

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

.....


Informacje wstępne:

Niniejszy dokument jest wzorem do opracowania instrukcji zarządzania systemem teleinformatycznym dla danego systemu/usługi, obowiązującym w Ministerstwie Finansów.

Instrukcja zarządzania systemem informatycznym musi być opracowana dla każdego wdrażanego i eksploatowanego systemu/usługi oraz jej opracowanie jest elementem koniecznym do dopuszczenia systemu/usługi do wykorzystania produkcyjnego.

Instrukcja zarządzania systemem informatycznym dla danego systemu/usługi musi być opracowana według niniejszego układu, z uwzględnieniem właściwych dla danego systemu/usługi elementów.

Wzór nie ma zastosowania do systemów teleinformatycznych akredytowanych do przetwarzania informacji niejawnych, znajdujących się w wykazie STI Pełnomocnika ds. informacji niejawnych.

| | | |
|---|--|---------------|
|  Ministerstwo Finansów | Instrukcja zarządzania systemem informatycznym | Strona: 2 /27 |
|---|--|---------------|

| MINISTERSTWO FINANSÓW / KRAJOWA ADMINISTRACJA SKARBOWA | | | | | | |
|--|--|-------------------|------|--|--------|--|
| Nazwa | INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM | | | | | |
| Krótki opis dokumentu | Dokument określa metody, środki i procedury zarządzania systemem oraz zabezpieczania systemu | | | | | |
| Właściciel dokumentu | Departament | | | | | |
| Opracowany przez | Nazwa komórki organizacyjnej | Departament | | | | |
| Akceptacja w zakresie merytorycznym | Imię i nazwisko, stanowisko | | Data | | Podpis | |
| Departament (...) | | | | | | |
| Akceptacja w zakresie bezpieczeństwa teleinformatycznego oraz zabezpieczeń technicznych | Imię i nazwisko, stanowisko | | Data | | Podpis | |
| Centrum Informatyki Resortu Finansów (CIRF) | | | | | | |
| Akceptacja w zakresie bezpieczeństwa informacji i przepisów dotyczących ochrony danych osobowych | Imię i nazwisko, stanowisko | | Data | | Podpis | |
| Departament Bezpieczeństwa i Ochrony Informacji (DB) | | | | | | |
| Zatwierdził | Imię i nazwisko, stanowisko | | Data | | Podpis | |

Historia zmian dokumentu

| Nr wersji | Data wydania | Opis | Akcja (*) | Rozdziały (**) | Autorzy (***) |
|-----------|--------------|----------------------|-----------|----------------|---------------|
| 1.00 | | Utworzenie dokumentu | N | W | |
| | | | | | |
| | | | | | |
| | | | | | |

(*) Akcje: W = Wstaw, Z = Zamień, We = Weryfikuj, N = Nowy

(**) Rozdziały: W = Wszystkie

(***) Autorzy: patrz metryka dokumentu.

SPIS TREŚCI

| | | |
|-------|---|----|
| 1 | WYKAZ SKRÓTÓW I TERMINÓW | 6 |
| 2 | CEL INSTRUKCJI ZARZĄDZANIA SYSTEMEM..... | 8 |
| 3 | ZAKRES I WARUNKI STOSOWANIA DOKUMENTU | 8 |
| 4 | DOKUMENTY POWIĄZANE..... | 8 |
| 5 | ODPOWIEDZIALNOŚĆ | 8 |
| | PODMIOTY ZEWNĘTRZNE BIORĄCE UDZIAŁ W REALIZACJI USŁUGI/PROCESU W SYSTEMIE | 11 |
| 6. | OPIS SYSTEMU | 11 |
| 6.1. | KLASYFIKACJA INFORMACJI - GRUPY INFORMACJI PRZETWARZANYCH W SYSTEMIE..... | 11 |
| 6.2. | PRZEPŁYW DANYCH I INFORMACJI W SYSTEMIE | 12 |
| 7. | ZARZĄDZANIE UPRAWNIENIAMI W SYSTEMIE..... | 12 |
| 7.1 | RODZAJE KONT UŻYTKOWIKÓW W SYSTEMIE I UPRAWNIENIA | 12 |
| 7.2 | WNIOSEK O NADAWANIE, MODYFIKACJĘ, ODBIÓR UPRAWNIEŃ..... | 12 |
| 7.3 | AKCEPTACJA LUB ODRZUCENIE WNIOSKU PRZEZ WŁAŚCIELA BIZNESOWEGO SYSTEMU | 12 |
| 7.4 | NADAWANIE, MODYFIKACJA, ODBIERANIE UPRAWNIEŃ | 12 |
| 7.5 | PRZEGLĄD PRAW DOSTĘPU UŻYTKOWNIKÓW | 13 |
| 8. | ŚRODKI I METODY UWIERZYTELNIANIA UŻYTKOWNIKÓW W SYSTEMIE | 13 |
| 9. | ROZPOCZYNIANIE, ZAWIESZANIE I KOŃCZENIE PRACY W SYSTEMIE | 13 |
| 10. | ZDALNY DOSTĘP DO SYSTEMU | 13 |
| 11. | BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE INFRASTRUKTURY TELEINFORMATYCZNEJ13 | |
| | 11.2 SPECYFICZNE WYMAGANIA W ZAKRESIE OCHRONY STACJI ROBOCZYCH UŻYTKOWNIKÓW WEWNĘTRZNYCH ORAZ ZEWNĘTRZNYCH | 15 |
| 12. | ŚRODKI OCHRONY ZASOBÓW INFORMACYJNYCH SYSTEMU | 15 |
| 11. | ADMINISTROWANIE BEZPIECZEŃSTWEM /PROCEDURY USTANWIONE PRZEZ WŁAŚCIELA BIZNESOWEGO SYSTEMU I DANYCH | 22 |
| 11.1 | PROCEDURY TWORZENIA KOPII ZAPASOWYCH | 22 |
| 11.2 | PROCEDURY EKSPLOATACYJNE..... | 22 |
| 11.3 | PROCEDURY AWARYJNE..... | 23 |
| 11.4 | ZASADY I SZCZEGÓLNE ŚRODKI OCHRONY DANYCH STANOWIĄCYCH INFORMACJE PRAWNIE CHRONIONE | 23 |
| 11.5 | OPIS INNYCH ZAŁOŻEŃ BEZPIECZNEJ EKSPLOTACJI, W TYM ROZLICZALNOŚĆ..... | 23 |
| 12 | SZKOLENIA..... | 23 |
| 13 | DEKLARACJA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH W SYSTEMIE..... | 23 |
| 13.1 | REJESTROWANIE I RAPORTOWANIE OPERACJI PRZETWARZANIA: | 23 |
| 13.2. | PRZETWARZANIE DANYCH OSOBOWYCH ZGODNIE Z RODO I/LUB „USTAWĄ POLICYJNĄ” - REALIZACJA PRAW OSÓB FIZYCZNYCH Z WYKORZYSTANIEM SYSTEMU INFORMATYCZNEGO..... | 24 |
| 14. | ZAŁĄCZNIKI..... | 26 |

