**Polityka Bezpieczeństwa Informacji dla Węzła Krajowego**

**(wyciąg)**

Metryka dokumentu

| Właściciel | Minister właściwy do spraw informatyzacji | | | | |
| --- | --- | --- | --- | --- | --- |
| Tryb zatwierdzenia: | Dokument zatwierdza Dyrektor, Ministerstwo Cyfryzacji | | | | |
| Stan | Zatwierdzony | | | Daty obowiązywania |  |
| Założenia | Dokument stanowi załącznik do Polityki Bezpieczeństwa Informacji WK | | | | |
| Adresaci | Uprawnieni Interesariusze systemu WK | | | | |
| Historia dokumentu | Wersja | Data | Autor | | Opis zmian |
| 1.0 | 16.07.2018 | Zespół ZBS/COI | | Utworzenie dokumentu |
| 2.0 | 29.10.2019 | Zespół MC | | Aktualizacja dokumentu (zmiana nagłówka) |
| 3.0 | 14.01.2020 | Zespół MC | | Aktualizacja dokumentu (zmiana numeru załącznika) |

Spis treści

[1. Cel 4](#_Toc525035611)

[2. Odpowiedzialność 4](#_Toc525035612)

[3. Definicje i skróty 4](#_Toc525035613)

[4. Wyciąg z Polityki Bezpieczeństwa Informacji dla Węzła Krajowego 6](#_Toc525035614)

[4.1. Zgodność prawna 6](#_Toc525035615)

[4.2. Opis systemu 7](#_Toc525035616)

[4.3. Zapewnienie bezpieczeństwa informacji 7](#_Toc525035617)

[4.4. Aktywa systemu 8](#_Toc525035618)

[4.5. Klasyfikacja i postępowanie z informacją 8](#_Toc525035619)

[4.6. Kontrola dostępu do informacji 10](#_Toc525035620)

[4.7. Obsługa nośników zawierających informacje 11](#_Toc525035621)

[4.8. Bezpieczeństwo fizyczne lub środowiskowe 13](#_Toc525035622)

[4.9. Zarządzanie ryzykiem 14](#_Toc525035623)

[4.10. Postepowanie z incydentami bezpieczeństwa informacji 15](#_Toc525035624)

[4.11. Monitoring i nadzór 16](#_Toc525035625)

# **Cel**

Celem niniejszego dokumentu jest wskazanie najważniejszych zasad obowiązujących w zakresie zarządzania bezpieczeństwem informacji Węzła Krajowego (WK), wynikających z Polityki Bezpieczeństwa Informacji dla Węzła Krajowego.

Przedmiotem dokumentu jest określenie kluczowych zasad dotyczących zapewnienia bezpieczeństwa informacji (danych) systemu Węzła Krajowego, obejmujących zabezpieczenia:

1. Organizacyjne obszaru zawierającego dane (informacje) podlegające ochronie,
2. Techniczne systemów informacyjnych zawierających dane podlegające ochronie.

w zakresie:

1. Aktywów systemu,
2. Klasyfikacji informacji,
3. Postępowania z informacją,
4. Kontroli dostępu do informacji,
5. Obsługi nośników zawierających informacje,
6. Bezpieczeństwa fizycznego i środowiskowego,
7. Postępowania z incydentami bezpieczeństwa informacji,
8. Zarządzanie ryzykiem,
9. Monitoringu i nadzoru.

# **Odpowiedzialność**

Niniejszy dokument stanowi wyciąg z Polityki Bezpieczeństwa Informacji dla Węzła Krajowego, przestrzeganie jego postanowień dotyczy wszystkich Interesariuszy systemu WK. Wszyscy Interesariusze, w szczególności ich pracownicy, współpracownicy mają obowiązek zapoznania się z treścią tego dokumentu.

# **Definicje i skróty**

**Aktywa** – sprzęt, oprogramowanie, bazy danych lub urządzenia wspomagające wykorzystywane przez System teleinformatyczny do jego prawidłowego funkcjonowania lub zabezpieczenia go.

**Analiza ryzyka** – oszacowanie prawdopodobieństwa oraz skutków zaistnienia zidentyfikowanego ryzyka.

**Audy**t – niezależna i obiektywna ocena (np. przedsiębiorstwa, procesów, procedur, polityk) zgodności z zadanymi parametrami bądź wskaźnikami (np. przepisy prawa, dobre praktyki, normy).

