NSC NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	Narodowy Standard Cyberbezpieczeństwa		
Nazwa standardu	Symbol	Wersja	Data wydania
Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego	**NSC 800-60 Część II**	1.0	01/09/2021

Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego

Część II

PEŁNOMOCNIK RZĄDU DS. CYBERBEZPIECZEŃSTWA

Warszawa 2021

Szanowni Państwo,

Departament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów udostępnia do wykorzystania w Państwa działalności zestaw publikacji specjalnych. Stanowią one rekomendację w postaci Narodowych Standardów Cyberbezpieczeństwa, o których mowa w kierunku interwencji 6.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, *Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń*. Mimo, że prezentowane standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST), to posiadają one mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, stosowane w zarządzaniu bezpieczeństwem informacji przez podmioty krajowego systemu cyberbezpieczeństwa, w tym podmioty realizujące zadania publiczne, operatorów usług kluczowych i dostawców usług cyfrowych.

Zaprezentowane publikacje stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę, jaka w tym zakresie stosowana jest w administracji federalnej USA.

Na prezentowany zestaw publikacji składają się następujące pozycje:[1]

- NSC[2] 199, *Standardy kategoryzacji bezpieczeństwa* – na podstawie FIPS 199;
- NSC 200, *Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych* – na podstawie FIPS 200;
- NSC 500-92, *Architektura referencyjna chmury obliczeniowej – rekomendacje* – na podstawie NIST SP 500-292;
- NSC 800-18, *Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych* – na podstawie NIST SP 800- 18;

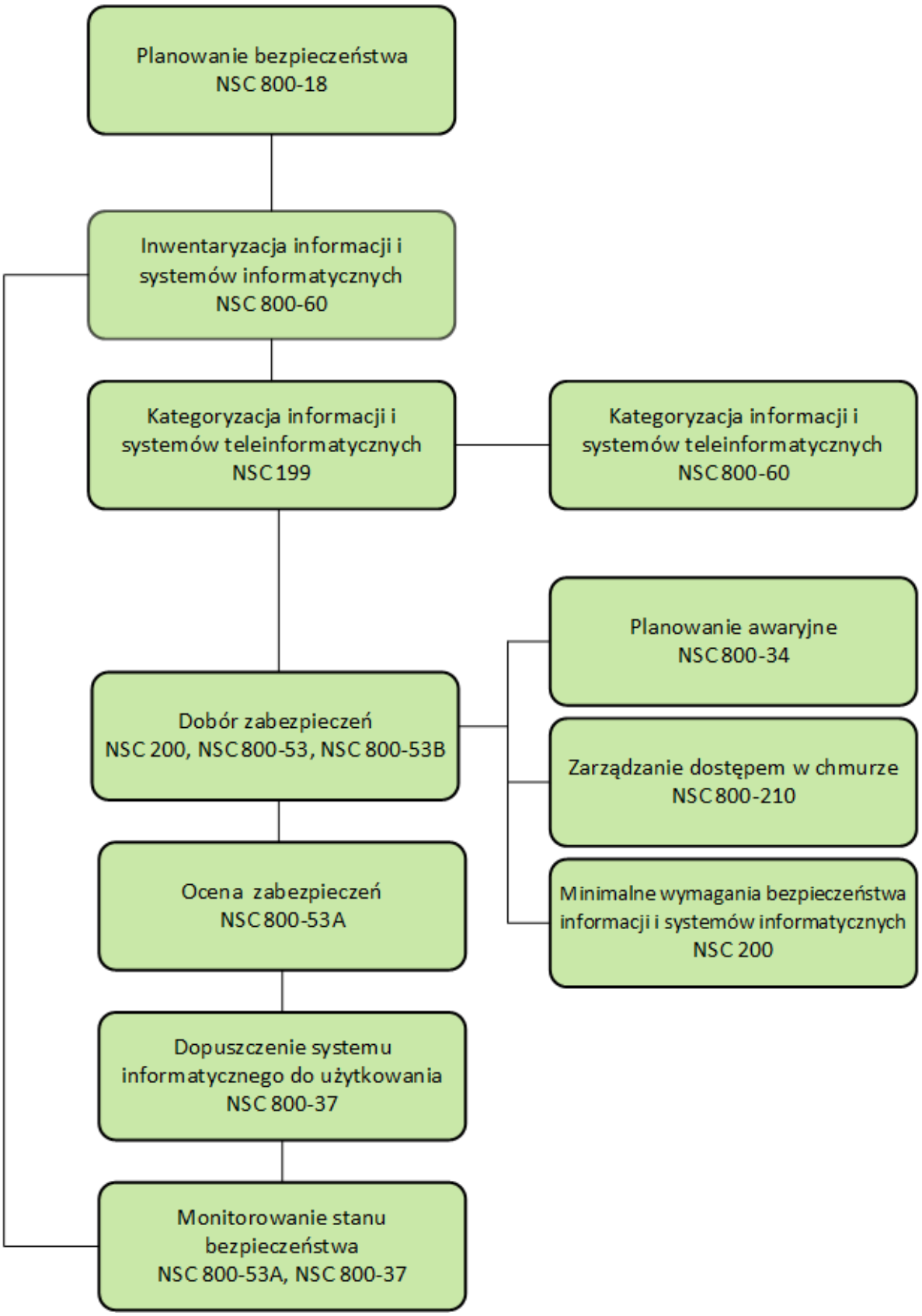
[1] Wymienione są podstawowe dokumenty. Każdy z nich może się odwoływać w rozdziale *Referencje* do szeregu powiązanych publikacji, które składają się na całościowy proces osiągania cyberbezpieczeństwa.

[2] NSC – Narodowy Standard Cyberbezpieczeństwa.

- NSC 800-30, *Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne* – na podstawie NIST SP 800-30;
- NSC 800-34, *Poradnik planowania awaryjnego* – na podstawie NIST SP 800-34;
- NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu* – na podstawie NIST SP 800-37;
- NSC 800-53, *Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53;
- NSC 800-53A, *Ocena środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji. Tworzenie skutecznych planów oceny* – na podstawie NIST SP 800-53A;
- NSC 800-53B, *Zabezpieczenia bazowe systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53B;
- NSC 800-60, *Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego* – na podstawie NIST SP 800-60;
- NSC 800-61, *Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego* – na podstawie NIST SP 800-61;
- NSC 800-210, *Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej* – na podstawie NIST SP 800-210.

Korzystając z tych publikacji można stosunkowo łatwo zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę.

Cykl zarządzania bezpieczeństwem bazujący na publikacjach NIST wykorzystuje następujące dokumenty:


Planowanie bezpieczeństwa
NSC 800-18
Inwentaryzacja informacji i systemów informatycznych
NSC 800-60
Kategoryzacja informacji i systemów teleinformatycznych
NSC 199
Kategoryzacja informacji i systemów teleinformatycznych
NSC 800-60
Planowanie awaryjne
NSC 800-34
Dobór zabezpieczeń
NSC 200, NSC 800-53, NSC 800-53B
Zarządzanie dostępem w chmurze
NSC 800-210
Ocena zabezpieczeń
NSC 800-53A
Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych
NSC 200
Dopuszczenie systemu informatycznego do użytkowania
NSC 800-37
Monitorowanie stanu bezpieczeństwa
NSC 800-53A, NSC 800-37

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował wiele standardów i wytycznych w celu zapewnienia wspólnego podejścia do problematyki bezpieczeństwa informacji i systemów teleinformatycznych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji, bezpieczeństwa systemów teleinformatycznych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością operacji organizacyjnych i majątku, osób fizycznych, innych organizacji i Państwa. Zarządzanie ryzykiem stanowi podstawę do wdrożenia stosownych zabezpieczeń w systemach informacyjnych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych, a także dzięki jednolitemu podejściu, ułatwia wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznymi i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi które zostały opracowane przez inne organizacje (np. ISO), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania tych innych standardów.

Publikacje NIST, co do zasady, nie są objęte restrykcjami wynikającymi z autorskich praw majątkowych. Są powszechnie dostępne oraz dozwolone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejście do zagadnień związanych z bezpieczeństwem informacji, systemów teleinformatycznych oraz ochrony prywatności, przez co ułatwiają podmiotom opracowanie i eksploatację systemu zarządzania tym bezpieczeństwem.

Biorąc pod uwagę wszystkie powyższe aspekty, autorzy niniejszej publikacji polecają opracowania NIST jako godne zaufania i rekomendują stosowanie ich przez polskie podmioty w opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania.

Podmioty, urządzenia lub materiały prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Identyfikacja taka nie ma na celu nakłaniania do nich lub ich poparcia, nie ma też na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w tym obszarze.

W niniejszym Narodowym Standardzie Cyberbezpieczeństwa (NSC) mogą znajdować się odniesienia do innych publikacji opracowywanych obecnie przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa zgodnie z przypisanymi mu obowiązkami ustawowymi. Informacje zawarte w tej publikacji, w tym koncepcje, praktyki i metodologie, mogą być wykorzystywane przez organizacje jeszcze przed ukończeniem innych towarzyszących temu standardowi publikacji. W związku z tym, do czasu ukończenia każdej publikacji, obowiązują aktualne wymagania, wytyczne i procedury, jeśli takie istnieją. W celach planistycznych i wprowadzania zmian, organizacje będą mogły uważnie śledzić rozwój tych nowych publikacji opracowywanych przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

Niniejsza publikacja, ***Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-60 vol. 2, Rev. 1.

Tam, gdzie to było możliwe i nie budziło kontrowersji, nazwy ról i kluczowych uczestników procesu zarządzania ryzykiem zostały podane w języku polskim. Pozostałe role i funkcje zostały przedstawione w języku angielskim. Do wszystkich tych ról / funkcji zastosowano akronimy terminologii angielskiej.

Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie NSC 7298, ***Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.***

SPIS TREŚCI

PODSUMOWANIE ZARZĄDCZE

Niniejsze wytyczne służą zapewnieniu odpowiedniego poziomu bezpieczeństwa informacji w systemach informatycznych podmiotów publicznych zgodnie z oszacowanym poziomem ryzyka.

Wytyczne mają na celu ułatwienie przypisania odpowiedniego poziomu bezpieczeństwa informacji zgodnie z poziomami wpływu zakłóceń / incydentów, które mogą wynikać z nieuprawnionego ujawnienia, modyfikacji lub wykorzystania systemu informatycznego lub informacji. Wytyczne te zakładają, że użytkownik zapoznał się ze standardami kategoryzacji bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych przedstawionymi w publikacji NSC[3] 199.

W celu dokonania kategoryzacji systemów informatycznych i informacji przetwarzanych w tych systemach, należy:

- Zapoznać się z terminami i definicjami kategoryzacji bezpieczeństwa zawartymi w NSC 199;
- Ustanowić proces kategoryzacji bezpieczeństwa;
- Do identyfikacji rodzajów informacji i systemów informacyjnych wykorzystać kategorie zawarte w niniejszej publikacji lub w miarę potrzeb dodać nowe, unikając jednak nadmiernemu rozdrobnieniu rodzajów informacji;
- Korzystając z niniejszej publikacji wyznaczyć **wstępne** poziomy wpływu zakłócenia / incydentu dla typowych rodzajów informacji przetwarzanych w poszczególnych działach administracji. Jest to **wstępna kategoryzacja**, która po przeprowadzeniu szacowania ryzyka, jeśli zachodzi taka potrzeba, **może podlegać modyfikacjom**;
- Dla konkretnego systemu teleinformatycznego rozpatrzeć poszczególne atrybuty bezpieczeństwa informacji, które mogą skutkować odchyleniami od wstępnego przypisania poziomu wpływu zakłócenia / incydentu na te atrybuty;
- Ustanowić sumaryczną kategorię systemu informatycznego, która będzie później wykorzystywana do ustanawiania zabezpieczeń zgodnie z publikacją NSC 800-53.

[3] NSC - Narodowy Standard Cyberbezpieczeństwa

Niniejszy dokument ma służyć jako źródło informacji, a nie obligatoryjne wymaganie i nie wszystkie zawarte w nim materiały będą odpowiednie dla wszystkich podmiotów organizacyjnych. Dokument ten obejmuje dwa tomy: Część I - Podstawowe wytyczne i Część II - Załączniki. Użytkownicy powinni zapoznać się z wytycznymi zawartymi w Części I, a następnie odwołać się tylko do tego konkretnego materiału z Części II (załączników), który dotyczy ich własnych systemów i aplikacji. Wstępne przypisania poziomu wpływu zakłócenia / incydentu podano w Części II, załącznik A i B.

ZAŁĄCZNIK A: POZIOMY WPŁYWU INCYDENTU NA INFORMACJE I SYSTEMY INFORMATYCZNE W ZAKRESIE FUNKCJI ZARZĄDZANIA I WSPARCIA

Wiele informacji i wiele systemów w organizacjach nie jest wykorzystywanych bezpośrednio do świadczenia usług dla obywateli, ale przede wszystkim do świadczenia usług administracyjnych lub biznesowych, które wspierają realizację zadań, do których powołany został dany podmiot. W Części I, sekcja 4.1.2, " Identyfikacja informacji zarządczej i wspierającej", zaproponowano zestaw typów informacji dotyczących zarządzania i wsparcia, które typowo występują w podmiotach publicznych.

Niektóre z funkcji zarządzania i wsparcia wykonywanych w celu wspomagania świadczenia usług lub zarządzania zasobami podmiotu są również wykonywane przez niektóre podmioty w zakresie świadczenia usług na rzecz klientów zewnętrznych (patrz zwłaszcza "A.2.8 *Ogólne zarządzanie* "). Większość z tych typów informacji może być włączona do Załącznika B jako typy informacji związane z realizacją zadań podmiotu. Ponieważ są one klasyfikowane jako funkcje wsparcia w zakresie świadczenia usług, to są zawarte w Części I sekcja 4.1.2 oraz w Załączniku A Części II. Aby ograniczyć liczbę powtórzeń, nie są one powtarzane w załączniku B.

Załącznik A.1, "Zalecane wstępne poziomy oddziaływania dla typów informacji dotyczących zarządzania i wsparcia", dokumentuje poziomy oddziaływania dla typów informacji określonych w Części I rozdział 4.1.2. Są to poziomy wstępne, podlegające przeglądowi i modyfikacji przez interesariuszy podmiotu. Wstępne poziomy wpływu stanowią jedynie pierwszy krok w przypisywaniu wpływu i są poddawane przeglądowi w kolejnych procesach oceny ryzyka. Nie są one przeznaczone do wykorzystania przez audytorów jako ostateczna lista kontrolna dla typów informacji i przypisywania skutków.

Większość systemów informatycznych wykorzystywanych zarówno w usługach bezpośrednich, jak i w działaniach wspierających administrację lub zarządzanie realizuje jedną lub więcej funkcji wsparcia w zakresie świadczenia usług opisanych w załączniku A.3 "Uzasadnienie i czynniki wpływające na informacje dotyczące wsparcia w zakresie

świadczenia usług". Funkcje wsparcia serwisowego, to codzienne działania niezbędne dla organizacji, które świadczą usługi dla ogółu społeczeństwa oraz usługi administracyjne lub zarządcze dla komórek organizacyjnych podmiotów publicznych odpowiedzialnych za świadczenie tych usług. Podobnie jak w przypadku informacji i systemów informatycznych dla administracji/biznesu, cele i wpływy w zakresie bezpieczeństwa są określane przez bezpośrednie zadania służbowe, które są wspierane. Jest prawdopodobne, że wszystkie systemy informatyczne podmiotów publicznych przechowują, przetwarzają i działają z wykorzystaniem informacji dotyczącej utrzymania infrastruktury informatycznej - IT (np. pliki z hasłami oraz ustawieniami dostępu do plików i sieci). Do tego zestawu informacji i procesów będzie miał zastosowanie co najmniej podstawowy zestaw zabezpieczeń w celu zabezpieczenia przed potencjalnym atakiem, niewłaściwym wykorzystaniem lub nadużywaniem informacji i procesów systemowych.

Informacje niezbędne do świadczenia usług administracyjnych lub biznesowych wspierających realizację celu działania podmiotu obejmują rodzaje informacji dotyczące zarządzania zasobami podmiotu publicznego, opisane w Załączniku A.3 "Uzasadnienie i czynniki wpływające na informacje dotyczące zarządzania zasobami podmiotu publicznego". Wszystkie podmioty publiczne pełniące bezpośrednie funkcje usługowe są wspierane przez systemy informatyczne, które wykonują czynności opisane w Załączniku A.3. Wiele podmiotów publicznych posiada własne systemy wsparcia. Inne uzyskują przynajmniej część usług wsparcia od innych organizacji. Niektóre zadania podmiotu mają na celu przede wszystkim wspieranie innych podmiotów publicznych w realizacji ich zadań dla klientów administracji publicznej. Jak wskazano powyżej, systemy informatyczne związane z bezpieczeństwem zależą od charakteru wspieranych usług bezpośrednich.

Duża część dyskusji na temat czynników wpływających na przypisanie poziomu wpływu jest wspólna dla wielu typów informacji. Ponieważ niniejsze wytyczne mają służyć jako dokument referencyjny, przewiduje się, że większość użytkowników będzie odnosić się tylko do jednego lub kilku rodzajów informacji, które ich dotyczą. Czynniki wpływu wspólne dla wszystkich typów informacji omówiono w Części I, sekcja 4.2.3 i 4.4.2.

A.1. ZALECANE WSTĘPNE POZIOMY WPŁYWU DLA TYPÓW INFORMACJI DOTYCZĄCYCH ZARZĄDZANIA I WSPARCIA

W tabeli A-1 przedstawiono osiem rodzajów informacji związanych ze świadczeniem usług pomocniczych oraz pięć rodzajów informacji dotyczących zarządzania zasobami podmiotów realizujących zadania publiczne. Każdy z rodzajów informacji związanych z podfunkcjami przedstawiono szczegółowo w dodatku A.2 i A.3. Funkcje zarządzania i wsparcia są codziennymi działaniami niezbędnymi do zapewnienia poprawnego funkcjonowania podmiotu publicznego.