1 WYKAZ SKRÓTÓW I TERMINÓW

/DO ZWERYFIKOWNIA I UZUPEŁNIENIA DLA DANEGO SYTEMU I INSTRUKCJI/

| | | |
|-----|--|--|
| 1) | IOD - Inspektor Ochrony Danych | Osoba wyznaczona przez Administratora, zgodnie z art. 37 RODO i art. 46 ustawy policyjnej, realizującą zadania określone w art. 39 ust. 1 RODO i art. 47 ust. 1 ustawy policyjnej, a także - w przypadku nieobecności IOD MF - osobę wyznaczoną przez Administratora do zastępowania IOD MF |
| 2) | Administrator | Administrator (danych osobowych) w rozumieniu art. 4 pkt. 7 RODO. |
| 3) | MF | Ministerstwo Finansów |
| 4) | Szef KAS | Szef Krajowej Administracji Skarbowej |
| 5) | IAS | Izba Administracji Skarbowej |
| 6) | UCS | Urząd Celno-Skarbowy |
| 7) | US | Urząd Skarbowy |
| 8) | KIS | Krajowa Informacja Skarbowa |
| 9) | KSS | Krajowa Administracja Skarbowa |
| 10) | CIRF | Centrum Informatyki Resortu Finansów |
| 11) | ASI - Administrator systemu teleinformatycznego | Pracownik, wyznaczony zgodnie z PBT przez dyrektora komórki organizacyjnej w Ministerstwie właściwej do spraw informatyzacji, przez dyrektora CIRF albo przez Dyrektora IAS, jeżeli IAS wykonuje zadania centrum kompetencyjnego lub zadania scentralizowane, o ile zakres zadań obejmuje administrowanie systemem teleinformatycznym służącym do przetwarzania danych osobowych, odpowiedzialnego za administrowanie i monitorowanie systemu teleinformatycznego służącego do przetwarzania danych osobowych oraz zapewnienie jego bezpiecznej eksploatacji, zgodnie z zadaniami określonymi w PBT; |
| 12) | AZU - Administrator zarządzający uprawnieniami | Pracownik, wyznaczony zgodnie z PBT przez dyrektora komórki organizacyjnej w Ministerstwie pełniący funkcję właściciela biznesowego systemu teleinformatycznego w porozumieniu z dyrektorem komórki organizacyjnej w Ministerstwie właściwej do spraw informatyzacji albo przez Dyrektora IAS, jeżeli IAS wykonuje zadania centrum kompetencyjnego lub zadania scentralizowane, o ile zakres zadań obejmuje zarządzanie uprawnieniami w systemie teleinformatycznym służącym do przetwarzania danych osobowych, wykonującego zadania w zakresie zarządzania uprawnieniami użytkowników w systemie teleinformatycznym służącym do przetwarzania danych osobowych; |
| 13) | Koordynator merytoryczny systemu teleinformatycznego | Pracownik wyznaczony przez dyrektora komórki organizacyjnej w Ministerstwie pełniący funkcję właściciela biznesowego systemu teleinformatycznego; |
| 14) | Właściciel biznesowy danych | Komórka organizacyjna w Ministerstwie odpowiedzialna merytorycznie za przetwarzanie danych, w szczególności danych osobowych, w zakresie wynikającym z zadań określonych w Regulaminie organizacyjnym Ministerstwa. Właściciel biznesowy danych może być jednocześnie Właścicielem biznesowym systemu teleinformatycznego; |
| 15) | Właściciel biznesowy systemu teleinformatycznego | Komórka organizacyjna w Ministerstwie odpowiedzialna za wykonywanie zadań właściciela biznesowego w odniesieniu do przypisanego systemu teleinformatycznego służącego do przetwarzania danych osobowych, w zakresie określonym w Regulaminie organizacyjnym Ministerstwa. |
| 16) | Użytkownik | Pracownik MF lub jednostki organizacyjnej KAS posiadający uprawnienia do dostępu do systemu/ korzystający z usługi |

| | | |
|-----|--------------------------------|--|
| 17) | Pracownik | Osoba fizyczna realizująca zadania na rzecz Ministerstwa lub na rzecz Jednostki na podstawie umowy o pracę, powołania, mianowania albo umowy cywilnoprawnej, osobę pełniącą w niej służbę, w tym funkcjonariusza Służby Celno-Skarbowej, oraz praktykanta, stażystę lub wolontariusza; |
| 18) | DB | Departament Bezpieczeństwa i Ochrony Informacji |
| 19) | DZI | Departament Zarządzania Informatyzacją |
| 20) | KAS | Krajowa Administracja Skarbowa |
| 21) | CRDP | Centralny Rejestr Danych Podatkowych |
| 22) | UPO | Upoważnienie do przetwarzania danych osobowych |
| 23) | IZSI | Instrukcja Zarządzania Systemem Informatycznym |
| 24) | PODO | Polityka Ochrony Danych Osobowych wprowadzona Zarządzeniem Ministra finansów, funduszy i polityki regionalnej z dnia 29 grudnia 2020 r. |
| 25) | Integralność | Właściwość polegająca na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony. |
| 26) | Dostępność | Właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym. |
| 27) | Niezawodność | Zapewnienie spójności oraz zamierzonych zachowań i skutków. |
| 28) | Poufność | Zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom. |
| 29) | Rozliczalność | Właściwość systemu pozwalająca przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie |
| 30) | Dane osobowe | Zgodnie z definicją z art. 4 pkt 1 RODO, dane osobowe to: „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej”. |
| 31) | Przetwarzanie danych osobowych | Zgodnie z definicją z art. 4 pkt 2 RODO przetwarzanie danych osobowych oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. |
| 32) | RODO | 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). |
| 33) | PBI | Polityka Bezpieczeństwa Informacji |
| 34) | PBT | Polityka Bezpieczeństwa Teleinformatycznego |
| 35) | | |
| 36) | | |
| 37) | | |

| | | |
|-----|--|--|
| 38) | | |
| 39) | | |
| 40) | | |
| 41) | | |
| 42) | | |

2 CEL INSTRUKCJI ZARZĄDZANIA SYSTEMEM

(zweryfikować i uzupełnić)

Celem opracowania Instrukcji Zarządzania Systemem Informatycznym, jest określenie zasad zarządzania i zabezpieczania systemu. Przyjęte rozwiązania w zakresie środków technicznych, organizacyjnych oraz fizycznych są poddawane przeglądowi i uaktualniane w razie potrzeby, w kontekście bezpieczeństwa danych przetwarzanych w systemie. Ochronie podlegają dane, infrastruktura teleinformatyczna, w tym sprzęt komputerowy, systemy operacyjne i informatyczne oraz pomieszczenia, w których odbywa się proces przetwarzania danych. Zamieszczone w Instrukcji zapisy mają na celu ochronę danych przetwarzanych w Systemie przed udostępnieniem ich osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem danych z naruszeniem przepisów prawa, w szczególności dotyczących informacji prawnie chronionych, nieuprawnioną zmianą danych, ich utratą, uszkodzeniem lub zniszczeniem.

Załącznikami do niniejszego dokumentu są instrukcje i procedury, zgodnie z wykazem zamieszczonym w pkt 14.

3 ZAKRES I WARUNKI STOSOWANIA DOKUMENTU

(zweryfikować i uzupełnić)

Instrukcja Zarządzania Systemem określa zasady ochrony danych przetwarzanych w systemie, wszystkich zasobów technicznych oraz obszarów przetwarzania. Określa również zasady postępowania użytkowników.

Dokument opisuje infrastrukturę sprzętowo-systemową oraz umiejscowienie systemu w ramach eksploatowanych w resorcie finansów systemów informatycznych realizujących podstawowe cele biznesowe. Dokument zawiera opis wzajemnych relacji wewnątrz systemu oraz powiązań międzysystemowych z systemami informatycznymi bezpośrednio związanymi z systemem Dokument zawiera opis elementów infrastruktury sieciowej, wyłącznie w zakresie pozwalającym na zrozumienie zasad funkcjonowania systemu, nie zawiera, więc pełnej charakterystyki środowiska sieciowego. W niniejszym dokumencie nie zostały zawarte szczegółowe informacje o systemach współpracujących z systemem.....oraz o zastosowanych w nich środkach ochrony.

4 DOKUMENTY POWIĄZANE

W tym punkcie należy przedstawić przepisy prawne, dokumenty normatywne, normy, standardy techniczne, wytyczne, umowy i inne opracowania związane z bezpieczeństwem systemu/usługi wykorzystane przy opracowaniu dokumentacji bezpieczeństwa systemu.

5 ODPOWIEDZIALNOŚĆ

(zweryfikować i uzupełnić)

Niniejszy dokument, dedykowany jest wszystkim osobom i podmiotom odpowiedzialnym za prawidłowe funkcjonowanie systemu oraz za jego eksploatację. Za przestrzeganie zasad wymienionych w niniejszej instrukcji i procedurach odpowiadają niżej wskazane osoby/podmioty, w związku z określonymi w IZIS lub politykach i procedurach z nią powiązanych, zadaniami i w ramach zakresu odpowiedzialności.

| NAZWA ROLI | OPIS ZAKRESU ODPOWIEDZIALNOŚCI |
|---------------|---|
| Administrator | Administratorem jest Określone w PODO zadania administratora danych, w odniesieniu do danych przetwarzanych w systemie realizuje zgodnie z |

