) przesyłania na serwery zewnętrzne (niezwiązane z ARiMR) niezabezpieczonymi kanałami plików z danymi wrażliwymi. Wyjątek stanowi wykonywanie zadań wynikających z przepisów prawa.

17) podłączania zewnętrznych nośników pamięci (np. CD/DVD, pamięci masowe, pa-mięci flash, smartphone) do stacji użytkownika, bez uprzedniego przeskanowania zawartości urządzenia programem antywirusowym na wydzielonej stacji komputerowej.

15. Zasady pracy zdalnej określone są w Porozumieniu w sprawie Zasad wykonywania pracy zdalnej w Agencji Restrukturyzacji i Modernizacji Rolnictwa z dnia 30.06.2023 r.

§ 6.

Korzystanie z poczty elektronicznej i innych elektronicznych systemów komunikacyjnych

1. Wszyscy pracownicy Agencji mają dostęp do wewnętrznej poczty elektronicznej.

2. Agencyjna poczta służy wyłącznie do celów służbowych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów teleinformatycznych Agencji podlega rejestrowaniu i filtrowaniu, o którym mowa w ust. 3.

3. Użytkownicy są świadomi, że wiadomości elektroniczne niezwiązane z działalnością Agencji, a zawierające słowa bądź temat uznane za niedozwolone, zgodnie z zasadami filtrowania komunikacji niepożądanej obowiązującymi w Agencji, będą zatrzymywane i następnie usuwane z systemu pocztowego.

4. Zalecanym formatem przesyłanych wiadomości jest „zwykły tekst". O ile nie jest to konieczne, nie należy tworzyć wiadomości w formacie HTML.

5. Użytkownicy obowiązani są do okresowego porządkowania i usuwania wiadomości zbędnych z folderów programu pocztowego tak, aby nie dopuścić do jego zablokowania z powodu przekroczenia dopuszczalnej pojemności skrzynki.

6. Zabronione jest:

1) rozsyłanie z komputerów Agencji oraz przyznanych użytkownikom kont poczty wiadomości, których treść nie jest związana z wykonywaną pracą, wyjątek stanowią komunikaty niestandardowe rozsyłane zgodnie z „Zasadami świadczenia przez Departament Informatyki usługi dystrybucji komunikatów do dużych grup odbiorców",

2) wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu),

3) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Agencji,

4) odbieranie przesyłek z nieznanych źródeł,

5) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.,

6) przesyłanie plików wykonywalnych typu: bat, com, exe oraz plików multimedialnych i plików graficznych nie związanych z pracą,

7) ukrywanie lub dokonywanie zmian tożsamości nadawcy,

8) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika,

9) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją Administratorowi systemu poczty elektronicznej na adres e-mail: spam@arimr.gov.pl,

10) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy,

11) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Agencji lub do poszukiwania dodatkowego zatrudnienia

§ 7.

Ochrona haseł i kluczy kryptograficznych

1. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.

2. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego przechowywanie.

3. Każdy użytkownik posiadający dostęp do systemów teleinformatycznych Agencji zobowiązany jest do:

1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystywanych do pracy w systemie teleinformatycznym Agencji,

2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia,

3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez Administratora Systemu,

4) poinformowania Administratora Systemu oraz Inspektora Bezpieczeństwa Informacji o podejrzeniu lub rzeczywistym ujawnieniu hasła,

5) stosowania haseł o minimalnej długości 12 znaków, zawierających kombinację ma-łych i dużych liter oraz cyfr i znaków specjalnych,

6) zmiany wykorzystywanych haseł w regularnych odstępach czasu.

4. Zabronione jest:

1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób,

2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.,

3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach,

4) udostępnianie haseł innym użytkownikom,

5) przeprowadzanie prób łamania haseł,

6) wpisywanie haseł „na stałe" (np. w skryptach logowania).