Tabela A–1 Informacje w procesach zarządczych i wspierających

Informacje wspierające dostarczanie usług
A.2.1 Kontrola i nadzór ✓ Działania naprawcze (zasady / akty prawa) ✓ Ewaluacja zadań ✓ Monitorowanie realizacji zadań
A.2.2 Tworzenie zasad regulacyjnych ✓ Opracowywanie zasad i wytycznych ✓ Konsultacje społeczne ✓ Tworzenie przepisów ✓ Publikacja przepisów
A.2.3 Planowanie i budżetowanie ✓ Tworzenie budżetu ✓ Planowanie środków ✓ Architektura korporacyjna ✓ Planowanie strategiczne ✓ Wykonanie budżetu ✓ Planowanie zatrudnienia ✓ Kontrola zarządcza

- ✓ Integracja budżetowania i efektywności
- ✓ Polityka podatkowa i fiskalna

A.2.4 Zarządzanie ryzykiem i jego ograniczanie

- ✓ Planowanie awaryjne
- ✓ Ciągłość operacji
- ✓ Odzyskiwanie usług

A.2.5 Realizacja dochodów

1. Windykacja
2. Pobieranie opłat od użytkownika
3. Sprzedaż aktywów

A.2.6 Sprawy publiczne

- ✓ Obsługa klienta
- ✓ Oficjalne rozpowszechnianie informacji
- ✓ Informowanie o usługach
- ✓ Komunikacja wewnętrzna i zewnętrzna

A.2.7 Relacje legislacyjne

- ✓ Śledzenie ustawodawstwa
- ✓ Opinie prawne
- ✓ Opracowanie wniosków *de lege ferenda*
- ✓ Współpraca z parlamentem

A.2.8 Ogólne zarządzanie

- ✓ Centralne operacje fiskalne
- ✓ Funkcje legislacyjne
- ✓ Funkcje wykonawcze
- ✓ Centralne zarządzanie własnością Skarbu Państwa
- ✓ Centralne zarządzanie personelem
- ✓ Zarządzanie podatkami

- ✓ Centralne zarządzanie dokumentacją i statystykami
- ✓ Informacje o dochodach
- ✓ Tożsamość osób i uwierzytelnianie
- ✓ Informacje o zdarzeniu związanym z uprawnieniami
- ✓ Informacje o reprezentacji odbiorcy płatności
- ✓ Informacje ogólne

A.3.1 Zarządzanie administracyjne

- ✓ Zarządzanie infrastrukturą, flotą i wyposażeniem
- ✓ Usługi pomocy technicznej
- ✓ Zarządzanie bezpieczeństwem
- ✓ Delegacje
- ✓ Organizacja miejsc pracy

A.3.2 Zarządzanie finansami

- ✓ Księgowość
- ✓ Kontrola funduszy
- ✓ Płatności
- ✓ Świadczenia i należności
- ✓ Zarządzanie aktywami i pasywami
- ✓ Raportowanie i informacje
- ✓ Rachunek kosztów / pomiar efektywności

A.3.3 Zarządzanie zasobami ludzkimi

- ✓ Strategia HR
- ✓ Pozyskiwanie personelu
- ✓ Organizacja i zarządzanie stanowiskiem
- ✓ Zarządzanie wynagrodzeniami
- ✓ Zarządzanie świadczeniami

- ✓ Zarządzanie wydajnością pracowników
- ✓ Relacje między pracownikami
- ✓ Stosunki pracy
- ✓ Zarządzanie separacją
- ✓ Rozwój zasobów ludzkich

A.3.4 Zarządzanie łańcuchem dostaw

- ✓ Nabywanie towarów
- ✓ Nabywanie usług
- ✓ Inwentaryzacja
- ✓ Zarządzanie logistyczne

A.3.5 Zarządzanie informacją i technologiami

- ✓ Zarządzanie cyklem życia / zmianą
- ✓ Konserwacja systemu
- ✓ Utrzymanie infrastruktury IT
- ✓ Bezpieczeństwo informacji
- ✓ Przechowywanie dokumentacji
- ✓ Zarządzanie informacją
- ✓ Monitorowanie systemu i sieci
- ✓ Udostępnianie informacji

Tabela A-2 zawiera podsumowanie wstępnych zaleceń dotyczących poziomu wpływu w odniesieniu do informacji administracyjnych, zarządczych i usługowych. Wstępne poziomy wpływu są zalecane dla każdego atrybutu bezpieczeństwa (poufność, integralność, dostępność) oraz dla każdego rodzaju informacji w zakresie zarządzania i wsparcia występującego w podmiocie publicznym. Poziomy wpływu na poufność, integralność i dostępność określają kategorię bezpieczeństwa każdego typu informacji.

Wskazówka dotycząca implementacji

Większość rządowych systemów informacyjnych uzyskuje dostęp, przetwarza i/lub rozpowszechnia więcej niż jedną klasę informacji. Przy określaniu wymogów bezpieczeństwa informacji w systemie należy uwzględnić cele i skutki związane ze wszystkimi rodzajami informacji i procesów obsługiwanych przez system informatyczny.

Każdy typ informacji może zawierać jeden lub więcej elementów. Na przykład informacje dotyczące zarządzania świadczeniami obejmują informacje dotyczące identyfikacji pracownika, informacje dotyczące programu świadczeń w odniesieniu do ubezpieczeń i innych produktów, informacje o kosztach, roszczeniach i polisach refundacyjnych, procedurach odszkodowań itp.

W niektórych przypadkach dla różnych elementów informacji właściwe są różne poziomy wpływu. Na przykład, elementy informacji dotyczące monitorowania programu odnoszącego się do usuwania luk w zabezpieczeniach informacji, mogą mieć inny poziom wpływu niż elementy informacji dotyczące monitorowania programu odnoszącego się do modernizacji mebli biurowych.

Każdy podmiot publiczny przetwarzający dany typ informacji może przetwarzać inną kombinację elementów. Obowiązki przypisane każdemu podmiotowi przetwarzającemu dany typ informacji mogą mieć wpływ na rzeczywisty poziom wpływu związany z informacjami w kontekście działalności tego podmiotu.

W tabeli A-2 w opisach typów informacji, które zostaną przedstawione poniżej, określono wyjątki od wstępnego przypisania skutków, umieszczając je szarą czcionką [szara czcionka] i opisano je jako mające zastosowanie ze względu na cel bezpieczeństwa. Szczegółowe opisy znajdują się w podtytule "Określanie wpływu szczególnych czynników wpływających na [cel ochrony]".

Załączniki A.2 i A.3 określają elementy informacyjne i konteksty, które mogą powodować odchylenia od podstawowego przypisania poziomu wpływu incydentu / zakłócenia. Na przykład, niektóre systemy przetwarzają informacje, których naruszenie ma wpływ na

bezpieczeństwo narodowe, infrastrukturę krytyczną lub kluczowe zasoby krajowe. Skutki związane z takimi systemami znajdują się poza zakresem niniejszego dokumentu (tj. informacje dotyczące bezpieczeństwa narodowego) lub mogą wymagać korekty w górę ze względu na poważniejsze konsekwencje naruszenia bezpieczeństwa.

Wiele rodzajów informacji jest również uzależnionych od cyklu życia. Oznacza to, że informacje, które wymagają ochrony w jednej fazie cyklu życia systemu informatycznego lub operacyjnego wykorzystania informacji, są publicznie dostępne w późniejszej fazie lub w następstwie jakiegoś zdarzenia. Na przykład informacje, które posiadają cechy poufności w okresie, w którym podmiot wykorzystuje je do podjęcia decyzji, mogą być powszechnie znane po jej podjęciu (np. informacje finansowe/budżetowe wykorzystywane podczas opracowywania wniosków w ramach działań związanych z zamówieniami).

Tabela A–2: Kategoryzacja bezpieczeństwa typów informacji i systemów informatycznych w zakresie informacji w procesach zarządczych i wspierających

	Poufność	**Integralność**	**Dostępność**
Kontrola i nadzór			
Działania naprawcze (zasady / akty prawa)	Niski[4]	**Niski**	**Niski**
Ewaluacja zadań	Niski	**Niski**	**Niski**
Monitorowanie realizacji zadań	Niski[5]	Niski	Niski
Tworzenie zasad regulacyjnych			
Opracowywanie zasad i wytycznych	Niski	Niski	**Niski**
Konsultacje społeczne	**Niski**	**Niski**	**Niski**
Tworzenie przepisów	Niski	Niski	**Niski**
Publikacja przepisów	**Niski**	**Niski**	**Niski**

[4] Szarą czcionką [szara czcionka] określono wyjątki od wstępnego przypisania skutków i opisano je, jako mające zastosowanie ze względu na cel bezpieczeństwa

[5] Wpływ na poufność przypisany typowi informacji „Monitorowanie zadań" może wymagać zwiększenia wpływu na poufność w przypadku innych typów informacji przetwarzanych przez system.

	Poufność	Integralność	Dostępność
Planowanie i budżetowanie			
Tworzenie budżetu	Niski	Niski	**Niski**
Planowanie środków	Niski	Niski	**Niski**
Architektura korporacyjna	Niski	Niski	**Niski**
Planowanie strategiczne	Niski	Niski	**Niski**
Wykonanie budżetu	Niski	Niski	**Niski**
Planowanie zatrudnienia	Niski	**Niski**	**Niski**
Kontrola zarządcza	Niski	Niski	**Niski**
Integracja budżetowania i efektywności	Niski	Niski	**Niski**
Polityka podatkowa i fiskalna	Niski	Niski	**Niski**
Zarządzanie ryzykiem i jego ograniczanie			
Planowanie awaryjne	Umiarkowany	**Umiarkowany**	Umiarkowany
Ciągłość operacji	Umiarkowany	**Umiarkowany**	Umiarkowany
Odzyskiwanie usług	Niski	**Niski**	Niski
Realizacja dochodów			
Windykacja	Umiarkowany	Niski	**Niski**
Pobieranie opłat od użytkownika	**Niski**	Niski	**Umiarkowany**
Sprzedaż aktywów	Niski	**Umiarkowany**	**Niski**
Sprawy publiczne			
Obsługa klienta	Niski	Niski	Niski
Oficjalne rozpowszechnianie informacji	**Niski**	Niski	Niski
Informowanie o usługach	**Niski**	Niski	**Niski**
Komunikacja wewnętrzna i zewnętrzna	Niski	Niski	**Niski**
Relacje legislacyjne			
Śledzenie ustawodawstwa	Niski	**Niski**	**Niski**
Opinie prawne	Niski	**Niski**	Niski

	Poufność	Integralność	Dostępność
Opracowanie wniosków *de lege ferenda*	Umiarkowany	**Niski**	Niski
Współpraca z parlamentem	Umiarkowany	**Niski**	Niski
Ogólne zarządzanie			
Centralne operacje fiskalne[6]	Umiarkowany	**Niski**	**Niski**
Funkcje legislacyjne	**Niski**	**Niski**	Niski
Funkcje wykonawcze	**Niski**	**Niski**	**Niski**
Centralne zarządzanie własnością Skarbu Państwa	Niski[7]	**Niski**	Niski[8]
Centralne zarządzanie personelem	Niski	Niski	Niski
Zarządzanie podatkami	Umiarkowany	Niski	Niski
Centralne zarządzanie dokumentacją i statystykami	Umiarkowany	**Niski**	**Niski**
Informacje o dochodach	**Umiarkowany**	Umiarkowany	Umiarkowany
Tożsamość osób i uwierzytelnianie	**Umiarkowany**	Umiarkowany	Umiarkowany
Informacje o zdarzeniu związanym z uprawnieniami	**Umiarkowany**	Umiarkowany	Umiarkowany
Informacje o reprezentacji odbiorcy płatności	**Umiarkowany**	Umiarkowany	Umiarkowany
Informacje ogólne[9]	Niski	Niski	Niski
Zarządzanie administracyjne			
Zarządzanie infrastrukturą, flotą i wyposażeniem	Niski[3]	Niski[4]	Niski[4]
Usługi pomocy technicznej	Niski	Niski	Niski
Zarządzanie bezpieczeństwem	Umiarkowany	**Umiarkowany**	Niski
Delegacje	Niski	**Niski**	**Niski**

[6] Funkcje związane z podatkami są związane z typem informacji o zarządzaniu podatkami.

