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

Zalecenia dla podmiotów wdrażających realizujących zadania delegowane w ramach PROW na lata 2014-2020

Warszawa, kwiecień 2015 r.

Spis treści:

SŁOWNIK TERMINÓW 3

I. OGÓLNE ZASADY WSPÓŁPRACY MIĘDZY AGENCJĄ PŁATNICZĄ A PODMIOTEM WDRAŻAJĄCYM 4

II. NADZÓR NAD BEZPIECZEŃSTWEM INFORMACJI. 5

III. PODSTAWOWE WYMAGANIA I OBOWIĄZKI UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO UDOSTĘPNIONEGO PRZEZ AGENCJĘ PŁATNICZĄ. 6

A. SZKOLENIA DLA UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO. 6
B. UŻYWANIE AUTORYZOWANYCH ŚRODKÓW DO PRZETWARZANIA INFORMACJI. 6
C. WYNOSZENIE MIENIA I KORZYSTANIE Z URZĄDZEŃ PRZENOŚNYCH 6
D. KORZYSTANIE Z SYSTEMU INFORMATYCZNEGO UDOSTĘPNIONEGO PRZEZ AGENCJĘ PŁATNICZĄ. 7
E. OCHRONA HASEŁ I KLUCZY KRYPTOGRAFICZNYCH 8
F. ZASADY „CZYSTEGO BIURKA I CZYSTEGO EKRANU” 8
G. ZGŁASZANIE ZDARZEŃ O NARUSZENIU BEZPIECZEŃSTWA INFORMACJI. 9

IV. BEZPIECZEŃSTWO FIZYCZNE. 11

A. OBSZARY BEZPIECZNE 11
B. ZARZĄDZANIE KLUCZAMI 12
C. LOKALIZACJA ORAZ OCHRONA SPRZĘTU I DOKUMENTACJI 13

V. BEZPIECZEŃSTWO INFORMACJI W ZARZĄDZANIU ZASOBAMI LUDZKIMI 14

VI. ZASADY EKSPLOATACJI SYSTEMU INFORMATYCZNEGO UDOSTĘPNIONEGO PRZEZ AGENCJE PŁATNICZĄ 15

1. OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM 15
2. ZASADY BEZPIECZEŃSTWA SIECI 15
3. IDENTYFIKACJA I UWIERZYTELNIANIE UŻYTKOWNIKÓW 15
4. ZARZĄDZANIE WYMIENNYMI NOŚNIKAMI DANYCH 16
5. KONSERWACJA I NAPRAWA SPRZĘTU 17
6. ZARZĄDZANIE DOSTĘPEM DO SYSTEMU INFORMATYCZNEGO 18

VII. OCHRONA DANYCH OSOBOWYCH 19

VIII. BEZPIECZEŃSTWO INFORMACJI W ZARZĄDZANIU CIĄGŁOŚCIĄ DZIAŁANIA 20

SŁOWNIK TERMINÓW

Występujące w opracowaniu zwroty i skróty oznaczają:

1) **Zalecenia** – niniejszy dokument „Zalecenia dla podmiotów wdrażających realizujących zadania delegowane w ramach PROW na lata 2014-2020";
2) **Agencja płatnicza –** Agencja Restrukturyzacji i Modernizacji Rolnictwa;
3) **podmiot wdrażający** – podmiot wykonujący zadania delegowane przez Agencję płatniczą w ramach PROW na lata 2014-2020 (samorząd województwa, Agencja Rynku Rolnego lub inny podmiot wdrażający, któremu Agencja płatnicza powierzyła wykonywanie tych zadań), realizujący zabezpieczenia zasobów informacyjnych;
4) **Plan Zapewnienia Ciągłości Działania (PZCD)** – plan kontynuowania działalności podmiotu wdrażającego zawierający udokumentowany zbiór procedur i informacji, które są opracowywane, integrowane oraz utrzymywane w gotowości do użycia w sytuacji kryzysowej;
5) **incydent bezpieczeństwa** – zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa informacji, zasobów materialnych lub zdrowia i życia pracowników;
6) **incydent związany z bezpieczeństwem informacji** – zdarzenie lub ciąg zdarzeń niepożądanych lub niespodziewanych, które stwarzają znaczne prawdopodobieństwo zakłócenia procesów biznesowych o istotnym znaczeniu w podmiocie wdrażającym albo ujawnienia informacji posiadających dużą wartość dla podmiotu wdrażającego lub chronionych z mocy prawa;
7) **informacja prawnie chroniona** – każda informacja, której utrata, ujawnienie lub udostępnienie osobie (podmiotowi) nieuprawnionemu mogłoby spowodować szkodę materialną lub niematerialną dla podmiotu wdrażającego lub naruszyć prawnie chroniony interes innych osób (podmiotów);
8) **informacja wrażliwa** – informacja, którą należy chronić ponieważ jej ujawnienie, modyfikacja, zniszczenie lub strata spowoduje zauważalną szkodę dla podmiotu wdrażającego;
9) **Inspektor Bezpieczeństwa Informacji (IBI)** – pracownik pełniący funkcję związaną z nadzorem nad bezpieczeństwem zasobów podmiotu wdrażającego, w tym nad bezpieczeństwem danych osobowych i innych informacji wrażliwych;
10) **logowanie** – proces uwierzytelniania użytkownika w systemie informatycznym udostępnionym przez Agencję płatniczą;
11) **nośnik informacji** – medium magnetyczne, optyczne, półprzewodnikowe lub papierowe, na którym zapisuje się i przechowuje informacje, forma utrwalenia dokumentu;
12) **strefa administracyjna** – obszar, gdzie kontrolowany jest ruch osobowy i materiałowy oraz, do którego dostęp posiadają wszyscy pracownicy podmiotu wdrażającego.