5. W zależności od funkcjonujących w Agencji systemów operacyjnych i aplikacji zasady określone w ust. 3 pkt 3, 5 i 6 oraz ust. 4 pkt 2 i 3 mogą być wymuszane ustawieniami systemu teleinformatycznego wprowadzanymi przez Administratora Systemu na podstawie zasad określonych w odrębnych dokumentach Agencji.

6. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania z uwzględnieniem wymagań określonych w Polityce krypto-grafii, w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.

7. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić Administratorowi Systemu oraz Inspektorowi Bezpieczeństwa Informacji.

8. W celu zabezpieczenia haseł dopuszcza się stosowanie menadżerów haseł. Stosowanie me-nadżera haseł wymaga wcześniejszej zgody dyrektora ds. informatyki.

§ 8.

Zgodność oprogramowania z prawami autorskimi

1. Użytkownicy nie mogą instalować oraz uruchamiać żadnych aplikacji, które nie zostały wcześniej formalnie dopuszczone do użytkowania.

2. Użytkownikowi nie wolno:

1) uruchamiać jakiegokolwiek innego oprogramowania niż to, które zostało mu przydzielone na danej stacji roboczej,

2) pobierać z sieci, kopiować, przechowywać lub rozprowadzać oprogramowania, utworów muzycznych i wideo oraz innych plików, których używanie może powodować naruszenie praw do własności intelektualnej,

3) kopiować i rozprowadzać bez upoważnienia oprogramowania stworzonego w Agencji lub na potrzeby Agencji,

4) samodzielnie usuwać oprogramowania, którego używa.

3. Każdy plik znajdujący się:

1) na wymiennym nośniku komputerowym,

2) otrzymany za pomocą poczty elektronicznej lub pobrany z Internetu, podlega sprawdzeniu za pomocą oprogramowania antywirusowego zainstalowanego na komputerze przypisanym do użytkownika.

4. W przypadku wykrycia jakichkolwiek plików lub oprogramowania innego niż to, które znajduje się w spisie, Administrator Systemu ma prawo do natychmiastowego ich skasowania bez uzgodnienia z użytkownikiem.

5. O przypadkach używania nieautoryzowanego oprogramowania Administrator Systemu in-formuje Inspektora Bezpieczeństwa Informacji.

6. Użytkownik ponosi finansowe i prawne konsekwencje posiadania nielegalnego oprogramowania w przypisanym mu komputerze, jeśli nie dopełnił obowiązków wskazanych w niniejszym Regulaminie.

§ 9.

Korzystanie z urządzeń komunikacji głosowej, wizyjnej

1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, pod-czas których może dochodzić do wymiany informacji wrażliwych, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.

2. Odczytanie wiadomości z automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.

3. Zabronione jest wykorzystywanie domyślnych („fabrycznych") haseł dla ww. urządzeń.

4. Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających informacje wrażliwe jest zabronione.

5. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających informacje wrażliwe.

§ 10.

Zasady „czystego biurka i czystego ekranu"

1. Palenie, jedzenie oraz picie na stanowiskach komputerowych oraz w pomieszczeniach, w których znajdują się środki przetwarzania informacji (pomieszczenia serwerowni i wę-złów teletechnicznych) jest zabronione.

2. W celu ograniczenia ryzyka nieuprawnionego dostępu, utraty lub uszkodzenia informacji w czasie godzin pracy i poza nimi użytkownik jest zobowiązany:

1) przechowywać dokumenty papierowe i wymienne nośniki komputerowe w odpowiednio zabezpieczonych meblach biurowych,

2) nie pozostawiać komputerów bez nadzoru w stanie aktywnej sesji dostępu do sieci,

3) po zakończeniu pracy wylogować się z systemu i wyłączyć komputer; niedopuszczalne jest zakończenie pracy bez wykonania pełnej i poprawnej procedury zamknięcia lub przez wyłączenie napięcia zasilającego,

4) po zakończeniu pracy uporządkować swoje stanowisko pracy, uniemożliwiając do-stęp osób nieupoważnionych do dokumentów zawierających informacje wrażliwe,

5) przestrzegać zasady niepozostawiania otwartych i niezabezpieczonych drzwi i/lub okien podczas nieobecności w pomieszczeniu,

