ZARZĄDZENIE Nr 88 /2022

Wójta Gminy Jedwabno

z dnia 1 września 2022 roku

w sprawie wprowadzenie Polityki Bezpieczeństwa SRP (Systemu Rejestrów Państwowych) do stosowania w Urzędzie Gminy w Jedwabnie.

Na podstawie Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2021.0.2070 tj.) - System Rejestrów Państwowych

zarządza się , co następuje:

§ 1.

1.Wprowadzam do stosowania przez wszystkich pracowników mających dostęp do aplikacji Źródło dokument „Polityka Bezpieczeństwa Informacji SRP (System Rejestrów Państwowych)

§ 2.

Jednolity tekst „Polityka Bezpieczeństwa Informacji SRP (System Rejestrów Państwowych) „ stanowi **załącznik nr 1** do niniejszego zarządzenia.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

Wójt

(Sławomir Ambroziak)

Potwierdzenie zapoznania z dokumentem „Polityka Bezpieczeństwa Informacji SRP (System Rejestrów Państwowych) „

Imię	Nazwisko	Data zapoznania	Podpis

Załącznik Nr 1 do

zarządzenia Nr ..... /2022

Wójta Gminy Jedwabno

z dnia .....

Polityka Bezpieczeństwa Informacji SRP (Systemu Rejestrów Państwowych)

Metryka dokumentu

Właściciel	Minister właściwy ds. informatyzacji			
Tryb zatwierdzenia:	Dokument zatwierdza Dyrektor departamentu w ministerstwie właściwym ds. informatyzacji odpowiedzialnego za eksploatację i utrzymanie SRP			
Stan	Zatwierdzony	Daty obowiązywania		
Założenia	Polityka Bezpieczeństwa Informacji SRP			
Adresaci	Interesariusze SRP			
Historia dokumentu	Wersja	Data	Autor	Opis zmian
	1.0	2017-12-28	Zespół ZBS	Utworzenie dokumentu
	2.0	2018-03-29	Zespół ZBS	Aktualizacja dokumentu RODO

Spis treści

Cz. I Zarządzanie bezpieczeństwem informacji

1. Kontekst Systemu Rejestrów Państwowych

1.1 Istota Systemu Rejestrów Państwowych i jego kontekst

Kontekst wewnętrzny

System Rejestrów Państwowych (SRP) to zintegrowany system informatyczny, scentralizowany zbiór rejestrów, zapewniający realizację kompetencji Państwa w zakresie **bieżącej obsługi** klientów administracji – obywateli, podmiotów gospodarczych i innych interesariuszy **korzystających** z rejestrów **państwowych** (w tym samych **urzędów**).

SRP funkcjonuje w oparciu o zasoby infrastrukturalne – sprzętowe, programowe i sieciowe Zintegrowanej Infrastruktury Rejestrów (ZIR) objętych polityką bezpieczeństwa informacji systemu ZIR.

Właściciel SRP - Minister właściwy ds. informatyzacji pozostaje właścicielem systemu i administratorem danych osobowych przetwarzanych w systemie i odpowiada za bezpieczeństwo danych i systemu.

Bezpieczeństwo SRP jest adresowane w niniejszej Polityce Bezpieczeństwa Informacji, w regulacjach dotyczących bezpieczeństwa systemów informatycznych, ochrony informacji niejawnych i ochrony danych osobowych funkcjonujących w ministerstwie właściwym ds. informatyzacji, a także w odpowiednich dokumentach strategicznych, dotyczących bezpieczeństwa narodowego Rzeczpospolitej Polskiej.

Niniejsza Polityka Bezpieczeństwa Informacji SRP, zwana dalej PBI SRP, powinna być dokumentem spójnym z innymi dokumentami strategicznymi w zakresie bezpieczeństwa informacji i systemów informatycznych oraz systemem zarządzania bezpieczeństwem informacji, w przypadku ich ustanowienia przez ministra właściwego ds. informatyzacji.

Kontekst zewnętrzny

Uwarunkowania prawne

SRP działa w ramach określonych przez akty prawne RP. Zastosowanie mają regulacje prawne (ustawy i rozporządzenia) właściwe dla:

- poszczególnych rejestrów **składających się** na SRP, **określające** m.in. cele i zakresy ich **działania**
- kategorii danych przetwarzanych w SRP
- **rozwiązań** teleinformatycznych **służących** do realizacji **zadań** publicznych.

Pełny wykaz regulacji prawnych, które mają zastosowanie wobec SRP zawarty jest w dokumencie ***Wykaz wymagań prawnych SRP***, stanowiącym załącznik nr 1.1 do niniejszej PBI.

1.2 Potrzeby i oczekiwania interesariuszy

Z racji roli i zakresu **oddziaływania** SRP na funkcjonowanie administracji publicznej istnieje szeroka lista jego interesariuszy i **użytkowników, mających** szczególne, **właściwe** sobie role, potrzeby i wymagania ustanowione regulacjami prawnymi **odnośnie funkcjonalności i bezpieczeństwa** systemu.

Identyfikacja i wykaz interesariuszy i **użytkowników** SRP oraz zakresu ich **oddziaływania** zawarty jest w dokumencie *Wykaz interesariuszy i użytkowników SRP*, stanowiącym załącznik nr 1.2 do niniejszej PBI.

1.3 Zakres stosowania Polityki Bezpieczeństwa Informacji

Polityka Bezpieczeństwa Informacji SRP obejmuje:

- w zakresie przedmiotowym:

  - dane przetwarzane w SRP oraz dane **służące** do **zarządzania** nim i **powstające** w trakcie rozwoju i eksploatacji systemu, zdefiniowane zgodnie z *Polityka klasyfikacji informacji SRP*, **stanowiącą załącznik** nr 2.9 do niniejszej PBI
  - System Rejestrów **Państwowych składający się** z bazy centralnej SRP oraz wszystkich aktualnie **funkcjonujących** w danym czasie rejestrów i aplikacji oraz komponentów wspólnych dla **całego** systemu
  - Stacje robocze instytucji **korzystających** z SRP
  - Sieci **dostępowe** wykorzystywane do transmisji danych w ramach funkcjonowania SRP

- w zakresie terytorialnym:

  - miejsca rozwoju i eksploatacji SRP: siedziba ministerstwa **właściwego** ds. informatyzacji, siedziba podmiotu **realizującego** zadania na rzecz ministra **właściwego** ds. informatyzacji w zakresie rozwoju, eksploatacji i utrzymania SRP
  - miejsca przetwarzania danych – lokalizacje centrów przetwarzania
  - miejsca przetwarzania danych – lokalizacje interesariuszy i **użytkowników** - instytucji **korzystających** z SRP

- w zakresie funkcjonalnym:

  - procesy cyklu **życia** systemu - projektowania i wytwarzania, rozwoju, eksploatacji, utrzymania i wycofywania starszych wersji SRP
  - procesy przetwarzania danych osobowych takie, jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, **udostępnianie, trwałe** usuwanie, przekazywanie
  - obszary: organizacyjny, techniczny i technologiczny, osobowy i fizyczny

- w zakresie instytucjonalnym i personalnym:

  - interesariuszy systemu, zgodnie z zakresem ich **oddziaływania** przedstawionym w **załączniku** nr 1.2 - *Wykaz interesariuszy i użytkowników SRP*.
  - pracowników, **współpracowników** i kontrahentów **każdego** z interesariuszy SRP, **mających dostęp** do systemu i jego dokumentacji w charakterze **właścicieli**, gestorów, **użytkowników**, administratorów **bezpieczeństwa**, operatorów, programistów, testerów lub innych ról, **wykonujących** operacje **i działania związane** z rozwojem, **eksploatacją**, utrzymanie

i wycofaniem starszych wersji SRP, **mających wpływ** na jego **prawidłowe** i nieprzerwane funkcjonowanie wyszczególnionych w **załączniku** nr 1.3 *Wykaz ról i odpowiedzialności SRP*.

1.4 System zarządzania bezpieczeństwem informacji

Polityka Bezpieczeństwa Informacji poprzez określone w niej zasady, procesy, polityki i procedury zarządzania i postępowania definiuje system zarządzania bezpieczeństwem informacji specyficzny i właściwy dla Systemu Rejestrów Państwowych.

Celem Polityki **Bezpieczeństwa** Informacji w takim rozumieniu jest zdefiniowanie i dostosowanie procesów **zarządczych** i operacyjnych w ramach PBI w celu sprawnego i efektywnego sterowania **działaniami** oraz **bieżącej** aktualizacji dokumentacji Polityki **Bezpieczeństwa** Informacji.

System **zarządzania bezpieczeństwem** informacji oznacza **całokształt środków,** procesów i **przedsięwzięć,** zdefiniowanych **niniejszą** PBI, które **składają się** na **zarządzanie** i zapewnienie **bezpieczeństwa** informacji oraz aktywów **objętych niniejszą** PBI i definiuje sposób **postępowania** oparty o **przyjętą metodykę zarządzania bezpieczeństwem** informacji i systemów, **opartą** na wymaganiach ISO 27001.

Szczegółowe rozwiązania organizacyjne i techniczne bezpieczeństwa informacji niejawnych uregulowane są w Dokumentacji bezpieczeństwa opracowanej zgodnie z wymaganiami ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnej. Dokumentacja ta jest poza zakresem niniejszej PBI SRP.

Referencyjność

Polityka Bezpieczeństwa Informacji dla SRP jest w pełni zgodna z międzynarodowym standardem zarządzania bezpieczeństwem informacji, normą ISO 27001, odzwierciedla jej strukturę, procesy i dobre praktyki, które są uznane za referencyjne dla opracowywanych polityk bezpieczeństwa informacji i systemów zarządzania bezpieczeństwem informacji dla administracji publicznej w przepisach prawa.

Właściciel SRP zapewnia stałą zgodność Polityki Bezpieczeństwa Informacji z wymaganiami ISO 27001 i wyraża zobowiązanie, że planowanie, wdrożenie, utrzymywanie i ciągłe doskonalenie zasad, procesów, polityk i procedur zarządzania i postępowania w odniesieniu do bezpieczeństwa informacji i systemu będzie realizowane zgodnie z wymaganiami określonymi w normie ISO 27001 oraz mającymi zastosowanie przepisami prawa.

W przypadku zmiany obowiązującej wersji normy ISO 27001 na nowszą, zastosowanie ma najnowsza wersja normy, co oznacza konieczność dostosowania do niej PBI dla SRP.

Struktura

Polityka Bezpieczeństwa Informacji opisuje zasady zarządzania i zapewnienia bezpieczeństwa informacji ustanowione dla SRP i składa się z 2 zasadniczych części:

- Cz. I **Zarządzanie bezpieczeństwem** informacji
- Cz. II Zapewnienie **bezpieczeństwa** - zabezpieczenia

Część I Zarządzanie bezpieczeństwem informacji opisuje system zarządzania bezpieczeństwem informacji, czyli organizacyjno-systemowe kwestie i procesy niezbędne do sprawnego planowania, wdrażania, funkcjonowania i doskonalenia bezpieczeństwa przetwarzanych w systemie informacji i samego SRP. W zakresie zarządzania bezpieczeństwem informacji zaadresowane są poniższe kwestie:

- Kontekst systemu SRP
- Przywództwo
- Planowanie
- Wsparcie
- Funkcjonowanie
- Ocena skuteczności
- Doskonalenie

Część II Zapewnienie bezpieczeństwa opisuje ustanowione dla zapewnienia bezpieczeństwa przetwarzanych w systemie informacji i samego SRP rozwiązania organizacyjne i techniczne, które są uzupełnione w politykach szczegółowych i procedurach operacyjnych, stanowiących załączniki do niniejszej polityki. W zakresie zapewnienia bezpieczeństwa informacji zaadresowane są poniższe kwestie:

- Polityki bezpieczeństwa informacji
- Organizacja bezpieczeństwa informacji
- Bezpieczeństwo zasobów ludzkich
- Zarządzanie aktywami
- Kontrola dostępu
- Kryptografia
- Bezpieczeństwo fizyczne i środowiskowe
- Bezpieczna eksploatacja
- Bezpieczeństwo komunikacji
- Pozyskiwanie, rozwój i utrzymanie systemów
- Relacje z dostawcami
- Zarządzanie incydentami związanymi z bezpieczeństwem informacji
- Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania
- Zgodność

Odstępstwa i wyjątki

Kwestia odstępstw i wyjątków została zaadresowana w punkcie 7.1 Odstępstwa, niezgodności, incydenty i działania korygujące niniejszej PBI oraz ***Procedurze nadzorowania odstępstw, niezgodności i działań korygujących SRP***, stanowiącej załącznik nr 1.8 do niniejszej PBI.

2. Przywództwo

2.1 Przywództwo i zaangażowanie

Właściciel SRP pełni rolę najwyższego kierownictwa w zakresie zarządzania bezpieczeństwem informacji Systemu Rejestrów Państwowych i przetwarzanych w nim danych.

Właściciel SRP wyraża swoje przywództwo, zaangażowanie i odpowiedzialność w zakresie bezpieczeństwa Systemu Rejestrów Państwowych ustanawiając niniejszą Politykę Bezpieczeństwa

Informacji SRP i zobowiązując wszystkich interesariuszy do jej przestrzegania i realizacji jej postanowień.

Właściciel SRP:

- zapewnia, **że** Polityka **Bezpieczeństwa** Informacji SRP, zdefiniowane **rozwiązania** organizacyjne i techniczne **bezpieczeństwa** oraz cele stosowania **zabezpieczeń** informacji **są** ustanowione i zgodne ze strategicznym kierunkiem rozwoju, eksploatacji i utrzymania SRP oraz celem zapewnienia wysokiego poziomu **bezpieczeństwa** SRP
- zapewnia, **że** zdefiniowane **rozwiązania** organizacyjne i techniczne **bezpieczeństwa są** zintegrowane z procesami cyklu **życia** systemu – projektowania, wytwarzania, rozwoju, eksploatacji i utrzymania SRP
- zapewnianie **niezbędne** zasoby osobowe, finansowe i lokalowe dla **wdrożenia,** utrzymywania i **ciągłego** doskonalenia **postanowień** niniejszej PBI
- **podkreśla** i komunikuje **duże** znaczenie skutecznego **zarządzania bezpieczeństwem** informacji i stosowania **postanowień** niniejszej PBI
- zapewnia **realizację** ustanowionego celu utrzymania wysokiego poziomu **bezpieczeństwa** SRP
- kieruje i wspiera **działania** osób i interesariuszy **zaangażowanych** w **realizację postanowień** niniejszej PBI
- promuje **ciągłe** doskonalenie
- wspiera **Interesariuszy SRP** oraz **Gestora SRP** w realizacji przywództwa w zakresie **bezpieczeństwa** w stopniu odpowiednim do zakresu ich **obowiązków**
- stosuje sankcje w rodzaju czasowego lub **stałego** odebrania **uprawnień dostępu** do systemu oraz sankcje **wynikające** z przepisów prawa za niestosowanie lub nieadekwatne stosowanie **postanowień** niniejszej PBI.

2.2 Polityka bezpieczeństwa informacji

Celem Polityki Bezpieczeństwa Informacji jest zapewnienie wysokiego poziomu bezpieczeństwa informacji przetwarzanych w systemie i samego systemu poprzez ustanowienie zasad, procesów, polityk i procedur zarządzania i postępowania.