**Audyt wewnętrzny** – jest działalnością niezależną i obiektywną, której celem jest wniesienie wartości dodanej i usprawnienie działalności operacyjnej organizacji. Polega na systematycznej i dokonywanej w uporządkowany sposób ocenie procesów: zarządzania ryzykiem, kontroli i ładu organizacyjnego,  
i przyczyniania się do poprawy ich działania.

**Dane identyfikujące osobę** – zestaw danych umożliwiających ustalenie tożsamości osoby fizycznej.

**Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

**Dokument elektroniczny** – oznacza każdą treść przechowywaną w postaci elektronicznej,  
w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne.

**Gestor systemu** – upoważniony przedstawiciel właściciela systemu WK.

**Incydent bezpieczeństwa** – zdarzenie zaburzające lub mogące zaburzyć poprawność przebiegu procesu (np. czynności, działania systemu, procesu biznesowego) o istotnym znaczeniu.

**Informacja** – zbiór określonych, spójnych danych.

**Interesariusz** – osoba bądź jednostka organizacyjna, która wpływa bądź może wpływać na określony zasób (np. proces, projekt, procedurę, system).

**ITSM** – system zarządzania zgłoszeniami.

**Kod źródłowy** – zapis programu komputerowego przy pomocy określonego języka programowania.

**Kryptografia** – przekazywanie informacji w sposób zabezpieczony przed niepowołanym dostępem.

**Najwyższe kierownictwo** – właściciel systemu.

**Nośnik Informacji** – dowolny nośnik umożliwiający przechowywanie informacji.

**PBI –** Polityka Bezpieczeństwa Informacji.

**Procedury eksploatacyjne** – opisanie czynności (instrukcja) oficjalnie obowiązujące w celu usprawnienia prowadzenia określonego procesu (np. procedury, instrukcje obsługi).

**Proces biznesowy** – logiczny ciąg działań mający na celu dostarczenie produktu lub usługi. Proces biznesowy realizowany jest w podziale na operacje wykonywane w wyodrębnionych komórkach  
i stanowiskach.

**Właściciel systemu** – Minister właściwy do spraw informatyzacji.

# **Wyciąg z Polityki Bezpieczeństwa Informacji WK**

# Zgodność z prawem

Akty prawne, będące otoczeniem prawnym dla Węzła Krajowego:

1. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej;
2. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
3. Rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie profilu zaufanego i podpisu zaufanego;
4. Rozporządzenie Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników;
5. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
6. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r.;  
   w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym;
7. Rozporządzenie wykonawcze Komisji (UE) 2015/1501 z dnia 8 września 2015 r.   
   w sprawie ram interoperacyjności na podstawie art. 12 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania  
   w odniesieniu do transakcji elektronicznych na rynku wewnętrznym;
8. Decyzja wykonawcza Komisji (UE) 2015/1984 z dnia 3 listopada 2015 r. w sprawie określenia okoliczności, formatów i procedur notyfikacji zgodnie z art. 9 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania  
   w odniesieniu do transakcji elektronicznych na rynku wewnętrznym;
9. Decyzja wykonawcza Komisji (UE) 2015/296 z dnia 24 lutego 2015 r. ustanawiająca proceduralne warunki współpracy między państwami członkowskimi w zakresie identyfikacji elektronicznej na podstawie art. 12 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014  
   w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

# Opis systemu

Węzeł Krajowy jest punktem styku między krajowymi dostawcami środków identyfikacji, jak  
i dostawcami usług korzystających z mechanizmu identyfikacji tożsamości. W procesie uwierzytelnienia mogą także brać udział inne węzły realizujące określone funkcje, na przykład Węzeł Transgraniczny (WT) pełniący rolę pośrednika w połączeniach z/do Unii Europejskiej czy tak zwany Węzeł Komercyjny obsługujący podmioty komercyjne.System WK jest budowany w oparciu o sprawdzone i bezpieczne rozwiązania technologiczne, z zachowaniem wszelkich wymogów bezpieczeństwa z zakresu wytwarzania i eksploatacji systemów IT. Systemy informatyczne zintegrowane z systemem informatycznym – centralnym WK, budowane są w sposób nadmiarowy, instalowane w odpowiednio przygotowanych lokalizacjach, zgodnie z wytycznymi PBI. Środowiska te są budowane z dbałością  
o bezpieczeństwo użytkownika końcowego, ze szczególnym uwzględnieniem jego danych osobowych czy poufnych informacji uwierzytelniających.