6) używać wygaszaczy ekranu zabezpieczonych hasłem,

7) zabezpieczać nieużywany w danym momencie komputer przed nieupoważnionym dostępem, włączając blokadę systemową; ponowny dostęp do komputera następuje po podaniu hasła,

8) w miarę możliwości ustawiać monitory komputerów w taki sposób, żeby uniemożliwić osobom nieupoważnionym wgląd w zawartość ekranu,

9) odpowiednio zabezpieczyć miejsca przyjmowania/wysyłania korespondencji papierowej,

10) włączać blokadę urządzeń kopiujących, zabezpieczając je w ten sposób przed nieuprawnionym użyciem,

11) zwracać uwagę i powodować usuwanie pozostawionych oryginałów lub kopii w pobliżu urządzeń kserograficznych,

12) zwracać szczególną uwagą na pracujące drukarki pozostawione bez nadzoru,

13) nie pozostawiać wymiennych nośników komputerowych w napędach bądź ogólnie dostępnych miejscach,

14) niszczyć niepotrzebne nośniki papierowe w niszczarkach, jak np. dokumenty błędnie wydrukowane, powielone kopie itp. (za wyjątkiem nośników zawierających informacje wrażliwe, których sposób niszczenia regulują odrębne przepisy, w tym przepisy kancelaryjno-archiwalne Agencji w zakresie brakowania dokumentacji nie-archiwalnej).

3. W uzasadnionych przypadkach realizacji zadań wymagających nieprzerwanego dostępu do zasobów teleinformatycznych (np. praca zdalna, długotrwałe wgrywanie patch'y, pobieranie dużych ilości danych, odbywające się poza godzinami pracy ze względu na przepustowość łącz, wydajność baz danych, itp.) dopuszczalne jest, w porozumieniu z komórką właściwą ds. informatyki, odstąpienie od wymogu podanego w ust. 2 pkt 3.

§ 11.

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

1. Przed przystąpieniem do pracy użytkownik obowiązany jest sprawdzić stację roboczą (komputer) i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub próbę naruszenia bezpieczeństwa informacji.

2. Do przypadków mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa, nie-właściwym funkcjonowaniu oprogramowania lub słabości systemu teleinformatycznego zalicza się:

1) nieautoryzowany dostęp do danych,

2) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach (np. wyłamane lub zacinające się zamki, naruszone plomby, nie domykające się bądź wybite okna, itp.),

3) utratę usługi, urządzenia lub funkcjonalności,

4) nieautoryzowaną modyfikację lub zniszczenie danych,

5) udostępnienie informacji wrażliwych osobom nieupoważnionym,

6) pozyskiwanie oprogramowania z nielegalnych źródeł,

7) pojawianie się nietypowych komunikatów na ekranie,

8) niemożność zalogowania się do systemu teleinformatycznego,

9) spowolnienie pracy oprogramowania,

10) niestabilna praca systemu teleinformatycznego,

11) brak reakcji systemu na działania użytkownika,

12) ponowny start lub zawieszanie się komputera,

13) ograniczenie funkcjonalności oprogramowania.

3. Za naruszenie zasad ochrony informacji wrażliwych uważa się w szczególności:

1) nieupoważniony dostęp, modyfikację, kopiowanie, udostępnienie lub zniszczenie /usunięcie informacji wrażliwych, zarówno w systemie teleinformatycznym, jak i na nośnikach papierowych i elektronicznych,

2) udostępnianie informacji wrażliwych nieuprawnionym podmiotom,

3) nieautoryzowany dostęp do danych przez połączenie sieciowe,

4) niedopełnienie obowiązku ochrony informacji wrażliwych przez umożliwienie do-stępu do danych (np. pozostawienie kopii danych, nie zablokowanie dostępu do systemu, brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi prze-bywającymi w pomieszczeniach, gdzie przetwarza się informacje wrażliwe),