Bezpieczeństwo informacji rozumiane jest jako zachowanie takich właściwości informacji i systemu informacyjnego, jak:

- **poufność – właściwość polegająca** na tym, **że** informacja nie jest **udostępniana** ani ujawniana nieautoryzowanym podmiotom (osobom, podmiotom lub procesom)
- **integralność– właściwość polegająca** na zapewnieniu **dokładności** i **kompletności**
- **dostępność– właściwość** bycia **dostępnym** i **użytecznym** na **żądanie** autoryzowanego podmiotu
- **rozliczalność- właściwość** systemu **pozwalająca przypisać określone działanie** w systemie do podmiotu oraz **umiejscowić** je w czasie
- **niezaprzeczalność– zdolność** do udowodnienia, **że wystąpiły** deklarowane zdarzenia lub **działania** oraz, **że wywołał** je dany podmiot
- **autentyczność – właściwość polegająca** na tym, **że** podmiot jest tym, za kogo **się** podaje
- **niezawodność – właściwość oznaczająca** spójne, zamierzone zachowanie i skutki

Bezpieczeństwo informacji realizowane jest w sposób i w zakresie adekwatnym do celu bezpieczeństwa PBI, określonego powyżej oraz celów bezpieczeństwa określonych w punkcie 3.2 poniżej, w zakresach przedmiotowym, terytorialnym, funkcjonalnym, instytucjonalnym i personalnym obowiązywania niniejszej PBI, określonych powyżej w punkcie 1.3 Zakres stosowania Polityki Bezpieczeństwa Informacji, poprzez działania i rozwiązania organizacyjne i techniczne określone w części II Zapewnienie bezpieczeństwa niniejszej PBI.

2.3 Role organizacyjne, zakresy odpowiedzialności i uprawnienia

W zarządzaniu bezpieczeństwem informacji SRP istotne znaczenie ma zdefiniowanie ról i ich odpowiedzialności. Dla SRP podstawą do tego są regulacje prawne dotyczące SRP oraz zapisy niniejszej PBI i związanych z nią procedur, które definiują role i ich funkcje w zapewnieniu bezpieczeństwa informacji w rozwoju, eksploatacji i utrzymaniu SRP.
Zdefiniowane role i odpowiedzialności w systemie bezpieczeństwa SRP znajdują się w ***Wykazie ról i odpowiedzialności SRP***, stanowiącym załącznik nr 1.3 do niniejszej PBI.

Role i ich odpowiedzialności podlegają okresowej weryfikacji przynajmniej jeden raz w roku i w razie potrzeby - aktualizacji. Aktualizacja powinna być przeprowadzona również każdorazowo w związku z rozbudową SRP o kolejne rejestry i zmianami prawnymi, które mogą definiować zmiany ról.

Gestor SRP jest odpowiedzialny za zdefiniowanie ról i odpowiedzialności w systemie bezpieczeństwa SRP oraz za ich przegląd i aktualizację.

3. Planowanie

Właściciel SRP oraz działający w jego imieniu **Gestor systemu SRP są** odpowiedzialni za zaplanowanie i zaprojektowanie **rozwiązań** organizacyjnych i technicznych **bezpieczeństwa** informacji SRP.
Rozwiązania organizacyjne i techniczne **bezpieczeństwa** systemu i informacji w nim przetwarzanych **są** planowane i projektowane w odniesieniu do celu **bezpieczeństwa, wyrażonego** w punkcie 2.2 **powyżej,** poprzez zastosowanie procesu **zarządzania** ryzykiem oraz wybór i **wdrożenie,** na podstawie jego wyników, adekwatnych **środków** sterowania ryzykiem **spośród zabezpieczeń** zawartych w **załączniku** A normy ISO 27001. Dla zapewnienia wysokiego poziomu **bezpieczeństwa** SRP **przyjęto** za **obowiązujące** wszystkie zabezpieczenia wymienione w **załączniku** A normy ISO 27001. Sposób implementacji wybranych **zabezpieczeń,** specyficzny i **właściwy** dla SRP zawarty jest w **części** II Zapewnienie **bezpieczeństwa** niniejszej PBI wraz z **załącznikami.**
Adekwatność przyjętych rozwiązań, ich **skuteczność** i **efektywność są** monitorowane i oceniane zarówno w trybie **ciągłym,** jak i poprzez **działania** realizowane okresowo, o których mowa w punkcie 6 niniejszej PBI.
Proces szacowania ryzyka, wyboru i **wdrożenia zabezpieczeń** jest realizowany cyklicznie, przy czym w kolejnych iteracjach **wdrożone już** zabezpieczenia, **określone** w **części** II Zapewnienie **bezpieczeństwa** niniejszej PBI, **należy** adekwatnie **modyfikować** lub **wdrażać** nowe zabezpieczenia, **jeśli** zajdzie taka **konieczność,** aby **osiągać** ustalony poziom **bezpieczeństwa.**

3.1 Zarządzanie ryzykiem

Gestor systemu SRP jest odpowiedzialny za **realizację** procesu **zarządzania** ryzykiem, ponadto jest **głównym właścicielem** ryzyka **bezpieczeństwa** informacji systemu.

Interesariusze systemu **są właścicielami** dziedzinowych ryzyk **bezpieczeństwa** informacji, w sytuacji, gdy ujawnione ryzyka ich **dotyczą**.

Zarządzanie ryzykiem naruszenia lub utraty zdefiniowanych atrybutów **bezpieczeństwa**, tj.: **poufności, integralności, dostępności, rozliczalności, niezaprzeczalności, autentyczności** i **niezawodności,** prowadzi **się** poprzez **działania** okresowe w trybach corocznym oraz ad hoc - w przypadkach zidentyfikowania **zagrożeń** dla **bezpieczeństwa** systemu i danych, w **związku** z rozwojem i zmianami w systemie oraz w przypadku powstania incydentów **bezpieczeństwa.**

Zarządzanie ryzykiem **bezpieczeństwa** informacji i systemu realizowane jest z zastosowaniem wytycznych z dokumentu *Polityka **zarządzania** ryzykiem SRP*, **stanowiącym** odpowiednio **załączniki** nr 1.4 do niniejszej PBI.

W procesie identyfikacji ryzyka **należy określić podatności** systemu **biorąc** pod **uwagę architekturę** systemu i jego **rozwiązania** technologiczne oraz wszystkie aktualnie **wdrożone rozwiązania** organizacyjne i techniczne **bezpieczeństwa** (w tym ich **stopień,** zakres i **siłę),** o których mowa w **części** II Zapewnienie **bezpieczeństwa** niniejszej PBI.

W procesie **postępowania** z ryzykiem **należy wybrać** adekwatne **środki** sterowania ryzykiem **spośród** zawartych w **załączniku** A normy ISO 27001, a zaimplementowanych w **części** II Zapewnienie **bezpieczeństwa** niniejszej PBI, **określając** ich odpowiedni **stopień,** zakres i **siłę,** jakie powinny **zostać wdrożone,** aby **zmitygować** ryzyko do akceptowalnego poziomu.

Katalog **zabezpieczeń** oparty jest o **załącznik** A normy ISO 27001 lecz nie jest **zamknięty** i **można zastosować również** inne **środki** sterowania ryzykiem nie wymienione w **załączniku** A normy ISO 27001.

Wdrożenie i realizacja w/w **rozwiązań** i **działań może wiązać się** ze zdefiniowaniem specyficznych **zadań (dotyczących** np. opracowania lub aktualizacji dokumentacji **bezpieczeństwa,** czy eksploatacyjnej, zakupem i **wdrożeniem rozwiązań** teleinformatycznych i oprogramowania, przeprowadzeniem specyficznych analiz).

Gestor systemu SRP przypisuje wybrane działania postępowania z ryzykiem do realizacji właściwym interesariuszom - **właścicielom** dziedzinowych ryzyk bezpieczeństwa, określając, jako minimum, charakter podejmowanych działań (np. inwestycyjne, techniczne, organizacyjne), opis działań oraz termin ich realizacji.

Opis ryzyk i wybrane dla nich działania postępowania z ryzykiem stanowią Plan postępowania z ryzykiem. Może on przybierać formę odrębnego dokumentu lub dodatkowych pól w Rejestrze ryzyk.

Gestor systemu SRP odpowiada za opracowanie Planu postępowania z ryzykiem.

Zaplanowane **działania** postępowania z ryzykiem zapewniają osiąganie założonych celów bezpieczeństwa, zdefiniowanych w punkcie 3.2 niniejszej PBI, zapobieganie występowaniu niepożądanych skutków i ich skuteczne zredukowanie oraz ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji zdefiniowanego poprzez postanowienia niniejszej PBI.

Zaplanowane **działania postępowania** z ryzykiem nie **mogą być** sprzeczne ani o **niższej** sile i **skuteczności** zabezpieczenia przed ryzykami **niż** te zdefiniowane w **części** II Zapewnienie **bezpieczeństwa** niniejszej PBI wraz z **załącznikami.**

W przypadku, gdy zaplanowane **działania postępowania** z ryzykiem **rozszerzają** zakres i **podnoszą siłę** i **skuteczność zabezpieczeń, należy** odpowiednio **zmodyfikować rozwiązania** organizacyjne i techniczne **bezpieczeństwa** (wytyczne, polityki, procedury) zawarte w **części** II Zapewnienie **bezpieczeństwa** niniejszej PBI.

Gestor SRP dokonuje akceptacji wyników szacowania ryzyka i wybranych sposobów **postępowania** z ryzykiem oraz akceptacji ryzyka.

Gestor SRP przekazuje **Właścicielowi SRP oświadczenie** o dokonanej analizie ryzyka wraz z **informacją** o ryzykach w formie Rejestru ryzyk, zgodnie z zapisami Metodyki oraz Plan **postępowania** z ryzykiem, o ile **został** ustanowiony jako **odrębny** dokument, a nie jako zapisy w Rejestrze ryzyk.

Wyniki procesu szacowania ryzyka **zostają** udokumentowane w arkuszu Rejestr ryzyk.

Rejestr ryzyk i Plan **postępowania** z ryzykiem, o ile **został** ustanowiony jako **odrębny** dokument, **podlegają** odpowiedniemu zaklasyfikowaniu i ochronie, zgodnie z zasadami **określonymi** w *Polityce klasyfikacji informacji SRP*, **stanowiącej załącznik** nr 2.9 do PBI.

Rejestr ryzyk i Plan **postępowania** z ryzykiem **podlegają** nadzorowaniu zgodnie z zasadami ustanowionymi w *Procedurze nadzoru nad **dokumentacją bezpieczeństwa***, **stanowiącą załącznik** nr 1.7 do PBI.

3.2 Cele bezpieczeństwa informacji i planowanie ich osiągnięcia

Cele **bezpieczeństwa są** spójne z podstawowym celem Polityki **Bezpieczeństwa** Informacji zapewnienia wysokiego poziomu **bezpieczeństwa** informacji przetwarzanych w systemie i samego SRP.

Wysoki poziom **bezpieczeństwa** jest **osiągany** poprzez:

- zapewnienie adekwatnej **poufności** informacji autoryzowanym podmiotom (osobom, podmiotom lub procesom)
- zapewnienie **pełnej integralności** i **zgodności** danych ze stanem faktycznym
- zapewnienie wysokiej **dostępności** i **użyteczności** danych i **usług** SRP
- zapewnienie **pełnej rozliczalności** systemu w odniesieniu do osób, podmiotów i systemów
- zapewnienie **pełnej niezaprzeczalności zdarzeń** lub **działań** i ich sprawstwa
- zapewnienie **pełnej identyfikowalności** osób, podmiotów i systemów
- zapewnienie wysokiej **niezawodności** systemu.

Cele te realizowane **są** przez **działania** w zakresie:

- Polityk **szczegółowych bezpieczeństwa** informacji – poprzez *zapewnienie wytycznych i wsparcia dla **działań** na rzecz **bezpieczeństwa** informacji,* zgodnie z wymaganiami biznesowymi i prawnymi
- Organizacji **bezpieczeństwa** informacji – poprzez *ustanowienie struktury **zarządzania*** w celu nadzorowania funkcjonowania **bezpieczeństwa** informacji systemu; *zapewnienie **bezpieczeństwa** pracy zdalnej i stosowania **urządzeń** mobilnych*

- **Bezpieczeństwa** zasobów ludzkich – poprzez ***uświadomienie*** *pracowników i kontrahentów w zakresie ich* ***obowiązków*** *i* ***odpowiedzialności odnośnie bezpieczeństwa*** *informacji; zapewnienie wymaganej weryfikacji osób zatrudnianych; zabezpieczenie interesów* ***właściciela*** *systemu w trakcie zmiany lub* ***zakończenia*** *zatrudnienia*
- **Zarządzania** aktywami – poprzez ***identyfikację*** *aktywów i przypisanie* ***odpowiedzialności*** *w zakresie ich ochrony,* ***określenie*** *poziomu ochrony informacji; zapobieganie nieuprawnionemu przetwarzaniu informacji zapisanych na* ***nośnikach***
- Kontroli **dostępu** – poprzez *ograniczenie* ***dostępu*** *do informacji i* ***środków*** *jej przetwarzania; zapewnienie uprawnionego* ***dostępu użytkownikom*** *oraz zapobieganie nieuprawnionemu* ***dostępowi*** *do systemów i* ***usług;*** *zapobieganie nieuprawnionemu* ***dostępowi*** *do systemów i aplikacji; zapewnienie* ***rozliczalności użytkowników***
- Kryptografii – poprzez *zapewnienie* **właściwego** i skutecznego wykorzystania kryptografii do ochrony ***poufności, autentyczności i integralności*** *informacji*
- **Bezpieczeństwa** fizycznego i **środowiskowego** – poprzez *zapobieganie nieuprawnionemu fizycznemu* ***dostępowi*** *i szkodom; zapobieganie utracie, uszkodzeniu aktywów i ich* ***integralności*** *oraz* ***zakłóceniom*** *w funkcjonowaniu systemu*
- Bezpiecznej eksploatacji – poprzez *zapewnienie poprawnej i bezpiecznej eksploatacji* ***środków*** *przetwarzania informacji; zapewnienie ochrony przed szkodliwym oprogramowaniem; ochrona przed* ***utratą*** *danych; rejestrowanie i gromadzenie* ***materiałów*** *dowodowych; zapewnienie* ***integralności*** *systemów produkcyjnych; zapobieganie wykorzystaniu technicznych* ***podatności;*** *minimalizacja* ***wpływu*** *audytu na funkcjonowanie systemów*
- **Bezpieczeństwa** komunikacji – poprzez *zapewnienie ochrony informacji* ***przesyłanych*** *w sieciach i innych* ***środkach*** *przetwarzania*
- Pozyskiwania, rozwoju i utrzymania systemów – poprzez *zapewnienie, aby* ***bezpieczeństwo*** *informacji* ***było uwzględniane*** *w* ***całym*** *cyklu* ***życia*** *systemów; zapewnienie ochrony danych testowych*
- Relacji z dostawcami – poprzez *zapewnienie ochrony aktywów w relacjach z dostawcami; utrzymanie uzgodnionego poziomu* ***bezpieczeństwa*** *informacji i* ***usług objętych*** *umowami z dostawcami*
- **Zarządzania** incydentami **związanymi** z **bezpieczeństwem** informacji – poprzez *zapewnienie spójnego i skutecznego* ***zarządzania*** *incydentami* ***związanymi*** *z* ***bezpieczeństwem*** *informacji oraz informowanie o zdarzeniach i* ***słabościach***
- **Bezpieczeństwa** informacji w **zarządzaniu ciągłością działania** – poprzez ***uwzględnienie ciągłości bezpieczeństwa*** *informacji w systemie* ***zarządzania ciągłością działania;*** *zapewnienie* ***dostępności środków*** *przetwarzania*
- **Zgodności** z wymaganiami – poprzez *unikanie naruszania przepisów prawa i innych* ***uregulowań dotyczących bezpieczeństwa*** *informacji; zapewnienie* ***wdrożenia*** *i stosowania zasad* ***bezpieczeństwa*** *informacji zgodnie z politykami organizacji i procedurami*

Realizacja w/w **działań** i celów prowadzona jest poprzez **wdrożenie właściwych** i adekwatnych **rozwiązań** i **działań** organizacyjnych i technicznych **określonych** w **części** II Zapewnienie **bezpieczeństwa** niniejszej PBI.

Stopień realizacji celów **bezpieczeństwa** podlega raportowaniu do **Gestora systemu SRP** w ramach realizacji procesu **przeglądu zarządzania** zdefiniowanego w pkt 6.3 **poniżej.**

4. Wsparcie

4.1 Zasoby

Właściciel SRP zapewnia **niezbędne** zasoby osobowe, finansowe i lokalowe dla ustanowienia i realizacji **wdrożenia,** utrzymywania i **ciągłego** doskonalenia **postanowień** niniejszej Polityki **Bezpieczeństwa** Informacji SRP w zakresie odpowiednim dla kompetencji ministra **właściwego** ds. informatyzacji.