| | |
|--|--|
| | <p>upoważnieniem Ministra Finansów, Funduszy i Polityki Regionalnej/Szefa KAS Dyrektor Departamentu (...), który w szczególności:</p> <ol style="list-style-type: none"> 1) sprawuje, nadzór nad bezpieczeństwem danych osobowych przetwarzanych za pomocą systemu, 2) zatwierdza dokumenty związane z systemem oraz zarządza nimi. |
| Właściciel biznesowy systemu teleinformatycznego | <p>Dyrektor Departamentu (...), wykonuje zadania właściciela biznesowego systemu, a w szczególności:</p> <ol style="list-style-type: none"> 1) zapewnia zgodność rozwiązań organizacyjnych systemu z obowiązującymi uregulowaniami prawnymi w tym zakresie, 2) sprawuje, nadzór nad bezpieczeństwem danych, w tym danych osobowych przetwarzanych za pomocą systemu, 3) określa i analizuje wymagania nefunkcjonalne systemu, 4) zapewnia spełnianie wymagań funkcjonalnych i pozafunkcjonalnych, 5) zatwierdza dokumenty związane z systemem, 6) aktualizuje dokumenty związane z systemem, 7) wyznacza AZU we współpracy z CIRF, 8) zatwierdza wnioski o nadanie, modyfikację lub odebranie uprawnień do systemu dla użytkowników z MF, 9) prowadzi ewidencję wszystkich użytkowników, 10) zgłasza i aktualizuje czynności przetwarzania danych osobowych realizowane przy wsparciu systemu w rejestrze czynności przetwarzania, zapewnia opis systemu w REJS i jego aktualizację, 11) zatwierdza raport bezpieczeństwa w systemie REJS, 12) współpracuje z IOD. |
| Właściciel biznesowy danych | <p>Dyrektor Departamentu (...), wykonuje zadania właściciela biznesowego danych, a w szczególności danych osobowych. Właściciel biznesowy danych:</p> <ol style="list-style-type: none"> 1) odpowiada za określenie i analizę wymagań funkcjonalnych, 2) odpowiada za określenie katalogu danych (w ramach klasyfikacji informacji) przetwarzanych w systemie; 3) zgłasza i aktualizuje czynności przetwarzania danych osobowych realizowane przy wsparciu systemu w rejestrze czynności przetwarzania, 4) współpracuje z IOD. |
| Koordynator merytoryczny systemu teleinformatycznego | <p>Pracownik wyznaczony przez dyrektora Departamentu (...) pełniący funkcję właściciela biznesowego systemu teleinformatycznego.</p> <p>Do zadań koordynatora merytorycznego systemu teleinformatycznego należy koordynacja zadań właściciela biznesowego systemu teleinformatycznego oraz:</p> <ol style="list-style-type: none"> 1) zarządzanie ryzykiem związanym z przetwarzaniem danych, w tym danych osobowych w systemie teleinformatycznym, zgodnie z procedurą zarządzania ryzykiem; 2) udzielanie wsparcia w zakresie znajomości funkcjonalności systemu; 3) zapewnienie zgodności systemu teleinformatycznego z wymaganiami wynikającymi z PODO oraz przywołanych w niej dokumentów, w tym polityk szczegółowych, procedur i instrukcji dotyczących systemów teleinformatycznych oraz ochrony danych osobowych; 4) zarządzanie procesem nadawania, modyfikacji i odbierania uprawnień, zgodnie z procedurą zarządzania uprawnieniami w systemach teleinformatycznych służących do przetwarzania danych osobowych; 5) inicjowanie działań mających na celu rozwój systemu teleinformatycznego; 6) współpraca z IOD w zakresie ochrony danych osobowych w systemie teleinformatycznym. |

| | |
|--|--|
| | |
| <p>Administrator Systemu Teleinformatycznego (ASI)</p> | <p>Do zadań ASI wyznaczonego przez CIRF należy utrzymanie systemu w zakresie:</p> <ol style="list-style-type: none"> 1) Sieci: <ul style="list-style-type: none"> • archiwizowanie konfiguracji urządzeń, • instalowanie nowych wersji oprogramowania, • konfigurowanie interfejsów sieciowych, • zarządzania siecią, • zarządzanie bezpieczeństwem sieci, 2) Kopii zapasowych: <ul style="list-style-type: none"> • wykonywanie backupów zgodnie z harmonogramem oraz odtwarzanie na żądanie, • konfiguracja systemu backupu w celu dotrzymania parametrów RTO i RPO dla danego bloku architektonicznego, • monitoring poprawności realizacji procesu backupu poszczególnych zasobów bloków architektonicznych, • utrzymywanie i przekazywanie aktualnej polityki backupu dla poszczególnych bloków architektonicznych, harmonogramu realizacji backupu, informacji dot. okien backupowych, • utrzymywanie aktualnej procedury określającej zasady odtwarzania zasobów poszczególnych bloków z backupu, • udział w realizacji ww. procedury, 3) Systemu operacyjnego, infrastruktury serwerowej, aktualizacji systemu: <ul style="list-style-type: none"> • zarządzanie infrastrukturą serwerową, oprogramowaniem systemu operacyjnego oraz nośnikami danych, • po wcześniejszym uzgodnieniu z właścicielem biznesowym danych i właścicielem biznesowym systemu teleinformatycznego – instalację zmian, poprawek nowych wersji systemu wraz z ich przetestowaniem, • monitorowanie wymaganego poziomu bezpieczeństwa dla platformy systemu operacyjnego, 4) Bazy danych: <ul style="list-style-type: none"> • zarządzanie bazą danych oraz oprogramowaniem systemu zarządzania bazą danych, • po wcześniejszym uzgodnieniu z właścicielem biznesowym danych i właścicielem biznesowym systemu teleinformatycznego – instalację zmian w bazach danych, związanych z aktualizacją do nowszej wersji systemu, • monitorowanie wymaganego poziomu bezpieczeństwa dla platformy bazodanowej, • zarządzanie przestrzenią dyskową oraz jej monitorowanie, 5) Infrastruktury technicznej, poprzez zarządzanie i utrzymanie technicznych systemów bezpieczeństwa oraz administracja pomieszczeń serwerowni, 6) Zapewnienie ciągłości działania systemu, prowadzenie monitoringu stanu bezpieczeństwa (m.in. poprzez bieżący przegląd stanu zabezpieczeń systemowych w celu wykrycia błędów, ataków, prób nieuprawnionego dostępu czy innych zagrożeń związanych z bezpieczeństwem systemu), 7) Wykonywanie czynności technicznych na aplikacji, instalowania nowych wydań i patch'y systemu z poziomu aplikacji, zapewniania sprawności technicznej aplikacji, zapewniania odpowiedniej wydajności aplikacji, |

| | |
|--|--|
| | <p>8) Współpraca z właścicielem biznesowym danych i właścicielem biznesowym systemu teleinformatycznego w zakresie analizy ryzyka w odniesieniu do przetwarzania danych w systemie teleinformatycznym;</p> <p>9) Zgłaszanie, zgodnie z procedurą zarządzania incydentami, wszelkich incydentów, awarii lub anomalii związanych z systemem teleinformatycznym służącym do przetwarzania danych;</p> <p>10) W przypadku otrzymania informacji o naruszeniu lub podejrzeniu naruszenia zabezpieczeń podejmowanie natychmiastowych działań mających na celu zabezpieczenie stanu systemu teleinformatycznego, przeciwdziałanie skutkom naruszenia oraz podejmowanie działań związanych z wdrożeniem zabezpieczeń w systemie, a także współpraca z IOD MF oraz DB w ramach czynności wyjaśniających naruszenia;</p> <p>11) Nadzór nad funkcjonowaniem zabezpieczeń dotyczących przesyłania danych, w szczególności informacji prawnie chronionych drogą teletransmisji;</p> |
| Administrator zarządzający uprawnieniami (AZU) | <p>Do zadań Administratora zarządzającego uprawnieniami należy:</p> <ol style="list-style-type: none"> 1) zarządzanie użytkownikami systemu, tj. weryfikacja i realizacja wniosków o nadanie, modyfikację lub odebranie uprawnień dostępu, w jednostkach organizacyjnych KAS lub w MF, w tym ewidencjonowanie ww. wniosków, 2) prowadzenie ewidencji użytkowników systemu, we właściwych dla AZU jednostkach KAS lub MF, 3) przeprowadzanie okresowych i doraźnych przeglądów kont i uprawnień użytkowników. |
| Użytkownicy | <p>Użytkownicy odpowiadają za:</p> <ol style="list-style-type: none"> 1) przestrzeganie zasad zawartych w niniejszej dokumentacji oraz w procedurach lub instrukcjach wydanych na jej podstawie, 2) ochronę przetwarzanych danych przed nieuprawnionym dostępem, modyfikacją, ujawnieniem, utratą, zniszczeniem, 3) zachowanie obowiązku tajemnicy danych oraz sposobów ich zabezpieczeń także po ustaniu zatrudnienia, 4) przetwarzanie danych zgodnie z posiadanymi upoważnieniami, 5) zgłaszanie sytuacji związanych z naruszeniem zasad ochrony danych osobowych i innych informacji prawnie chronionych, zgodnie z obowiązującymi zasadami i procedurami w tym zakresie. |

PODMIOTY ZEWNĘTRZNE BIORĄCE UDZIAŁ W REALIZACJI USŁUGI/PROCESU W SYSTEMIE

W tym punkcie należy opisać jakie podmioty zewnętrzne mają dostęp do systemu, ich role (w tym użytkowników zewnętrznych) wyodrębnione w zależności od rodzaju poszczególnych modułów i aplikacji wchodzących w skład systemu. Poza rolami związanymi bezpośrednio z funkcjonalnością merytoryczną systemu należy również opisać role w obszarze technicznym, związane z obsługą infrastruktury sprzętowo-systemowej. Należy określić dla poszczególnych ról:

- jakie muszą spełniać wymagania,
- jakie mają obowiązki i zakres odpowiedzialności,
- jaki poziom uprawnień.