5) stworzenie niezabezpieczonego kanału dystrybucji informacji wrażliwych,

6) nielegalne bądź nieświadome ujawnienie informacji wrażliwych,

7) pozyskiwanie informacji wrażliwych z nielegalnych źródeł,

8) przetwarzanie informacji wrażliwych niezgodne z uprawnionym celem i zakresem,

9) niepodjęcie działań zmierzających do eliminacji wirusów komputerowych lub innych programów zagrażających integralności systemu teleinformatycznego,

10) ujawnienie indywidualnych haseł dostępu do informacji wrażliwych w systemie,

11) przesyłanie informacji wrażliwych przez Internet bez zabezpieczenia danych zgod-nie z obowiązującą w ARiMR polityką haseł.

12) przesyłanie dokumentów papierowych i nośników elektronicznych z informacjami wrażliwymi bez zabezpieczenia,

13) wykonanie nieuprawnionych kopii informacji wrażliwych,

14) kradzież nośników zawierających informacje wrażliwe lub oprogramowanie,

15) kradzież sprzętu służącego do przetwarzania informacji wrażliwych,

16) spowodowanie utraty informacji wrażliwych w systemie teleinformatycznym, na kopiach bezpieczeństwa i na innych nośnikach,

17) dopuszczenie do braku aktualnych kopii bezpieczeństwa informacji wrażliwych lub brak odpowiednich nośników do sporządzania kopii,

18) niewłaściwe niszczenie nośników z informacjami wrażliwymi pozwalające na ich odczyt,

19) naruszenie zasad ochrony fizycznej pomieszczeń, w których przetwarza się informacje wrażliwe,

20) dopuszczenie do przetwarzania informacji wrażliwych pracowników bez odpowiednich upoważnień,

21) nie przeszkolenie pracowników w zakresie zasad bezpieczeństwa informacji wrażliwych,

22) ujawnienie danych osobowych adresatów e-mail osobom nieuprawnionym,

23) inne sytuacje wskazujące lub potwierdzające naruszenie bezpieczeństwa informacji wrażliwych w Agencji.

4. Wszelkie działania użytkownika związane z samodzielnym naprawianiem, potwierdzaniem lub testowaniem potencjalnych słabości systemu są zabronione.

5. Dokonywanie zmian w miejscu naruszenia ochrony bez wiedzy i zgody Administratora Systemu lub Inspektora Bezpieczeństwa Informacji lub Administratora Zabezpieczeń Fizycznych (w zależności od rodzaju naruszenia), jest dopuszczalne jedynie w sytuacji, gdy zachodzi konieczność ratowania życia lub zdrowia osób oraz mienia w przypadku ich bez-pośredniego zagrożenia.

6. W przypadku zauważenia zdarzenia mogącego świadczyć lub świadczącego o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania, błędów lub awarii systemu użytkownik:

1) zabezpiecza dostęp do miejsca lub urządzenia w sposób umożliwiający odtworzenie okoliczności naruszenia bezpieczeństwa lub niewłaściwego funkcjonowania oprogramowania,

2) wstrzymuje pracę na stacji roboczej i odseparowuje komputer od sieci,

3) niezwłocznie informuje Help Desk ARiMR (w przypadku wystąpienia zdarzenia związanego z systemem teleinformatycznym) lub Administratora Zabezpieczeń Fizycznych (jeżeli zdarzenie dotyczy bezpieczeństwa fizycznego i środowiskowego), a także bezpośredniego przełożonego,

4) niezależnie od zapisów pkt 3) niezwłocznie informuje Inspektora Ochrony Danych oraz Inspektora Bezpieczeństwa Informacji w przypadku naruszenia zasad ochrony danych osobowych, przy czym sposób poinformowania Inspektora Ochrony Danych powinien nastąpić w sposób zapewniających, iż informacja zostanie odebrana w możliwie naj-krótszym czasie od jej przekazania,

5) w przypadku zakwalifikowania przez IBI danego zdarzenia jako incydent, wypełnia w porozumieniu z nim część A raportu o incydencie bezpieczeństwa informacji (wzór raportu określa załącznik nr 3 do Regulaminu zarządzania incydentami).