Interesariusze SRP **zapewniają niezbędne** zasoby osobowe, finansowe i lokalowe dla realizacji **wdrożenia,** utrzymywania i **ciągłego** doskonalenia **postanowień** niniejszej Polityki **Bezpieczeństwa** Informacji SRP w zakresie odpowiednim dla zakresu **oddziaływania** i kompetencji **każdego** z interesariuszy.

4.2 Kompetencje

Właściciel SRP oraz **każdy** z interesariuszy SRP **zapewniają** odpowiednie kompetencje w zakresie **bezpieczeństwa** informacji SRP swoich pracowników, **współpracowników** i kontrahentów **mających dostęp** do danych, do systemu i jego dokumentacji technicznej i eksploatacyjnej, i **realizujących** funkcje **związane** z **eksploatacją,** utrzymaniem i rozwojem systemu.

Kompetencje w/w osób powinny **być** adekwatne do zakresów **odpowiedzialności** zdefiniowanych dla poszczególnych ról w systemie.

Niezbędne kompetencje poszczególnych ról w systemie **zarządzania bezpieczeństwem** informacji SRP **dotyczą** odpowiednio aspektów prawnych i organizacyjnych, technicznych i technologicznych, osobowych i fizycznych **bezpieczeństwa.**

Kompetencje rozumiane **są** jako wiedza, **umiejętności** i **doświadczenie** i **osiągane są** poprzez **wykształcenie,** szkolenia, **staże, udział** seminariach, konferencjach, itp.
Dla zapewnienia odpowiednich kompetencji określany jest zakres niezbędnych kompetencji dla każdej z ról, prowadzone są w/w działania prowadzące do osiągnięcia tych kompetencji i okresowo dokonywana jest ocena posiadanych kompetencji.

Proces realizowany jest w trybie **ciągłym** przez **właściwe** komórki organizacyjne **każdego** z interesariuszy SRP.

Proces jest realizowany zgodnie z *Polityką bezpieczeństwa zasobów ludzkich SRP*, **stanowiącą załącznik** nr 2.3 do niniejszej PBI.

4.3 Uświadamianie

Właściciel SRP oraz **każdy** z interesariuszy SRP **zapewniają właściwy** poziom **świadomości** w zakresie **bezpieczeństwa** informacji SRP swoich pracowników, **współpracowników** i kontrahentów **mających dostęp** do danych, do systemu i jego dokumentacji technicznej i eksploatacyjnej, i **realizujących** funkcje **związane** z **eksploatacją,** utrzymaniem i rozwojem systemu. **Świadomość** w zakresie **bezpieczeństwa** w/w osób powinna **być** adekwatna do zakresów **odpowiedzialności** zdefiniowanych dla poszczególnych ról w systemie.

Osoby **pełniące** poszczególne role w systemie **zarządzania bezpieczeństwem** informacji SRP powinny **być świadome:**

- polityki bezpieczeństwa informacji, w tym celów i rozwiązań organizacyjnych i technicznych bezpieczeństwa,

- ich wkładu i oddziaływania na skuteczność PBI i poziom bezpieczeństwa systemu i przetwarzanych danych,
- konsekwencji niezachowania zgodności z wymogami niniejszej PBI.

Proces zapewnienia świadomości w zakresie bezpieczeństwa informacji SRP realizowany jest poprzez szkolenie wstępne przed rozpoczęciem pracy, czy współpracy i powtarzane cyklicznie, nie rzadziej niż co 2 lata, szkolenia okresowe oraz w trybie ciągłym poprzez podnoszenie kwestii bezpieczeństwa przez przełożonych i wzajemnie pomiędzy pracownikami interesariuszy w związku z realizacją zadań eksploatacji, utrzymania i rozwoju systemu.
Proces jest realizowany zgodnie z ***Polityką bezpieczeństwa*** *zasobów ludzkich*, **stanowiącą załącznik** nr 2.3 do niniejszej PBI.

4.4. Komunikacja

W systemie **zarządzania bezpieczeństwem** informacji SRP funkcjonuje proces komunikacji w zakresie **bezpieczeństwa** informacji SRP. Komunikacja ta jest prowadzona na poziomach **wewnętrznym** i **zewnętrznym** oraz **zarządczym** i operacyjnym.

Gestor SRP odpowiada za **prawidłowość** i **skuteczność** procesu komunikacji.

Komunikacja na poziomie **wewnętrznym** obejmuje **komunikację pomiędzy** ministerstwem **właściwym** ds. informatyzacji a podmiotami **bezpośrednio zaangażowanymi** w **działania** na rzecz systemu w **całym** jego cyklu **życia** (projektowanie, wytwarzanie, **eksploatację**, rozwój i wycofanie), tzn. ministerstwem **właściwym** ds. **wewnętrznych** i administracji i podmiotem **realizującym** zadania na rzecz ministra **właściwego** ds. informatyzacji oraz **wewnątrz** tych organizacji.

Komunikacja na poziomie **zewnętrznym** obejmuje **komunikację pomiędzy** ministerstwem **właściwym** ds. informatyzacji a interesariuszami SRP oraz **wewnątrz** tych organizacji.

Komunikacja na poziomie **zarządczym** nadzorowana jest przez **Właściciela SRP** lub w jego imieniu przez **Gestora systemu SRP** i obejmuje kwestie **dotyczące zarządzania bezpieczeństwem** informacji SRP i **związane** z tym raporty, analizy, plany, decyzje itp, zaadresowane w procesach i procedurach **zarządzania bezpieczeństwem** informacji niniejszej PBI.

Komunikacja na poziomie operacyjnym realizowana jest przez wszystkich interesariuszy i dotyczy wszelkich operacyjnych, **bieżących** aspektów **bezpieczeństwa** danych i systemu, w tym incydentów **bezpieczeństwa, związanych** z rozwojem, **eksploatacją** i utrzymaniem systemu.

Komunikacja obejmuje wszelkie kwestie **dotyczące**:

- **obowiązującej** Polityki **Bezpieczeństwa** Informacji SRP i celów **bezpieczeństwa**
- **obowiązujących rozwiązań** organizacyjnych i technicznych **bezpieczeństwa** - polityk **szczegółowych** i procedur **dotyczących bezpieczeństwa** informacji i systemu oraz ich zmian
- **obowiązujących wymagań dotyczących bezpieczeństwa** informacji i systemu, **wymagań** prawnych wobec systemu, **wymagań** funkcjonalnych i niefunkcjonalnych dla SRP
- zakresu operacyjnego **działania** interesariuszy i ich **odpowiedzialności** w zakresie **bezpieczeństwa**

- wyników szacowania ryzyka, planów postępowania z ryzykiem i stopnia ich realizacji
- stanu bezpieczeństwa systemu, stopnia spełniania wymagań dotyczących bezpieczeństwa, stopnia realizacji i skuteczności rozwiązań organizacyjnych i technicznych bezpieczeństwa, podejmowanych działań z tym związanych
- wyników audytów wewnętrznych bezpieczeństwa i realizacji zaleceń poaudytowych
- wszelkich odstępstw, niezgodności, incydentów i prób naruszenia bezpieczeństwa, i podejmowanych w związku z tym działań i ich statusu
- planowanych, projektowanych i realizowanych zmian, przebudowy i rozbudowy SRP, i ich wpływu na bezpieczeństwo danych i systemu
- inne kwestie uznane za ważne dla bezpieczeństwa informacji i systemu.

Komunikacja dotycząca bezpieczeństwa informacji SRP odbywa się z zachowaniem zasad bezpieczeństwa, tj.: poufności, dostępności, integralności, rozliczalności, niezaprzeczalności, niezawodności, o ile jest to możliwe dla danego, stosowanego medium komunikacyjnego.

Komunikacja realizowana jest poprzez:

- poprzez uzgodnione i zatwierdzone kanały komunikacji – pocztę elektroniczną, systemy informatyczne tj. ITSM, platformę internetową, nośniki danych, dedykowane łącze VPN, komunikację bezpośrednią, korespondencję papierową
- z zastosowaniem środków zabezpieczających takich jak szyfrowanie, anonimizacja, pseudonimizacja danych, o ile jest to możliwe dla danego, stosowanego medium komunikacyjnego
- w ramach uprawnionych grup osób zainteresowanych, bezpośrednio do właściwych adresatów
- z zachowaniem jednoznacznie zdefiniowanej ścieżki akceptacji podejmowanych działań, wynikającej ze zwierzchności hierarchicznej ról
- wg zasady wiedzy uzasadnionej, oznaczającej dostęp do wiedzy ograniczony wyłącznie do zagadnień koniecznych do realizacji powierzonych zadań
- w rygorze czasowym i terminowym wynikającym z regulacji prawnych oraz uzgodnionego trybu operacyjnego
- z zachowaniem trybu pełnego dokumentowania działań i decyzji.

Szczegóły dotyczące przedmiotu, formy i uczestników komunikacji określają każda z poszczególnych procesów, procedur i polityk niniejszej PBI, we właściwym dla siebie kontekście i zakresie.

Zasady bezpiecznej komunikacji określone są w części II PBI oraz w *Procedurze komunikacji w zakresie bezpieczeństwa SRP*, stanowiącej załącznik nr 1.7 do PBI i w *Polityce przesyłania informacji SRP*, stanowiącej załącznik nr 2.21 do PBI.

Proces komunikacji dotyczącej bezpieczeństwa informacji SRP podlega okresowej, minimum corocznej, weryfikacji i w razie takiej potrzeby - aktualizacji.

Wszelkie zmiany w procesie komunikacji dotyczącej bezpieczeństwa informacji i systemu wymagają niezwłocznego poinformowania wszystkich interesariuszy i zapewnienia zaznajomienia się z wprowadzonymi zmianami.

4.5 Udokumentowane informacje

Gestor SRP zapewnia właściwy nadzór na Polityką Bezpieczeństwa Informacji i związanymi z nią dokumentami, stanowiącymi dokumentację bezpieczeństwa.

Dokumentację bezpieczeństwa stanowią dokumenty w formie papierowej i elektronicznej oraz zapisy w systemach informatycznych.

Dokumentację bezpieczeństwa stanowią między innymi:

- Polityka **Bezpieczeństwem** Informacji SRP, wraz z **załączonymi** politykami **szczegółowymi** i procedurami **stanowiącymi integralną część** PBI
- Wykazy, rejestry i zestawienia ustanowione **niniejszą Polityką Bezpieczeństwa** Informacji, **stanowiące załączniki** do niej tj. np. Wykaz **wymagań** prawnych, Wykaz interesariuszy, Wykaz ról i **odpowiedzialności** i inne w razie ich **późniejszego załączania**
- Polityka **zarządzania** ryzykiem - Rejestry ryzyk, Plany **postępowania** z ryzykiem, o ile nie **zostały** zawarte w Rejestrze ryzyk
- Dokumentacja audytu **wewnętrznego bezpieczeństwa** – programy, plany audytu, raporty z audytów i zalecenia poaudytowe
- Dokumentacja **przeglądu zarządzania** – dokumentacja danych **wejściowych** na **przegląd zarządzania,** raporty z **przeglądów zarządzania,** zgodnie z punktem 6.3 PBI **poniżej**
- Dokumentacja operacyjnego monitorowania **zdarzeń** w systemie, **związanych** z przetwarzaniem danych
- Dokumentacja **dotycząca zgłoszenia** i **obsługi** incydentów **bezpieczeństwa**
- Raporty z testów **bezpieczeństwa** wraz z rekomendacjami
- Dokumentacja **dotycząca** projektowania, analizy, wytwarzania, eksploatacji, rozwoju, zmiany i wycofania systemu w **części związanej** z **bezpieczeństwem** informacji SRP

Dokumentację bezpieczeństwa stanowią również inne dokumenty i zapisy, o ile dotyczą bezpieczeństwa informacji SRP. Spis dokumentów wchodzących w skład niniejszej polityki został określony w dokumencie *Wykaz załączników do Polityki Bezpieczeństwa Informacji SRP*, załączniku nr 1 do niniejszej polityki.

Polityka Bezpieczeństwa Informacji oraz związana z nią dokumentacja bezpieczeństwa podlegają nadzorowi w celu zapewnienia ich:

- **przydatności i adekwatności**
- **użyteczności i dostępności**
- **poufności, integralności**
- **uniemożliwieniem niewłaściwego użycia.**

Nadzór nad dokumentacją jest realizowany poprzez zapewnienie odpowiednich dla charakteru SRP sposobów postępowania oraz uprawnień i odpowiedzialności obejmujących:

- opracowywanie, aktualizowanie i zatwierdzanie
- **dystrybucję, dostęp,** wyszukiwanie i wykorzystywanie
- przechowywanie i zabezpieczanie
- nadzorowanie zmian
- **likwidację.**

Zasady realizacji nadzoru nad dokumentacją bezpieczeństwa informacji SRP udokumentowane są w *Procedurze nadzoru nad dokumentacją bezpieczeństwa SRP*, stanowiącej załącznik nr 1.7 do niniejszej PBI oraz w *Wykazie osób/stanowisk odpowiedzialnych za opracowanie, przegląd, ocenę i udostępnianie polityk bezpieczeństwa informacji w systemie*, stanowiącym załącznik nr 2.1 do niniejszej PBI.

5. Wdrożenie i funkcjonowanie

Właściciel SRP zatwierdza i **wdraża niniejszą Politykę Bezpieczeństwa** Informacji SRP, **stosując właściwy** tryb administracyjny – **zarządzenie** ministra.
Zarządzenie **Właściciela SRP**, **wprowadzające** postanowienia niniejszej PBI, wskazuje okres **przejściowy** do dnia jej **obowiązywania**.

Każdy z interesariuszy SRP jest **zobowiązany** do stosowania **postanowień** niniejszej Polityki oraz do zapewnienia jej **znajomości** i stosowania przez **każdego** pracownika, **współpracownika** i kontrahenta **mającego dostęp** do danych, do systemu i jego dokumentacji technicznej i eksploatacyjnej, i **realizujących** funkcje **związane** z **eksploatacją**, utrzymaniem i rozwojem systemu.
Każdy z interesariuszy jest **zobowiązany** do **wdrożenia postanowień** niniejszej PBI poprzez adekwatne dostosowanie wszelkich **rozwiązań** technicznych i organizacyjnych, **działań**, procesów oraz wprowadzenie stosownych regulacji **wewnętrznych** na **dzień** jej **obowiązywania**.

Niewywiązywanie się z realizacji **postanowień** niniejszej Polityki **Bezpieczeństwa** Informacji przez interesariuszy oraz ich pracowników, **współpracowników** i kontrahentów powoduje adekwatne sankcje, **możliwe** do zastosowania przez ministra **właściwego** ds. informatyzacji, jak np. czasowe lub **stałe** odebranie **uprawnień dostępu** do systemu oraz **możliwe** do zastosowania przez danego interesariusza, jako **pracodawcę**, adekwatne sankcje, zgodne z przepisami prawa pracy.

6. Ocena wyników

6.1 Monitorowanie, pomiary, analiza i ocena

Status **wdrożenia** niniejszej Polityki **Bezpieczeństwa** Informacji oraz stan i **skuteczność wdrożonych rozwiązań** organizacyjnych i technicznych **bezpieczeństwa** dla SRP przez **każdego** z interesariuszy podlega monitorowaniu, pomiarom, analizie i ocenie przez **Właściciela SRP**.
Właściciel SRP korzysta z **uprawnień** kontrolnych nadanych mu na mocy ustawy o ewidencji **ludności** i ustawy o dowodach osobistych
W imieniu **Właściciela SRP funkcję** nadzoru nad procesem sprawuje **Gestor SRP**.

Procesom monitorowania, pomiaru, analizy i oceny **podlegają** m.in.:

- **stopień osiągnięcia** ustalonego poziomu **bezpieczeństwa**
- **stopień osiągnięcia** ustalonych celów **bezpieczeństwa**
- poziom ryzyka i **stopień** jego mitygacji
- **występowanie**, skala, zakres **oddziaływania** i skutki incydentów **bezpieczeństwa** i **niezgodności** realizacji **rozwiązań** organizacyjnych i technicznych **bezpieczeństwa względem postanowień** niniejszej PBI

- stopień i poziom **wdrożenia** i realizacji **rozwiązań** organizacyjnych i technicznych **bezpieczeństwa** u **każdego** z interesariuszy SRP.