6. OPIS SYSTEMU

6.1. KLASYFIKACJA INFORMACJI - GRUPY INFORMACJI PRZETWARZANYCH W SYSTEMIE

W tym punkcie należy zaznaczyć które grupy informacji zgodnie z klasyfikacją informacji określoną w PBI są przetwarzane w systemie. W przypadku III grupy należy wskazać, wszystkie grupy informacji prawnie chronionych, które są przetwarzane w systemie.

| Grupa | Nazwa | TAK/NIE |
|-------|---|---------|
| II | Informacje międzynarodowe, do których dostęp podlega ograniczeniu | |
| III | Inne informacje prawnie chronione (w szczególności tj: dane osobowe, tajemnica skarbową, tajemnica celna, tajemnica informacji finansowej, tajemnica przedsiębiorstwa, tajemnica zawodowa, tajemnica bankowa, tajemnica postępowania przygotowawczego) | |
| IV | Informacje przeznaczone wyłącznie do użytku wewnętrznego - niestanowiące informacji publicznej | |
| V | Informacje publiczne i informacje sektora publicznego, w tym publicznie dostępne dokumenty Parlamentu Europejskiego, Rady i Komisji | |

6.2. PRZEPŁYW DANYCH I INFORMACJI W SYSTEMIE

W tym punkcie należy przedstawić koncepcję obiegu informacji i danych w systemie (schemat graficzny) oraz określić przepływy danych do/z innych systemów (wewnętrznych i zewnętrznych).

7. ZARZĄDZANIE UPRAWNIENIAMI W SYSTEMIE

Do obsługi systemu oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą być dopuszczone wyłącznie osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych, których administratorem jest Minister Finansów, Funduszy i Polityki Regionalnej/Szef KAS. Do przetwarzania innych informacji prawnie chronionych mogą być dopuszczone osoby po spełnieniu wymogów określonych w przepisach szczególnych. (należy wymienić szczególne wymagania związane z dostępem do określonych grup informacji przetwarzanych w systemie)

Propozycje podrozdziałów do szczegółowego opisu poniżej (do wypełnienia)

7.1 RODZAJE KONT UŻYTKOWIKÓW W SYSTEMIE I UPRAWNIENIA

W tym miejscu należy opisać m.in. rodzaje ról w systemie, z uwzględnieniem ról administracyjnych, ról dla użytkowników zewnętrznych oraz odnieść się do zasad nadawania uprawnień w zdalnym dostępie.

7.2 WNIOSEK O NADAWANIE, MODYFIKACJĘ, ODBIÓR UPRAWNIENI

W tym miejscu należy wskazać kto wnioskuje o nadanie, modyfikację, odbiór uprawnień, jakie informacje są wymagane we wniosku lub załączyć wzór, określić czy do wniosku należy załączyć dodatkowe dokumenty i jakie, w jakiej formie składany jest wniosek, jak/do kogo należy go przekazać. Należy również odnieść się do kwestii do integracji z kontem domenowym.

.....

7.3 AKCEPTACJA LUB ODRZUCENIE WNIOSKU PRZEZ WŁAŚCICIELA BIZNESOWEGO SYSTEMU

Należy określić ścieżkę procedowania wniosku, warunki jego zatwierdzania.

.....

7.4 NADAWANIE, MODYFIKACJA, ODBIERANIE UPRAWNIENI

Należy opisać przebieg rejestracji użytkownika w systemie przez AZU – rejestrację użytkownika w systemie, nadanie identyfikatora, zakresu uprawnień i ew. hasła początkowego użytkownikowi, a także opisać wyrejestrowanie użytkownika z systemu, gdzie/w jaki sposób jest prowadzony rejestr użytkowników, gdzie przechowywane są wnioski o nadanie/modyfikację/odbior uprawnień i w jakiej formie. Należy również opisać zasady nadawania uprawnień dla administratorów.

.....

7.5 PRZEGLĄD PRAW DOSTĘPU UŻYTKOWNIKÓW

Należy wskazać kto odpowiada za przeglądy, ich zakres, jak często są wykonywane, sposób dokumentowania.

.....

8. ŚRODKI I METODY UWIERZYTELNIANIA UŻYTKOWNIKÓW W SYSTEMIE

Należy opisać stosowane metody, środki uwierzytelnienia i procedury związane z ich zarządzaniem np. specyficzne wymagania co do haseł, loginów, sposób przekazywania danych uwierzytelniających itp.

.....

9. ROZPOCZYNANIE, ZAWIESZANIE I KOŃCZENIE PRACY W SYSTEMIE

W tym miejscu należy opisać zasady rozpoczynania, zawieszenia i kończenia pracy użytkowników systemu, kolejne czynności, jakie powinny być podejmowane przy uruchamianiu systemu informatycznego, jak i kończeniu pracy. Zasady opisane w tym punkcie mogą podlegać dodatkowym uszczegółowieniom, w zależności od warunków stanowiska pracy i lokalnych zabezpieczeń stosowanych w poszczególnych jednostkach KAS lub w MF.

10. ZDALNY DOSTĘP DO SYSTEMU

W tym miejscu należy odnieść się do kwestii eksploatacji/częściowej eksploatacji systemu z wykorzystaniem funkcjonującego w resorcie systemu zdalnego dostępu.

- ☐ system może być eksploatowany w zdalnym dostępie
- ☐ system nie może być eksploatowany w zdalnym dostępie
- ☐ system może być eksploatowany w zdalnym dostępie, po spełnieniu poniższych warunków:
 - 1)
 - 2)
 - 3)

11. BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE INFRASTRUKTURY TELEINFORMATYCZNEJ

Krytyczne lub wrażliwe środki przetwarzania informacji należy umieszczać w obszarach bezpiecznych, chronionych fizyczną granicą przez odpowiednie bariery bezpieczeństwa oraz zabezpieczenia wejścia zgodnie z PBF i PBT. W tym punkcie należy wskazać zabezpieczenia fizyczne i środowiskowe, stosowane w celu ochrony informacji i środków przetwarzania informacji dla danego systemu oraz w jaki sposób odbywa się ochrona fizyczna przed nieuprawnionym dostępem fizycznym, uszkodzeniami lub zakłóceniami pracy. W szczególności należy określić, które z niżej wymienionych zabezpieczeń wdrożono.

Lokalizacja infrastruktury teleinformatycznej (również infrastruktury zapasowej):

.....

| Zabezpieczenia pomieszczeń, w których znajdują się elementy infrastruktury teleinformatycznej, w tym pomieszczeń serwerowni | | |
|---|--|-------------|
| Rodzaj zabezpieczeń | Opis zabezpieczeń | JEST/NIE MA |
| zabezpieczenia fizyczne (w tym budowlano-mechaniczne, elektroniczne) i środowiskowe | drzwi, okna, ściany i stropy w pomieszczeniach, zapewniają właściwą odporność mechaniczną, przeciwpożarową i przeciwwłamaniową | |
| | dostęp do pomieszczeń objęty jest systemem kontroli dostępu | |

| | | |
|---------------|--|--|
| | system sygnalizacji włamania i napadu zapewnia niezwłoczne powiadomienie służby ochrony | |
| | teren budynku objęty jest systemem monitoringu z zastosowaniem kamer przemysłowych, które przez całą dobę monitorowane są przez służbę ochrony | |
| | stosowany jest system kontroli osób i przedmiotów | |
| | w pomieszczeniach gdzie ulokowane są komponenty infrastruktury teleinformatycznej zapewnione jest utrzymywanie parametrów środowiskowych (np. temperatury, wilgotności, zapylenia itp.) na poziomie określonym przez ich producentów . | |
| | stosowane rozwiązania zapewniających automatyczne monitorowanie i regulację parametrów środowiskowych | |
| | urządzenia kontrolujące parametry środowiskowe charakteryzują się właściwą wydajnością oraz redundancją (na wypadek awarii) | |
| | systemy zabezpieczeń przeciwpożarowych zapewnia niezwłoczne powiadomienie osób odpowiedzialnych za wszczęcie akcji gaśniczej i ratunkowej | |
| | systemu ochrony przeciwpożarowej obejmuje urządzenia automatycznego gaszenia | |
| | stosowane są czynniki gaszące minimalizujące ryzyko uszkodzenia urządzeń elektronicznych i zapisanych w nich danych | |
| | wdrożono mechanizmy zapewniające ciągłość zasilania elektrycznego (zasilanie awaryjne (UPS), generator prądotwórczy, stosowanie zwielokrotnionych linii elektrycznych) | |
| organizacyjne | wdrożone zostały zasady kontroli ruchu osobowego, pojazdów i materiałów | |
| | wdrożona została zasada czystego biurka i czystego ekranu | |
| | wdrożone zostały zasady wnoszenia i ochrony aktywów teleinformatycznych poza siedzibę | |
| | skuteczność funkcjonowania mechanizmów mających na celu zapewnienie właściwych warunków fizycznych i środowiskowych w lokalizacjach, w których znajdują się kluczowe elementy infrastruktury teleinformatycznej, podlega okresowej weryfikacji | |
| | elementy infrastruktury teleinformatycznej podlegają regularnym | |

| | | |
|--|---|--|
| | przeglądom i konserwacji zgodnie z zaleceniami producentów | |
| | usługi serwisowe są świadczone wyłącznie przez autoryzowane i uprawnione jednostki serwisowe | |
| | usługi serwisowe w stosunku do urządzeń, w pamięci których są zapisane dane/informacje objęte tajemnicą, wykonywane są w strefach chronionych i pod kontrolą uprawnionych pracowników | |
| | wdrożono zasady wycofywania z użycia i niszczenia nośników zawierających dane prawnie chronione w sposób uniemożliwiający odczytanie danych oraz rozliczalność procesu | |
| | wdrożono procedury zarządzania incydentami bezpieczeństwa | |