6) w przypadku wstępnego zakwalifikowania przez IBI danego zdarzenia jako naruszenie ochrony danych osobowych, wypełnia w porozumieniu z nim zgłoszenie naruszenia (wzór zgłoszenia określa załącznik nr 4 Regulaminu zarządzania incydentami).

§ 12.

Postępowanie dyscyplinarne w przypadku naruszenia bezpieczeństwa

1. Nieprzestrzeganie zasad określonych w dokumentach określających politykę bezpieczeństwa informacji stosowanych na danym stanowisku pracy przez użytkownika stanowi naruszenie podstawowych obowiązków pracowniczych i podlega odpowiedzialności dyscyplinarnej określonej w Regulaminie pracy.

2. Każdy przypadek wskazany w ust. 1 jest analizowany przez Inspektora Bezpieczeństwa In-formacji, który w porozumieniu z Administratorem Systemu, Administratorem Zabezpieczeń Fizycznych we współpracy z kierującym daną komórką/jednostka organizacyjną, dokonuje kwalifikacji naruszenia. W szczególności umyślne działanie może zostać zakwalifikowane jako ciężkie naruszenie obowiązków pracowniczych.

3. Każdy przypadek naruszenia bezpieczeństwa informacji zgłaszany jest niezwłocznie dyrektorowi komórki właściwej ds. bezpieczeństwa informacji przez Inspektora Bezpieczeństwa Informacji i opisywany zgodnie z Regulaminem zarządzania incydentami.

Załącznik nr 9 do Umowy Nr ...../DK/202../.... z dnia.....

Załącznik nr 12 do Polityki bezpieczeństwa informacji w ARiMR

REGULAMIN EKSPLOATACJI SYSTEMÓW TELEINFORMATYCZNYCH (ICT)

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. identyfikatory, 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 (kopia bezpieczeństwa) - duplikat danych, przechowywany na innym niż macierzystym nośniku komputerowym, służący do odtworzenia systemu, aplikacji, bazy danych lub dokumentu;
8) niezaprzeczalność - możliwość przeprowadzenia dowodu, że działanie lub zdarzenie miało miejsce, tak że nie można temu działaniu lub zdarzeniu później zaprzeczyć;
9) podatność - słabość aktywu lub grupy aktywów, która może być wykorzystana przez jedno lub więcej zagrożeń;
10) profil dostępu - zestaw uprawnień, funkcji i zasobów systemu informatycznego dostępnych poszczególnym użytkownikom systemu;
11) rozliczalność - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (ISO 7498-2: 1989);
12) spam - niepożądana przesyłka poczty elektronicznej kierowana do niezdefiniowanego adresata, generująca koszty po jego stronie;
13) uwierzytelnianie - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (np. użytkownika lub innej aplikacji, systemu);
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 - uzgodniona i zaakceptowana wcześniej zmiana konfiguracji urządzeń lub sposobu/ zakresu świadczenia usług;
17) zmiana infrastruktury/ usługa awaryjna - zmiana podejmowana w trybie nagłym wynikająca z konieczności usunięcia awarii lub błędu w systemie;
18) przywilej - specjalne uprawnienie wyższe od podstawowego prawa dostępu w systemie lub aplikacji (np. umożliwiające zarządzanie użytkownikami, rolami, itp.), stosowane jedynie dla wybranych pracowników, w szczególności uprawnienie administratora;
19) ICT - technologie informacyjno-komunikacyjne

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 Procesu/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 tę 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 (ang. 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 domeny, 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. Sprzęt teleinformatyczny użytkowany w Agencji chroniony jest podczas pracy dedykowanymi systemami zabezpieczającymi, takimi jak np. systemy AV (antywirusowe, antyspamowe), systemy wykrywające i blokujące ataki IDS/IPS, zapory NGFW (ang. Next-generation firewall), serwery proxy, sondy filtrujące ruch sieciowy, itp.
2. Użytkowane poza systemem Agencji wymienne komputerowe nośniki danych, 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 i moduły behawioralne.
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 podlegają rejestrowaniu w dzienniku pracy systemu

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 dyrektorowi komórki właściwej ds. bezpieczeństwa.