[7] Wysoki, gdy zagrożone jest bezpieczeństwo głównych elementów infrastruktury krytycznej lub kluczowych zasobów krajowych.

[8] Umiarkowany lub wysoki w sytuacjach awaryjnych, w których występują procesy o kluczowym znaczeniu dla bezpieczeństwa ludzi lub głównych zasobów.

[9] Ten typ informacji został dodany jako typ informacji "inne". W związku z tym podmioty mogą wykorzystywać ten rodzaj informacji do identyfikacji dodatkowych rodzajów informacji, które nie zostały zdefiniowane i przypisywania im poziomów wpływu.

	Poufność	Integralność	Dostępność
Organizacja miejsc pracy	**Niski**	**Niski**	**Niski**
Zarządzanie finansami			
Zarządzanie aktywami i pasywami	Niski	Niski	**Niski**
Raportowanie i informacje	Niski	**Umiarkowany**	**Niski**
Kontrola funduszy	Umiarkowany	**Umiarkowany**	**Niski**
Księgowość	Niski	Umiarkowany	**Niski**
Płatności	Niski	Umiarkowany	Niski
Pobory i należności	**Niski**	**Umiarkowany**	**Niski**
Rachunek kosztów / pomiar efektywności	**Niski**	**Umiarkowany**	**Niski**
Zarządzanie zasobami ludzkimi			
Strategia HR	Niski	**Niski**	**Niski**
Pozyskiwanie personelu	Niski	**Niski**	**Niski**
Organizacja i zarządzanie stanowiskami pracy	Niski	**Niski**	**Niski**
Zarządzanie odszkodowaniami	Niski	Niski	**Niski**
Zarządzanie świadczeniami	Niski	**Niski**	**Niski**
Zarządzanie wydajnością pracowników	Niski	**Niski**	**Niski**
Relacje między pracownikami	Niski	**Niski**	**Niski**
Stosunki pracy	Niski	**Niski**	Niski
Zarządzanie rozdzielnością	Niski	**Niski**	**Niski**
Rozwój zasobów ludzkich	Niski	**Niski**	**Niski**
Zarządzanie łańcuchem dostaw			
Nabywanie towarów	Niski	Niski	Niski
Inwentaryzacja	Niski	**Niski**	Niski
Zarządzanie logistyką	Niski	**Niski**	Niski
Nabywanie usług	Niski	Niski	**Niski**
Zarządzanie informacją i technologiami			
Rozwój systemu	**Niski**	Umiarkowany	**Niski**

	Poufność	Integralność	Dostępność
Zarządzanie cyklem życia / zmianą	Niski	Umiarkowany	**Niski**
Utrzymanie systemu	**Niski**	Umiarkowany	**Niski**
Utrzymanie infrastruktury IT[10]	Niski	Niski	Niski
Bezpieczeństwo systemu informatycznego	**Niski**	**Umiarkowany**	**Niski**
Przechowywanie dokumentacji	Niski	Niski	**Niski**
Zarządzanie informacją[11]	Niski	Umiarkowany	**Niski**
Monitorowanie systemu i sieci	Umiarkowany	Umiarkowany	**Niski**
Wymiana informacji	**N/D[12]**	**N/D**	**N/D**

[10] Wpływ na poufność przypisany typowi informacji dotyczących utrzymania infrastruktury informatycznej może wymagać zwiększenia z uwagi na poufność typów informacji przetwarzanych przez system.

[11] Wpływ na poufność przypisany do typu informacji o zarządzaniu informacją, może wymagać zwiększenia, z uwagi na poufność typów informacji przetwarzanych przez system.

[12] N/D – nie dotyczy.

A.2. PRZESŁANKI I CZYNNIKI W ZAKRESIE INFORMACJI WSPOMAGAJĄCYCH ŚWIADCZENIE USŁUG ORAZ INFORMACJI W ZAKRESIE WSPARCIA TECHNICZNEGO

Funkcje wspomagające świadczenie usług zapewniają istotne zasady, podstawy programowe i zarządcze wspierające działania podmiotów realizujących zadania publiczne.

Cele w zakresie bezpieczeństwa i poziomy wpływu incydentu / zakłócenia na informacje i systemy wsparcia w zakresie świadczenia usług są na ogół ustalane na podstawie charakteru wspieranych usług bezpośrednich i ich elementów składowych. Jeśli system przechowuje, przetwarza lub przekazuje informacje dotyczące bezpieczeństwa narodowego, jest on zdefiniowany jako system bezpieczeństwa narodowego i nie jest objęty zakresem niniejszych wytycznych. Działania wspierające świadczenie usług są zdefiniowane w niniejszej sekcji.

A.2.1. KONTROLA I NADZÓR

Informacje dotyczące kontroli i nadzoru są wykorzystywane do zapewnienia, że działania i programy podmiotów realizujących zadania publiczne i ich zewnętrznych partnerów biznesowych są zgodne z obowiązującym prawem i przepisami oraz zapobiegają marnotrawstwu, oszustwom i nadużyciom.

A.2.2. TWORZENIE ZASAD REGULACYJNYCH

Tworzenie regulacji prawnych obejmuje działania związane z wnoszeniem wkładu w proces stanowienia prawa oraz przy opracowywaniu zasad i wskazówek dotyczących wdrażania prawa.

A.2.3. PLANOWANIE I BUDŻETOWANIE

Planowanie i budżetowanie obejmuje działania polegające na określaniu kierunku strategicznego, identyfikacji i ustanawianiu zadań i procesów umożliwiających zmianę oraz alokację zasobów (kapitału i pracy) pomiędzy te zadania i procesy.

A.2.4. ZARZĄDZANIE RYZYKIEM I JEGO OGRANICZANIE

Wewnętrzne zarządzanie ryzykiem i jego ograniczanie obejmuje wszystkie działania związane z procesami analizy narażenia na ryzyko i ustalaniem odpowiednich środków zaradczych. Należy zauważyć, że zagrożenia dla informacji i systemów informatycznych związane z wewnętrznym zarządzaniem ryzykiem i działaniami ograniczającymi ryzyko mogą mieć nieodłączny wpływ na odporność, na kompromitację / uszkodzenia i naprawę szkód w odniesieniu do szerokiego zakresu infrastruktury krytycznej i kluczowych zasobów krajowych.

A.2.5. REALIZACJA OD DOCHODÓW

Obejmuje pobór podatków od dochodów przez podmioty realizujące zadania publiczne ze wszystkich źródeł. Uwaga: Pobór podatków jest rozliczany w ramach typu informacji o zarządzaniu podatkami w obszarze zadań publicznych.

A.2.6. SPRAWY PUBLICZNE

Działania w zakresie spraw publicznych obejmują wymianę informacji i komunikację między rządem, samorządem, obywatelami, przedsiębiorcami i innymi zainteresowanymi stronami w ramach bezpośredniego wspierania usług publicznych, porządku publicznego lub interesu narodowego.

A.2.7. RELACJE LEGISLACYJNE

Relacje legislacyjne obejmują działania mające na celu opracowanie, śledzenie i zmianę przepisów prawa publicznego za pośrednictwem służb legislacyjnych rządu.

A.2.8. OGÓLNE ZARZĄDZANIE

Ogólne zarządzanie obejmuje ogólne koszty funkcjonowania podmiotów rządowych, w tym działania legislacyjne i wykonawcze, wykonywanie działalności w zakresie podatków, personelu i majątku oraz świadczenie usług, których nie można racjonalnie sklasyfikować w żadnym innym obszarze wsparcia usług. Zgodnie z przyjętą zasadą wszystkie działania, które są mniej lub bardziej związane z innymi obszarami wsparcia usług lub rodzajami informacji, powinny być uwzględniane w tych obszarach, a niewymienione jako część sektora

instytucji rządowych i samorządowych. Ten obszar wsparcia usług jest zarezerwowany dla operacji zarządzania na szczeblu centralnym. Większość działań związanych z zarządzaniem świadczeniem usług (w oparciu o cel działania) nie zostałaby tu uwzględniona.

W przeciwieństwie do innych funkcji wsparcia usług, niektóre typy informacji sektora instytucji rządowych i samorządowych są powiązane z konkretnymi centralnej administracji rządowej.

A.3. UZASADNIENIE I CZYNNIKI DOTYCZĄCE ZARZĄDZANIA ZASOBAMI

Funkcje zarządzania zasobami to działania wspierające wewnętrzną pracę biurową, które umożliwiają podmiotowi skuteczne działanie. Cele bezpieczeństwa i wpływ funkcji zarządzania zasobami są określane przez ostatecznie wspierane zadania usługowe. Jest prawdopodobne, że wszystkie systemy informacyjne podmiotu realizującego zadania publiczne przechowują, przetwarzają i działają z wykorzystaniem informacji dotyczącej infrastruktury IT (np. plików haseł oraz ustawień dostępu do plików i sieci). Podstawowy zestaw zabezpieczeń będzie miał zastosowanie do tych informacji i procesów w celu zapobieżeniu potencjalnemu uszkodzeniu, niewłaściwego użycia lub nadużycia informacji lub procesów systemowych.