Procesy monitorowania, pomiaru, analizy i oceny realizowane **są** na poziomach **zarządczym** i operacyjnym.

Procesy monitorowania, pomiaru, analizy i oceny na poziomie **zarządczym** realizowane **są** cyklicznie dla zapewnienia **niezbędnego** zasobu informacji, **właściwej** oceny i podejmowania decyzji **odnośnie skuteczności wdrożenia** niniejszej PBI. W zakresie tych **działań** realizowane **są** audyty **wewnętrzne** i **przeglądy zarządzania bezpieczeństwa** informacji SRP opisane w pkt 6.2 i 6.3 **poniżej.**

Procesy monitorowania, pomiaru, analizy i oceny na poziomie operacyjnych realizowane **są** w trybie **ciągłym** dla zapewnienia **bieżących** informacji, **właściwej** oceny, podejmowania decyzji i **działań odnośnie** funkcjonowania systemu. **Bieżące działania** w tym zakresie to np. analiza incydentów, ocena **skuteczności obsługi** incydentów **bezpieczeństwa,** analiza **niezgodności** realizacji **rozwiązań** organizacyjnych i technicznych **bezpieczeństwa** i dokonywania ich **usprawnień.**

Wyniki monitorowania, pomiaru, analizy i oceny **podlegają** udokumentowaniu (w formie papierowej i/lub elektronicznej) i nadzorowaniu zgodnie z ***Procedurą*** *nadzoru nad* ***dokumentacją bezpieczeństwa*** *SRP*, **stanowiącą załącznik** nr 1.7 do niniejszej PBI.

Udokumentowane wyniki monitorowania, pomiaru, analizy i oceny **podlegają** odpowiedniemu zaklasyfikowaniu i ochronie, zgodnie z zasadami **określonymi** w *Polityce klasyfikacji informacji SRP*, **stanowiącej załącznik** nr 2.9 do PBI.

6.2 Audyt wewnętrzny

Gestor SRP zapewnia **realizację** audytów **bezpieczeństwa** informacji SRP.

Audyt **bezpieczeństwa** ma na celu **ocenę zgodności** i dostarczenie informacji, czy Polityka **Bezpieczeństwa** Informacji jest adekwatna do **konieczności** zapewnienia wysokiego poziomu **bezpieczeństwa** SRP i informacji w nim przetwarzanych, **wynikającego** m.in. z przepisów prawa i niniejszej PBI oraz, czy postanowienia niniejszej Polityki **dotyczące rozwiązań** organizacyjnych i technicznych **bezpieczeństwa są** skutecznie **wdrożone** i utrzymywane.

Audyt **wewnętrzny bezpieczeństwa** SRP realizowany jest przez **każdego** z interesariuszy **mającego** interakcje z SRP i **oddziaływującego** niego, **włącznie** z ministerstwem **właściwym** ds. informatyzacji, w obszarze (zakresie) ich interakcji z systemem i **oddziaływania** na niego (eksploatacji, rozwoju, utrzymania).

Audyt **wewnętrzny bezpieczeństwa** SRP prowadzony jest w sposób cykliczny i planowy, zgodnie z **wewnętrznymi** regulacjami (regulaminami, procedurami) interesariuszy w zakresie audytu **wewnętrznego,** z **uwzględnieniem** tego, **że** kryterium audytu jest niniejsza PBI i jej postanowienia, a zakres audytu obejmuje kwestie **bezpieczeństwa** SRP i danych w nim przetwarzanych oraz, **że:**

- w ministerstwie **właściwym** ds. informatyzacji i w podmiocie **realizującym działania** w zakresie rozwoju i utrzymania systemu na rzecz **Właściciela SRP** audyt realizowany jest corocznie w zakresie wszystkich **postanowień** niniejszej PBI
- w podmiocie **realizującym działania** w zakresie rozwoju i utrzymania SRP na rzecz **Właściciela SRP** audyt realizowany jest corocznie w zakresie **bezpieczeństwa** technicznego i **zgodności** technicznej SRP oraz z **związku wdrażaniem** zmian rozwojowych w systemie

- w instytucjach **korzystających** z SRP audyt realizowany jest corocznie w zakresie wybranych **postanowień** PBI, adekwatnych do zakresu ich interakcji z systemem, np. Polityki **bezpieczeństwa** stacji roboczych, **zarządzania** uprawnieniami, **bezpieczeństwa** fizycznego i osobowego.

Właściciel SRP, na mocy zapisów ustawy o ewidencji **ludności** i ustawy o dowodach osobistych, prowadzi audyty **bezpieczeństwa** u interesariuszy w celu sprawowania nadzoru i kontroli nad **bezpieczeństwem** SRP i przetwarzanych danych. **Gestor SRP** ustala odsetek interesariuszy, którzy **zostaną** poddani audytowi w danym roku.

Audyty realizowane przez **Właściciela SRP są niezależne** od audytów realizowanych przez **każdego** z interesariuszy.

Kierownictwo jednostek organizacyjnych interesariuszy systemu zapewnia **niezależność, obiektywność** i **bezstronność** procesu audytu oraz **adekwatną ochronę** wyników audytu.

Wyniki audytu **podlegają** odpowiedniemu zaklasyfikowaniu i ochronie, zgodnie z zasadami **określonymi** w *Polityce klasyfikacji informacji SRP*, **stanowiącej załącznik** nr 2.9 do PBI.

Wyniki audytu **są** udokumentowane w postaci Raportu z audytu i **zawierają** opis i **ocenę zgodności** stanu zastanego z postanowieniami niniejszej PBI oraz zalecenia w zakresie **osiągnięcia pełnej zgodności** z postanowieniami niniejszej PBI. **Wyartykułowane** w Raporcie z audytu zalecenia **mają** charakter **wiążący** dla audytowanego podmiotu.

Niewywiązywanie się z realizacji **zaleceń** powoduje adekwatne sankcje wobec interesariuszy i ich pracowników, **możliwe** do zastosowania odpowiednio przez ministra **właściwego** ds. informatyzacji lub interesariusza.

Raport z audytu podlega nadzorowaniu zgodnie z zasadami ustanowionymi w *Procedurze nadzoru nad dokumentacją bezpieczeństwa SRP*, **stanowiącą załącznik** nr 1.7 do PBI.

6.3 Przegląd zarządzania bezpieczeństwem informacji

Gestor SRP zapewnia **realizację przeglądów zarządzania bezpieczeństwem** informacji SRP.

Przegląd zarządzania bezpieczeństwem informacji SRP **(Przegląd zarządzania)** ma na celu zapewnienie **stałej przydatności, adekwatności** i **skuteczności** Polityki **Bezpieczeństwa** Informacji w zakresie zapewnienia wysokiego poziomu **bezpieczeństwa** SRP i danych w nim przetwarzanych.

Przegląd zarządzania jest **działaniem zarządczym**, cyklicznym, **polegającym** na zebraniu danych **dotyczących** stanu i poziomu **bezpieczeństwa** informacji i systemu oraz **skuteczności** ustanowionych i **wdrożonych rozwiązań** organizacyjnych i technicznych **bezpieczeństwa**, ocenie na ich podstawie luk, **niezgodności** i potrzeb oraz **podjęciu** decyzji, co do realizacji **niezbędnych działań** dla zapewnienia wysokiego poziomu **bezpieczeństwa** SRP i przetwarzanych w nim danych oraz **ciągłego** doskonalenia PBI.

Przegląd zarządzania bezpieczeństwem informacji SRP realizowany jest przez ministra **właściwego** ds. informatyzacji cyklicznie, w trybie rocznym, w pierwszym kwartale danego roku.

Udział w przeglądzie zarządzania bezpieczeństwem informacji **biorą:**

- **Właściciel SRP** lub jego przedstawiciel

- Minister **właściwy** ds. **wewnętrznych** i administracji lub jego przedstawiciel
- **Gestor SRP**
- Kierownictwo oraz kluczowe osoby funkcyjne komórek istotnych dla **bezpieczeństwa** informacji SRP ministerstwa **właściwego** ds. informatyzacji
- Inspektor Ochrony Danych (IOD) w ministerstwie **właściwym** ds. informatyzacji
- **Pełnomocnik** ds. ochrony cyberprzestrzeni w ministerstwie **właściwym** ds. informatyzacji
- Kierownik jednostki podmiotu **realizującego** zadania na rzecz ministerstwa **właściwego** ds. informatyzacji w zakresie rozwoju i utrzymania SRP
- Kierownictwo oraz kluczowe osoby funkcyjne komórek istotnych dla **bezpieczeństwa** informacji i SRP podmiotu **realizującego** zadania na rzecz ministerstwa **właściwego** ds. informatyzacji

Przegląd zarządzania bezpieczeństwem informacji powinien **uwzględniać** dane **wejściowe,** poddawane analizie i ocenie:

- czynniki **zewnętrzne** i **wewnętrzne** kontekstu funkcjonowania SRP istotne dla jego **bezpieczeństwa** i ich zmiany
- status i stan **działań podjętych** w **następstwie wcześniejszych przeglądów zarządzania bezpieczeństwem**
- **stopień osiągnięcia** ustalonego poziomu **bezpieczeństwa**
- **stopień osiągnięcia** ustalonych celów **bezpieczeństwa**
- **skuteczność** niniejszej Polityki **Bezpieczeństwa** Informacji
- **skuteczność wdrożenia rozwiązań** organizacyjnych i technicznych **bezpieczeństwa** oraz potrzeby ich aktualizacji
- **występowanie, skalę,** zakres **oddziaływania** i skutki incydentów **bezpieczeństwa** i **niezgodności** realizacji **rozwiązań** organizacyjnych i technicznych **bezpieczeństwa**
- **stopień** i poziom **wdrożenia** i realizacji **rozwiązań** organizacyjnych i technicznych **bezpieczeństwa** u wszystkich interesariuszy systemu
- wyniki audytów **bezpieczeństwa** i **stopień** realizacji **zaleceń** autowych
- wyniki szacowania ryzyka i **stopień** realizacji decyzji, co do **postępowania** z ryzykiem
- informacje od interesariuszy
- stan prawny i zmiany **wymagań** prawnych.

Wynikiem **przeglądu zarządzania bezpieczeństwem** informacji **są** decyzje i **działania związane** zapewnieniem wysokiego poziomu **bezpieczeństwa** informacji SRP **odnośnie postanowień** niniejszej PBI, zmiany lub **zwiększenia skuteczności rozwiązań** organizacyjnych i technicznych **bezpieczeństwa,** zapewnienia adekwatnych zasobów osobowych i technicznych oraz decyzje i **działania dotyczące ciągłego** doskonalenia i zmian systemu **zarządzania bezpieczeństwem** informacji ustanowionego **niniejszą Polityką Bezpieczeństwa** Informacji.

Wyniki **przeglądu zarządzania bezpieczeństwem** informacji **są** udokumentowane w postaci Raportu z **przeglądu zarządzania bezpieczeństwem.** Decyzje **podjęte** podczas **przeglądu zarządzania** i **wyartykułowane** w Raporcie z **przeglądu zarządzania bezpieczeństwem mają** charakter **wiążący.**

Raport z **przeglądu zarządzania bezpieczeństwem** informacji podlega nadzorowaniu zgodnie z zasadami ustanowionymi w *Procedurze nadzoru nad dokumentacją bezpieczeństwa SRP*, **stanowiącą załącznik** nr 1.7 do PBI.

Raport z **przeglądu zarządzania bezpieczeństwem** informacji podlega odpowiedniemu zaklasyfikowaniu i ochronie, zgodnie z zasadami **określonymi** w *Polityce klasyfikacji informacji SRP*, **stanowiącej załącznik** nr 2.9 do PBI.

7. Doskonalenie

7.1 Odstępstwa, niezgodności, incydenty i działania korygujące

Zapewnienie **właściwego** nadzorowania i procesowania **odstępstw, niezgodności,** incydentów i **działań korygujących** jest kluczowe dla zapewnienia wysokiego poziomu **bezpieczeństwa** SRP.

Gestor SRP odpowiada za **właściwe** i efektywne nadzorowanie i procesowanie **odstępstw, niezgodności,** incydentów i **działań korygujących.**

Nadzorowanie incydentów

W ramach **obsługi** incydentów procedowane **są** zdarzenia i **działania** niezgodne z postanowieniami niniejszej PBI ZIR, **wpływające** negatywnie na stan **bezpieczeństwa** informacji i SRP.

Działania te realizowane **są** zgodnie z zasadami **określonymi** w punkcie **Zarządzanie** incydentami **związanymi** z **bezpieczeństwem** informacji, **części** II niniejszej PBI Zapewnienie **bezpieczeństwa** oraz ustanowionymi procedurami:

- *Procedura **zgłaszania** incydentów **związanych** z **bezpieczeństwem** informacji SRP,*
- *Procedura reakcji na incydenty **związane** z **bezpieczeństwem** informacji SRP*

stanowiącymi odpowiednio **załączniki** nr 2.28 i 2.27 do niniejszej PBI.

Nadzorowanie odstępstw

Proces nadzorowania **odstępstw** zwiększa **bezpieczeństwo** informacji poprzez zapobieganie wykonywaniu nieuzasadnionych zmian technicznych, czy architektonicznych w SRP oraz zmian sposobu realizacji zadań i procesów rozwoju, eksploatacji lub utrzymania SRP. Zapewnia nadzór nad wszelkimi zaakceptowanymi zmianami, czy modyfikacjami wprowadzanymi, jako **odstępstwa** od ustanowionych zasad i reguł w PBI SRP oraz wprowadza określone **reguły** w zakresie komunikacji oraz odpowiednią ścieżkę akceptacji.

Odstępstwo jest czasowym, jednorazowym **bądź** powtarzalnym, **działaniem** lub **rozwiązaniem** technicznym **dotyczącym** rozwoju, eksploatacji lub utrzymania SRP, które nie jest zgodne z postanowieniami PBI, **zwiększającym podatność** SRP na **materializację zagrożeń** dla **bezpieczeństwa** danych i SRP, a którego realizacja jest uzasadniona interesem **wyższej** wagi i na które **została** wydana zgoda **Właściciela** SRP. **Odstępstwo** jest kontrolowanym **„obejściem"** standardowych, zatwierdzonych **rozwiązań** organizacyjnych lub technicznych **bezpieczeństwa.**

Odstępstwa powinny dopuszczane w sposób przemyślany i ograniczone tylko do odstępstw koniecznych i być ściśle nadzorowane.
Wszelkie odstępstwa i wyjątki od zasad określonych w PBI mogą mieć istotny wpływ na poziom bezpieczeństwa, a jednocześnie mogą pozytywnie wpływać na elastyczność i efektywność zarządzania bezpieczeństwem, dlatego ich stosowanie zostało przewidziane w niniejszej PBI w odniesieniu do procesów, polityk i procedur.
Odstępstwa procedowane i dokumentowane są w systemie ITSM utrzymywanym przez podmiot realizujący zadania na rzecz ministra właściwego ds. informatyzacji w zakresie rozwoju i utrzymania SRP.

Procedowanie odstępstwa odbywa się w sposób spójny i zgodny z *Procedurą zarządzania zmianą SRP*, stanowiącą załącznik 1.5 do PBI.

Nadzorowanie niezgodności

Niezgodność jest działaniem lub rozwiązaniem technicznym w zakresie rozwoju, eksploatacji lub utrzymania SRP, które nie jest zgodne z postanowieniami PBI i zatwierdzonymi rozwiązaniami technicznymi bezpieczeństwa, które zostały wprowadzone bez uzyskania stosownej zgody.

Niezgodności zwiększają podatność SRP na materializację zagrożeń dla bezpieczeństwa danych i SRP, i same stanowią takie zagrożenia, dlatego wymagają objęcia nadzorem.