Zarządzanie kopiami zapasowymi i archiwalnymi

1. Kopie zapasowe systemów, aplikacji, baz danych i dokumentów w postaci cyfrowej 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.

7. Dla wskazanych dokumentów, systemów, baz danych i aplikacji podlegających tworzeniu kopii zapasowych:

1) Administrator Systemu w porozumieniu z Właścicielem Procesu/Właścicielem Zasobu określa strategię tworzenia kopii uwzględniającą: częstotliwość tworzenia kopii, rodzaj kopii (przyrostowa, pełna, różnicowa), ilość kopii, miejsce, okres i sposób przechowywania kopii, rotację nośników,

2) Administrator Systemu określa 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. Przykładowy 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/Właścicielem Ryzyka 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.
20. W przypadku, gdy transportowane nośniki zawierają dane osobowe w postaci niezaszyfrowanej, przed realizacją usługi należy podpisać z Podmiotem zewnętrznym dodatkową umowę powierzenia przetwarzania danych osobowych.

§ 7.

Zarządzanie poprawkami technicznymi

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

7) aktualizowanie aplikacji, systemów operacyjnych oraz usług sieciowych do aktualnych, bezpiecznych i stabilnych wersji, posiadających wsparcie techniczne producenta,

8) fizycznych zabezpieczeń dostępu do systemów,

9) rozdzielenia środowisk produkcyjnych od testowych i developerskich.

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 itp.).
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, systemy antymalwerowe).
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 Administrator Systemu 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 12 znaków, zawierających małe i wielkie litery oraz cyfry i znaki specjalne,
   5) wymuszenie zmiany haseł z ustaloną częstotliwością, w przypadku systemów przetwarzających dane osobowe zmiana hasła następuje nie rzadziej niż co 90 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/Właściciela Ryzyka, którego wzór zamieszczono w załączniku nr 4 do niniejszego Regulaminu.
2. Poziom uprawnień umożliwiający uruchamianie programów narzędziowych jest udokumentowany.
3. Administrator Systemu rejestruje 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/Właściciel Ryzyka 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/Właściciel Ryzyka 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/Właściciel Ryzyka w Centrali oraz w razie potrzeby, dyrektor oddziału regionalnego (zgodnie z §6 ust. 4 Polityki), który jest także Właścicielem Ryzyka w określonym terytorialnie zakresie zarządzania, dla użytkowników w oddziale regionalnym i przynależnych biurach powiatowych.
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/Właściciel Ryzyka 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/Właściciel Ryzyka na podstawie informacji dostarczonych przez Administratora Systemu.
3. W szczególności, Właściciel Procesu/Właściciel Zasobu/Właściciel Ryzyka 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/Właściciel Ryzyka, po zaakceptowaniu i wdrożeniu rozwiązań, o których mowa w ust. 3 pkt 3.
5. W umowie z Podmiotem zewnętrznym dotyczącej utrzymania systemów teleinformatycznych Agencji uwzględnia się zapis zobowiązujący Podmiot zewnętrzny do stosowania zasad i procedur wynikających z dokumentów polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji. Umowa z Podmiotem zewnętrznym może zawierać uszczegółowienie bądź rozszerzenie zasad wynikających z dokumentów polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji wynikające ze specyfiki danego projektu.
6. Doraźne działania serwisowe Podmiotów zewnętrznych (nie mające charakteru stałego utrzymania systemów teleinformatycznych) są dokumentowana przez Administratora Systemu w dzienniku pracy systemu. Zapis w dzienniku zawiera, co najmniej:
   1) dokładny czas rozpoczęcia i zakończenia działania serwisowego,
   2) identyfikacja osoby realizującej działania serwisowe po stronie Podmiotu zewnętrznego oraz nadzorującej te działania po stronie Agencji,
   3) dokładny opis przeprowadzonych działań wraz ze wskazaniem statusu tych działań (wymagające kontynuacji, zakończone).
7. Doraźne działania serwisowe w systemie teleinformatycznym osób, nie będących uprawnionymi pracownikami Agencji dokonywane są w obecności Administratora Systemu.