# Zapewnienie bezpieczeństwa informacji

Proces zarządzania bezpieczeństwem informacji jest działaniem realizowanym w sposób ciągły,  
w oparciu o podejście systemowe zapewniające w sposób uniwersalny adekwatność stosowanych środków ochrony informacji. Wszystkie czynności realizowane w tym procesie podlegają dokumentowaniu oraz cyklicznemu przeglądowi oraz są na bieżąco monitorowane. Zapewnienie ochrony informacji jest realizowane w wielu płaszczyznach jednocześnie zarówno w zakresie organizacyjnym jak i technicznym.

Wszyscy Interesariusze systemu WK wnoszą wkład w zapewnienie jego bezpieczeństwa w zakresie informacji (danych).

Najwyższe kierownictwo – Minister właściwy ds. informatyzacji oświadcza, że będzie dbał   
o zapewnienie wysokiego poziomu bezpieczeństwa przetwarzania informacji w Krajowym Węźle Identyfikacji Elektronicznej, w oparciu o obowiązujące przepisy prawa, odpowiednie normy, jak również w oparciu o dobre praktyki z dziedziny bezpieczeństwa informacji.

Wszelkie działania operacyjne w zakresie zarządzania systemem bezpieczeństwa informacji pozostają w zakresie odpowiedzialności Gestora systemu WK.

# Aktywa systemu

Aktywa systemu związane z bezpieczeństwem informacji oraz środkami przetwarzania informacji są zidentyfikowane oraz jest sporządzona i na bieżąco aktualizowana ich ewidencja. W ramach aktywów ewidencjonowaniu podlegają procesy biznesowe, repozytoria danych oraz pozostałe zasoby  
(np. zasoby ludzkie czy sprzęt). Dla każdego z aktywów określono właścicieli i użytkowników oraz zakres ich dopuszczalnego użycia.

# Klasyfikacja i postępowanie z informacją

Procedura oznaczania informacji opiera się o zasadę oceny konsekwencji udostępnienia informacji podlegających ochronie. Oznaczanie informacji polega modelowo na podziale informacji na informację publiczną oraz informacje podlegające szczególnej ochronie. W przypadku centrów przetwarzania danych (datacenter) należy mieć na uwadze, że głównym obszarem podlegającym klasyfikacji informacji są repozytoria danych, przechowujące informacje w postaci znormalizowanej (bazy danych) czy rozproszonej (systemy plików).

Żaden „dokument roboczy”, czyli będący w trakcie tworzenia, nie może zostać upubliczniony na żadnym etapie jego opracowywania.

Przyjęto następujące zasady klasyfikacji informacji:

1. Informacja publiczna,
2. Informacja chroniona (dane osobowe, tajemnica przedsiębiorstwa, tajemnica branżowa),
3. Informacja niejawna.

Klasyfikacja dotyczy informacji zapisanych na dowolnych nośnikach danych, w szczególności:

1. Nośniki elektroniczne (np. dyski, karty pamięci),
2. Nośniki papierowe (np. karki papieru, klisze),
3. Informacje przekazywane werbalnie (mowa, gesty).

Każda sklasyfikowana informacja podlega odpowiednim zasadom w zakresie jej oznaczania:

1. Oznaczenie „informacja publiczna” lub wyraźne oznaczenie potwierdzające zatwierdzenie dokumentu, dotyczy informacji publicznie dostępnych bez specjalnych ograniczeń,
2. Oznaczenie „Dane osobowe” dotyczy informacji zawierających dane osobowe,
3. Oznaczenie „Tajemnica przedsiębiorstwa” dotyczy informacji będących tajemnicą własnego przedsiębiorstwa (nie dotyczy instytucji publicznych) lub przedsiębiorstwa kontrahenta,
4. Informacje niejawne – obsługa prowadzona zgodnie z wymaganiami ustawy o ochronie informacji niejawnych.