I. OGÓLNE ZASADY WSPÓŁPRACY MIĘDZY AGENCJĄ PŁATNICZĄ A PODMIOTEM WDRAŻAJĄCYM

Podmiot wdrażający zobowiązany jest dostosować bezpieczeństwo informacji – w obszarze przetwarzania danych dotyczących zadań delegowanych na podstawie umowy delegowania zadań Agencji płatniczej do podmiotów wdrażających – do wymagań normy ISO/IEC 27002 oraz od dnia 16.10.2016 r. do normy ISO/IEC 27001, z uwzględnieniem niniejszych *Zaleceń*.

Zalecenia przekładają się na następujące zasady współpracy między Agencją płatniczą a podmiotem wdrażającym:

1. Wytyczne zawarte w Zaleceniach nie zastępują norm: ISO/IEC 27001 oraz ISO/IEC 27002, stanowią jedynie uzupełnienie wymaganych do wdrożenia i stosowania w obszarze dotyczącym zadań delegowanych norm ISO/IEC 27002 i ISO/IEC 27001.
2. Przyjęty model współpracy zakłada, że podmioty wdrażające korzystają z dostępu do systemu informatycznego udostępnionego przez Agencję płatniczą używając określonych formularzy internetowych (tj. poprzez przeglądarkę internetową).
3. Zawarte w Zaleceniach wytyczne powinny znaleźć odzwierciedlenie w wewnętrznych dokumentach podmiotów wdrażających i być wprowadzone w życie w sposób formalnie przyjęty przez te podmioty.
4. Wymagane jest, aby wdrożenie Zaleceń dotyczących bezpieczeństwa informacji w podmiotach wdrażających odbyło się zgodnie z Harmonogramem dojścia do osiągnięcia gotowości do wykonywania przez podmioty wdrażające zadań delegowanych przez Agencję płatniczą w ramach PROW na lata 2014-2020 i znalazło odzwierciedlenie w Deklaracji gotowości lub Warunkowej deklaracji gotowości.

II. NADZÓR NAD BEZPIECZEŃSTWEM INFORMACJI.

1. Kierownik podmiotu wdrażającego realizuje nadzór i kontrolę nad bezpieczeństwem informacji bezpośrednio lub za pośrednictwem wyznaczonego pracownika pełniącego funkcję Inspektora Bezpieczeństwa Informacji (IBI).
2. Czynności kontrolne w ramach nadzoru nad bezpieczeństwem informacji realizowane są w terminach określonych harmonogramem realizacji zadań kontrolnych, nadzorczych i szkoleniowych opracowywanym na każdy rok kalendarzowy.
3. Harmonogram realizacji zadań kontrolnych, nadzorczych i szkoleniowych opracowuje Inspektor Bezpieczeństwa Informacji w uzgodnieniu z kierownikiem podmiotu wdrażającego lub osobiście kierownik podmiotu wdrażającego.
4. Wskazane jest prowadzenie następujących czynności kontrolnych:
   1) kontrola uprawnień dostępu użytkowników, tj. czy:
      - stosowane są unikalne identyfikatory zgodne z przyjętym schematem;
      - zablokowane zostały wszystkie zbędne identyfikatory (konta użytkowników);
      - przyznane uprawnienia dostępu do systemu informatycznego są zgodne z wnioskiem o nadanie / zmianę uprawnień, określonym przez Agencję płatniczą;
      - przyznane uprawnienia są zgodne z profilem dostępu (zakresem odpowiedzialności i uprawnień) na danym stanowisku pracy;
      - uprawnienia zawarte we wniosku o nadanie / zmianę uprawnień, określonym przez Agencję płatniczą, są zgodne z zakresem upoważnienia do przetwarzania danych osobowych;
      - terminy obowiązywania uprawnień są aktualne;
      - użytkownicy zostali poinformowani o zakresie swoich uprawnień i pisemnie potwierdzili zapoznanie się z nimi;
   2) kontrola wymagań bezpieczeństwa na stanowiskach realizujących zadania delegowane:
      - sprawdzenie, czy dostęp do systemu informatycznego wynikający z realizacji zadań delegowanych jest zgodny z aktualnym zakresem obowiązków pracownika;
   3) kontrola ewidencji osób, którym nadano upoważnienia do przetwarzania danych osobowych, tj. czy:
      - prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych jest kompletna i poprawna;
      - osoby upoważnione zostały przeszkolone z zakresu ochrony danych osobowych i podpisały stosowne oświadczenie.
5. Z każdej kontroli powinien być sporządzony raport.