8. Osobie reprezentującej Podmiot zewnętrzny, wykonującej działania serwisowe, nie mogą zostać nadane uprawnienia administratora. Jeśli wyjątkowa sytuacja uzasadnia taką potrzebę, to nadanie uprawnienia wymaga zgody Właściciela Procesu/Właściciela Zasobu. Niezwłocznie po zakończeniu pracy uprawnienia administratora oraz jakiekolwiek inne uprawnienia nadane osobie reprezentującej Podmiot zewnętrzny muszą zostać odebrane.
9. W przypadku dokonywania zmian konfiguracji (naprawy, rekonfiguracje) przez stronę trzecią Agencja zapewnia odpowiednie uprawnienia do użycia oprogramowania narzędziowego służącego do celów zarządzania konfiguracją.

Rozdział 4.
Zarządzanie zmianami w systemach teleinformatycznych Agencji

§ 20.
Odbiór systemu teleinformatycznego

1. Kryteria odbioru obejmują dostarczenie:
   1) w przypadku oprogramowania - dokumentacji technicznej, instrukcji dla administratora i użytkownika,
   2) w przypadku infrastruktury - dokumentacji powykonawczej obejmującej w szczególności schemat połączeń fizycznych i logicznych elementów infrastruktury.
2. Ponadto, kryteria odbioru obejmują:
   1) wymagania wydajnościowe i pojemnościowe systemu teleinformatycznego,
   2) dokumenty potwierdzające, że instalacja nowych systemów nie będzie miała negatywnego wpływu na istniejące systemy, szczególnie w chwilach największego obciążenia (jeżeli ma zastosowanie),
   3) dokumenty potwierdzające, że wpływ nowych systemów na bezpieczeństwo informacji został oszacowany i że zastosowano odpowiednie środki techniczne i organizacyjne, zapewniające poziom bezpieczeństwa zgodny z polityką oraz przepisami prawa,
   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/Właściciel Ryzyka, zaś za wykonywanie 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/Właściciela Ryzyka.
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 podlegają 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 szafach zlokalizowanych w strefie administracyjnej.
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. Za zapewnienie bezpieczeństwa informacjom wrażliwym przewożonym pomiędzy lokalizacjami odpowiada pracownik przewożący.

§ 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/Właściciela Ryzyka.
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/ Właściciela Ryzyka.
2. Pracownik wyznaczony przez Właściciela Procesu/Właściciela Zasobu/Właściciela Ryzyka 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 Agencj ą 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 Administrator Systemu udostępnia na żądanie Właściciela Procesów/Właściciela Zasobów/Właściciela Ryzyka. Na podstawie przekazanego rejestru Właściciele Procesów/Właściciele Zasobów/Właściciele Ryzyka przeprowadzają przegląd uprawnień 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/Właściciela Ryzyka. 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/Właścicieli Ryzyka.
9. Konta domenowe użytkowników nieużywane przez okres 30 dni są 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 na danym 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 minimum algorytmem AES lub Twofish.
9. Do przechowywania hasła awaryjnego 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/Właściciela Ryzyka 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/Właściciela Ryzyka 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/Właściciela Ryzyka 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 informacji wyznaczony zespół w komórce właściwej ds. bezpieczeństwa, a także zespół Administratora 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, 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 mogą być prowadzone w oparciu o logi systemowe oraz inne rejestry zapewniające informacje o których mowa w ust. 1-4.
7. Dzienniki prowadzone są przez administratora odpowiedzialnego za dany serwer, urządzenie sieciowe, aplikację.
8. Dzienniki systemowe lub ich części prowadzone są w formie elektronicznej lub papierowej (dziennik może być prowadzony wg wzoru określonego w załączniku nr 3).
9. 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 jest na bieżąco monitorowany przez Administratora Systemu.
9. Zasilacze bezprzerwowe, 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 podlegają 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)

Decyzj a 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)