Postępowanie z informacją, która została poddana procedurze klasyfikacji oraz oznaczania:

1. Informacje oznaczone jako „informacja publiczna” mogą zostać upublicznione,
2. Informacje oznaczone jako dane osobowe lub tajemnica przedsiębiorstwa nie mogą być upubliczniane (tylko w szczególnych przypadkach, gdy informacje podlegające ochronie zostaną usunięte lub zamazane dopuszczalne jest ich upublicznienie),
3. Informacje niejawne nie mogą zostać upublicznione, a ich użycie wewnętrzne może odbywać się tylko w zgodzie z przepisami ustawy o ochronie informacji niejawnych.

# Kontrola dostępu do informacji

**Dostęp fizyczny**

Zarówno miejsca instalacji systemu WK, jak i systemów z nim zintegrowanych podlegają zasadom regulacji dostępu fizycznego, zapobiegającym nieuprawnionemu dostępowi fizycznemu do obiektów oraz zasobów tam zainstalowanych i są regulowane odpowiednimi przepisami wewnętrznymi Interesariuszy.

**Dostęp informatyczny w zakresie integracji z systemem WK**

Integracja między systemem informatycznym – centralnym WK, a dołączanym systemem innego Interesariusza realizowana jest z uwzględnieniem następujących zasad:

1. Spełnienie warunków formalnych oraz technicznych opisanych powyżej (decyzja oraz zasady integracji),
2. Generacja certyfikatów dla integrowanych systemów do obsługi usług sieciowych realizujących technicznie proces integracji,
3. Generacja kluczy i certyfikatów niezbędnych do integracji sieciowej systemów wraz z poufnymi informacjami uwierzytelniającymi (np. numer PIN),
4. Wymiana między Gestorem systemu WK i Interesariuszem odpowiednich certyfikatów i kluczy niezbędnych do zapewnienia bezpieczeństwa informacji poprzez realizację rozliczalności oraz niezaprzeczalności transakcji,
5. Weryfikacja skuteczności integracji oraz ocena wpływu na działanie systemu WK.

Dostęp do zasobów systemu WK lub systemu z nim zintegrowanego podlega zawieszeniu w sytuacji wydania przez Ministra właściwego do spraw informatyzacji decyzji o zawieszeniu możliwości korzystania z danego systemu zintegrowanego z systemem informatycznym – centralnym WK.

Dostęp do zasobów systemu WK lub systemu z nim zintegrowanego jest odbierany w sytuacji wydania przez Ministra właściwego do spraw informatyzacji decyzji o zawieszeniu możliwości korzystania  
z danego systemu zintegrowanego na podstawie odpowiednich przepisów prawa.

**Dostęp informatyczny w zakresie dostępu uprzywilejowanego**

Procedura kontroli (zarządzania) dostępu do systemu WK realizowanego w ramach właściwości Interesariuszy wymaga miedzy innymi:

1. Potwierdzenia znajomości Polityki Bezpieczeństwa Informacji,
2. Zastosowania zabezpieczeń kryptograficznych,
3. Rozliczalności dostępu,
4. Zgody uprawnionych przedstawicieli Interesariuszy,
5. Posiadania poufnych informacji uwierzytelniających,
6. W przypadku pracy zdalnej wymagane są dodatkowe zabezpieczenia takie jak na przykład: szczególna zgoda uprawnionych przedstawicieli Interesariusza, bezpieczne połączenia,  
   np. VPN.

**Dostęp informatyczny w zakresie uprzywilejowanych programów narzędziowych**

Przez użycie uprzywilejowanych programów narzędziowych określono proces wykorzystywania oprogramowania specjalistycznego, narzędziowego, którego użycie nie podlega lub podlega  
w stopniu znacznie ograniczonym mechanizmom kontroli dostępu oraz jakimkolwiek zabezpieczeniom – na przykład specjalny dostęp bezpośrednio do bazy danych, bezpośredni dostęp do pamięci masowej (plików) czy podłączenie dedykowanych programów nadzorujących (PIM, systemy raportowe). Użycie takich narzędzi wymaga specjalnego nadzoru oraz odpowiednich zgód osób uprawnionych u Interesariusza.

**Kontrola i przegląd uprawnień**

W celu zapewnienia skuteczności procesu nadawania, zmiany i odbierania dostępu do systemów informatycznych WK, obowiązkiem Interesariuszy jest przeprowadzać przeglądy nadanych uprawnień do systemów WK w zakresie swojego odziaływania.