Proces nadzorowania niezgodności zwiększa bezpieczeństwo informacji poprzez:

- identyfikację niezgodności, ich charakteru, zakresu, sposobu i zasięgu oddziaływania, wywoływanych skutków
- podejmowanie właściwych działań zabezpieczających sytuację, czy stan techniczny, zapobiegających działaniu w niewłaściwy, niezgodny z PBI działaniami lub wykorzystywaniu, stosowaniu niewłaściwych, niezgodnych z PBI rozwiązań technicznych
- usuwanie stanu organizacyjnego i technicznego niezgodnego ze stanem właściwym, określonym w PBI oraz dokumentacją technicznej systemu, skorygowanie niezgodnego zabezpieczenia lub działania do stanu określonego w PBI.
- zapobieganie wykonywaniu nieuzasadnionych zmian technicznych, czy architektonicznych w SRP oraz zmian sposobu realizacji zadań i procesów rozwoju, eksploatacji lub utrzymania SRP.
- monitorowanie i zarządzanie następstwami niezgodności
- poinformowanie właściwej komórki ds. bezpieczeństwa w jednostkach interesariuszy, stosownie do posiadanego zakresu uprawnień i kompetencji

Wymienione wyżej działania realizowane są przez odpowiednie role w strukturach interesariuszy SRP.

Role zaangażowane w obsługę odstępstw i niezgodności na poziomie **Właściciela SRP** to **Gestor SRP**, kierownictwo i zespoły komórek organizacyjnych odpowiedzialnych za rozwój, eksploatację i utrzymanie SRP, IOD, ABSI, PBC. **Gestor SRP** jest odpowiedzialny za nadzorowanie niezgodności i decydowanie, co do sposobu jej rozwiązania.

Role zaangażowane w obsługę odstępstw i niezgodności w ministerstwie właściwym ds. wewnętrznych to kierownictwo i zespoły komórek organizacyjnych odpowiedzialnych za rozwój, eksploatację i utrzymanie lokalizacji centrów przetwarzania i infrastruktury teleinformatycznej SRP, kierownictwo

i zespoły komórki bezpieczeństwa, IOD, PBC. Rola odpowiedzialna za nadzorowanie niezgodności pozostaje upoważniona przez **Gestora SRP.**

Role zaangażowane w obsługę odstępstw i niezgodności w podmiocie realizującym zadania na rzecz ministra właściwego ds. informatyzacji to kierownictwo i zespoły komórek organizacyjnych odpowiedzialnych za rozwój, eksploatację i utrzymanie SRP, kierownictwo i zespoły komórki bezpieczeństwa, IOD), PBC. . Rola odpowiedzialna za nadzorowanie niezgodności pozostaje upoważniona przez **Gestora SRP.**

Niezgodności procedowane i dokumentowane są w systemie ITSM utrzymywanym przez podmiot realizujący zadania na rzecz ministra właściwego ds. informatyzacji w zakresie rozwoju i utrzymania SRP.

Nadzorowanie działań korygujących

Działania korygujące to działania mające na celu niedopuszczenie do powtórnego wystąpienia zaistniałych odstępstw, niezgodności i incydentów.
Działania korygujące zwiększają odporność i zmniejszają podatności SRP na materializację zagrożeń dla bezpieczeństwa danych i SRP, i stanowią działania przeciwdziałające zagrożeniom. Działania korygujące wymagają objęcia nadzorem.
Działania korygujące realizowane są na poziomie właściciela SRP – ministra właściwego ds. informatyzacji. **Gestor SRP** odpowiedzialny jest za skuteczne prowadzenie działań korygujących.

W ramach działań korygujących realizowany jest proces:

- oceny zaistniałych odstępstw, niezgodności i incydentów,
- identyfikacji ich przyczyn,
- wdrożenia działań eliminujących te przyczyny, tak aby odstępstwa, niezgodności, czy incydenty nie występowały ponownie.

Wymienione wyżej działania realizowane są przez odpowiednie role w strukturach interesariuszy SRP.
Role zaangażowane w obsługę działań korygujących na poziomie właściciela SRP – ministra właściwego ds. informatyzacji to **Gestor SRP,** kierownictwo i zespoły komórek organizacyjnych odpowiedzialnych za rozwój, eksploatację i utrzymanie SRP, IOD, ABSI, PBC. **Gestor SRP** jest odpowiedzialny za nadzorowanie działań korygujących i decydowanie, co do charakteru podejmowanych działań.

Role zaangażowane w obsługę działań korygujących w ministerstwie właściwym ds. wewnętrznych to kierownictwo i zespoły komórek organizacyjnych odpowiedzialnych za rozwój, eksploatację i utrzymanie lokalizacji centrów przetwarzania i infrastruktury teleinformatycznej SRP, kierownictwo i zespoły komórki bezpieczeństwa, IOD, PBC. Rola odpowiedzialna za nadzorowanie niezgodności pozostaje upoważniona przez **Gestora SRP.**

Role zaangażowane w obsługę działań korygujących w podmiocie realizującym zadania na rzecz ministra właściwego ds. informatyzacji to kierownictwo i zespoły komórek organizacyjnych odpowiedzialnych za rozwój, eksploatację i utrzymanie SRP, kierownictwo i zespoły komórki bezpieczeństwa, IOD, PBC. Rola odpowiedzialna za nadzorowanie niezgodności pozostaje upoważniona przez **Gestora SRP.**

Działania korygujące procedowane i dokumentowane są w systemie ITSM utrzymywanym przez podmiot realizujący zadania na rzecz ministra właściwego ds. informatyzacji w zakresie rozwoju i utrzymania SRP.

Procesy **obsługi odstępstw, niezgodności** i **działań korygujących** realizowane **są** zgodnie z ***Procedurą*** *nadzorowania* ***odstępstw, niezgodności*** *i* ***działań korygujących*** *SRP*, **stanowiącą załącznik** nr 1.8 do niniejszej PBI.

Wszelkie informacje **dotyczące odstępstw, niezgodności,** incydentów **bezpieczeństwa** i **działań korygujących podlegają** udokumentowaniu odpowiednio w Rejestrze **odstępstw,** Rejestrze **niezgodności,** Rejestrze incydentów, Rejestrze **działań korygujących** (w formie papierowej i/lub elektronicznej) i nadzorowaniu zgodnie z zasadami ustanowionymi w *Procedurze nadzoru nad* ***dokumentacją bezpieczeństwa*** *SRP*, **stanowiącej załącznik** nr 1.7 do PBI.

Informacje **dotyczące częstości,** zakresu, skutków i przyczyn **odstępstw i niezgodności** oraz **podjętych działań korygujących** i ich **skuteczności podlegają** okresowej komunikacji do Gestora SRP, zgodne z wytycznymi *Procedury komunikacji w zakresie* ***bezpieczeństwa*** *SRP*, **stanowiącej załącznik** nr 1.6 do PBI, w tym przynajmniej raz w roku w ramach realizowanego **przeglądu zarządzania bezpieczeństwem** informacji, o którym mowa w punkcie 6.3 PBI **powyżej.**

Informacje w/w **podlegają** odpowiedniemu zaklasyfikowaniu i ochronie, zgodnie z zasadami **określonymi** w Polityce klasyfikacji informacji, **stanowiącej załącznik** nr 2.9 do PBI.

7.2 Ciągłe doskonalenie

Polityka **Bezpieczeństwa** Informacji i ustanowione jej postanowieniami **rozwiązania** organizacyjne i techniczne **bezpieczeństwa podlegają ciągłemu** doskonaleniu w odniesieniu do jej **przydatności, adekwatności i skuteczności** w **osiąganiu** i zapewnianiu wysokiego poziomu **bezpieczeństwa.**

Ciągłe doskonalenie prowadzi **się** w odniesieniu do ustanowionego celu zapewnienia wysokiego poziomu **bezpieczeństwa** i celów **szczegółowych** z cyklicznym zastosowaniem procesów **zarządzania** ryzykiem, **wdrażania rozwiązań,** monitorowania, pomiaru, analizy i oceny, audytu **wewnętrznego, przeglądu zarządzania i działań korygujących** zgodnie z zasadami opisanymi **powyżej** w **treści** niniejszej PBI.

Inicjatywy **doskonalące** postanowienia niniejszej PBI oraz **funkcjonujące rozwiązania** organizacyjne i techniczne **wdrażane są** w trybie **zarządzania zmianą.**

Cz. II Zapewnienie bezpieczeństwa – Zabezpieczenia

Lp.	Wymaganie ISO 27001	Implementacja w Systemie	Dokument szczegółowy
A.5. Polityki Bezpieczeństwa			
A.5.1 Kierunki bezpieczeństwa informacji określane przez kierownictwo			
1	(A5.1.1) Polityki bezpieczeństwa informacji.	Dokument główny Polityki Bezpieczeństwa Informacji Systemu Rejestrów Państwowych (PBI SRP), polityki niższego poziomu oraz wymagane procedury i instrukcje dotyczące bezpieczeństwa informacji w systemie zwane razem politykami bezpieczeństwa informacji, a także ich aktualizacje zatwierdza minister właściwy do spraw informatyzacji lub wyznaczona przez niego osoba, a następnie dokumenty udostępniane są w całości lub części uprawnionym pracownikom, interesariuszom, a także gdy jest to wymagane osobom/podmiotom świadczącym usługi w systemie. Za udostępnianie treści dokumentów oraz sporządzanie wyciągów odpowiedzialny jest właściciel biznesowy systemu, który może przekazać zadania z tym związane innej osobie. W załączniku do niniejszego dokumentu ujęty jest „Wykaz osób/stanowisk odpowiedzialnych za opracowanie, przegląd, ocenę i udostępnianie polityk bezpieczeństwa informacji w systemie".	Załącznik nr 2.1 ***Wykaz osób/stanowisk odpowiedzialnych za opracowanie, przegląd, ocenę i udostępnianie polityk bezpieczeństwa informacji w systemie SRP.***

2	(A5.1.2) Przegląd polityk bezpieczeństwa informacji.	Polityki poddawane są regularnym przeglądom nie rzadziej niż raz do roku oraz zawsze, gdy wystąpią istotne zmiany w obszarach ich oddziaływania, przy czym przegląd ten powinien obejmować: ocenę możliwości udoskonalenia polityk w systemie oraz podejścia do zarządzania bezpieczeństwem informacji z uwzględnieniem zmian prawnych, organizacyjnych, technicznych oraz warunków biznesowych. Za proces ten odpowiedzialny jest jednoznacznie przypisany właściciel o zatwierdzonej odpowiedzialności. W załączniku do niniejszego dokumentu ujęty jest *Wykaz osób/stanowisk odpowiedzialnych za opracowanie, przegląd i ocenę polityk bezpieczeństwa informacji w systemie.*	Załącznik nr 2.1 ***Wykaz osób/stanowisk odpowiedzialnych za opracowanie, przegląd, ocenę i udostępnianie polityk bezpieczeństwa informacji w systemie SRP.***
A.6. Organizacja bezpieczeństwa informacji			
A.6.1 Organizacja wewnętrzna			
3	(A6.1.1) Role i odpowiedzialność za bezpieczeństwo informacji.	Za bezpieczeństwo informacji, ochronę poszczególnych aktywów i realizację określonych procesów bezpieczeństwa informacji odpowiadają wyznaczone formalnie osoby. Osoby te mogą przekazywać zadania związane z bezpieczeństwem, jednak pozostają za nie odpowiedzialne. W załączniku do niniejszego dokumentu znajduje się *Wykaz osób/stanowisk odpowiedzialnych za ochronę poszczególnych aktywów i realizację określonych procesów bezpieczeństwa informacji oraz obowiązków w zakresie zarządzania*	Załącznik nr 2.2 ***Wykaz aktywów systemu i określonych procesów bezpieczeństwa informacji oraz osób/stanowisk odpowiedzialnych za ich ochronę i realizację obowiązków w zakresie zarządzania ryzykiem SRP.***

		ryzykiem.	
4	(A6.1.2) Rozdzielanie obowiązków.	Gdy jest to możliwe, obowiązki i odpowiedzialności osób odpowiedzialnych za bezpieczeństwo informacji pozostające w konflikcie są rozdzielane w celu zredukowania ryzyka niewłaściwego (umyślnego lub nieumyślnego) użycia aktywów. Oznacza to, że w ramach tego samego procesu w systemie pojedyncza osoba nie powinna realizować ról wzajemnie od siebie zależnych, np. w procesie nadawania uprawnień osoba wnioskująca o dostęp nie może być jednocześnie osobą decydującą o nadaniu uprawnień. W tym celu w systemie zapewniona jest rozliczalność działań związanych z dostępem do aktywów, ich modyfikacji i korzystania. Do redukcji ryzyka niewłaściwego użycia aktywów w systemie wykorzystywane są również dodatkowe zabezpieczenia w postaci: • monitorowania aktywności, • analizy logów, • nadzoru kierownictwa.	Załącznik nr 1.3 ***Wykaz ról i odpowiedzialności SRP.***
5	(A6.1.3) Kontakty z organami władzy.	W zakresie bezpieczeństwa informacji są utrzymywane kontakty z organami władzy, a także organami regulacyjnymi i normalizacyjnymi. Kontakty takie określa m.in. *Procedura reakcji na incydenty związane z bezpieczeństwem informacji SRP.*	Załącznik nr 2.27 ***Procedura reakcji na incydenty związane z bezpieczeństwem informacji SRP***
6	(A6.1.4) Kontakty z grupami	Osoby odpowiedzialne za bezpieczeństwo informacji w systemie utrzymują kontakty z uznanymi specjalistami w	Załącznik nr 2.3 ***Polityka bezpieczeństwa zasobów ludzkich SRP***

	zainteresowanych specjalistów.	tym obszarze, jak również specjalistycznymi forami oraz stowarzyszeniami zawodowymi w celu bieżącego uzupełniania wiedzy, wymiany informacji o nowych technologiach, produktach, zagrożeniach i podatnościach. Gdy jest to możliwe proces ten jest realizowany poprzez udział w szkoleniach, konferencjach, warsztatach oraz innych formach edukacji. Zdobyta wiedza powinna być udokumentowana i wykorzystywana do poszerzania wiedzy innych osób realizujących zadania w systemie. Nadzór nad tym procesem sprawuje osoba odpowiedzialna za realizację programu szkoleniowego w systemie wyznaczona przez gestora systemu.	
7	(A6.1.5) Bezpieczeństwo informacji w zarządzaniu projektami.	Bezpieczeństwo informacji jest uwzględniane w ramach zarządzania wszystkimi projektami realizowanymi w systemie. W szczególności: • cele bezpieczeństwa informacji są włączane do celów projektów, • bezpieczeństwo informacji jest częścią wszystkich etapów stosowanej metodyki projektu, • dobór zabezpieczeń jest oparty o szacowanie ryzyka zrealizowane już na wstępnym etapie projektu. W celu realizacji zabezpieczenia w proces zarządzania projektem włączony jest zawsze przedstawiciel komórki bezpieczeństwa.	Załącznik nr 2.4 ***Polityka bezpieczeństwa prac rozwojowych SRP***