A.3.1. ZARZĄDZANIE ADMINISTRACYJNE

Zarządzanie administracyjne obejmuje bieżące zarządzanie i utrzymanie infrastruktury wewnętrznej. Informacja administracyjna jest zazwyczaj rutynowa i ma stosunkowo niewielki wpływ. Niektóre informacje administracyjne dotyczące zarządzania są jednak albo bardzo wrażliwe (np. zarządzanie logistyczne materiałami jądrowymi lub innymi materiałami niebezpiecznymi, informacje dotyczące zarządzania bezpieczeństwem oraz informacje dotyczące zarządzania poświadczeniami bezpieczeństwa), albo krytyczne (np. informacje dotyczące inwentaryzacji i zarządzania logistycznego potrzebne do wsparcia operacji krytycznych pod względem czasu). Informacje dotyczące bezpieczeństwa narodowego nie są objęte zakresem niniejszych wytycznych. Rutynowe systemy zarządzania administracyjnego, które nie przetwarzają informacji niejawnych, nie są zazwyczaj wyznaczonymi krajowymi systemami bezpieczeństwa, nawet jeżeli mają zasadnicze znaczenie dla bezpośredniego wypełniania misji wojskowych lub wywiadowczych.

A.3.2. ZARZĄDZANIE FINANSAMI

Zarządzanie finansami obejmuje zagregowany zestaw praktyk i procedur księgowych, które pozwalają na dokładne i efektywne zarządzanie wszystkimi dochodami, funduszami i wydatkami podmiotu. Wpływ na poufność informacji związanych z zarządzaniem finansami wiąże się zazwyczaj z wrażliwością istnienia konkretnych projektów, programów lub

technologii, które mogą zostać ujawnione w wyniku nieuprawnionego ujawnienia informacji. Zakłócenia integralność może wynikać z udanego oszustwa i może wpłynąć na wizerunek podmiotu, a działania naprawcze często zakłócają jego działalność. Stała utrata lub niedostępność informacji dotyczących zarządzania finansami może sparaliżować działalność podmiotu.

A.3.3. ZARZĄDZANIE ZASOBAMI LUDZKIMI

Działania związane z zarządzaniem zasobami ludzkimi obejmują wszystkie działania związane z rekrutacją i zarządzaniem personelem.

A.3.4. ZARZĄDZANIE ŁAŃCUCHEM DOSTAW

Zarządzanie łańcuchem dostaw obejmuje zakupy, śledzenie dostaw oraz ogólne zarządzanie towarami i usługami.

A.3.5. ZARZĄDZANIE INFORMACJĄ I TECHNOLOGIAMI

Zarządzanie IT obejmuje koordynację zasobów i systemów informatycznych niezbędnych do wspierania lub umożliwienia usług publicznych. Wpływ na informacje związane z funkcjonowaniem systemów informatycznych zasadniczo musi być brany pod uwagę nawet wtedy, gdy wszystkie informacje dotyczące celu działania przetwarzane przez system mają być dostępne dla ogółu społeczeństwa. Mogą występować różnice w podejściu integralności i dostępności w stosunku do kwestii poufności. Informacje, które zostały upublicznione, z definicji nie wymagają ochrony poufności. Natomiast ochrona integralności i dostępności nie może być utrzymana w stosunku do kopii informacji, które zostały rozpowszechnione publicznie. Zapewnienie integralności i dostępności może być utrzymane tylko poprzez utrzymywanie kopii zapasowych informacji w systemach informatycznych kontrolowanych przez podmiot.

ZAŁĄCZNIK B: POZIOMY WPŁYWU INCYDENTU NA INFORMACJE I SYSTEMY INFORMATYCZNE W ZAKRESIE ZADAŃ REALIZOWANYCH PRZEZ PODMIOT PUBLICZNE

Ogólnie rzecz biorąc, poszczególne podmioty publiczne powinny określić rodzaje informacji dotyczących celu ich działania, które są przetwarzane przez ich systemy. Niniejszy załącznik określa niektóre rodzaje informacji, które mogą być przetwarzane przez te podmioty. Materiał ten zawiera informacje o zadaniach i potencjalnych skutkach nieautoryzowanego ujawnienia, modyfikacji lub niedostępności informacji związanych z realizowanymi zadaniami.

Podstawowym celem systemów informacyjnych podmiotów realizujących zadania publiczne jest wspieranie świadczenia podstawowych usług dla społeczeństwa. Niniejsza sekcja dotyczy typów informacji związanych zarówno z usługami świadczonymi przez podmioty publiczne na rzecz obywateli, jak i mechanizmów wykorzystywanych do osiągnięcia celów rządu lub świadczenia usług na rzecz obywateli. Mechanizmy służące realizacji zadań obejmują bodźce finansowe, bezpośrednie i pośrednie wsparcie rządowe. Zadania rządu lub mechanizmy służące realizacji zadań podzielone na 26 obszarów i są wymienione w tabeli B-1. Ponieważ niektóre z obszarów podlegają szczególnym regulacjom prawnym nie są one ujęte w kategoryzacji bezpieczeństwa przedstawionej w tabeli B-2. Każdy obszar zadań i sposób realizacji odpowiada obszarowi usług dla obywateli lub sposobowi realizacji usług dla obywateli. Nie istnieje odwzorowanie usług i trybów dostawy do ministerstw i agencji rządowych w ujęciu "jeden do jednego". Niektóre ministerstwa lub agencje skupiają się na jednym zadaniu. Inne obsługują wiele zadań w ramach danego obszaru. Jeszcze inne świadczą usługi związane z kilkoma różnymi obszarami.

Rodzaj informacji jest związany z zadaniem z obszaru administracji rządowej i trybem realizacji. Tożsamość każdego typu informacji jest określona przez zadanie, z którą jest związana. Niektóre z funkcji zarządzania i wsparcia wykonywanych w celu wspierania świadczenia usług lub zarządzania zasobami publicznymi są również wykonywane przez niektóre podmioty w zakresie świadczenia usług dla obywateli. Większość tych rodzajów

informacji może być zawarta w załączniku B jako rodzaje informacji wynikające z zadań. Są one klasyfikowane jako funkcje wsparcia w zakresie świadczenia usług i są one zawarte w części I, sekcja 4.1.2 oraz w Załączniku A, i nie są powtarzane w Załączniku B.

Wspólne czynniki określania wpływu incydentu / zakłócenia opisane w części I, sekcja 4.2.3 i 4.4, mają również zastosowanie do informacji wynikających z realizowanych zadań.

Tabela B-2. Typy informacji wynikające z zadań administracji rządowej oraz mechanizmy ich realizacji

B.1 Obrona i bezpieczeństwo narodowe Obrona narodowa na poziomie: ✓ strategicznym ✓ operacyjnym ✓ taktycznym
B.2 Bezpieczeństwo wewnętrzne ✓ Bezpieczeństwo granic i transportu ✓ Ochrona kluczowych aktywów i infrastruktury krytycznej ✓ Ochrona przed skutkami katastrof i klęsk żywiołowych
B.3 Operacje wywiadowcze ✓ Planowanie wywiadowcze ✓ Zbieranie danych wywiadowczych ✓ Analiza i opracowania wywiadu ✓ Rozpowszechnianie danych wywiadowczych ✓ Przetwarzanie danych wywiadowczych

B.4 Zarządzanie kryzysowe

- ✓ Monitorowanie i przewidywanie
- ✓ Przygotowanie i planowanie na wypadek katastrof
- ✓ Działania naprawcze i odtworzeniowe
- ✓ Działania ratunkowe

B.5 Sprawy zagraniczne i handel międzynarodowy

- ✓ Sprawy zagraniczne
- ✓ Rozwój międzynarodowy i pomoc humanitarna
- ✓ Handel międzynarodowy

B.6 Zasoby naturalne

- ✓ Zarządzanie zasobami wodnymi
- ✓ Ochrona zasobów, gospodarka morska i gospodarka przestrzenna
- ✓ Zarządzanie zasobami rekreacyjnymi i turystyka
- ✓ Modernizacja i rozwój rolnictwa

B.7 Energia

- ✓ Źródła energii
- ✓ Oszczędzanie energii
- ✓ Zarządzanie zasobami energetycznymi
- ✓ Produkcja energii

B.8 Zarządzanie środowiskiem

- ✓ Monitorowanie i prognozowanie
- ✓ Przeciwdziałanie zmianom klimatycznym
- ✓ Kontrola i zapobieganie skażeniom

B.9 Rozwój ekonomiczny

- ✓ Rozwój usług i produkcji
- ✓ Ochrona własności intelektualnej
- ✓ Nadzór nad sektorem finansowym
- ✓ Stabilizacja dochodów sektora przemysłowego

B.10 Usługi społeczne i socjalne

- ✓ Promocja mieszkalnictwa
- ✓ Rozwój społeczny i regionalny
- ✓ Służby socjalne
- ✓ Usługi pocztowe

B.11 Transport

- ✓ Transport lądowy
- ✓ Transport wodny
- ✓ Transport powietrzny
- ✓ Operacje kosmiczne

B.12 Edukacja

- ✓ Edukacja
- ✓ Szkolnictwo wyższe
- ✓ Ochrona dziedzictwa narodowego
- ✓ Wystawy i muzea

B.13 Sprawy pracy

- ✓ Szkolenie zawodowe i zatrudnianie
- ✓ Prawo pracy
- ✓ Bezpieczeństwo pracy (BHP)