# Obsługa nośników zawierających informacje

**Postać papierowa (lub pokrewne)**

Cykl życia użytych nośników papierowych jest pochodną rodzaju informacji naniesionych na te nośniki i co za tym idzie, podlega wszelkim wytycznym dotyczącym obsługi tych informacji, zgodnie  
z obowiązującymi w tym zakresie wytycznymi dotyczącymi klasyfikacji informacji. Okres przechowywania użytych nośników (z naniesioną informacją) jest regulowany odpowiednimi przepisami prawa, a w przypadku gdy nie mają zastosowania określone przepisy prawa przyjmuje się, że dane powinny być przechowywane w sposób odpowiednio zabezpieczony przez okresnie krótszy niż 2 lata od momentu ustania przyczyny, dla której zostały wytworzone. Po ustalonym okresie musi zostać niezwłocznie podjęta decyzja w zakresie dalszego postepowania z tym nośnikiem tj. jego archiwizacji lub zniszczeniu.

**Postać elektroniczna**

Każdy cyfrowy nośnik informacji przed przekazaniem go do eksploatacji powinien być odpowiednio zewidencjonowany (w oparciu co najmniej o numer seryjny, nazwę oraz typ) przez Interesariusza.

Przyjęto, że wszystkie rodzaje nośników umieszczonych w systemie informatycznym – centralnym WK jak i systemach z nim zintegrowanych, zawierają dane podlegające szczególnej ochronie, mającej na celu zapewnienie ich bezpieczeństwa. Nośniki cyfrowe użyte w systemie WK muszą być zabezpieczone  
w sposób uniemożliwiający dostęp do nich przez osoby nieupoważnione, poprzez ograniczenie dostępu fizycznego do serwerowni - miejsca jego zainstalowania.

Administratorzy, uprzywilejowani użytkownicy, wykonują czynności związane z obsługą informatyczną systemu WK, prowadzone z siedziby uprawnionych Interesariuszy. W trakcie prowadzonych prac używane są urządzenia IT będące cyfrowymi nośnikami danych (na przykład: karty pamięci, karty SIM, pendrive, certyfikaty fizyczne) lub urządzenia wykorzystujące takie nośniki (na przykład: komputery przenośne, karty pamięci, smartfony). Nośniki te podlegają szczególnej ochronie i muszą być wyposażone na poziomie warstwy danych (np. system plików, możliwość komunikacji) w mechanizm zabezpieczenia kryptograficznego lub umożliwiać zastosowanie innych mechanizmów zabezpieczenia danych (na przykład: szyfrowanie plików, kompresja z hasłem).

Po zakończeniu eksploatacji nośnik powinien zostać nieodwracalnie zniszczony – zlikwidowany, przy użyciu urządzeń oraz oprogramowania podanego w załączniku nr 2.8 do Polityki Bezpieczeństwa Informacji Węzła Krajowego.

Uwaga: Nie podlegają procedurze likwidacji nośniki stanowiące dowody w sprawie lub zabezpieczone w ramach zabezpieczania informacji, które mogą stanowić materiał dowodowy.

# Bezpieczeństwo fizyczne lub środowiskowe

**Ochrona obiektów serwerowni**

Ochrona fizyczna jest jednym z elementów kompleksowego zabezpieczenia centrum przetwarzania danych (ze szczególnym uwzględnieniem bezpieczeństwa informacji). Obiekty powinny być zaprojektowane i zabezpieczone w taki sposób, aby w przypadku próby naruszenia bezpieczeństwa, zapewnić możliwość reakcji uprawnionym służbom (np. służbie ochrony). Wszystkie systemy zapewniające bezpieczeństwo informacji w centrum przetwarzania danych WK jak i systemów z nim zintegrowanych powinny być budowane z zapewnieniem nadmiarowości ich elementów  
(np. podwójna klimatyzacja, podwójne źródło zasilania czy niezależne systemy gaśnicze czy systemy kontroli dostępu).

Ochrona środowiskowa centrum przetwarzania danych zapewnia realizację optymalnych warunków pracy urządzeń IT oraz zapewnia bezpieczeństwo i ochronę przed czynnikami środowiskowymi takimi jak pożar, zalanie, podtopienie czy zanik energii elektrycznej.