11.2 SPECYFICZNE WYMAGANIA W ZAKRESIE OCHRONY STACJI ROBOCZYCH UŻYTKOWNIKÓW WEWNĘTRZNYCH ORAZ ZEWNĘTRZNYCH

Minimalne wymagania w zakresie ochrony stacji roboczych użytkowników zostały określone w PBT. Należy wskazać dodatkowe, specyficzne dla danego systemu wymagania.

12. ŚRODKI OCHRONY ZASOBÓW INFORMACYJNYCH SYSTEMU

W tym punkcie znajduje się zestawienie wybranych zabezpieczeń wymienionych w załączniku A do normy ISO 27001. Należy przedstawić (potwierdzić) środki, które zastosowano w systemie dla ograniczenia ryzyka wystąpienia zdarzeń negatywnie wpływających na bezpieczeństwo informacji w nim przetwarzanych. Część wymienionych w tabeli zabezpieczeń odnosi się do wymagań szczegółowo wskazanych i opisanych w niniejszej instrukcji. Należy potwierdzić wdrożone zabezpieczenia, a w przypadku braku zabezpieczenia podać planowaną datę wdrożenia i/lub przyczynę braku zabezpieczenia. W każdym punkcie wpisano domyślnie brak zabezpieczenia.

| Punkt z załącznika A do normy ISO 27001 | kategoria | Wymagane zabezpieczenie | wdrożone zabezpieczenie |
|---|--|--|-------------------------|
| A.6.2 | Urządzenia mobilne i telepraca | Cel: Zapewnić bezpieczeństwo telepracy i stosowania urządzeń mobilnych | |
| A.6.2.1 | Polityka stosowania urządzeń mobilnych | Należy wprowadzić zabezpieczenia wspierające w celu zarządzania ryzykami, wynikającymi z użytkowania urządzeń mobilnych. | nie wdrożono |
| A.6.2.2 | Telepraca | Należy wdrożyć zabezpieczenia w celu ochrony informacji pobieranych, przetwarzanych i przechowywanych w miejscach wykonywania telepracy. | nie wdrożono |
| A.8 | Zarządzanie aktywami | | |

| | | | |
|---------------|--|---|--------------|
| A.8.1 | Odpowiedzialność za aktywa | <i>Cel: Zidentyfikować aktywa organizacji i zdefiniować właściwą odpowiedzialność w dziedzinie ich ochrony</i> | |
| A.8.1.1 | Inwentaryzacja aktywów | Należy zdefiniować informacje, inne aktywa związane z informacjami oraz środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów. | nie wdrożono |
| A.8.1.2 | Własności aktywów | Aktywa znajdujące się w ewidencji należy przypisać ich właścicielom. | nie wdrożono |
| A.8.1.3 | Akceptowalne użycie aktywów | Należy zdefiniować, udokumentować i wdrożyć zasady akceptowalnego użycia informacji oraz aktywów związanych z informacjami i środkami przetwarzania informacji. | nie wdrożono |
| A.8.1.4 | Zwrot aktywów | Wszyscy pracownicy i użytkownicy podmiotów zewnętrznych, w momencie zakończenia zatrudnienia, umowy lub porozumienia, powinni zwrócić wszystkie posiadane aktywa organizacji. | nie wdrożono |
| A.8.3 | Postępowanie z nośnikami | <i>Cel: Zapobiec nieuprawnionemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu informacji zapisanych na nośnikach.</i> | |
| A.8.3.1 | Zarządzanie nośnikami wymiennymi | Należy wdrożyć procedury zarządzania nośnikami wymiennymi, zgodnie ze schematem klasyfikacji przyjętym w organizacji. | nie wdrożono |
| A.8.3.2 | Wycofywanie nośników | Nośniki, które nie będą dłużej wykorzystywane, należy bezpiecznie wycofać, zgodnie z formalnymi procedurami | nie wdrożono |
| A.8.3.3 | Przekazywanie nośników | Nośniki zawierające informacje należy chronić przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu. | nie wdrożono |
| A.9.4 | Kontrola dostępu do systemów i aplikacji | <i>Cel: Zapobiec nieuprawnionemu dostępowi do systemów i aplikacji.</i> | |
| A.9.4.4 | Użycie uprzywilejowanych programów narzędziowych | Wykorzystanie programów narzędziowych, umożliwiających obejście zabezpieczeń systemów i aplikacji, powinno podlegać ograniczeniom i ścisłemu nadzorowi. | nie wdrożono |
| A.9.4.5 | Kontrola dostępu do kodów źródłowych | Dostęp do kodu źródłowego programów powinien być ograniczony. | nie wdrożono |
| A.10 | Kryptografia | | |
| A.10.1 | Zabezpieczenia kryptograficzne | <i>Cel: Zapewnić właściwe i skuteczne wykorzystanie kryptografii do ochrony poufności, autentyczności i/lub integralności informacji.</i> | |

| | | | |
|---------------|--|---|--------------|
| A.10.1.1 | Polityka stosowania zabezpieczeń kryptograficznych | Należy opracować i wdrożyć politykę stosowania zabezpieczeń kryptograficznych do ochrony informacji. | nie wdrożono |
| A.10.1.2 | Zarządzanie kluczami | Należy opracować politykę dotyczącą korzystania, ochrony i okresów ważności kluczy kryptograficznych i wdrożyć ją na wszystkich etapach cyklu życia kluczy. | nie wdrożono |
| A.12 | Bezpieczna eksploatacja | | |
| A.12.1 | Procedury eksploatacyjne i odpowiedzialność | <i>Cel: Zapewnić poprawną i bezpieczną eksploatację środków przetwarzania informacji.</i> | |
| A.12.1.1 | Dokumentowanie procedur eksploatacyjnych | Procedury eksploatacyjne powinny być udokumentowane i udostępniane wszystkim potrzebującym ich użytkownikom. | nie wdrożono |
| A.12.1.2 | Zarządzanie zmianami | Zmiany w organizacji, procesach biznesowych, środkach przetwarzania informacji i systemach, które mają wpływ na bezpieczeństwo informacji, powinny być nadzorowane. | nie wdrożono |
| A.12.1.3 | Zarządzanie pojemnością | Należy monitorować i dostosowywać wykorzystywanie zasobów oraz przewidywać wymagania pojemności w przyszłości, dla zapewnienia właściwej wydajności systemu. | nie wdrożono |
| A.12.1.4 | Oddzielenie środowisk rozwojowych, testowych i produkcyjnych | Należy oddzielić środowiska rozwojowe, testowe i produkcyjne celem redukcji ryzyk związanych z nieuprawnionym dostępem lub zmianami w środowisku produkcyjnym. | nie wdrożono |
| A.12.2 | Ochrona przed szkodliwym oprogramowaniem | <i>Cel: Zapewnić informacjom i środkom informacji ochronę przed szkodliwym oprogramowaniem.</i> | |
| A.12.2.1 | Zabezpieczenie przed szkodliwym oprogramowaniem | Należy wdrożyć zabezpieczenia wykrywające, zapobiegające i odtwarzające, które służą ochronie przed szkodliwym oprogramowaniem, w połączeniu z właściwym uświadamianiem użytkowników. | nie wdrożono |
| A.12.3 | Kopie zapasowe | <i>Cel: Chronić przed utratą danych.</i> | |
| A.12.3.1 | Zapaszowe kopie informacji | Zapaszowe kopie informacji, oprogramowania i obrazów systemów należy regularnie wykonywać i testować, zgodnie z ustaloną polityką kopii zapasowych. | nie wdrożono |
| A.12.4 | Rejestrowanie zdarzeń i monitorowanie | <i>Cel: Rejestrować zdarzenia i zbierać materiał dowodowy.</i> | |