B.14 Zdrowie

- ✓ Dostęp do opieki zdrowotnej
- ✓ Zdrowie publiczne i bezpieczeństwo konsumentów
- ✓ Administracja opieki zdrowotnej
- ✓ Usługi dostarczania opieki zdrowotnej
- ✓ Badania w zakresie opieki zdrowotnej i edukacja pracowników opieki zdrowotnej

B.15 Zabezpieczenie społeczne

- ✓ Emerytury i renty
- ✓ Zasiłek dla bezrobotnych
- ✓ Pomoc społeczna
- ✓ Odszkodowania

B.16 Egzekwowanie prawa

- ✓ Ściganie w sprawach karnych
- ✓ Dochodzenia i śledztwa
- ✓ Ochrona obywateli
- ✓ Ochrona rządu
- ✓ Ochrona własności
- ✓ Kontrola substancji
- ✓ Zapobieganie przestępczości
- ✓ Kontrola obrotu

B.17 Postępowania sądowe i arbitrażowe

- ✓ Procesy sądowe
- ✓ Obrona prawna
- ✓ Dochodzenie prawne
- ✓ Prokuratura i spory sądowe
- ✓ Postępowanie arbitrażowe

B.18 Więziennictwo i resocjalizacja

- ✓ Sprawy więziennictwa
- ✓ Resocjalizacja przestępców

B.19 Nauka i innowacyjność

- ✓ Badania naukowe i technologiczne oraz innowacje
- ✓ Eksploracja kosmosu i innowacje

B.20 Tworzenie i zarządzanie wiedzą

- ✓ Badania i rozwój
- ✓ Statystyka publiczna
- ✓ Doradztwo i konsultacje
- ✓ Upowszechnianie wiedzy

B.21 Zgodność i egzekwowanie przepisów

- ✓ Kontrole i audyty
- ✓ Standaryzacja
- ✓ Zgody i licencje

B.22 Tworzenie i zarządzanie dobrami publicznymi

- ✓ Produkcja przemysłowa
- ✓ Budownictwo
- ✓ Zarządzanie zasobami publicznymi, zarządzaniem infrastrukturą
- ✓ Zarządzanie infrastrukturą informatyczną

B.23 Pomoc publiczna

- ✓ Dotacje państwowe
- ✓ Bezpośredni transfer środków do podmiotów
- ✓ Ulgi podatkowe

B.24 Kredyty i ubezpieczenia

- ✓ Kredyty bezpośrednie
- ✓ Poręczenia kredytowe
- ✓ Ogólne ubezpieczenia

B.25 Przepływy finansowe Rząd - JST ✓ Dotacje ✓ Dofinansowanie projektów ✓ Dotacje celowe ✓ Pożyczki rządowe
B.26 Bezpośrednie usługi dla obywateli ✓ Operacje wojskowe ✓ Operacje cywilne

Tabela B-2 zawiera wstępne oceny wpływu dla każdego rodzaju informacji w tabeli D-1. W tabeli D-2 wyjątki od wstępnych ocen skutków są określone poprzez wyświetlenie ocen skutków czcionką szarą [czcionka szara]. Szczegółowe opisy znajdują się w sekcji "Określenie wpływu szczególnych czynników wpływających na [cel ochrony]".

Wskazówka dotycząca implementacji

Poziomy wpływu przypisane do kilku typów informacji należy uznać za zależne od kontekstu. Na przykład, dany typ informacji w niektórych podmiotach może zawierać elementy informacji, których kompromitacja może zagrażać życiu ludzkiemu. W innych podmiotach ten sam typ informacji może nie zawierać takich elementów.

Wiele z wymienionych typów informacji jest również uzależnionych od cyklu życia. Oznacza to, że informacje, które wymagają ochrony w początkowej fazie procesu, mogą być publicznie dostępne na późniejszym etapie lub w następstwie jakiegoś zdarzenia. Na przykład informacje, które posiadają atrybuty poufności w okresie, w którym podmiot wykorzystuje je do podjęcia decyzji, mogą być publicznie dostępne po podjęciu decyzji (np. informacje finansowe/budżetowe wykorzystywane podczas opracowywania wniosków w ramach działań związanych z zamówieniami).

W poniższych sekcjach opisano atrybuty informacji, które mają wpływ na ocenę skutków dla każdego rodzaju informacji.

Tabela B-2: Kategoryzacja informacji dotyczących realizowanych zadań

	Poufność	Integralność	Dostępność
Obrona i bezpieczeństwo narodowe[13]			
Bezpieczeństwo wewnętrzne			
Bezpieczeństwo granic i transportu	Umiarkowany	Umiarkowany	Umiarkowany
Ochrona kluczowych aktywów i infrastruktury krytycznej	**Wysoki**	**Wysoki**	**Wysoki**
Ochrona przed skutkami katastrof i klęsk żywiołowych	**Wysoki**	**Wysoki**	**Wysoki**
Operacje wywiadowcze[14]			
Zarządzanie kryzysowe			
Monitorowanie i przewidywanie	Niski	**Wysoki**	**Wysoki**
Przygotowanie i planowanie na wypadek katastrof	Niski	Niski	Niski
Działania naprawcze i odtworzeniowe	**Niski**	**Niski**	**Niski**
Działania ratunkowe	Niski	**Wysoki**	**Wysoki**
Sprawy zagraniczne i handel międzynarodowy			
Sprawy zagraniczne	**Wysoki**	**Wysoki**	Umiarkowany
Rozwój międzynarodowy i pomoc humanitarna	Umiarkowany	Niski	Niski

[13] Poziom wpływu na atrybuty bezpieczeństwa informacji określany jest przez kierownika jednostki organizacyjnej sprawującego kontrolę nad systemem informatycznym.

[14] Tamże.

	Poufność	Integralność	Dostępność
Handel międzynarodowy	**Wysoki**	**Wysoki**	**Wysoki**
Zasoby naturalne			
Zarządzanie zasobami wodnymi	Niski	**Niski**	**Niski**
Ochrona zasobów, gospodarka morska i gospodarka przestrzenna	Niski	Niski	Niski
Zarządzanie zasobami rekreacyjnymi i turystyka	Niski	Niski	Niski
Modernizacja i rozwój rolnictwa	Niski	**Niski**	**Niski**
Energia			
Źródła energii	Niski[15]	Umiarkowany[16]	Umiarkowany[9]
Oszczędzanie energii	Niski	Niski	Niski
Zarządzanie zasobami energetycznymi	Umiarkowany	Niski	**Niski**
Produkcja energii	Niski	Niski	**Niski**
Zarządzanie środowiskiem			
Monitorowanie i prognozowanie	Niski	Umiarkowany	**Niski**
Przeciwdziałanie zmianom klimatycznym	**Umiarkowany**	**Niski**	**Niski**
Kontrola i zapobieganie skażeniom	**Niski**	**Niski**	**Niski**
Rozwój ekonomiczny			
Rozwój usług i produkcji	Niski	**Niski**	**Niski**
Ochrona własności intelektualnej	Niski	**Niski**	**Niski**
Nadzór nad sektorem finansowym	Umiarkowany	Niski	**Niski**

[15] Wysoki, gdy zagrożone jest bezpieczeństwo materiałów radioaktywnych, wysoce łatwopalnych paliw, linii przesyłowych lub procesów sterowania.

[16] Zazwyczaj Umiarkowany lub Wysoki, gdy w grę wchodzą procedury krytyczne dla realizowanych zadań.

	Poufność	Integralność	Dostępność
Stabilizacja dochodów sektora przemysłowego	**Umiarkowany**	**Niski**	**Niski**
Usługi społeczne i socjalne			
Promocja mieszkalnictwa	Niski	**Niski**	**Niski**
Rozwój społeczny i regionalny	Niski	**Niski**	**Niski**
Służby socjalne	Niski	**Niski**	**Niski**
Usługi pocztowe	Niski	Umiarkowany	**Umiarkowany**
Transport			
Transport lądowy	Niski	Niski	Niski
Transport wodny	Niski	Niski	Niski
Transport powietrzny	Niski	Niski	Niski
Operacje kosmiczne	Niski	**Wysoki**	**Wysoki**
Edukacja			
Edukacja podstawowa i ponadpodstawowa	**Niski**	**Niski**	**Niski**
Szkolnictwo wyższe	Niski	Niski	**Niski**
Ochrona dziedzictwa narodowego	Niski	Niski	**Niski**
Wystawy i Muzea	Niski	Niski	**Niski**
Sprawy pracy			
Szkolenie zawodowe i zatrudnianie	Niski	Niski	**Niski**
Prawa pracy	**Niski**	**Niski**	**Niski**
Bezpieczeństwo pracy (BHP)	**Niski**	**Niski**	**Niski**
Zdrowie			
Dostęp do opieki zdrowotnej	Niski	**Umiarkowany**	Niski
Zdrowie publiczne i bezpieczeństwo konsumentów	Niski	Umiarkowany	Niski