**Ochrona punktów dostępu do centrum przetwarzania danych**

Przez punkt dostępu do centrum przetwarzania danych WK rozumie się dedykowane miejsca  
w siedzibie uprawnionych Interesariuszy, z których prowadzone są pośrednio (przy wykorzystaniu sieci teleinformatycznych) prace w centrum przetwarzania WK. Miejsca te (pomieszczenia) traktowane  
są w sposób szczególny ze względu na czynności techniczne tam prowadzone tj. uprzywilejowany dostęp informatyczny do zasobów WK. Obiekty powinny być wyposażone w systemy zapewniające bezpieczeństwo informacji w centrum przetwarzania danych WK jak i systemów z nim zintegrowanych z zapewnieniem nadmiarowości ich elementów (np. podwójna klimatyzacja, podwójne źródło zasilania czy niezależne systemy gaśnicze, systemy kontroli dostępu).

Należy pamiętać o ustaleniu zasad regulujących dostęp fizyczny do pomieszczeń, urządzeń  
i nośników (np. dostęp do sprzętu komputerowego administratorów, obsługa kluczy do pomieszczeń) takie jak: zasady przyjmowania gości, zarządzanie kluczami do pomieszczeń, zasady dostępu do urządzeń (np. podczas prac serwisowych wykonywanych przez firmy zewnętrzne), szkolenie  
i uświadamianie personelu. Rejestrowane i utrwalane są wszystkie incydenty bezpieczeństwa dotyczące ochrony fizycznej i środowiskowej.

# Zarządzanie ryzykiem

Poprzez zarządzanie ryzkiem rozumie się proces, którego zadaniem jest określenie zagrożeń  
w poddawanym ocenie obszarze oraz ich minimalizacja. Polityka zarzadzania ryzykiem opiera się na metodyce zaproponowanej przez organizację ISO opisanej w dokumencie PN-ISO/IEC 27005. Celem  
w przypadku zapewnienia bezpieczeństwa informacji jest zachowanie co najmniej: poufności, integralności oraz dostępności informacji.

Proces zarządzania ryzykiem wiąże się ze stosowaniem określonych reguł we wszystkich obszarach  
i czynnościach, które mogą być zagrożone wystąpieniem określonych słabości (podatności). Działania zmierzające do obsługi danego ryzyka powinny być prowadzone cyklicznie (np. systematyczna ocena podatności systemu wraz z analizą ryzyka) jak również, jeżeli wymaga tego sytuacja – ad-hoc (np. ocena ryzyka wynikającego ze zmiany w procesie lub zmiany w oprogramowaniu). Do stosowania wynikających z dokumentu zasad zarzadzania ryzkiem obowiązani są wszyscy Interesariusze systemu WK.

Proces zarzadzania ryzkiem powinien obejmować następujące części:

1. Identyfikacja kontekstu (otoczenia) – określenie zakresu i granic oraz kryteriów: oceny, skutków i akceptacji ryzyka.
2. Szacowanie ryzyka – identyfikacja, analiza oraz ocena ryzyka.
3. Postępowanie z ryzykiem – modyfikacja, akceptacja, unikanie oraz podzielenie ryzyka.
4. Akceptacja ryzyka – ostateczna akceptacja ryzyka po zastosowaniu wszelkich działań mających na celu dopasowania ryzyka do przyjętych oczekiwań.

Przyjęto, że w pierwszej kolejności podczas prowadzenia procesów zarządzania ryzykiem należy stosować techniki jakościowe, oparte na wiedzy eksperckiej dające w dosyć szybkim okresie pogląd całościowy ocenianych aktywów, a w przypadku konieczności uzyskania większej szczegółowości uzupełnić je w wymagającym tego obszarze, przy użyciu metod ilościowych.

Wszystkie czynniki, które mogą mieć wpływ na poziom zidentyfikowanego już ryzyka, jak również powodować nowe zagrożenia, muszą podlegać procesowi monitorowania oraz przeglądu tego obszaru. Monitoringowi podlegają zarówno zabezpieczenia, w wymiarze ich wpływu na redukcję poziomu zagrożenia, czy też redukcję możliwości wykorzystania podatności, jak również same podatności i zagrożenia. Każdy przegląd powinien być udokumentowany i odbywać się, co najmniej raz do roku, jak również ad-hoc w sytuacji zmian wynikających ze specyfiki organizacji czy danego systemu IT. W procesie analizy ryzyka powinni brać udział uprawnieni przedstawiciele wszystkich uczestniczących w systemie Interesariuszy.