| | | | |
|----------|---|--|--------------|
| A.12.4.1 | Rejestrowanie zdarzeń | Należy tworzyć, przechowywać i systematycznie przeglądać dzienniki zdarzeń rejestrujące działania użytkowników, wyjątki, usterki oraz zdarzenia związane z bezpieczeństwem informacji. | nie wdrożono |
| A.12.4.2 | Ochrona informacji w dziennikach zdarzeń | Środki służące rejestrowaniu zdarzeń oraz informacji w dziennikach zdarzeń należy chronić przez manipulacją i nieuprawnionym dostępem. | nie wdrożono |
| A.12.4.3 | Rejestrowanie działań administratorów i operatorów | Działania administratorów i operatorów systemów należy rejestrować, a dzienniki chronić i systematycznie przeglądać. | nie wdrożono |
| A.12.4.4 | Synchronizacja zegarów | Zegary wszystkich istotnych systemów przetwarzania informacji w organizacji lub domenie bezpieczeństwa należy zsynchronizować z jednym wzorcowym źródłem czasu. | nie wdrożono |
| A.12.5 | Nadzór nad oprogramowaniem produkcyjnym | Cel: Zapewnić integralność systemów produkcyjnych. | |
| A.12.5.1 | Instalacja oprogramowania w systemach produkcyjnych | Należy wdrożyć procedury nadzoru nad instalacją oprogramowania w systemach produkcyjnych. | nie wdrożono |
| A.12.6 | Zarządzanie podatnościami technicznymi | Cel: Zapobiec wykorzystaniu podatności technicznych. | |
| A.12.6.1 | Zarządzanie podatnościami technicznymi | Informacje o podatnościach technicznych wykorzystywanych systemów informacyjnych należy niezwłocznie pozyskiwać, oceniać stopień narażenia organizacji na te podatności i podejmować odpowiednie środki w celu przeciwdziałania związanemu z min ryzyku. | nie wdrożono |
| A.13 | Bezpieczeństwo komunikacji | | |
| A.13.1 | Zarządzanie bezpieczeństwem sieci | Cel: Zapewnić ochronę informacji w sieciach oraz wspomagających je środkach przetwarzania informacji. | |
| A.13.1.1 | Zabezpieczenia sieci | Sieci powinny być zarządzane i nadzorowane w celu ochrony informacji w systemach i aplikacjach. | nie wdrożono |
| A.13.2 | Przesyłanie informacji | Cel: Utrzymywać bezpieczeństwo informacji przesyłanych wewnątrz organizacji i wymienianych z podmiotami zewnętrznymi | |

| | | | |
|---------------|---|---|--------------|
| A.13.2.1 | Polityki i procedury przesyłania informacji | Należy wdrożyć formalne polityki przesyłania informacji, procedury i zabezpieczeń w celu ochrony wymiany informacji przesyłanych z użyciem wszystkich rodzajów środków łączności. | nie wdrożono |
| A.13.2.2 | Porozumienia dotyczące przesyłania informacji | Porozumienia powinny uwzględniać bezpieczne przesyłanie informacji biznesowych między organizacją i podmiotami zewnętrznymi. | nie wdrożono |
| A.13.2.3 | Wiadomości elektroniczne | Informacje przekazywane w formie wiadomości elektronicznych powinny być odpowiednio chronione. | nie wdrożono |
| A.13.2.4 | Umowy o zachowaniu poufności | Należy zidentyfikować, regularnie przeglądać i dokumentować wymagania odnoszące się do umów o zachowanie poufności lub nieujawnianiu informacji, w sposób odzwierciedlający potrzeby organizacji w zakresie ochrony informacji. | nie wdrożono |
| A.14 | Pozyskiwanie, rozwój i utrzymanie systemów | | |
| A.14.1 | Wymagania związane z bezpieczeństwem systemów informacyjnych | <i>Cel: Zapewnić, żeby bezpieczeństwo informacji było nieodłączną częścią systemów informacyjnych w całym cyklu życia. Dotyczy to również wymagań wobec systemów informacyjnych dostarczających usług w sieciach publicznych.</i> | |
| A.14.1.1 | Analiza i specyfikacja wymagań bezpieczeństwa informacji | Wymagania dotyczące bezpieczeństwa informacji należy włączyć do wymagań stawianych nowym systemom informacyjnym lub rozbudowie systemów istniejących. | nie wdrożono |
| A.14.1.2 | Zabezpieczanie usług aplikacyjnych w sieciach publicznych | Informacje przesyłane w sieciach publicznych, związane z usługami świadczonymi przez aplikacje, należy chronić przed nieuczciwymi działaniami, sporami dotyczącymi umów oraz nieuprawnionym ujawnieniem lub zmianami. | nie wdrożono |
| A.14.1.3 | Ochrona transmisji usług aplikacyjnych | Informacje związane z transakcjami dokonywanymi w ramach usług świadczonych przez aplikacje należy chronić, aby zapobiec przerwaniu transmisji, błędom w trasowaniu, nieuprawnionym zmianom wiadomości, nieuprawnionemu ujawnieniu, nieuprawnionemu powielaniu lub odtworzeniu. | nie wdrożono |
| A.14.2 | Bezpieczeństwo w procesach rozwoju i wsparcia | <i>Cel: Zapewnić projektowanie i wdrożenie bezpieczeństwa informacji w ramach cyklu życia systemów informacyjnych.</i> | |
| A.14.2.1 | Polityka bezpieczeństwa prac rozwojowych | Zależy ustanowić zasady prac nad rozwojem oprogramowania i systemów oraz stosować je w pracach rozwojowych prowadzonych wewnątrz organizacji. | nie wdrożono |
| A.14.2.2 | Procedury kontroli zmian w systemach | Należy nadzorować zmiany w systemach podczas ich cyklu rozwojowego, z zastosowaniem formalnych procedur kontroli zmian. | nie wdrożono |

| | | | |
|---------------|---|---|--------------|
| A.14.2.3 | Przegląd techniczny po zmianach w platformie produkcyjnej | Po dokonaniu zmian w platformach produkcyjnych należy przeprowadzić przegląd aplikacji oraz przetestować je, aby uzyskać pewność, że zmiany nie miały niekorzystnego wpływu na działalność organizacji i bezpieczeństwo. | nie wdrożono |
| A.14.2.4 | Ograniczenia dotyczące zmian w pakietach oprogramowania | Modyfikacje w pakietach oprogramowania należy dokonywać z rozważą i ograniczać się do zmian niezbędnych, a wszystkie takie zmiany ściśle nadzorować. | nie wdrożono |
| A.14.2.6 | Bezpieczne środowisko rozwojowe | Ochrona bezpiecznego środowiska przeznaczonego do rozwoju systemu oraz prac integracyjnych obejmujących całość cyklu rozwojowego systemu. | nie wdrożono |
| A.14.2.7 | Prace rozwojowe zlecane podmiotom zewnętrznym | Nadzorowanie i monitorowanie prac rozwojowych nad systemem zleconych podmiotom zewnętrznym. | nie wdrożono |
| A.14.2.8 | Testowanie bezpieczeństwa systemów | Funkcje bezpieczeństwa należy testować w czasie prac rozwojowych. | nie wdrożono |
| A.14.2.9 | Testy akceptacyjne systemów | Dla modernizacji systemu, jego nowej wersji należy ustanowić program testów akceptacyjnych i kryteria z nimi związane. | nie wdrożono |
| A.14.3 | Dane testowe | <i>Cel: Zapewnić ochronę danych stosowanych do testów.</i> | |
| A.14.3.1 | Ochrona danych testowych | Dane testowe należy starannie wybierać, chronić i nadzorować. | nie wdrożono |
| A.15 | Relacje z dostawcami | | |
| A.15.1 | Bezpieczeństwo informacji w relacjach z dostawcami | <i>Cel: Zapewnić ochronę aktywów organizacji udostępnianych dostawcom.</i> | |
| A.15.1.1 | Polityka bezpieczeństwa informacji w relacjach z dostawcami | Należy uzgodnić z dostawcą i udokumentować wymagania bezpieczeństwa informacji celem zmniejszenia ryzyk związanych z dostępem dostawcy do aktywów organizacji. | nie wdrożono |
| A.15.1.2 | Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami | Należy ustanowić wszystkie istotne wymagania dotyczące bezpieczeństwa informacji i uzgodnić je z każdym dostawcą, który może uzyskać dostęp, przetwarzać, przechowywać, przysyłać lub dostarczać elementy infrastruktury teleinformatycznej dla przetwarzania informacji należących do organizacji. | nie wdrożono |