III. PODSTAWOWE WYMAGANIA I OBOWIĄZKI UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO UDOSTĘPNIONEGO PRZEZ AGENCJĘ PŁATNICZĄ.

A. Szkolenia dla użytkowników systemu informatycznego.

1. Warunkiem uzyskania dostępu przez pracownika do systemu informatycznego powinno być odbycie szkolenia z zakresu bezpieczeństwa informacji.
2. Okresowo (nie rzadziej niż raz na rok) powinny być przeprowadzane szkolenia doskonalące z zakresu bezpieczeństwa informacji. Szkolenia powinny obejmować zagadnienia, które w szczególności dotyczą:
   1) zapoznania użytkowników z obowiązującymi regulacjami prawnymi dotyczącymi ochrony informacji;
   2) przygotowania użytkowników do właściwego korzystania z powierzonych zasobów (instrukcje użytkowania sprzętu i aplikacji, itp.);
   3) sposobu postępowania w przypadku zdarzenia związanego z naruszeniem bezpieczeństwa informacji,
   4) sposobów postępowania w sytuacjach awaryjnych i kryzysowych.

B. Używanie autoryzowanych środków do przetwarzania informacji.

1. Każdy środek do przetwarzania informacji powinien podlegać inwentaryzacji i autoryzacji (dopuszczenie do pracy w systemie informatycznym).
2. Użytkownik ponosi odpowiedzialność za powierzony sprzęt i oprogramowanie oraz sposób jego eksploatacji.
3. Użytkowników obowiązuje zakaz testowania lub podejmowania prób przełamywania zabezpieczeń systemu informatycznego.

C. Wynoszenie mienia i korzystanie z urządzeń przenośnych

1. Przez urządzenia przenośne, które mogą służyć do przetwarzania i przechowywania informacji poza siedzibą rozumie się nie tylko wszelkie formy komputerów osobistych, ale także wszelkie rodzaje organizerów, telefonów przenośnych, kart procesorowych, papieru i innych rodzajów nośników informacji używanych do pracy poza biurem podmiotu wdrażającego.
2. Komputery przenośne podlegają szczególnej ochronie polegającej na zabezpieczaniu dostępu do komputera hasłem. Ich używanie poza strefą administracyjną musi mieć uzasadnienie w realizowanych przez użytkownika zadaniach.
3. Na użytkowniku urządzenia przenośnego spoczywa obowiązek jego ochrony, w szczególności zabrania się pozostawiania bez opieki tego typu urządzenia w samochodach, przedziałach wagonów 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 biurem podmiotu wdrażającego, jeśli pozostają w postaci niezaszyfrowanej.
5. Każdy użytkownik, któremu powierzono urządzenie przenośne, przed rozpoczęciem użytkowania go poza biurem podmiotu wdrażającego, obowiązany jest do wystąpienia do pracownika bądź komórki odpowiedzialnej za utrzymanie infrastruktury

informatycznej z wnioskiem o zapewnienie środków techniczno-organizacyjnych gwarantujących poufność i integralność przetwarzanych informacji. Do środków tych zalicza się zabezpieczenia kryptograficzne oraz ochronę antywirusową.

6. W przypadku utraty powierzonego urządzenia przenośnego używanego poza biurem podmiotu wdrażającego użytkownik niezwłocznie powinien powiadomić o tym fakcie bezpośredniego przełożonego, a w przypadku kradzieży niezwłocznie zgłosić ten fakt na policję.

D. **Korzystanie z systemu informatycznego udostępnionego przez Agencję płatniczą.**

1. Każdy użytkownik otrzymuje prawa dostępu wyłącznie w zakresie niezbędnym do realizowania powierzonych zadań na danym stanowisku pracy.
2. Prawa dostępu są przydzielone po nadaniu użytkownikowi identyfikatora i hasła dostępu lub innych danych uwierzytelniających użytkownika, na podstawie wniosku o nadanie / zmianę uprawnień, złożonego na wzorze i zgodnie z zasadami określonymi przez Agencję płatniczą.
3. Każdy użytkownik musi posiadać w systemie informatycznym unikalny identyfikator.
4. Użytkownik ponosi odpowiedzialność za wszelkie czynności wykonane z użyciem jego identyfikatora i hasła.
5. W przypadku dłuższej nieobecności na stanowisku pracy użytkownik obowiązany jest zakończyć aktywne sesje i wylogować się. Ponadto, użytkownik każdorazowo w przypadku oddalenia się od stacji roboczej obowiązany jest zablokować dostęp do systemu informatycznego.
6. Na stacjach roboczych, na których wykonywane są zadania delegowane, powinno być zabronione m.in.:
   1) umożliwianie dostępu do systemu informatycznego osobom nieupoważnionym;
   2) rejestrowanie się w systemie informatycznym na identyfikatorze innego użytkownika;
   3) korzystanie z konta innego użytkownika;
   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 systemu informatycznego;
   6) samowolnego modyfikowania ustawień związanych z bezpieczeństwem w systemie informatycznym;
   7) świadome wprowadzanie błędnych danych do systemu informatycznego;
   8) udostępnianie danych osobom nieupoważnionym;
   9) przeglądanie stron internetowych o treściach pornograficznych, erotycznych, rasistowskich, użytkowanych przez grupy przestępcze i terrorystyczne;
   10) pobieranie z Internetu, kopiowanie, instalowanie, przechowywanie lub rozpowszechnianie nieautoryzowanego oprogramowania i danych;