# Postepowanie z incydentami bezpieczeństwa informacji

**Zgłaszanie incydentów**

Każdy z Interesariuszy systemu informatycznego przy podejrzeniu wystąpienia incydentu bezpieczeństwa informacji zobowiązany jest do zgłoszenia go udostępnionymi kanałami. Zgłoszenie to może odbywać się w zależności od Interesariuszy następującymi kanałami:

1. Telefonicznie,
2. Poprzez e-mail,
3. Poprzez zgłoszenie w systemie.

**Obsługa incydentów**

Zgłoszenie podlega klasyfikacji. W przypadku kiedy zgłoszenie jest traktowane jako incydent bezpieczeństwa informacji, zostaje ono niezwłocznie przekazane do wyznaczonych uprawnionych pracowników osób odpowiedzialnych za bezpieczeństwo informacji u Interesariusza.

Jeżeli incydent dotyczył cyberprzestrzeni obszaru WK należy niezwłocznie poinformować o tym fakcie CERT (<https://www.cert.pl/zglos-incydent/>).

W przypadku zdarzeń o dużej złożoności wymagających udziału specjalistów z danej dziedziny bezpieczeństwa, zgłoszenie jest przekazywane do kolejnej specjalistycznej linii wsparcia.

W przypadku naruszenia bezpieczeństwa w domenie gov.pl, a także podmiotów należących do tak zwanej krytycznej infrastruktury państwa, ze szczególnym uwzględnieniem:

1. Włamań lub prób włamań,
2. Ograniczania dostępności zasobów sieciowych (DDoS),
3. Działań z użyciem złośliwych kodów (rozsyłanie wirusów),

zgłoszenie należy dodatkowo kierować do zespołu reagowania cert.gov.pl poprzez email [cert@cert.gov.pl](mailto:cert@cert.gov.pl) lub telefonicznie 22 585 93 73.

W przypadku stwierdzenia, że incydent mógł mieć znamiona przestępstwa lub stwierdzi taką potrzebę zobowiązany jest do zabezpieczenia materiałów dowodowych. Czynność zabezpieczania powinna odbywać się w obecności świadków, a z czynności zabezpieczenia materiału dowodowego powinien zostać spisany protokół zawierający m. in. dane osoby zabezpieczającej i świadków, dokładną datę  
i czas, przebieg i przedmiot zabezpieczenia.

**Incydenty dotyczące naruszenia danych osobowych**

Inspektor ochrony danych Interesariusza odpowiedziany jest za dokonanie szczegółowej analizy incydentu bezpieczeństwa. W przypadku stwierdzenie naruszenia ochrony danych osobowych, Inspektor jest zobowiązany w ciągu 72 godzin do zgłoszenia naruszenia ochrony danych do Urzędu Ochrony Danych Osobowych. Zgłoszenie powinno odbyć się przez dedykowany portal udostępniony przez Urząd Ochrony Danych Osobowych w zgodzie z wytycznymi przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

# Monitoring i nadzór

**Przegląd zarządzania**

Ocena skuteczności wdrożonych zasad zapewniających bezpieczeństwo informacji jest kluczowym elementem systemu zarządzania bezpieczeństwem informacji. Ocena dokonywana jest cyklicznie, podczas przeglądu zarządzania gdzie analizowane są takie elementy jak: wyniki audytów systemu, skuteczność zastosowanych zabezpieczeń, zarządzanie incydentami bezpieczeństwa, realizacja celów bezpieczeństwa informacji, działania korygujące.

**Audyt wewnętrzny**

Audyt wewnętrzny służy potwierdzeniu zgodności systemu Węzła Krajowego z wymaganiami dotyczącymi bezpieczeństwa informacji, zarówno w kontekście przepisów prawa stanowionego jak  
i innych regulacji normatywnych czy wewnętrznych. Jest mechanizmem niezależnej oceny, weryfikującym poziom świadomości i kompetencji użytkowników. Audyt wewnętrzny jest procesem systematycznym – cyklicznie powtarzalnym, który musi być przeprowadzony co najmniej raz do roku.