| | | | |
|----------|---|--|--------------|
| A.15.1.3 | Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych | Porozumienia z dostawcami powinny uwzględniać wymagania odnoszące się do ryzyk w bezpieczeństwie informacji, związanych z usługami technologii i telekomunikacyjnych oraz łańcuchem dostaw produktów. | nie wdrożono |
| A.15.2 | Zarządzanie usługami świadczonymi przez dostawców | Cel: Utrzymać uzgodniony poziom bezpieczeństwa informacji i świadczonych usług zgodnie z umowami z dostawcami. | |
| A.15.2.1 | Monitorowanie i przegląd usług świadczonych przez dostawców | Zapewniono regularne monitorowanie, przeglądanie i audytowanie dostarczanych usług zewnętrznych. | nie wdrożono |
| A.15.2.2 | Zarządzanie zmianami w usługach świadczonych przez dostawców | Należy zarządzać zmianami w zakresie świadczenia usług przez dostawców, w tym utrzymaniem i doskonaleniem istniejących, procedur i zabezpieczeń, z uwzględnieniem krytyczności informacji, procedur biznesowych, których dotyczą oraz ponownego szacowania ryzyka. | nie wdrożono |
| A.17.2 | Nadmiarowość | Cel: Zapewnić dostępność środków przetwarzania informacji. | |
| A.17.2.1 | Dostępność środków przetwarzania informacji | Środki przetwarzania informacji należy wdrażać z nadmiarem wystarczającym do spełnienia wymagań dostępności. | nie wdrożono |
| A.18 | Zgodność | | |
| A.18.1 | Zgodność z wymaganiami prawnymi i umownymi | Cel: Unikać naruszenia zobowiązań prawnych, regulacyjnych lub umownych związanych z bezpieczeństwem informacji oraz innych wymagań dotyczących bezpieczeństwa. | |
| A.18.1.1 | Określenie stosownych wymagań prawnych i umownych | Wszelkie istotne wymagania prawne, regulacyjne, umowne oraz podejście organizacji do ich przestrzegania należy zidentyfikować, udokumentować i aktualizować dla każdego systemu informacyjnego oraz całości organizacji. | nie wdrożono |
| A.18.1.2 | Prawa własności intelektualnej | Należy wdrożyć odpowiednie procedury zapewniające zgodność z wymaganiami prawnymi, regulacyjnymi i umownymi, związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania | nie wdrożono |
| A.18.1.3 | Ochrona zapisów | Zapisy należy chronić przed utratą, zniszczeniem, fałszowaniem, nieuprawnionym dostępem i nieuprawnionym opublikowaniem, stosownie do wymagań prawnych, regulacyjnych, umownych i biznesowych. | nie wdrożono |

| | | | |
|----------|--|--|--------------|
| A.18.1.4 | Prywatność i ochrona danych identyfikujących osobę | Należy zapewnić prywatność i ochronę danych identyfikujących osobę stosownie do odpowiednich przepisów prawa i regulacji | nie wdrożono |
| A.18.1.5 | Regulacje dotyczące zabezpieczeń kryptograficznych | Zabezpieczenia kryptograficzne należy stosować zgodnie z odpowiednimi umowami, przepisami i regulacjami | nie wdrożono |
| A.18.2 | Przeglądy bezpieczeństwa informacji | <i>Cel: Zapewnić zgodnie z politykami organizacji i procedurami wdrożenie i stosowanie zasad bezpieczeństwa informacji.</i> | |
| A.18.2.2 | Zgodność z politykami bezpieczeństwa i standardami | Kierownicy powinni regularnie dokonywać przeglądu zgodności przetwarzania informacji i procedur z odpowiednimi politykami bezpieczeństwa standardami i innymi wymaganiami dotyczącymi bezpieczeństwa, w zakresie przydzielonej im odpowiedzialności. | nie wdrożono |
| A.18.2.3 | Sprawdzenie zgodności technicznej | Należy regularnie przeglądać systemy informacyjne celem sprawdzenia ich zgodności z politykami bezpieczeństwa i standardami obowiązującymi w organizacji. | nie wdrożono |

11. ADMINISTROWANIE BEZPIECZEŃSTWEM /PROCEDURY USTANOWIONE PRZEZ WŁAŚCICIELA BIZNESOWEGO SYSTEMU I DANYCH

Administrowanie bezpieczeństwem systemu ma na celu utrzymanie zakładanego poziomu bezpieczeństwa przetwarzanych w systemie informacji, obejmującego aspekty dostępności, integralności i poufności. Wszystkie czynności dotyczące systemu, wykonywane przez administratorów, użytkowników i osoby postronne (np. serwis) muszą być ujęte w procedury, zapewniające możliwość wykonania przez wykwalifikowany personel.

W tym punkcie należy wskazać zasady eksploatacji systemu i jego administrowania, gwarantujące utrzymanie bezpieczeństwa, należy wskazać wszystkie procedury związane z przetwarzaniem danych oraz warunkami technicznymi i organizacyjnymi, jakimi powinny odpowiadać urządzenia i systemy.

Procedury powinny być opracowane z uwzględnieniem obowiązujących w Ministerstwie Finansów standardów i wzorców. Należy określić założenia dokumentowania i wprowadzania w życie procedur dla systemu.

Procedury związane z systemem można podzielić na dwie grupy:

- procedury dedykowane, opracowane na potrzeby tego systemu,
- procedury uniwersalne, obowiązujące w resorcie, mające zastosowanie dla innych systemów lub elementów infrastruktury sprzętowo-systemowej.

Założenia do procedur i procedury powinny zostać opracowane w następujących grupach:

11.1 PROCEDURY TWORZENIA KOPII ZAPASOWYCH

Należy określić zakres - dla jakich danych wykonywane będą kopie zapasowe, typ nośników, na których kopie będą wykonywane oraz narzędzia programowe i urządzenia mające być do tego celu wykorzystywane, harmonogram wykonywania kopii zapasowych, sposób, miejsce i czas przechowywania elektronicznych nośników informacji oraz kopii zapasowych, sposób ich zabezpieczenia przed nieuprawnionym dostępem, sposób i formę autoryzacji zmian na nośnikach i usuwania danych, sposoby właściwej i trwałej likwidacji niepotrzebnych danych, kontrola poprawności wykonywania kopii zapasowych/zasady testowania kopii, itp.)

11.2 PROCEDURY EKSPLOATACYJNE

Wymienić procedury związane z eksploatacją systemu, instalacją i modyfikacją oprogramowania, konfiguracji parametrów aplikacji itp.

11.3 PROCEDURY AWARYJNE

Wymienić procedury mające na celu utrzymanie ciągłości działania systemu, które należy wykonywać w przypadku wystąpienia sytuacji awaryjnych w pracy systemu np.: odtwarzania danych z kopii zapasowych, postępowania w przypadku awarii sprzętowej itp.

11.4 ZASADY I SZCZEGÓLNE ŚRODKI OCHRONY DANYCH STANOWIĄCYCH INFORMACJE PRAWNIE CHRONIONE

Dotyczy np. danych stanowiących tajemnicę skarbową lub danych osobowych.

11.5 OPIS INNYCH ZAŁOŻEŃ BEZPIECZNEJ EKSPLOATACJI, W TYM ROZLICZALNOŚĆ

W tym punkcie należy wymienić co najmniej zasady dokumentowania działań użytkowników lub obiektów systemowych, polegających na dostępie do systemu z uprawnieniami administracyjnymi, konfiguracji systemu, w tym konfiguracji zabezpieczeń w postaci elektronicznych zapisów w dziennikach systemowych (logach) i okres przechowywania informacji od dnia ich zapisu (rozliczalność). W zakresie wynikającym z analizy ryzyka, proszę wskazać odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci działań użytkowników nieposiadających uprawnień administracyjnych, zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny.

12 SZKOLENIA

Wszyscy użytkownicy pracujący z systemem powinni zostać przeszkoleni w zakresie bezpiecznej eksploatacji systemu oraz z być zapoznani z obowiązującymi regulacjami prawnymi dotyczącymi ochrony danych i systemów informatycznych. Każdy użytkownik powinien posiadać wiedzę adekwatną do swego zakresu obowiązków, wykonywanych zadań i przypisanego zakresu odpowiedzialności.

W tym punkcie należy opisać wymagane szkolenia związane z wdrożeniem i eksploatacją systemu dla grup pracowniczych (np. użytkowników, administratorów, kierowników jednostek) w zakresie:

- eksploatacji systemu,
- bezpieczeństwa danych i systemu.

Należy opisać również wymaganą infrastrukturę i materiały szkoleniowe (bazy szkoleniowe, scenariusze, podręczniki, e-learning) potrzebne do realizacji szkoleń.

Należy wskazać czy są opracowane instrukcje/podręczniki użytkownika i gdzie są dostępne. Należy również opisać inne metody wspomagania użytkownika w zakresie bezpiecznej eksploatacji takie, jak np.: usługa Help Desk, infolinia, itp.