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

E. **Ochrona haseł i kluczy kryptograficznych**

1. Hasła użytkowników lub inne dane uwierzytelniające muszą podlegać szczególnej ochronie.
2. Każdy użytkownik systemu informatycznego w podmiocie wdrażającym zobowiązany jest do:
   1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;
   2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
   3) poinformowania Inspektora Bezpieczeństwa Informacji lub kierownika podmiotu wdrażającego o podejrzeniu lub rzeczywistym ujawnieniu hasła;
   4) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych;
   5) zmiany wykorzystywanych haseł w regularnych odstępach czasu.
3. Zabronione powinno być:
   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).
4. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.
5. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić Inspektorowi Bezpieczeństwa Informacji lub kierownikowi podmiotu wdrażającego.

F. **Zasady „czystego biurka i czystego ekranu”**

1. Podmiot wdrażający powinien wprowadzić „politykę czystego biurka i ekranu” obejmującą następujące zasady:
   1) wszelkie dokumenty papierowe i nośniki elektroniczne zawierające dane związane z wykonywaniem zadań delegowanych, kiedy nie są używane, powinny być przechowywane w zamkniętym urządzeniu meblowym (sejf, szafa lub inna forma zabezpieczenia) szczególnie, jeśli w pomieszczeniu biurowym czasowo nie ma pracownika wykonującego te zadania i odpowiadającego za bezpieczeństwo danych;

2) monitory stacji roboczych należy ustawiać w taki sposób, żeby uniemożliwić osobom nieupoważnionym wgląd w zawartość ekranu;
3) komputery osobiste i stacje robocze pozostawiane bez nadzoru lub czasowo nieużywane muszą być wyrejestrowane z sieci lub zablokowane (za pomocą mechanizmu blokowania ekranu i klawiatury kontrolowanego hasłem, tokenem lub za pomocą innego podobnego mechanizmu);
4) po zakończeniu pracy należy wylogować się z systemu i wyłączyć komputer; niedopuszczalne jest zakończenie pracy bez wykonania pełnej i poprawnej procedury zamknięcia systemu lub przez wyłączenie napięcia zasilającego;
5) po zakończeniu pracy stanowisko pracy powinno być uporządkowane, w celu uniemożliwienia dostępu osób nieupoważnionych do dokumentów (w szczególności zawierających dane osobowe);
6) punkty przyjmowania i wysyłania korespondencji oraz nie nadzorowane faksy muszą być pod stałą ochroną;
7) w miejscach, gdzie przetwarzane są dane dotyczące zadań delegowanych powinien być wprowadzony zakaz korzystania bez autoryzacji z fotokopiarek lub innych technik kopiowania (np. skanerów, aparatów cyfrowych itp.);
8) wszelkie wydruki zawierające informacje związane z zadaniami delegowanymi powinny być niezwłocznie usuwane z drukarek, a wydruki uszkodzone natychmiast niszczone w niszczarce dokumentów;
9) nie należy pozostawiać wymiennych nośników komputerowych w napędach, bądź ogólnie dostępnych miejscach;
10) należy przestrzegać zasady niepozostawiania otwartych i niezabezpieczonych drzwi lub okien podczas nieobecności w pomieszczeniu.

G. **Zgłaszanie zdarzeń o naruszeniu bezpieczeństwa informacji.**

1. Przed przystąpieniem do pracy użytkownik obowiązany jest sprawdzić stację roboczą (komputer) i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub próbę naruszenia bezpieczeństwa informacji.
2. Do przypadków mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania lub słabości systemu informatycznego zalicza się m.in.:
   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) pojawianie się nietypowych komunikatów na ekranie;
   6) niemożność zalogowania się do systemu informatycznego;
   7) spowolnienie pracy oprogramowania;
   8) niestabilna praca systemu informatycznego;

9) brak reakcji systemu na działania użytkownika;
10) ponowny start lub zawieszanie się komputera;
11) ograniczenie funkcjonalności oprogramowania.

3. Wszelkie działania użytkownika związane z samodzielnym naprawianiem, potwierdzaniem lub testowaniem potencjalnych słabości systemu są zabronione.
4. Dokonywanie zmian w miejscu naruszenia ochrony bez wiedzy i zgody Inspektora Bezpieczeństwa Informacji lub kierownika podmiotu wdrażającego jest dopuszczalne jedynie w sytuacji, gdy zachodzi konieczność ratowania życia lub zdrowia osób oraz mienia w przypadku ich bezpośredniego zagrożenia.
5. W przypadku zauważenia zdarzenia mogącego świadczyć lub świadczącego o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania, błędach 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 Inspektora Bezpieczeństwa Informacji lub kierownika podmiotu wdrażającego oraz swojego bezpośredniego przełożonego.