A.6.2 Urządzenia mobilne i telepraca			
8	(A6.2.1) Polityka stosowania urządzeń mobilnych.	W zakresie użytkowania mobilnych urządzeń w systemie są wprowadzone niezbędne zabezpieczenia oraz polityka ich stosowania – *Polityka użytkowania urządzeń mobilnych w SRP.*	Załącznik nr 2.5 ***Polityka użytkowania urządzeń mobilnych w SRP***
9	(A6.2.2) Telepraca	W zakresie przetwarzania informacji w ramach telepracy oraz pracy zdalnej, są wprowadzone niezbędne zabezpieczenia oraz polityka postępowania – *Polityka przetwarzania informacji w ramach pracy zdalnej w SRP.*	Załącznik nr 2.6 ***Polityka przetwarzania informacji w ramach pracy zdalnej w SRP***
A.7. Bezpieczeństwo osobowe			
A.7.1 Przed zatrudnieniem			
10	(A7.1.1) Postępowanie sprawdzające.	W ramach postępowania sprawdzającego kandydaci do pracy są weryfikowani w systemie we wszystkich wymaganych na danym stanowisku aspektach, w oparciu o obowiązujące przepisy prawa oraz regulacje i zasady przyjęte w ministerstwie właściwym do spraw informatyzacji lub instytucjach interesariuszy – w zależności od miejsca wykonywania pracy i funkcji pełnionej w systemie. W dokumencie *Polityka Bezpieczeństwa informacji przetwarzanych na stacjach roboczych Systemu Rejestrów Państwowych* zawarte są wytyczne dotyczące bezpieczeństwa osobowego	Załącznik nr 2.3 ***Polityka bezpieczeństwa zasobów ludzkich SRP*** Załącznik nr 2.16 ***Polityka bezpieczeństwa informacji przetwarzanych na stacjach roboczych Systemu Rejestrów Państwowych SRP***

		w odniesieniu do interesariuszy zewnętrznych systemu, którzy przetwarzają w nim informacje. Zabezpieczenie powinno być stosowane również w odniesieniu do osób/podmiotów świadczących usługi w systemie (weryfikacja kontrahentów, potwierdzenie referencji).	
11	(A7.1.2) Warunki zatrudnienia.	W umowach o pracę oraz umowach z osobami/podmiotami świadczącymi usługi w systemie jest uwzględniana odpowiedzialność stron w obszarze bezpieczeństwa informacji, w szczególności kandydaci są informowani o rolach i odpowiedzialnościach. Wymogiem jest: • podpisywanie porozumień o zachowaniu poufności i nieujawnianiu informacji przed uzyskaniem dostępu do informacji i środków przetwarzania informacji, • zobowiązanie do stosowania przepisów dotyczących ochrony danych identyfikujących osobę oraz ochrony praw autorskich, • komunikowanie odpowiedzialności w zakresie przetwarzania informacji powierzonych przez podmioty zewnętrzne, • komunikowanie odpowiedzialności z tytułu naruszenia wymagań bezpieczeństwa w systemie, w tym o konsekwencjach nie przestrzegania postanowień zbioru polityk bezpieczeństwa informacji.	Załącznik nr 2.3 ***Polityka bezpieczeństwa zasobów ludzkich SRP*** Załącznik nr 2.16 ***Polityka bezpieczeństwa informacji przetwarzanych na stacjach roboczych Systemu Rejestrów Państwowych SRP***

A.7.2 Podczas zatrudnienia			
12	(A7.2.1) Odpowiedzialność kierownictwa.	Kierownictwo odpowiedzialne za funkcjonowanie systemu wymaga od pracowników, interesariuszy oraz osób/podmiotów świadczących usługi w systemie stosowania zasad bezpieczeństwa informacji zgodnie z obowiązującymi politykami, procedurami i instrukcjami. W tym celu realizowany jest program uświadamiający, a pracownicy, interesariusze i osoby/podmioty świadczące usługi w systemie potwierdzają zapoznanie się z obowiązującymi przepisami i zasadami oraz zobowiązują się do ich stosowania.	Załącznik nr 2.7 ***Oświadczenie o zapoznaniu się i zobowiązaniu do stosowania zasad bezpieczeństwa SRP*** Załącznik nr 2.3 ***Polityka bezpieczeństwa zasobów ludzkich SRP***
13	(A7.2.2) Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji.	Każdy pracownik ministerstwa właściwego do spraw informatyzacji realizujący zadania w systemie, interesariusze oraz w uzasadnionych sytuacjach osoby/podmioty świadczące usługi w systemie otrzymują aktualizacje polityk, procedur i instrukcji odnoszących się do ich stanowiska pracy oraz uczestniczą w organizowanych szkoleniach z zakresu bezpieczeństwa informacji. W tym zakresie obowiązuje zatwierdzony program działania.	Załącznik nr 2.3 ***Polityka bezpieczeństwa zasobów ludzkich SRP***
14	(A7.2.3) Postępowanie dyscyplinarne.	Postępowania dyscyplinarne w stosunku do pracowników, którzy naruszyli polityki oraz procedury i instrukcje z zakresu bezpieczeństwa informacji w systemie, są prowadzone w oparciu o aktualne przepisy prawa i tylko wtedy, gdy pracownicy zostali z nimi	Załącznik nr 2.3 ***Polityka bezpieczeństwa zasobów ludzkich SRP.***

		zapoznani.	
A.7.3 Zakończenie i zmiana zatrudnienia			
15	(A7.3.1) Zakończenie zatrudnienia lub zmiana zakresu obowiązków.	W warunkach zatrudnienia pracowników oraz osób/podmiotów świadczących usługi w systemie są określone odpowiedzialności i obowiązki w zakresie bezpieczeństwa informacji, które pozostają w mocy po ustaniu stosunku pracy lub właściwej umowy.	Załącznik nr 2.3 ***Polityka bezpieczeństwa zasobów ludzkich SRP***
A.8. Zarządzanie aktywami			
16	(A8.1.1) Inwentaryzacja aktywów.	Aktywa Systemu związane z bezpieczeństwem informacji oraz środkami przetwarzania informacji są zidentyfikowane oraz jest sporządzona i na bieżąco aktualizowana ich ewidencja. Ewidencja jest prowadzona i aktualizowana przez właścicieli aktywów wg wzoru stanowiącego załącznik do niniejszego dokumentu - *Wykaz aktywów systemu i określonych procesów bezpieczeństwa informacji oraz osób/stanowisk odpowiedzialnych za ich ochronę i realizację obowiązków w zakresie zarządzania ryzykiem.*	Załącznik nr 2.2 ***Wykaz aktywów systemu i określonych procesów bezpieczeństwa informacji oraz osób/stanowisk odpowiedzialnych za ich ochronę i realizację obowiązków w zakresie zarządzania ryzykiem SRP***
17	(A8.1.2) Własność aktywów.	Ewidencjonowane aktywa systemu mają jednoznacznie przypisanego właściciela odpowiedzialnego za ich prawidłowe zarządzanie w całym cyklu życia, m.in.	Załącznik nr 2.2 ***Wykaz aktywów systemu i określonych procesów bezpieczeństwa informacji oraz osób/stanowisk odpowiedzialnych za ich ochronę i realizację***

		• inwentaryzację, • klasyfikację i ochronę, • okresowy przegląd uprawnień dostępu zgodnie z polityką kontroli dostępu, • nadzór nad usuwaniem i niszczeniem. Wykaz właścicieli aktywów oraz grup aktywów składających się na usługi systemu jest prowadzony i na bieżąco aktualizowany przez wyznaczoną przez Gestora systemu osobę wg wzoru stanowiącego załącznik do powyższego dokumentu *Wykaz aktywów systemu i określonych procesów bezpieczeństwa informacji oraz osób/stanowisk odpowiedzialnych za ich ochronę i realizację obowiązków w zakresie zarządzania ryzykiem.*	***obowiązków w zakresie zarządzania ryzykiem SRP***
18	(A8.1.3) Akceptowalne użycie aktywów.	W systemie obowiązuje zasada akceptowalnego użycia informacji oraz aktywów i środków związanych z przetwarzaniem informacji, tzn. każda osoba/podmiot realizująca zadania w systemie ponosi odpowiedzialność za wykorzystanie zasobów przetwarzania informacji w ramach swojego zakresu odpowiedzialności.	Załącznik nr 2.8 ***Polityka akceptowalnego użycia aktywów SRP***
19	(A8.1.4) Zwrot aktywów	Pracownicy, interesariusze oraz osoby/podmioty świadczące usługi w systemie w momencie zakończenia zatrudnienia lub okresu obowiązywania umowy zwracają wszystkie posiadane i udostępnione im aktywa systemu. W tym zakresie obowiązuje formalny proces, na który składa się zwrot wydanych wcześniej fizycznych i elektronicznych aktywów systemu oraz przekazanie i udokumentowanie wiedzy, którą dysponują	Załącznik nr 2.8 ***Polityka akceptowalnego użycia aktywów SRP***

		osoby/podmioty kończące zatrudnienie.	
A.8.2 Klasyfikacja informacji			
20	(A8.2.1) Klasyfikowanie informacji.	Informacje w Systemie są klasyfikowane przez właścicieli zasobów informacyjnych z uwzględnieniem wymagań prawnych i biznesowych. W tym zakresie obowiązują jednolite zasady dla całego systemu. Jako podstawowy obowiązuje schemat klasyfikacji informacji uwzględniony w dokumencie *Polityka klasyfikacja informacji.*	Załącznik nr 2.9 ***Polityka klasyfikacji Informacji SRP***
21	(A8.2.2) Oznaczanie informacji.	W systemie funkcjonują zasady dotyczące oznaczania informacji, które uwzględniają dowolną postać informacji oraz przyjęty schemat klasyfikacji ujęte w dokumencie *Polityka klasyfikacji Informacji.*	Załącznik nr 2.9 ***Polityka klasyfikacji Informacji SRP***
22	(A8.2.3) Postępowanie z aktywami.	W systemie obowiązują następujące zasady dotyczące przetwarzania informacji: • Dostęp do informacji prawnie chronionych systemu (dane osobowe, dane dotyczące prywatności) jest ograniczony jedynie do osób/podmiotów uprawnionych na podstawie: o przepisów prawa (m.in. interesariusze systemu, organy władzy) i jest udzielany w oparciu o obowiązujące wnioski i formularze, o zawartych umów dotyczących eksploatacji i utrzymania systemu.	Załącznik nr 2.9 ***Polityka klasyfikacji Informacji SRP***

		• Dostęp do informacji chronionych systemu, których ujawnienie powoduje lub może spowodować negatywny wpływ na bezpieczeństwo systemu i zawartych w nim informacji ograniczony jest jedynie do osób/podmiotów uprawnionych na podstawie:
		  ○ zgody wydanej przez kierownika jednostki organizacyjnej, właściciela systemu lub właściciela zasobu należącego do systemu,
		  ○ przepisów prawa (organy władzy, organy kontrolne),
		  ○ zawartych umów dotyczących eksploatacji, utrzymania i rozwoju systemu.
		• Informacje chronione są przekazywane uprawnionym osobom/podmiotom o potwierdzonej tożsamości z zastosowaniem:
		  ○ transmisji danych (dla użytkowników posiadających dostęp do systemu teleinformatycznego SRP),
		  ○ zabezpieczonych nośników danych (szyfrowane),
		  ○ listem poleconym (za pośrednictwem dedykowanych punktów udostępniania danych),
		  ○ innych metod określonych w przepisach prawa lub umowach dotyczących eksploatacji i utrzymania systemu.	

		• Osoby/podmioty, którym udostępnione są informacje chronione zobowiązane są do podpisania stosownego oświadczenia o zachowaniu poufności.	
A.8.3 Postępowanie z nośnikami			
23	(A8.3.1) Zarządzanie nośnikami wymiennymi.	W SRP obowiązują następujące zasady dotyczące zarządzania nośnikami służącymi do przetwarzania informacji chronionych: • jako nośniki informacji w systemie należy traktować nośniki elektroniczne, magnetyczne, optyczne oraz papierowe, • nośniki należy chronić przed: o zniszczeniem lub fizycznym uszkodzeniem na skutek oddziaływania czynników mechanicznych, wysokiej temperatury, wody, substancji żrących, promieniowania elektromagnetycznego, kurzu oraz innych czynników, które mogą uniemożliwić odczytanie zawartych na nich informacji, o kradzieżą, o celowym lub przypadkowym usunięciem informacji, • nośniki, które były wykorzystywane w systemie mogą być ponownie użyte poza systemem, pod warunkiem usunięcia z nich informacji chronionych w sposób uniemożliwiający ich odtworzenie,	Załącznik nr 2.10 ***Polityka postępowania z nośnikami SRP***

		• w SRP dla nośników stosowane są techniki kryptograficzne zawsze, gdy wymagana jest poufność lub integralność, • jeśli istnieje obawa pogorszenia jakości nośnika na którym przechowywane są istotne dane systemu – dane przenoszone są na nowy nośnik zanim dojdzie do ich utraty, • istotne dane systemu przechowywane są na wielokrotnych kopiach nośników oraz w różnych lokalizacjach fizycznych, • nośniki wymienne w systemie powinny być rejestrowane, a kopiowanie na nie informacji powinno być monitorowane.	
24	(A8.3.3) Przekazywanie nośników.	Nośniki są chronione przed nieuprawnionym dostępem oraz przed utratą integralności podczas transportu.	Załącznik nr 2.10 ***Polityka postępowania z nośnikami SRP***
25	(A8.3.2) Wycofywanie nośników.	W Systemie obowiązują zasady dotyczące wycofania niewykorzystywanych nośników oraz trwałego usuwania danych na nich zawartych.	Załącznik nr 2.10 ***Polityka postępowania z nośnikami SRP***

A.9. Kontrola dostępu			
A.9.1 Wymagania biznesowe wobec kontroli dostępu			
26	(A9.1.1) Polityka kontroli dostępu.	W systemie obowiązuje *Polityka kontroli dostępu* zgodna z wymaganiami biznesowymi oraz wymaganiami bezpieczeństwa informacji.	Załącznik nr 2.11 ***Polityka kontroli dostępu SRP***
27	(A9.1.2) Dostęp do sieci i usług sieciowych.	Użytkownicy systemu mają dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali uprawnienia. W tym zakresie obowiązują zasady opisane w dokumencie *Polityka kontroli dostępu*.	Załącznik nr 2.11 ***Polityka kontroli dostępu SRP***
A.9.2 Zarządzanie dostępem użytkowników			
28	(A9.2.1) Rejestrowanie i wyrejestrowywanie użytkowników.	W systemie funkcjonuje formalny proces rejestrowania i wyrejestrowywania użytkowników w celu przydzielania praw dostępu.	Załącznik nr 2.11 ***Polityka kontroli dostępu SRP***
29	(A9.2.2) Przydzielanie dostępu użytkownikom.	W systemie funkcjonuje formalny proces przydzielania dostępu użytkownikom w celu nadawania lub odbierania praw dostępu. Dotyczy to wszystkich kategorii użytkowników oraz wszystkich usług.	Załącznik nr 2.11 ***Polityka kontroli dostępu SRP***
30	(A9.2.3) Zarządzanie prawami	W ograniczonym zakresie i w warunkach umożliwiających właściwy nadzór przewiduje się	Załącznik nr 2.11 ***Polityka kontroli dostępu SRP***

	uprzywilejowanego dostępu.	przydzielanie praw uprzywilejowanego dostępu.	
31	(A9.2.4) Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników.	Przydzielanie informacji uwierzytelniających podlega procesowi zarządzania.	Załącznik nr 2.11 ***Polityka kontroli dostępu SRP***
32	(A9.2.5) Przegląd praw dostępu użytkowników.	Właściciele aktywów są zobowiązani do regularnego przeglądania praw dostępu użytkowników, nie rzadziej niż raz na kwartał oraz zawsze kiedy nastąpią zmiany w systemie.	Załącznik nr 2.11 ***Polityka kontroli dostępu SRP***
33	(A9.2.6) Odbieranie lub dostosowywanie praw dostępu.	Prawa dostępu pracowników oraz osób/podmiotów świadczących usługi w systemie po zakończeniu zatrudnienia lub obowiązywania właściwej umowy są odbierane lub dostosowywane do zaistniałych zmian.	Załącznik nr 2.11 ***Polityka kontroli dostępu SRP***
A.9.3 Odpowiedzialność użytkowników			
34	(A9.3.1) Stosowanie poufnych informacji uwierzytelniających.	Użytkownicy mają obowiązek przestrzegania przyjętych w systemie zasad stosowania informacji uwierzytelniających. Obowiązuje bezwzględny zakaz omijania zabezpieczeń oraz udostępniania innym osobom przydzielonych informacji uwierzytelniających.	Załącznik nr 2.11 ***Polityka kontroli dostępu SRP***