13 DEKLARACJA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH W SYSTEMIE

Zaznaczyć właściwe; informacje wykorzystać przy wypełnieniu zakładki „Bezpieczeństwo” w systemie REJS rejs.mf.gov.pl

13.1 REJESTROWANIE I RAPORTOWANIE OPERACJI PRZETWARZANIA:

DLA KAŻDEJ OSOBY FIZYCZNEJ, KTÓREJ DANE SĄ PRZETWARZANE W SYSTEMIE ZAPEWNIONO ODNOTOWANIE:

- ☐ daty pierwszego wprowadzenia danych do systemu
- ☐ identyfikatora użytkownika wprowadzającego dane
- ☐ działań użytkowników w systemie
- ☐ źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą
- ☐ informacji o odbiorcach, którym dane zostały udostępnione oraz dacie i zakresie udostępnienia

DLA KAŻDEJ OSOBY FIZYCZNEJ, KTÓREJ DANE SĄ PRZETWARZANE W SYSTEMIE ZAPEWNIONO WYGENEROWANIE RAPORTU ZAWIERAJĄCEGO:

- ☐ datę pierwszego wprowadzenia danych do systemu
- ☐ identyfikator użytkownika wprowadzającego dane
- ☐ działania użytkowników w systemie
- ☐ źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą
- ☐ informacje o odbiorcach, którym dane zostały udostępnione oraz dacie i zakresie udostępnienia

13.2. PRZETWARZANIE DANYCH OSOBOWYCH ZGODNIE Z RODO I/LUB „USTAWĄ POLICYJNĄ” - REALIZACJA PRAW OSÓB FIZYCZNYCH Z WYKORZYSTANIEM SYSTEMU INFORMATYCZNEGO

Wypełnić w odniesieniu do zidentyfikowanych podstaw przetwarzania danych osobowych; tabele, które nie mają zastosowania usunąć.

DLA KAŻDEJ OSOBY FIZYCZNEJ, KTÓREJ DANE SĄ PRZETWARZANE MOŻLIWE JEST:

| przetwarzanie jest niezbędne do wypełnienia przez Administratora obowiązku wynikającego z przepisów (art. 6 ust. 1 lit. c RODO) | TAK/NIE |
|--|---------|
| udostępnienie danych osobie, której one dotyczą (RODO art. 15 ust. 3) | |
| edytowanie/ sprostowanie danych (RODO art. 16) | |
| oznaczenie danych jako podlegających ograniczonemu przetwarzaniu (RODO art. 18) | |
| oznaczenie danych jako podlegających czasowemu lub całkowitemu ograniczeniu lub zakazowi przetwarzania (RODO art. 58. ust. 2 lit. f) | |

| przetwarzanie jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów (art. 13 ust. 1 „ustawy policyjnej”) | TAK/NIE |
|--|---------|
| udostępnienie danych osobie, której one dotyczą ("ustawa policyjna" art. 23) | |
| edytowanie/ sprostowanie danych ("ustawa policyjna" art. 24 ust. 1 pkt 1) | |
| oznaczenie danych jako podlegających ograniczonemu przetwarzaniu ("ustawa policyjna" art. 25 ust. 1) | |
| oznaczenie danych jako podlegających czasowemu lub całkowitemu ograniczeniu lub zakazowi przetwarzania ("ustawa policyjna" art. 8 ust. 2 pkt 6) | |

| przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi (art. 6 ust. 1 lit. e RODO - stosowany, kiedy nie ma wyraźnego przepisu prawa, ale może być wykazany interes publiczny lub sprawowanie władzy publicznej w odpowiednim zakresie, wynikającym z przepisów) | TAK/NIE |
|--|---------|
| udostępnienie danych osobie, której one dotyczą (RODO art. 15 ust. 3) | |

| | |
|--|--|
| edytowanie/ sprostowanie danych (RODO art. 16) | |
| usunięcie danych (RODO art. 17) | |
| oznaczenie danych jako podlegających ograniczonemu przetwarzaniu (RODO art. 18) | |
| oznaczenie danych, w stosunku do przetwarzania których wniesiono sprzeciw (RODO art. 21) | |
| oznaczenie danych jako niepodlegających profilowaniu i automatycznemu podejmowaniu decyzji (RODO art. 22) | |
| oznaczenie danych jako podlegających czasowemu lub całkowitemu ograniczeniu lub zakazowi przetwarzania (RODO art. 58. ust. 2 lit. f) | |

| przetwarzanie jest niezbędne do wykonania umowy z osobą, która jest jej stroną, lub w celu zawarcia takiej umowy (art. 6 ust. 1 lit. b RODO); | TAK/NIE |
|--|----------------|
| udostępnienie danych osobie, której one dotyczą (RODO art. 15 ust. 3) | |
| edytowanie/ sprostowanie danych (RODO art. 16) | |
| usunięcie danych (RODO art. 17) | |
| oznaczenie danych jako podlegających ograniczonemu przetwarzaniu (RODO art. 18) | |
| wyeksportowanie danych do ustrukturyzowanego, znanego formatu (RODO art. 20) | |
| oznaczenie danych jako niepodlegających profilowaniu i automatycznemu podejmowaniu decyzji (RODO art. 22) | |
| oznaczenie danych jako podlegających czasowemu lub całkowitemu ograniczeniu lub zakazowi przetwarzania (RODO art. 58. ust. 2 lit. f) | |

| przetwarzanie jest niezbędne do celów, które wynikają z prawnie uzasadnionych interesów realizowanych przez Administratora (art. 6 ust. 1 lit. f RODO – przesłanki tej nie można stosować, kiedy Administrator wykonuje zadania organu) | TAK/NIE |
|--|----------------|
| udostępnienie danych osobie, której one dotyczą (RODO art. 15 ust. 3) | |
| edytowanie/ sprostowanie danych (RODO art. 16) | |
| usunięcie danych (RODO art. 17) | |
| oznaczenie danych jako podlegających ograniczonemu przetwarzaniu (RODO art. 18) | |
| oznaczenie danych, w stosunku do przetwarzania których wniesiono sprzeciw (RODO art. 21) | |

| | |
|--|--|
| oznaczenie danych jako niepodlegających profilowaniu i automatycznemu podejmowaniu decyzji (RODO art. 22) | |
| oznaczenie danych jako podlegających czasowemu lub całkowitemu ograniczeniu lub zakazowi przetwarzania (RODO art. 58. ust. 2 lit. f) | |

| przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (art. 6 ust. 1 lit. d RODO) | TAK/NIE |
|--|----------------|
| udostępnienie danych osobie, której one dotyczą (RODO art. 15 ust. 3) | |
| edytowanie/ sprostowanie danych (RODO art. 16) | |
| usunięcie danych (RODO art. 17) | |
| oznaczenie danych jako podlegających ograniczonemu przetwarzaniu (RODO art. 18) | |
| oznaczenie danych jako niepodlegających profilowaniu i automatycznemu podejmowaniu decyzji (RODO art. 22) | |
| oznaczenie danych jako podlegających czasowemu lub całkowitemu ograniczeniu lub zakazowi przetwarzania (RODO art. 58. ust. 2 lit. f) | |

| przetwarzanie na podstawie zgody (art. 6 ust. 1 lit. a RODO); | TAK/NIE |
|--|----------------|
| odnotowanie faktu cofnięcia zgody, na podstawie której dane były przetwarzane (RODO art. 7 ust. 3) | |
| udostępnienie danych osobie, której one dotyczą (RODO art. 15 ust. 3) | |
| edytowanie/ sprostowanie danych (RODO art. 16) | |
| usunięcie danych (RODO art. 17) | |
| oznaczenie danych jako podlegających ograniczonemu przetwarzaniu (RODO art. 18) | |
| wyeksportowanie danych do ustrukturyzowanego, znanego formatu (RODO art. 20) | |
| oznaczenie danych jako podlegających czasowemu lub całkowitemu ograniczeniu lub zakazowi przetwarzania (RODO art. 58. ust. 2 lit. f) | |

14. ZAŁĄCZNIKI

1. Analiza ryzyka dla bezpieczeństwa danych osobowych i/lub informacji przetwarzanych z wykorzystaniem systemu
2. Ocena skutków dla ochrony danych (jeśli wymagana)

3. Wniosek o nadanie/odebranie/modyfikację uprawnień do systemu
4. Propozycje wpisu lub aktualizacji czynności przetwarzania w rejestrze czynności przetwarzania danych osobowych lub/i
5. Propozycje wpisu lub aktualizacji wykazu kategorii czynności przetwarzania
6. Wszystkie inne procedury i instrukcje opracowane dla systemu, nie wymienione w pkt. 11.