IV. BEZPIECZEŃSTWO FIZYCZNE.

1. Zakres stosowania środków bezpieczeństwa fizycznego i środowiskowego powinien wynikać z przeprowadzonego i udokumentowanego szacowania ryzyka.
2. Szacowanie ryzyka i określanie wymagań bezpieczeństwa przeprowadza się w oparciu o:
   1) charakterystykę obiektu i pełnione przez niego funkcje, w szczególności rodzaj umieszczonych w nim zasobów podlegających ochronie (ludzie, dokumentacja, sprzęt komputerowy, itp.);
   2) określenie kategorii potencjalnych zagrożeń obiektu;
   3) opisu topografii, konstrukcji obiektu i architektury, najbliższego otoczenia (zabezpieczenia budowlane i mechaniczne, ogrodzenie, bramy, furty, oświetlenie, miejsca do parkowania, drogi komunikacyjne i ewakuacyjne, inne budowle i elementy towarzyszące);
   4) odnotowanych w przeszłości czynów przestępczych (rodzaj i typ czynu przestępczego, działania zewnętrzne, wewnętrzne, data, rozmiary, wartość szkody, wynik śledztwa);
   5) aktualnego stanu bezpieczeństwa obiektu;
   6) opisu i oceny funkcjonalności i poprawności zainstalowanych technicznych systemów zabezpieczenia, ich poprawności eksploatacji i aktualnego stanu technicznego (poziom technologiczny, sprawność, dokumentacja, serwisowanie);
   7) aktualnego stanu ochrony fizycznej obiektu;
   8) opisu stosowanych procedur i rozwiązań organizacyjnych;
   9) wniosków, co do odpowiedniości (w stosunku do rodzaju i stopnia zagrożeń) kompletności i poprawności zastosowanych zabezpieczeń (mechanicznych, technicznych i proceduralno–organizacyjnych);
   10) propozycji doskonalenia systemów oraz procedur ochrony obiektu.
3. Za opracowanie oraz stałą aktualizację planu ochrony fizycznej uwzględniającego wyniki szacowania ryzyka winien odpowiadać kierownik podmiotu wdrażającego lub pracownik, któremu powierzono zakres obowiązków związanych z zapewnieniem bezpieczeństwa fizycznego.

A. Obszary bezpieczne

1. Każdy podmiot wdrażający powinien wydzielić z obszaru zajmowanego przez komórki organizacyjne strefę administracyjną i strefę ogólnodostępną. Stacje robocze obsługujące zadania delegowane powinny być zlokalizowane w strefie administracyjnej.
2. Ochrona strefy administracyjnej oraz zastosowane środki bezpieczeństwa powinny być zgodne z zasadami określonymi w ustawie o ochronie osób i mienia i wynikać z opracowanego Planu Ochrony podmiotu wdrażającego.
3. W uzasadnionych przypadkach, gdy czynności związane z realizacją zadań delegowanych muszą być wykonywane przez podmiot wdrażający w ogólnodostępnej strefie, należy dodatkowo przyjąć następujące zasady:

1) strefa administracyjna dla zadań delegowanych może zostać zawężona do miejsc przechowywania bieżącej dokumentacji dotyczącej tych zadań, np. do zamykanych szaf biurowych;
2) stanowiska komputerowe, na których przetwarzane są informacje dotyczące zadań delegowanych powinny:
   - być tak usytuowane, aby uniemożliwić nieuprawnionym osobom przebywającym w pomieszczeniu podgląd danych wyświetlanych na monitorze lub wyprowadzanych na drukarkę;
   - stanowisko powinno być fizycznie wydzielone od pozostałej części pomieszczenia (np. barierką, słupkami i taśmą oddzielającą, itp.);
3) pracownicy w trakcie wykonywania zadań delegowanych odpowiadają bezpośrednio za zabezpieczenie stanowiska komputerowego oraz miejsc przechowywania dokumentacji przed fizycznym dostępem osób trzecich, w tym także przed możliwością podglądu informacji wyświetlanych na ekranie monitora lub drukowanych na drukarce;
4) w przypadku czasowej nieobecności pracownika wykonującego zadania delegowane, stanowisko komputerowe oraz miejsca przechowywania dokumentacji muszą być skutecznie zabezpieczone przed dostępem lub podglądem osób nieupoważnionych;

4. Wykonywanie w ogólnodostępnej strefie zadań delegowanych przez podmiot wdrażający musi być poprzedzone szacowaniem ryzyka i jest dopuszczalne wtedy, gdy poziom ryzyka nie przekracza akceptowalnego poziomu ryzyka.

B. **Zarządzanie kluczami**

1. Klucze wydawać należy na podstawie rejestru osób upoważnionych do ich pobierania, po sprawdzeniu tożsamości osoby pobierającej klucz. Fakt wydania kluczy i przyjęcia ich na przechowanie musi być odnotowywany.
2. Za organizację wydawania kluczy do pomieszczeń, w tym za przyznanie i odebranie prawa do ich pobierania, odpowiada kierownik podmiotu wdrażającego lub osoba przez niego wyznaczona.
3. Klucze do szaf i mebli biurowych, w których przechowywane są dokumenty zawierające informacje wrażliwe, nie mogą po zakończeniu pracy pozostawać w zamkach. Za organizację przechowywania takich kluczy odpowiada kierownik podmiotu wdrażającego lub osoba przez niego wyznaczona.
4. Pozostawanie osób po godzinach służbowych w pracy wymaga, aby spełnione były następujące warunki:
   1) każdy pracownik pozostający po godzinach służbowych w pracy musi mieć wyrażoną zgodę na pozostanie przez kierownika komórki organizacyjnej;
   2) jeśli po godzinach służbowych pozostaje więcej niż jedna osoba, kierownik komórki organizacyjnej (lub urzędu) wyznacza z tej grupy osobę, która będzie odpowiedzialna za właściwe zabezpieczenie obiektu (m.in. uzbrojenie instalacji alarmowej, zamknięcie drzwi wejściowych bądź dopilnowanie tych czynności w przypadku, gdy ktoś inny to wykonuje);