A.9.4 Kontrola dostępu do systemów i aplikacji			
35	(A9.4.1) Ograniczanie dostępu do informacji.	Dostęp do informacji oraz funkcji systemu i aplikacji jest ograniczony zgodnie z *Polityką kontroli dostępu*.	Załącznik nr 2.11 ***Polityka kontroli dostępu SRP***
36	(A9.4.2) Procedury bezpiecznego logowania.	Obowiązuje procedura bezpiecznego logowania, tam gdzie *Polityka kontroli dostępu* tego wymaga.	Załącznik nr 2.11 ***Polityka kontroli dostępu SRP***
37	(A9.4.3) System zarządzania hasłami.	Systemy zarządzania hasłami powinny zapewniać wybór haseł o wymaganej jakości.	Załącznik nr 2.11 ***Polityka kontroli dostępu***
38	(A9.4.4) Użycie uprzywilejowanych programów narzędziowych.	Omijanie zabezpieczeń systemów i aplikacji w oparciu o specjalistyczne programy narzędziowe podlega ścisłemu nadzorowi i ograniczeniom. W tym zakresie obowiązuje *Procedura stosowania specjalistycznych programów narzędziowych w systemie*.	Załącznik nr 2.12 ***Procedura stosowania specjalistycznych programów narzędziowych w systemie SRP***
39	(A9.4.5) Kontrola dostępu do kodów źródłowych programów.	Dostęp do kodu źródłowego programów jest ograniczony.	Załącznik nr 2.11 ***Polityka kontroli dostępu SRP***

A.10. Kryptografia			
A.10.1 Zabezpieczenia kryptograficzne			
40	(A10.1.1) Polityka stosowania zabezpieczeń kryptograficznych.	W systemie funkcjonują zasady dotyczące ochrony informacji przy wykorzystaniu zabezpieczeń kryptograficznych.	Załącznik nr 2.13 ***Polityka zabezpieczeń kryptograficznych SRP***
41	(A10.1.2) Zarządzanie kluczami.	W systemie funkcjonują zasady dotyczące ochrony i okresów ważności kluczy kryptograficznych.	Załącznik nr 2.13 ***Polityka zabezpieczeń kryptograficznych SRP***
A.11. Bezpieczeństwo fizyczne i środowiskowe			
A.11.1 Obszary bezpieczne			
42	(A11.1.1) Fizyczna granica obszaru bezpiecznego.	Obszary zawierające chronione informacje oraz środki przetwarzania informacji dla części centralnej systemu umieszcza się w strefach bezpieczeństwa.	Załącznik nr 2.14 ***Polityka ochrony fizycznej i środowiskowej SRP***
43	(A11.1.2) Fizyczna granica obszaru bezpiecznego.	Dostęp do stref bezpieczeństwa centralnej części systemu jest chroniony i zabezpieczony przed nieuprawnionym dostępem poprzez stosowanie: środków ochrony budowlano-mechanicznych, elektronicznych oraz czynnej ochrony fizycznej (służba	Załącznik nr 2.14 ***Polityka ochrony fizycznej i środowiskowej SRP***

		ochrony obiektu).	
44	(A11.1.3) Zabezpieczenie biur, pomieszczeń i obiektów.	Obiekty i pomieszczenia systemu objęte są fizycznymi zabezpieczeniami uwzględniającymi ograniczenie dostępu publicznego, ograniczenie do minimum informacji dotyczących przeznaczenia obiektów, pomieszczeń systemu i przetwarzanych w nim informacji, a także zastosowanie zabezpieczeń przed podglądem i podsłuchem informacji.	Załącznik nr 2.14 ***Polityka ochrony fizycznej i środowiskowej SRP***
45	(A11.1.4) Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi.	W systemie stosuje się zabezpieczenia uwzględniające ochronę przed zagrożeniami zewnętrznymi i środowiskowymi, w tym, przed katastrofami naturalnymi, wypadkami i wrogim atakiem.	Załącznik nr 2.14 ***Polityka ochrony fizycznej i środowiskowej SRP***
46	(A11.1.5) Praca w obszarach bezpiecznych.	Praca w strefach bezpieczeństwa wykonywana jest w oparciu o dokument *Polityka ochrony fizycznej i środowiskowej.*	Załącznik nr 2.14 ***Polityka ochrony fizycznej i środowiskowej SRP***
47	(A11.1.6) Obszary dostaw i załadunku.	Nad punktami dostępu do systemu takimi jak drzwi wejściowe do obiektów/pomieszczeń, obszary dostaw i załadunku, sprawuje się nadzór.	Załącznik nr 2.14 ***Polityka ochrony fizycznej i środowiskowej SRP***
A.11.2 Sprzęt			
48	(A11.2.1) Lokalizacja i ochrona	Rozmieszczenie sprzętu systemu jest zaplanowane w taki sposób, aby możliwa była jego ochrona przed nieuprawnionym dostępem oraz wpływem zagrożeń	Załącznik nr 2.14 ***Polityka ochrony fizycznej i środowiskowej SRP***

	sprzętu.	środowiskowych.	
49	(A11.2.2) Systemy wspomagające.	Sprzęt jest chroniony przed skutkami awarii systemów wspomagających (np. podsystemu zasilania gwarantowanego, podsystemu kontroli warunków środowiskowych).	Załącznik nr 2.14 ***Polityka ochrony fizycznej i środowiskowej SRP***
50	(A11.2.3) Bezpieczeństwo okablowania.	Okablowanie zasilające oraz teleinformatyczne, przenoszące dane lub wspomagające usługi informacyjne jest chronione przed przechwyceniem, zakłóceniem lub uszkodzeniem.	Załącznik nr 2.14 ***Polityka ochrony fizycznej i środowiskowej SRP***
51	(A11.2.4) Konserwacja sprzętu.	Sprzęt jest prawidłowo i na bieżąco konserwowany z uwzględnieniem wymagań producentów w oparciu o zasoby własne oraz niezbędne umowy serwisowe.	Załącznik nr 2.14 ***Polityka ochrony fizycznej i środowiskowej SRP***
52	(A11.2.5) Wynoszenie aktywów.	Informacje, programy oraz sprzęt mogą być wynoszone poza siedzibę systemu tylko po spełnieniu wymagań w zakresie bezpieczeństwa informacji i uzyskaniu właściwej zgody.	Załącznik nr 2.14 ***Polityka ochrony fizycznej i środowiskowej SRP***
53	(A11.2.6) Bezpieczeństwo sprzętu i aktywów poza siedzibą.	Aktywa wynoszone poza siedzibę systemu muszą być zabezpieczone przed wystąpieniem zagrożeń związanych z pracą poza siedzibą.	Załącznik nr 2.14 ***Polityka ochrony fizycznej i środowiskowej SRP***
54	(A11.2.7)	Przed zbyciem lub przekazaniem sprzętu do ponownego	Załącznik nr 2.10 **Polityka postępowania z**

	Bezpieczne zbywanie lub przekazywanie do ponownego użycia.	użycia nośniki danych sprawdzane są pod kątem prawidłowego usunięcia lub nadpisania chronionych danych oraz licencjonowanych programów.	**nośnikami SRP** Załącznik nr 2.16 ***Polityka bezpieczeństwa informacji przetwarzanych na stacjach roboczych Systemu Rejestrów Państwowych SRP***
55	(A11.2.8) Pozostawianie sprzętu użytkownika bez opieki.	Użytkownicy są zobowiązani do zapewnienia ochrony sprzętu systemu pozostawionego bez opieki. Szczegółowe zalecenia w tym zakresie uwzględnione są w kolejnym zabezpieczeniu *Polityka czystego biurka i czystego ekranu* (A11.2.9) w niniejszym opracowaniu oraz dokumencie *Polityka ochrony fizycznej i środowiskowej*. Zalecenia dla części lokalnej systemu uwzględnione są w dokumencie *Polityka bezpieczeństwa informacji przetwarzanych na stacjach roboczych Systemu Rejestrów Państwowych* stanowiącym załącznik do PBI SRP.	Załącznik nr 2.14 ***Polityka ochrony fizycznej i środowiskowej SRP*** Załącznik nr 2.16 ***Polityka bezpieczeństwa informacji przetwarzanych na stacjach roboczych Systemu Rejestrów Państwowych SRP***
56	(A11.2.9) Polityka czystego biurka i czystego ekranu.	W miejscach przetwarzania danych SRP wprowadza się politykę czystego biurka dla dokumentów papierowych i przenośnych nośników danych oraz politykę czystego ekranu dla środków przetwarzania informacji, zgodnie z którą: • nieużywane chronione informacje powinny być przechowywane w sejfie, zamykanej szafie lub zamykanej szufladzie, • stanowisko pracy, powinno być tak zaplanowane, aby nikt postronny nie mógł podglądać chronionych informacji niezależnie	Załącznik nr 2.14 ***Polityka ochrony fizycznej i środowiskowej SRP*** Załącznik nr 2.16 ***Polityka bezpieczeństwa informacji przetwarzanych na stacjach roboczych Systemu Rejestrów Państwowych SRP***

		od ich formy, • należy zamknąć drzwi na klucz lub w inny sposób blokować dostęp przy każdym nawet krótkotrwałym opuszczeniu pomieszczenia, w którym są przetwarzane informacje zawarte w SRP lub dotyczące systemu. Należy chować do zamykanej szafy lub szuflady wszelkie istotne dokumenty i nośniki danych (płyty, taśmy, dyski przenośne, karty mikroprocesorowe, PIN kody itp.). Jeśli opuszczane są pomieszczenia typu open space, dodatkowo powinny być aktywowane dostępne zabezpieczenia mechaniczne, np. linka typu Kensington, • przed odejściem od komputera zawsze powinny być zamykane sesje lub blokowane ekran i klawiatura (np. przy użyciu hasła, tokenu, innego mechanizmu uwierzytelniania użytkownika). Jeśli są dostępne, należy używać też innych zabezpieczeń, w tym mechanicznych, np. linki typu Kensington, • korzystanie z kopiarek, sieciowych urządzeń wielofunkcyjnych i innych urządzeń kopiujących w systemie powinno odbywać się tylko po autoryzacji, • wydruki i kopiowane dokumenty dotyczące SRP lub przetwarzanych w nim informacji – nie powinny być pozostawiane nawet na chwilę bez opieki, aby nikt postronny nie mógł się z nimi zapoznać,	

		• po zakończeniu lub w przerwie spotkania, szkolenia dotyczącego SRP w miejscu spotkania należy zabezpieczyć komputer, usunąć wszystkie informacje z tablic ścieralnych, zniszczyć lub zabezpieczyć notatki papierowe i na flipchartach, tak aby nikt postronny nie mógł się z nimi zapoznać, • wszystkie dokumenty, nośniki danych, karty mikroprocesorowe wraz z PIN kodami, istotne z punktu widzenia bezpieczeństwa informacji po zakończeniu pracy powinny być zamykane w zabezpieczonych i w miarę możliwości ognioodpornych szafach. To w razie kradzieży, katastrofy naturalnej lub wrogiego ataku zabezpieczy je przed dostaniem się w niepowołane ręce, uszkodzeniem lub zniszczeniem, • po zakończeniu pracy powinny być zamykane wszystkie aktywne sesje oraz powinno następować wylogowanie się z serwerów lub aktywacja oprogramowania, które blokuje klawiaturę i ekran, • istotne aktywa systemu (w tym informacje) powinny być zabezpieczone również w sytuacjach kryzysowych i w stanach podwyższonych poziomów gotowości do działania, o ile pozwalają na to okoliczności.	

A.12 Bezpieczna eksploatacja			
A.12.1 Procedury eksploatacyjne i odpowiedzialność			
57	(A12.1.1) Dokumentowanie procedur eksploatacyjnych.	Procedury eksploatacyjne są udokumentowane i udostępniane zespołom utrzymaniowym funkcjonującym w ramach struktur technicznych ministerstwa właściwego ds. informatyzacji oraz podmiotu realizującego zadania z zakresu eksploatacji i utrzymania systemu na rzecz ministerstwa właściwego ds. informatyzacji jak również innym uprawnionym użytkownikom jeśli jest to wymagane do realizacji zadań w systemie.	Załącznik nr 2.15 ***Ewidencja procedur eksploatacyjnych SRP***
58	(A12.1.2) Zarządzanie zmianami.	Zmiany w procesach biznesowych, środkach przetwarzania informacji i systemach, które mają wpływ na bezpieczeństwo informacji są nadzorowane.	***Polityka Bezpieczeństwa Informacji*, cz.1.**
59	(A12.1.3) Zarządzanie pojemnością.	Wykorzystanie zasobów jest monitorowane i przewiduje się dostosowywanie ich wielkości, dla zapewniania właściwej wydajności systemu.	Załącznik nr 2.15 ***Ewidencja procedur eksploatacyjnych*** dotyczy zarządzania zasobami.
60	(A12.1.4) Oddzielanie środowisk rozwojowych, testowych i produkcyjnych.	Środowiska rozwojowe, testowe i produkcyjne są rozdzielone w celu redukcji ryzyk związanych z nieuprawnionym dostępem lub ze zmianami w środowisku produkcyjnym.	Załącznik nr 2.4 ***Polityka bezpieczeństwa prac rozwojowych***

A.12.2 Ochrona przed szkodliwym oprogramowaniem			
61	(A12.2.1) Zabezpieczenia przed szkodliwym oprogramowaniem.	Wdraża się zabezpieczenia wykrywające, zapobiegające i odtwarzające, które w połączeniu z właściwym uświadomieniem użytkowników służą ochronie przed szkodliwym działaniem.	Załącznik nr 2.16 ***Polityka bezpieczeństwa informacji przetwarzanych na stacjach roboczych Systemu Rejestrów Państwowych***
A.12.3 Kopie zapasowe			
62	(A12.3.1) Zapasowe kopie informacji.	Zapasowe kopie informacji, oprogramowania i obrazów systemów są regularnie wykonywane i testowane, zgodnie z ustaloną polityką kopii zapasowych.	Załącznik nr 2.17 ***Polityka kopii zapasowych w SRP***
A.12.4 Rejestrowanie zdarzeń i monitorowanie			
63	(A12.4.1) Rejestrowanie zdarzeń.	Tworzy się, przechowuje i systematycznie przegląda dzienniki zdarzeń rejestrujące działania użytkowników, usterki oraz zdarzenia związane z bezpieczeństwem informacji.	Załącznik nr 2.15 ***Ewidencja procedur eksploatacyjnych*** dotyczy monitorowania zdarzeń
64	(A12.4.2) Ochrona informacji w dziennikach zdarzeń.	Środki służące rejestrowaniu zdarzeń oraz informacji w dziennikach zdarzeń są chronione przed manipulacją i nieuprawnionym dostępem.	Załącznik nr 2.15 ***Ewidencja procedur eksploatacyjnych*** dotyczy monitorowania zdarzeń.
65	(A12.4.3) Rejestrowanie działań administratorów i operatorów.	Działania administratorów i operatorów systemów są rejestrowane, a dzienniki chronione i systematycznie przeglądane.	Załącznik nr 2.15 ***Ewidencja procedur eksploatacyjnych*** dotyczy monitorowania zdarzeń.