	Poufność	Integralność	Dostępność
Administracja opieki zdrowotnej	Niski	Umiarkowany	**Niski**
Usługi dostarczania opieki zdrowotnej	Niski	**Wysoki**	Niski
Badania w zakresie opieki zdrowotnej i edukacja pracowników opieki zdrowotnej	**Niski**	**Umiarkowany**	**Niski**
Zabezpieczenie społeczne			
Emerytury i niepełnosprawność	**Umiarkowany**	Umiarkowany	Umiarkowany
Zasiłek dla bezrobotnych	Niski	**Niski**	**Niski**
Pomoc społeczna	Niski	**Niski**	**Niski**
Odszkodowania	Niski	**Niski**	**Niski**
Egzekwowanie prawa			
Ściganie w sprawach karnych	Niski	Niski	**Umiarkowany**
Dochodzenia i śledztwa	Umiarkowany	Umiarkowany	Umiarkowany
Ochrona obywateli	Umiarkowany	Umiarkowany	Umiarkowany
Ochrona rządu	Umiarkowany	Niski	Niski
Ochrona własności	Niski	Niski	Niski
Kontrola substancji	Umiarkowany	Umiarkowany	Umiarkowany
Zapobieganie przestępczości	Niski	**Niski**	Niski
Kontrola obrotu	**Umiarkowany**	Umiarkowany	**Umiarkowany**
Postępowania sądowe i arbitrażowe			
Procesy sądowe	Umiarkowany	**Niski**	Niski
Obrona prawna	Umiarkowany	Wysoki	Niski
Dochodzenie prawne	Umiarkowany	Umiarkowany	Umiarkowany
Prokuratura i spory sądowe	Niski	Umiarkowany	Niski
Postępowanie arbitrażowe	Umiarkowany	**Niski**	**Niski**
Więziennictwo i resocjalizacja			

	Poufność	Integralność	Dostępność
Sprawy więziennictwa	**Niski**	Umiarkowany	Niski
Resocjalizacja przestępców	Niski	**Niski**	**Niski**
Nauka i innowacyjność			
Badania naukowe i technologiczne oraz innowacje	Niski	**Umiarkowany**	**Niski**
Eksploracja kosmosu i innowacje	Niski	**Umiarkowany**	**Niski**
Tworzenie i zarządzanie wiedzą			
Badania i rozwój	Niski	**Umiarkowany**	**Niski**
Statystyka publiczna	Niski	**Niski**	**Niski**
Doradztwo i konsultacje	Niski	**Niski**	**Niski**
Upowszechnianie wiedzy	Niski	Niski	Niski
Zgodność i egzekwowanie przepisów			
Kontrole i audyty	Umiarkowany	**Umiarkowany**	**Niski**
Standaryzacja	**Niski**	**Niski**	**Niski**
Zgody i licencje	Niski	**Niski**	**Niski**
Tworzenie i zarządzanie dobrami publicznymi			
Produkcja	**Niski**	**Niski**	**Niski**
Budowa	Niski	**Niski**	**Niski**
Zarządzanie zasobami publicznymi, zarządzanie infrastrukturą	Niski	**Niski**	Niski
Zarządzanie infrastrukturą informatyczną	Niski	Niski	Niski
Pomoc publiczna			
Dotacje państwowe	Niski	Niski	**Niski**
Bezpośredni transfer środków do podmiotów	Niski	Niski	Niski

	Poufność	Integralność	Dostępność
Ulgi podatkowe	Niski	**Niski**	**Niski**
Dotacje państwowe	**Umiarkowany**	**Niski**	**Niski**
Kredyty i ubezpieczenia			
Kredyty bezpośrednie	Niski	Niski	**Niski**
Poręczenia kredytowe	Niski	**Niski**	**Niski**
Ogólne ubezpieczenia	Niski	**Niski**	Niski
Przepływy finansowe Rząd - JST			
Dotacje	Niski	**Niski**	**Niski**
Dofinansowanie projektów	Niski	**Niski**	**Niski**
Dotacje celowe	Niski	**Niski**	**Niski**
Pożyczki rządowe	**Niski**	**Niski**	**Niski**
Bezpośrednie usługi dla obywateli			
Operacje wojskowe[17]	**N/D**	**N/D**	**N/D**
Operacje cywilne	**N/D**	**N/D**	**N/D**

B.1. OBRONA I BEZPIECZEŃSTWO NARODOWE

Operacje obronne i bezpieczeństwa narodowego chronią i wspierają interesy bezpieczeństwa narodowego Rzeczypospolitej Polskiej, a jeśli środek odstraszający zawodzi, zdecydowanie pokonują zagrożenia dla tych interesów. Działania w zakresie obrony i bezpieczeństwa narodowego obejmują operacje wojskowe, ochronę granic i gromadzenie danych wywiadowczych. Operacje obronne dzielą się na następujące elementy:

- **Poziom strategiczny** – Ustanawianie krajowych i wielonarodowych celów wojskowych, ustalanie kolejności inicjatyw, określanie limitów i ocena ryzyka wykorzystania sił zbrojnych i innych instrumentów władzy państwowej,

[17] Jako sposób świadczenia usług wynikających z zadań, kategoryzacja bezpieczeństwa funkcji „Bezpośrednie usługi dla obywateli" podfunkcje Operacje wojskowe i Operacja cywilna jest uzależniona od usług związanych z usługami świadczonymi obywatelom ([np. opieka zdrowotna, reagowanie w nagłych wypadkach, rekultywacja środowiska) powinny być kategoryzowane zgodnie z rodzajem informacji wynikających z tych zadań.

opracowywanie planów obronnych dla osiągnięcia tych celów oraz zapewnienie zasobów militarnych i innych zdolności zgodnie z planami strategicznymi;

- **Poziom operacyjny** – łączenie taktyki i strategii poprzez ustanowienie celów operacyjnych niezbędnych do osiągnięcia celów strategicznych, sekwencjonowanie zdarzeń w celu osiągnięcia celów operacyjnych, inicjowanie działań i stosowanie zasobów w celu doprowadzenia do tych zdarzeń i podtrzymania ich efektów;
- **Poziom taktyczny** – uporządkowany układ i manewr elementów bojowych w stosunku do siebie i do przeciwnika w celu osiągnięcia celów bojowych.

Skutki dla informacji i systemów informatycznych związanych z zadaniami obronnymi i bezpieczeństwa narodowego mogą mieć wpływ na bezpieczeństwo szerokiej gamy infrastruktur krytycznych i kluczowych zasobów krajowych. Systemy, które obejmują dowodzenie i kierowanie siłami zbrojnych, kontrolę nad bronią, sprzętem stanowiącym integralną część broni lub systemami uzbrojenia, mają zasadnicze znaczenie dla bezpośredniej realizacji misji wojskowych lub są w inny sposób wykorzystywane w operacjach ściśle wojskowych, są zdefiniowane w prawie jako krajowe systemy bezpieczeństwa. Informacje dotyczące bezpieczeństwa narodowego i krajowe systemy bezpieczeństwa nie są objęte zakresem niniejszych wytycznych. Cele w zakresie bezpieczeństwa i poziomy wpływu związane z tymi systemami są określane przez Ministerstwo Obrony Narodowej.

B.2. BEZPIECZEŃSTWO WEWNĘTRZNE

Bezpieczeństwo Wewnętrzne polega na ochronie państwa przed atakami terrorystycznymi. Obejmuje to analizę zagrożeń i danych wywiadowczych, ochronę granic i lotnisk, ochronę infrastruktury krytycznej oraz koordynację reagowania w sytuacjach kryzysowych. Zadania Bezpieczeństwa Wewnętrznego są zdefiniowane przez Strategię Bezpieczeństwa Narodowego i ustawy.

B.3. OPERACJE WYWIADOWCZE

Operacje wywiadowcze polegają na opracowywaniu i zarządzaniu wiarygodnymi, kompleksowymi i terminowymi danymi wywiadu zagranicznego na tematy związane

z bezpieczeństwem narodowym. Systemy informatyczne, ich funkcja, działanie lub wykorzystanie, które wiążą się z działalnością wywiadowczą lub mają zasadnicze znaczenie dla bezpośredniej realizacji misji wywiadowczych, są zdefiniowane w prawie jako systemy bezpieczeństwa narodowego. Informacje dotyczące bezpieczeństwa narodowego i krajowe systemy bezpieczeństwa nie są objęte zakresem niniejszych wytycznych. Cele bezpieczeństwa i poziomy wpływu związane z krajowymi systemami bezpieczeństwa są określane przez kierownika jednostki organizacyjnej sprawującego kontrolę nad systemem.

B.4. ZARZĄDZANIE KRYZYSOWE

Zarządzanie kryzysowe obejmuje działania niezbędne do przygotowania, złagodzenia, reagowania i naprawy skutków wszystkich klęsk żywiołowych i humanitarnych, zarówno naturalnych, jak i spowodowanych przez człowieka.

Kompromitacja wielu informacji związanych z którymkolwiek z zadań w ramach obszaru objętego misją zarządzania kryzysowego może mieć poważny wpływ na bezpieczeństwo szerokiej gamy krytycznej infrastruktury i kluczowych zasobów krajowych.

B.5. SPRAWY ZAGRANICZNE I HANDEL MIĘDZYNARODOWY

Sprawy zagraniczne i handel międzynarodowy obejmują działania pozamilitarne, które promują politykę i interesy Rzeczypospolitej Polskiej poza naszymi granicami krajowymi, w tym negocjacje w sprawie rozwiązywania konfliktów, ustanawiania traktatów i umów. Ponadto funkcja ta obejmuje: zagraniczny rozwój gospodarczy i rozwój społeczny/polityczny; stosunki dyplomatyczne z innymi państwami; pomoc humanitarną, techniczną i inną pomoc rozwojową dla innych państw; oraz handel światowy. Informacje, które są chronione przez procedury ustanowione i przyjęte na podstawie kryteriów określonych w przepisach prawa, które mają być utrzymywane w tajemnicy w interesie polityki zagranicznej, są związane z bezpieczeństwem narodowym. Cele bezpieczeństwa i poziomy wpływu związane z takimi informacjami dotyczącymi bezpieczeństwa narodowego są określane przez ministra sprawującego kontrolę nad systemem i znajdują się poza zakresem niniejszych wytycznych.

B.6. ZASOBY NATURALNE

Obszar zadań "Zasoby naturalne" obejmuje wszystkie działania związane z planowaniem ochrony, zarządzaniem gruntami, turystyką i zabytkami, które mają wpływ na zasoby naturalne i rekreacyjne kraju, zarówno prywatne jak i publiczne. Uwaga: Zasoby naturalne związane z energią są objęte obszarem objętym zadania "Zarządzanie energią".