3) jeśli w danym dniu pozostają pracownicy po godzinach służbowych, to obowiązkiem osoby upoważnionej do zabezpieczenia i zamknięcia obiektu po zakończonej pracy, jest pobranie kluczy – na podstawie uzyskanej zgody na pozostanie w pracy.

C. **Lokalizacja oraz ochrona sprzętu i dokumentacji**

1. Środki przetwarzania informacji dotyczącej zadań delegowanych muszą spełniać następujące wymagania bezpieczeństwa:
   1) lokalizacja sprzętu powinna zapewnić minimalizację niepotrzebnego dostępu do obszarów pracy;
   2) lokalizacja środków przetwarzania powinna minimalizować ryzyko podejrzenia przez nieuprawnione osoby, a lokalizacja urządzeń przechowujących informacje zabezpieczać przed nieautoryzowanym dostępem.
2. Pomieszczenia, w których znajdują się szafy do przechowywania dokumentacji dotyczącej zadań delegowanych, powinny posiadać system sygnalizacji pożaru oraz system sygnalizacji włamania.
3. Urządzenia infrastruktury zabezpieczającej muszą być przeglądane i konserwowane zgodnie z instrukcjami i wymaganiami ich producentów.

V. BEZPIECZEŃSTWO INFORMACJI W ZARZĄDZANIU ZASOBAMI LUDZKIMI

1. Warunki przystąpienia do pracy, w zależności od zakresu obowiązków, powinny uwzględniać następujące aspekty bezpieczeństwa:
   1) przeszkolenie pracownika w zakresie tematycznym wynikającym z obowiązków i odpowiedzialności na zajmowanym stanowisku;
   2) oświadczenie pracownika o zapoznaniu się z odpowiednimi regulaminami, procedurami i przepisami w sprawie bezpieczeństwa informacji;
   3) przeszkolenie pracownika z zakresu bezpieczeństwa informacji (w tym ochrony danych osobowych), które przeprowadzić należy przed uzyskaniem dostępu do zasobów informacyjnych Agencji płatniczej;
   4) zobowiązanie pracownika do zachowania w poufności informacji prawnie chronionych, również poza biurem podmiotu wdrażającego i godzinami pracy, a także po ustaniu zatrudnienia bądź zakończeniu wykonywania usług na rzecz podmiotu wdrażającego;
   5) nadanie upoważnienia pracownikowi do przetwarzania danych osobowych.

VI. ZASADY EKSPLOATACJI SYSTEMU INFORMATYCZNEGO UDOSTĘPNIONEGO PRZEZ AGENCJĘ PŁATNICZĄ.

A. Ochrona przed szkodliwym oprogramowaniem

1. Stacje robocze i serwery podmiotu wdrażającego powinny być objęte ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory (firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie informatycznym.
2. Użytkowane poza systemem podmiotu wdrażającego wymienne nośniki komputerowe, przed rozpoczęciem pracy z tymi nośnikami w systemie informatycznym, należy sprawdzić za pomocą aktualnego oprogramowania antywirusowego.

B. Zasady bezpieczeństwa sieci

1. Sieć informatyczna podmiotu wdrażającego powinna być podłączona do sieci ogólnodostępnych (w szczególności sieci publicznej Internet) przy użyciu specjalnych systemów zabezpieczających, np. aplikacji i urządzeń typu firewall, systemów IDS (Intrusion Detection System) i IPS (Intrusion Prevention System).
2. Reguły filtrowania zapór sieciowych powinny być ustalane i regularnie weryfikowane w zależności od pojawiających się zagrożeń.
3. Wymagania odnoszące się do elementów bezpieczeństwa, poziomu usług i zarządzania wszystkimi usługami sieci muszą być jednoznacznie określone i włączone do odpowiednich umów na dostarczanie tych usług, niezależnie od tego, czy są one częściowo realizowane własnymi środkami, czy zlecane w całości na zewnątrz.