66	(A12.4.4) Synchronizacja zegarów.	Zegary wszystkich istotnych komponentów systemu są zsynchronizowane z jednym wzorcowym źródłem czasu.	Załącznik nr 2.15 ***Ewidencja procedur eksploatacyjnych*** dotyczy monitorowania zdarzeń.
A.12.5 Nadzór nad oprogramowaniem produkcyjnym			
67	(A12.5.1) Instalacja oprogramowania w systemach produkcyjnych.	Wdraża się procedury nadzoru nad instalacją oprogramowania w systemach produkcyjnych.	Załącznik nr 2.19 ***Procedura nadzoru nad instalacją oprogramowania w systemach produkcyjnych***
A.12.6 Zarządzanie podatnościami technicznymi			
68	(A12.6.1) Zarządzanie podatnościami technicznymi.	Informacje o podatnościach technicznych wykorzystywanych systemów i oprogramowania są niezwłocznie pozyskiwane oraz oceniany jest stopień narażenia na te podatności i podejmowane są środki w celu przeciwdziałania związanemu z nimi ryzyku.	Załącznik nr 2.15 ***Ewidencja procedur eksploatacyjnych*** dotyczy monitorowania zdarzeń.
69	(A12.6.2) Ograniczenia w instalowaniu oprogramowania.	Ustanawia się i wdraża zasady instalowania oprogramowania w systemie.	Załącznik nr 2.19 ***Procedura nadzoru nad instalacją oprogramowania w systemach produkcyjnych SRP*** Załącznik nr 2.16 ***Polityka bezpieczeństwa informacji przetwarzanych na stacjach roboczych Systemu Rejestrów Państwowych SRP***

A.12.7 Rozważania dotyczące audytu systemów informacyjnych			
70	(A12.7.1) Zabezpieczenia audytu systemów informacyjnych.	Wymagania audytu oraz działania obejmujące weryfikację systemów produkcyjnych są starannie zaplanowane i uzgadniane, w celu zminimalizowania zakłóceń w procesach biznesowych.	***Polityka Bezpieczeństwa Informacji SRP* cz. 1**
A.13. Bezpieczeństwo komunikacji			
A.13.1 Zarządzanie bezpieczeństwem sieci			
71	(A13.1.1) Zabezpieczenia sieci.	W celu ochrony informacji w systemach i aplikacjach, sieci są zarządzane oraz nadzorowane.	Załącznik nr 2.20 ***Polityka korzystania z sieci i usług sieciowych systemu SRP***
72	(A13.1.2) Bezpieczeństwo usług sieciowych.	Umowy dotyczące usług sieciowych, świadczonych wewnętrznie lub zlecanych na zewnątrz, zawierają zidentyfikowane mechanizmy zabezpieczeń, poziomy świadczenia usług i wymagania dotyczące zarządzania.	Załącznik nr 2.20 ***Polityka korzystania z sieci i usług sieciowych systemu SRP***
73	(A13.1.3) Rozdzielanie sieci.	Grupy usług informacyjnych, użytkowników i systemów informacyjnych są rozdzielone w strukturze sieci.	Załącznik nr 2.20 ***Polityka korzystania z sieci i usług sieciowych systemu SRP***
A.13.2 Przesyłanie informacji			
74	(A13.2.1) Polityki i procedury przesyłania informacji.	W systemie wdrożona jest formalna *Polityka przesyłania informacji* uwzględniająca zabezpieczenia w celu ochrony wymiany informacji przesyłanych przy użyciu wszystkich rodzajów środków łączności.	Załącznik nr 2.21 ***Polityka przesyłania informacji SRP***

75	(A13.2.2) Porozumienia dotyczące przesyłania informacji.	Bezpieczne przesyłanie informacji biznesowych dotyczących systemu z podmiotami zewnętrznymi uwzględniane jest we właściwych porozumieniach. Obowiązują w tym zakresie jednolite standardy w resorcie właściwym do spraw informatyzacji.	Załącznik nr 2.21 ***Polityka przesyłania informacji SRP***
76	(A13.2.3) Wiadomości elektroniczne.	Informacje przekazywane w formie wiadomości elektronicznych są zabezpieczane.	Załącznik nr 2.21 ***Polityka przesyłania informacji SRP***
77	(A13.2.4) Umowy o zachowaniu poufności.	Wymagania odnoszące się do umów o zachowaniu poufności są regularnie przeglądane w sposób odzwierciedlający potrzeby w zakresie ochrony informacji. Za proces ten jest odpowiedzialna osoba wyznaczona przez Gestora systemu.	
A.14. Pozyskiwanie, rozwój i utrzymanie systemów			
A.14.1 Wymagania związane z bezpieczeństwem systemów informacyjnych			
78	(A14.1.1) Analiza i specyfikacja wymagań bezpieczeństwa informacji.	Wymagania dotyczące bezpieczeństwa informacji są włączane do wymagań stawianych nowym i rozbudowywanym systemom informacyjnym.	
79	(A14.1.2) Zabezpieczanie usług aplikacyjnych w sieciach publicznych.	Informacje przesyłane w sieciach publicznych, związane z usługami świadczonymi przez aplikacje są zabezpieczane.	Załącznik nr 2.23 ***Zasady projektowania bezpiecznych systemów SRP***

80	(A14.1.3) Ochrona transakcji usług aplikacyjnych.	Informacje związane z transakcjami dokonywanymi w ramach usług świadczonych przez aplikacje są zabezpieczane.	Załącznik nr 2.*23* ***Zasady projektowania bezpiecznych systemów SRP***
A.14.2 Bezpieczeństwo w procesach rozwoju i wsparcia			
81	(A14.2.1) Polityka bezpieczeństwa prac rozwojowych.	Ustanawia się i stosuje zasady pracy nad rozwojem oprogramowania i systemów. W tym zakresie obowiązuje *Polityka bezpieczeństwa prac rozwojowych*.	Załącznik nr 2.4 ***Polityka bezpieczeństwa prac rozwojowych SRP***
82	(A14.2.2) Procedury kontroli zmian w systemach.	Nadzoruje się zmiany w systemach podczas ich cyklu życia, przy użyciu *Procedury kontroli zmian* oraz w oparciu o właściwe środki techniczne.	Załącznik nr 2.24 ***Procedura kontroli zmian oprogramowania SRP***
83	(A14.2.3) Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej.	Po dokonaniu zmian w platformach produkcyjnych przeprowadza się przegląd krytycznych aplikacji biznesowych oraz testuje się je pod kątem funkcjonalności i bezpieczeństwa.	Załącznik nr 2.24 ***Procedura kontroli zmian oprogramowania SRP***
84	(A14.2.4) Ograniczenia dotyczące zmian w pakietach oprogramowania.	Modyfikacje oprogramowania ograniczane są do zmian uzasadnionych i niezbędnych, a wszystkie zmiany są ściśle nadzorowane.	Załącznik nr 2.24 ***Procedura kontroli zmian oprogramowania SRP***

85	(A14.2.5) Zasady projektowania bezpiecznych systemów.	Ustanawia się i stosuje *Zasady projektowania bezpiecznych systemów.*	Załącznik nr 2.23 ***Zasady projektowania bezpiecznych systemów SRP***
86	(A14.2.6) Bezpieczne środowisko rozwojowe.	W systemie są tworzone i odpowiednio chronione bezpieczne środowiska przeznaczone do rozwoju oraz prac integracyjnych obejmujących całość cyklu rozwojowego.	Załącznik nr 2.4 ***Polityka bezpieczeństwa prac rozwojowych SRP***
87	(A14.2.7) Prace rozwojowe zlecane podmiotom zewnętrznym.	Prace rozwojowe dotyczące systemu zlecane podmiotom zewnętrznym są nadzorowane i monitorowane.	Załącznik nr 2.25 ***Polityka bezpieczeństwa informacji w relacjach z dostawcami SRP***
88	(A14.2.8) Testowanie bezpieczeństwa systemów.	Funkcje bezpieczeństwa testowane są w czasie prac rozwojowych.	Załącznik nr 2.26 ***Wytyczne dotyczące prowadzenia testów oprogramowania SRP***
89	(A14.2.9) Testy akceptacyjne systemów.	Dla nowych i modernizowanych komponentów systemu ustanawiane są programy testów akceptacyjnych.	Załącznik nr 2.26 ***Wytyczne dotyczące prowadzenia testów oprogramowania***
A.14.3 Dane testowe			
90	(A14.3.1) Ochrona danych	Dane testowe są starannie wybierane, a w przypadku wykorzystywania danych rzeczywistych chronione i	Załącznik nr 2.26 ***Wytyczne dotyczące prowadzenia testów oprogramowania SRP***

	testowych.	nadzorowane.	
A.15. Relacje z dostawcami			
A.15.1 Bezpieczeństwo informacji w relacjach z dostawcami			
91	(A15.1.1) Polityka bezpieczeństwa informacji w relacjach z dostawcami.	Wymagania w zakresie bezpieczeństwa informacji są uzgadniane z dostawcą i dokumentowane. W tym zakresie obowiązuje *Polityka bezpieczeństwa informacji w relacjach z dostawcami.*	Załącznik nr 2.25 ***Polityka bezpieczeństwa informacji w relacjach z dostawcami SRP***
92	(A15.1.2) Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami.	Wymagania bezpieczeństwa informacji są indywidualnie uzgadniane w porozumieniach z dostawcami, którzy uzyskują dostęp do systemu, przetwarzają, przechowują, przesyłają informacje lub dostarczają elementy infrastruktury służące do jej przetwarzania.	Załącznik nr 2.25 ***Polityka bezpieczeństwa informacji w relacjach z dostawcami SRP***
93	(A15.1.3) Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych.	Porozumienia z dostawcami uwzględniają wymagania odnoszące się do ryzyk w bezpieczeństwie informacji związanych z usługami technologii informacyjnych i telekomunikacyjnych oraz łańcuchem dostaw produktów.	Załącznik nr 2.25 ***Polityka bezpieczeństwa informacji w relacjach z dostawcami SRP***
A.15.2 Zarządzanie usługami świadczonymi przez dostawców			
94	(A15.2.1) Monitorowanie i	Dostarczane usługi zewnętrzne są regularnie	Załącznik nr 2.25 ***Polityka bezpieczeństwa***

	przegląd usług świadczonych przez dostawców.	monitorowane, przeglądane i audytowane.	***informacji w relacjach z dostawcami SRP***
95	(A15.2.2) Zarządzenie zmianami w usługach świadczonych przez dostawców.	W systemie realizowane jest zarządzanie zmianami w zakresie usług dostarczanych przez dostawców.	Załącznik nr 2.25 ***Polityka bezpieczeństwa informacji w relacjach z dostawcami SRP***
A.16. Zarządzanie incydentami związanymi z bezpieczeństwem informacji			
A.16.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami			
96	(A16.1.1) Odpowiedzialność i procedury	Ustanawia się odpowiedzialność oraz procedurę zapewniające szybką, skuteczną i zorganizowaną reakcję na incydenty związane z bezpieczeństwem informacji.	Załącznik nr 2.27 ***Procedura reakcji na incydenty związane z bezpieczeństwem informacji SRP***
97	(A16.1.2) Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji.	Zdarzenia związane z bezpieczeństwem informacji zgłaszane są tak szybko, jak tylko to jest możliwe.	Załącznik nr 2.28 ***Procedura zgłaszania incydentów związanych z bezpieczeństwem informacji SRP***
98	(A16.1.3) Zgłaszanie słabości związanych z bezpieczeństwem informacji.	Pracownicy oraz osoby/podmioty realizujące zadania w systemie są zobowiązani do odnotowywania i zgłaszania wszelkich zaobserwowanych lub podejrzewanych słabości związanych z bezpieczeństwem informacji w komponentach	Załącznik nr 2.28 ***Procedura zgłaszania incydentów związanych z bezpieczeństwem informacji SRP***

		systemu lub usługach.	
99	(A16.1.4) Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji.	Zdarzenia związane z bezpieczeństwem informacji są analizowane i w uzasadnionych przypadkach kwalifikowane, jako incydenty związane z bezpieczeństwem informacji.	Załącznik nr 2.27 ***Procedura reakcji na incydenty związane z bezpieczeństwem informacji SRP***
100	(A16.1.5) Reagowanie na incydenty związane z bezpieczeństwem informacji.	Obowiązuje *Procedura reakcji na incydenty związane z bezpieczeństwem informacji SRP.*	Załącznik nr 2.27 ***Procedura reakcji na incydenty związane z bezpieczeństwem informacji SRP***
101	(A16.1.6) Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji.	Analizy incydentów związanych z bezpieczeństwem informacji są wykorzystywane do zminimalizowania prawdopodobieństwa wystąpienia przyszłych incydentów i ograniczenia ich skutków.	Załącznik nr 2.27 ***Procedura reakcji na incydenty związane z bezpieczeństwem informacji SRP***
102	(A16.1.7) Gromadzenie materiału dowodowego.	W systemie stosuje się *Procedurę przetwarzania informacji, które mogą stanowić materiał dowodowy* uwzględniającą identyfikację, gromadzenie, pozyskiwanie i utrwalanie informacji.	Załącznik nr 2.29 ***Procedurę przetwarzania informacji, które mogą stanowić materiał dowodowy SRP***

A.17. Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania			
A.17.1 Ciągłość bezpieczeństwa informacji			
103	(A17.1.1) Planowanie ciągłości bezpieczeństwa informacji.	W systemie określone są wymagania dotyczące bezpieczeństwa informacji i ciągłości zarządzania tym bezpieczeństwem w sytuacjach kryzysowych lub podczas katastrof i wrogich ataków.	Załącznik nr 2.18 ***Wymagania dotyczące zarządzania ciągłością działania SRP***
104	(A17.1.2) Wdrożenie ciągłości bezpieczeństwa informacji.	W systemie są wdrożone i utrzymywane procesy, procedury i zabezpieczenia dla utrzymywania wymaganego poziomu ciągłości bezpieczeństwa informacji w niekorzystnych sytuacjach.	Załącznik nr 2.18 ***Wymagania dotyczące zarządzania ciągłością działania SRP***
105	(A17.1.3) Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji.	Wdrożone zabezpieczenia ciągłości bezpieczeństwa informacji są regularnie weryfikowane.	Załącznik nr 2.18 ***Wymagania dotyczące zarządzania ciągłością działania SRP***
A.17.2 Nadmiarowość			
106	(A17.2.1) Dostępność środków przetwarzania informacji.	W celu spełnienia wymagań w zakresie dostępności środki przetwarzania informacji są wdrażane z nadmiarem, zarówno na poziomie technicznym jak i organizacyjnym.	***Polityka Bezpieczeństwa Informacji* cz.1**

A.18. Zgodność z wymaganiami			
A.18.1 Zgodność z wymaganiami prawnymi i umownymi			
107	(A18.1.1) Określenie stosownych wymagań prawnych i umownych.	W systemie dokumentowane i aktualizowane są wszystkie istotne wymagania prawne, regulacyjne, umowne oraz weryfikowane jest na bieżąco podejście do ich przestrzegania.	***Polityka Bezpieczeństwa Informacji* cz.1**
108	(A18.1.2) Prawa własności intelektualnej.	W zakresie praw własności intelektualnej i użytkowania prawnie zastrzeżonego oprogramowania wdraża się *Procedurę ochrony prawnie zastrzeżonego oprogramowania*.	***Polityka Bezpieczeństwa Informacji* cz.1**
109	(A18.1.3) Ochrona zapisów.	Informacje w postaci zapisów istotnych dla systemu są chronione przed utratą, zniszczeniem, zafałszowaniem, nieuprawnionym dostępem i nieuprawnionym opublikowaniem zgodnie z wymaganiami prawnymi, regulacyjnymi, umownymi oraz biznesowymi.	***Polityka Bezpieczeństwa Informacji* cz.1**
110	(A18.1.4) Prywatność i ochrona danych identyfikujących osobę.	Zapewnia się prywatność i ochronę danych identyfikujących osobę stosownie do odpowiednich przepisów prawa i regulacji.	***Polityka Bezpieczeństwa Informacji* cz.1**
111	(A18.1.5) Regulacje dotyczące zabezpieczeń kryptograficznych.	Zabezpieczenia kryptograficzne są stosowane zgodnie z odpowiednimi umowami, przepisami i regulacjami.	Załącznik nr 2.13 ***Polityka zabezpieczeń kryptograficznych***

A.18.2 Przeglądy bezpieczeństwa informacji			
112	(A18.2.1) Niezależny przegląd bezpieczeństwa informacji.	Podejście do zarządzania bezpieczeństwem informacji w systemie oraz jego wdrożenie są poddawane niezależnemu przeglądowi w zaplanowanych odstępach czasu lub wtedy, gdy następują istotne zmiany.	***Polityka Bezpieczeństwa Informacji* cz.1**
113	(A18.2.2) Zgodność z politykami bezpieczeństwa i standardami.	Kierownicy regularnie dokonują przeglądów zgodności przetwarzania informacji i procedur z odpowiednimi politykami bezpieczeństwa, standardami i innymi wymaganiami dotyczącymi bezpieczeństwa, w zakresie przydzielonej im odpowiedzialności.	***Polityka Bezpieczeństwa Informacji* cz.1**
114	(A18.2.3) Sprawdzanie zgodności technicznej.	System jest regularnie przeglądany celem sprawdzenia jego zgodności z polityką bezpieczeństwa informacji i standardami obowiązującymi w ministerstwie właściwym do spraw informatyzacji.	***Polityka Bezpieczeństwa Informacji* cz.1**

WÓJT
Sławomir Ambroziak