B.7. ENERGIA

Obszar zadań „Energia" odnosi się do wszystkich działań podejmowanych przez rząd w celu zapewnienia zamówień i zarządzania zasobami energetycznymi, w tym produkcją, sprzedażą i dystrybucją energii, jak również zarządzania zasobami zużytego paliwa. Zarządzanie energią obejmuje wszystkie rodzaje energii produkowanej masowo (np. hydroelektryczną, jądrową, wiatrową, słoneczną lub z paliw kopalnych). W tym obszarze zadań znajduje się również nadzór nad przedsiębiorcami prywatnymi.

B.8. ZARZĄDZANIE ŚRODOWISKIEM

Zarządzanie środowiskowe obejmuje wszystkie funkcje wymagane do określenia odpowiednich standardów środowiskowych i zapewnienia zgodności w tym obszarze.

B.9. ROZWÓJ EKONOMICZNY

Rozwój gospodarczy obejmuje działania niezbędne do promowania rozwoju handlowego/przemysłowego oraz do uregulowania polskiego sektora finansowego w celu ochrony inwestorów. Obejmuje on również zarządzanie i kontrolę gospodarki krajowej oraz podaży pieniądza, a także ochronę własności intelektualnej i innowacji. Uwaga: Promocja polskiej przedsiębiorczości za granicą została ujęta w funkcji "Sprawy zagraniczne i handel międzynarodowy".

B.10. USŁUGI SPOŁECZNE I SOCJALNE

Usługi społeczne i socjalne obejmują wszelkie działania mające na celu tworzenie, rozszerzanie lub poprawę rozwoju społecznego i społeczności lokalnych, stosunków społecznych i usług socjalnych w Polsce. Obejmuje to wszelkie działania mające na celu lokalny lub ogólnokrajowy rozwój społeczny i ogólne usługi socjalne oraz ogólne programy

rozwoju społeczności lokalnych i usług socjalnych, jak również programy zarobkowych i niezarobkowych świadczeń, które promują te cele.

B.11. TRANSPORT

Transport obejmuje wszystkie rządowe działania związane z bezpiecznym przejazdem, przewozem lub transportem towarów lub osób. Należy pamiętać, że wpływ na niektóre informacje i wiele systemów informatycznych związanych z działalnością transportową może mieć wpływ nie tylko na bezpieczeństwo infrastruktury transportowej, ale także na szeroką gamę innych krytycznych infrastruktur i kluczowych zasobów krajowych.

B.12. EDUKACJA

Edukacja odnosi się do tych działań, które przekazują społeczeństwu wiedzę lub zrozumienie danego przedmiotu. Edukacja może odbywać się w formalnej szkole, kolegium, na uniwersytecie lub w innym programie szkoleniowym. Ten obszar zadań obejmuje wszystkie programy rządowe, które promują edukację społeczeństwa, w tym zarówno programy realizowane zarobkowo, jak i niezarobkowo.

B.13. SPRAWY PRACY

Zarządzanie siłą roboczą obejmuje te działania, które wspierają dobrostan i efektywność siły roboczej poprzez poprawę jej umiejętności, warunków pracy, zwiększanie możliwości rentownego zatrudnienia i wzmacnianie swobodnych negocjacji zbiorowych.

B.14. ZDROWIE

Zdrowie publiczne obejmuje rządowe programy i działania, których zadaniem jest zapewnienie zdrowia i dobrego samopoczucia społeczeństwa. Zadania te obejmują bezpośrednie świadczenie usług zdrowotnych i szczepień ochronnych, jak również monitorowanie i śledzenie wskaźników zdrowia publicznego w celu wykrywania trendów i identyfikacji powszechnych chorób / zachorowań. Obejmuje to również programy świadczeń zdrowotnych zarówno zarobkowych, jak i niezarobkowych. Należy zauważyć, że wpływ na niektóre informacje i systemy informatyczne dotyczące zdrowia publicznego może mieć wpływ na bezpieczeństwo krytycznych elementów infrastruktury zdrowia publicznego.

B.15. ZABEZPIECZENIE SPOŁECZNE

Zabezpieczenie społeczne obejmuje działania mające na celu zapewnienie członkom społeczeństwa niezbędnych środków - zarówno finansowych, jak i innych - do utrzymania odpowiedniego poziomu życia. Obejmuje to wszystkie programy świadczeń, zarówno te zarobkowe, jak i niezarobkowe, które realizują te cele dla członków społeczeństwa.

B.16 EGZEKWOWANIE PRAWA

Egzekwowanie prawa obejmuje ochronę ludzi, miejsc i rzeczy przed działalnością przestępczą wynikającą z nieprzestrzegania prawa. Obejmuje to patrole, tajne operacje, reagowanie na wezwania alarmowe, a także aresztowania, interwencje i konfiskaty mienia. Wpływ na niektóre informacje i systemy informatyczne związane z zadaniami w zakresie egzekwowania prawa może mieć także wpływ na bezpieczeństwo szerokiej gamy krytycznej infrastruktury i kluczowych zasobów krajowych. Niektóre informacje związane z egzekwowaniem prawa na szczeblu rządowym są klasyfikowane jako informacje dotyczące bezpieczeństwa narodowego. Zasady regulujące ustanawianie poziomów wpływu i kontroli związanych z informacjami dotyczącymi bezpieczeństwa narodowego są regulowane przez oddzielny zestaw polityk i nie wchodzą w zakres niniejszych wytycznych. Wpływ na poufność i integralność jest często określany przez wymagania ustawowe i regulacyjne, które różnią się w zależności od ich istoty od ustaleń niniejszych wytycznych.

B.17. POSTĘPOWANIA SĄDOWE I ARBITRAŻOWE

Działalność sądowa obejmuje wszystkie działania w zakresie wymiaru sprawiedliwości.

B.18. WIĘZIENNICTWO I RESOCJALIZACJA

Działania w obszarze „Więziennictwo i resocjalizacja" obejmują wszystkie działania rządowe, które zapewniają skuteczne uwięzienie i resocjalizację skazanych przestępców.

B.19. NAUKA I INNOWACYJNOŚĆ

Działania w obszarze „Nauka i innowacyjność" obejmują wszystkie działania rządowe mające na celu zaspokojenie krajowej potrzeby rozwoju wiedzy w tym obszarze. Obejmuje to ogólne programy badawcze i technologiczne, działania związane z badaniem kosmosu oraz inne

programy badawcze i technologiczne, które mają różne cele i nie mogą być łatwo sklasyfikowane w innym obszarze zadań lub innych rodzajach informacji.

B.20. TWORZENIE I ZARZĄDZANIE WIEDZĄ

Tworzenie i zarządzanie wiedzą obejmuje programy i działania, w ramach których rząd tworzy lub rozwija treści lub zbiór wiedzy, których przetwarzanie i analiza może przynieść nieodłączne korzyści zarówno dla sektora publicznego, jak i prywatnego.

B.21. ZGODNOŚĆ I EGZEKWOWANIE PRZEPISÓW

Zgodność z przepisami i ich egzekwowanie wiąże się z bezpośrednim monitorowaniem i nadzorem nad konkretną osobą, grupą, branżą lub społecznością uczestniczącą w działalności regulowanej za pomocą mechanizmów rynkowych, funkcji kierowania i kontroli lub innych środków zarządzania postępowaniem lub zachowaniem.

B.22. TWORZENIE I ZARZĄDZANIE DOBRAMI PUBLICZNYMI

Budowa, produkcja, administracja i zarządzanie towarami, strukturami, obiektami, wspólnymi zasobami itp. wykorzystywanymi dla ogólnego dobra całego społeczeństwa.

B.23. POMOC PUBLICZNA

Publiczna Pomoc Finansowa to zapewnianie różnym podmiotom świadczeń finansowych, zarówno na cele zarobkowe, jak na cele niezarobkowe.

B.24. KREDYTY I UBEZPIECZENIA

Kredyty i ubezpieczenia obejmują wykorzystanie funduszy rządowych na pokrycie kosztów dotacji do bezpośredniej pożyczki lub gwarancji kredytowej lub na ochronę członków społeczeństwa przed stratami finansowymi.

B.25. PRZEPŁYWY FINANSOWE RZĄD – JEDNOSTKI SAMORZĄDU TERYTORIALNEGO

Przepływy finansowe do samorządów terytorialnych obejmują przekazywanie funduszy lub pomocy finansowej przez rząd do samorządu.

D.26. BEZPOŚREDNIE USŁUGI DLA OBYWATELI

Bezpośrednie usługi dla obywateli odnoszą się do dostarczania towarów lub usług dla obywateli przez rząd bez udziału innych osób, warunków lub organizacji.

ZAŁĄCZNIK C REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych – na podstawie FIPS 200
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53A	Ocena środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informatycznych oraz organizacji – na podstawie NIST SP 800-53B
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informatycznego – na podstawie NIST SP 800-60

STANDARDS, AND GUIDELINES	
FIPS 199	*Standards for Security Categorization of Federal Information and Information Systems*, February 2004
FIPS 200	*Minimum Security Requirements for Federal Information and Information Systems*, March 2006
NIST SP 800-18	*Guide for Developing Security Plans for Federal Information Systems*, February 2006
NIST SP 800-30	*Risk Management Guide for Information Technology Systems*, July 2002
NIST SP 800-34	*Contingency Planning Guide for Information Technology Systems*, June 2002
NIST SP 800-37	*Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004
NIST SP 800-39	*Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011
NIST SP 800-53	*Security and Privacy Controls for Information Systems and Organizations*, September 2020
NIST SP 800-53A	*Guide for Assessing the Security Controls in Federal Information Systems*, December 2014
NIST SP 800-59	*Guideline for Identifying an Information System as a National Security System*, August 2003
NIST SP 800-64	*Security Considerations in the Information System Development Life Cycle*, June 2004.