C. Identyfikacja i uwierzytelnianie użytkowników

1. Prawa dostępu do systemu informatycznego przydziela poszczególnym pracownikom podmiotu wdrażającego pracownik pełniący rolę lokalnego administratora podmiotu wdrażającego. Rolę tę nadaje administrator systemu informatycznego Agencji płatniczej. Dostęp do funkcji administracyjnych systemu z poziomu podmiotu wdrażającego jest możliwy tylko dla użytkownika w roli lokalnego administratora podmiotu wdrażającego.
2. Lokalny administrator podmiotu wdrażającego prowadzi rejestr użytkowników z nadanymi uprawnieniami.
3. Do obowiązków lokalnego administratora podmiotu wdrażającego należy także sprawdzanie i blokowanie zbędnych identyfikatorów użytkowników oraz ich kont, aby nie mogły być one wykorzystane powtórnie przez innych użytkowników.
4. Lokalny administrator podmiotu wdrażającego poprzez ustawienia systemowe wymusza natychmiastową zmianę hasła początkowego, przydzielonego użytkownikowi, na nowe przez niego wybrane. Hasło tymczasowe, dostarczane w przypadku, gdy użytkownik zapomni hasła, może być wydane dopiero po pozytywnej weryfikacji tożsamości użytkownika.
5. Zabronione jest przekazywanie haseł przez osoby trzecie lub za pośrednictwem otwartych wiadomości poczty elektronicznej.

6. Kontrola praw dostępu użytkowników realizowana jest przez lokalnego administratora podmiotu wdrażającego według następujących zasad:
   1) prawa dostępu użytkowników są przeglądane w regularnych odstępach czasu (nie rzadziej niż co sześć miesięcy) oraz każdorazowo po wprowadzeniu zmian w tych prawach;
   2) w przypadku zmiany miejsca zatrudnienia pracownika, dokonuje się dodatkowego przeglądu i ponownego nadania praw dostępu;
   3) przydzielone uprawnienia są kontrolowane w regularnych odstępach czasu w celu sprawdzenia, czy nie przyznano nadmiarowych uprawnień;
   4) uprawnienia do korzystania ze specjalnie uprzywilejowanych praw dostępu (np. prawa administratora) winny być przeglądane nie rzadziej niż co trzy miesiące;
   5) powinna być prowadzona rejestracja zmian uprzywilejowanych kont na potrzeby okresowych przeglądów;
   6) każde dokonanie kontroli praw dostępu użytkowników powinno zostać udokumentowane sporządzeniem raportu, który należy załączyć do prowadzonej dokumentacji przez lokalnego administratora podmiotu wdrażającego.

D. Zarządzanie wymiennymi nośnikami danych

1. Wymienne nośniki informacji (tzn. taśmy, dyskietki, pamięci typu flash, wyjmowane dyski twarde, płyty CD i DVD oraz wydruki) zawierające informację prawnie chronioną należy przechowywać w miejscach uniemożliwiających dostęp do nich osobom nieuprawnionym.
2. Wszystkie nośniki informacji muszą być przechowywane w bezpiecznym środowisku w warunkach zgodnych z wymaganiami producenta. W przypadku, gdy czas życia nośnika (określony przez producenta) jest krótszy od sumarycznego czasu przechowywania informacji, należy dodatkowo zapewnić, aby na skutek pogorszenia się jakości nośnika nie nastąpiła utrata informacji.
3. Magnetyczne nośniki informacji zawierające kopie bezpieczeństwa oraz informacje archiwalne należy przechowywać w specjalnych, atestowanych, metalowych szafach do przechowywania magnetycznych nośników informacji. Pozostałe nośniki przechowywać i zabezpieczać należy zgodnie z wymaganiami obowiązującymi dla informacji na nich zapisanych.
4. Ograniczać należy do niezbędnego minimum liczby wytwarzanych kopii i wydruków.
5. Zbędne wydruki, notatki, kopie dokumentów, itp. – jeśli zawierają informację prawnie chronioną – muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich treści.
6. Wszystkie nośniki informacji (dyskietki, taśmy magnetyczne, płyty CD-ROM, wymienne dyski twarde, wydruki komputerowe i inne) wytworzone w systemach informatycznych i zawierające informacje prawnie chronione, muszą być ewidencjonowane i oznakowane.
7. Etykiety nośników informacji powinny posiadać identyfikator lub numer umożliwiający ich jednoznaczną klasyfikację i znajdujący odzwierciedlenie w dzienniku ewidencji nośników.

8. Na podstawie etykiety nośnika informacji i danych zawartych w dzienniku ewidencji nośników powinno być możliwe ustalenie:
   1) numeru ewidencyjnego nośnika,
   2) typu nośnika,
   3) daty zapisu na nośniku,
   4) nazwy komórki organizacyjnej składującej informacje,
   5) określenia rodzaju przechowywanej informacji,
   6) imienia i nazwiska osoby dokonującej zapisu.
9. Wycofane nośniki informacji, które były wykorzystywane do przetwarzania informacji chronionych, nie mogą być wynoszone poza teren jednostki wdrażającej, w której były użytkowane, bez wcześniejszego skutecznego usunięcia danych.
10. Uszkodzone nośniki, takie jak dyski twarde, dyskietki i taśmy magnetyczne, płyty CD-ROM i inne komputerowe nośniki danych, zawierające informację prawnie chronioną, należy komisyjnie niszczyć w sposób uniemożliwiający odczytanie zapisanych na nich informacji (np. zgniatanie, łamanie, działanie silnym polem magnetycznym).
11. Wycofanie z eksploatacji wymiennych nośników komputerowych, przekazanie do naprawy lub ponownego użycia powinno być poprzedzone archiwizacją, a następnie skutecznym usunięciem zapisanych danych.

E. Konserwacja i naprawa sprzętu

1. Sprzęt informatyczny winien podlegać konserwacji według ustalonego planu, wynikającego z zaleceń jego producenta.
2. Konserwacja i naprawy mogą być prowadzone jedynie przez uprawniony personel lub podmiot zewnętrzny świadczący tego rodzaju usługi na podstawie umowy lub w ramach gwarancji.
3. W przypadku, gdy na nośnikach informacji, stanowiących integralną część sprzętu przekazywanego do naprawy, znajduje się informacja prawnie chroniona, sprzęt taki naprawiany powinien być pod nadzorem uprawnionego pracownika podmiotu wykonującego zadania delegowane. Jeżeli taki nadzór nie jest możliwy, informacja prawnie chroniona musi zostać skutecznie usunięta. O ile zachodzi taka możliwość, usuwana informacja powinna być uprzednio zarchiwizowana.
4. Jeżeli gwarant, w ramach naprawy gwarancyjnej, żąda zwrotu urządzenia służącego do przechowywania informacji, informacja prawnie chroniona znajdująca się w takim urządzeniu musi zostać z niego trwale usunięta. Sposób usuwania danych z nośnika powinny określać szczegółowe procedury.
5. Umowy zawierające gwarancję dostawcy lub producenta muszą zawierać sformułowania umożliwiające realizację postanowień ust. 4 bez utraty gwarancji.
6. W przypadku zbywania sprzętu, bądź przekazywania go do ponownego użycia, należy skutecznie usunąć z niego informacje prawnie chronione. Sposób usuwania danych muszą określać szczegółowe procedury.

F. Zarządzanie dostępem do systemu operacyjnego

1. Wszystkie konta użytkowników na stacjach roboczych, na których wykonywane są zadania delegowane, powinny być skonfigurowane z uprawnieniami systemowymi „użytkownik”.
2. Użytkownik systemu operacyjnego powinien być jednoznacznie identyfikowany poprzez indywidualny identyfikator (nazwę) użytkownika.
3. Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego użytkownika.
4. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.
5. Uprawnienia dostępu mogą być nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzeby wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień administratora (przywilejów) powinno być traktowane jako incydent związany z bezpieczeństwem informacji.

VII. OCHRONA DANYCH OSOBOWYCH

1. Kierownik podmiotu wdrażającego wykonuje obowiązki Administratora danych wobec powierzonych mu danych.
2. Kierownik podmiotu wdrażającego odpowiada za realizację ustawowych obowiązków Administratora danych, a w szczególności, w odniesieniu do wykonywania zadań delegowanych, odpowiada za:
   1) zgodne z prawem przetwarzanie danych osobowych;
   2) zapewnienie, aby zgromadzone dane osobowe były merytorycznie poprawne, a ich zakres i rodzaj był adekwatny do celów, w jakich są przetwarzane;
   3) nadawanie upoważnień do przetwarzania danych osobowych;
   4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, o której mowa w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
   5) zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
3. Upoważnienie do przetwarzania danych osobowych nadaje się przed dopuszczeniem osoby do wykonywania obowiązków służbowych związanych z przetwarzaniem danych osobowych. Upoważnienie odbiera się niezwłocznie po ustaniu celu, dla którego zostało nadane.
4. Upoważnienie do przetwarzania danych osobowych nadawane jest pracownikom, bez względu na podstawę prawną zatrudnienia, po odbyciu szkolenia z ochrony danych osobowych, a fakt odbycia przeszkolenia pracownik powinien potwierdzić podpisując stosowne oświadczenie.

VIII. BEZPIECZEŃSTWO INFORMACJI W ZARZĄDZANIU CIĄGŁOŚCIĄ DZIAŁANIA

1. W przypadku, gdy podmiot wdrażający nie posiada planu PZCD, niezbędne jest opracowanie dokumentu, który określi warunki realizacji zadań delegowanych w sytuacji wystąpienia kryzysu. Dokument taki powinien uwzględniać następujące czynniki:
   1) rozpoznanie i uzgodnienie wszystkich procedur awaryjnych i zakresów odpowiedzialności w obszarze zadań delegowanych;
   2) wdrożenie procedur awaryjnych tak, aby umożliwić naprawę i przywrócenie działania w wymaganym czasie z uwzględnieniem zewnętrznych zależności biznesowych (pomiędzy podmiotem wdrażającym a Agencją płatniczą) oraz realizowanych procesów;
   3) dokumentację uzgodnionych procedur oraz procesów operacyjnych i pomocniczych;
   4) przeszkolenie personelu w zakresie uzgodnionych procedur awaryjnych, w tym w zakresie zarządzania w sytuacjach kryzysowych;
   5) procedury awaryjne objęte powyższym dokumentem powinny być przetestowane w roku, w którym uruchomiono realizację zadań delegowanych, a następnie w cyklu rocznym testy winny być powtarzane.
2. Jeśli podmiot wykonujący zadania delegowane opracował i utrzymuje aktualny plan działania PZCD, to do powyższego planu należy włączyć procedury określające sposób postępowania z zadaniami delegowanymi na wypadek wystąpienia kryzysu.