



Kancelaria Prezesa  
Rady Ministrów

---

NARODOWY STANDARD CYBERBEZPIECZEŃSTWA  
NSC 200 wer. 2.1

10 marca 2023

---

# Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych

---

Publikacja dostępna pod adresem:



[Narodowe Standardy Cyberbezpieczeństwa](#)



DEPARTAMENT CYBERBEZPIECZEŃSTWA

## PREAMBUŁA

*Szanowni Państwo,*

oddajemy w Państwa ręce zestaw publikacji specjalnych - Narodowe Standardy Cyberbezpieczeństwa, o których mowa w interwencji 2.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, *Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń*. Standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST) i posiadają mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, na których oparte jest zarządzanie bezpieczeństwem informacji w podmiotach krajowego systemu cyberbezpieczeństwa.

Standardy stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę stosowaną w tym zakresie w administracji federalnej USA.

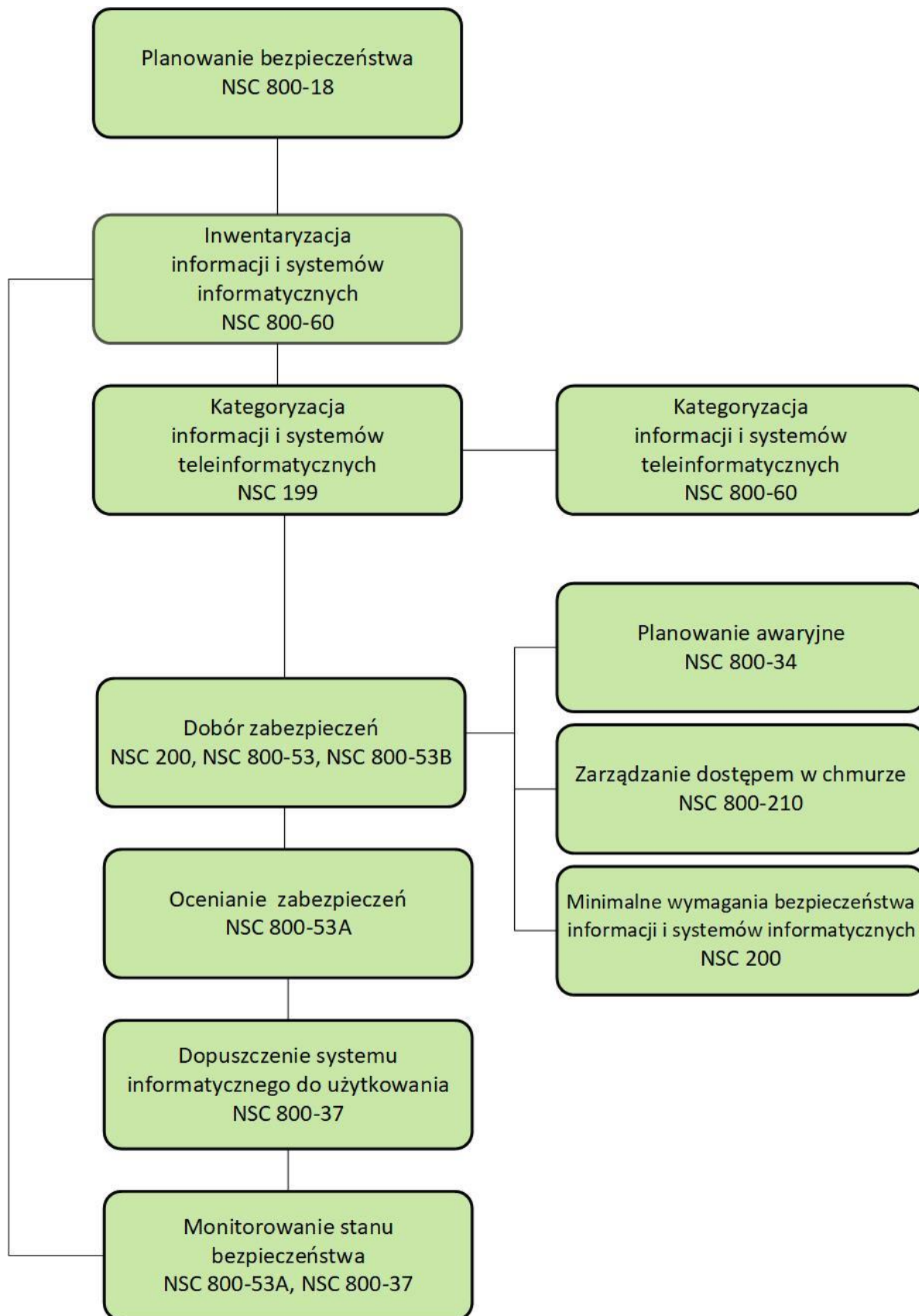
Zestaw publikacji specjalnych obejmuje następujące pozycje:

- NSC 199, Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199.
- NSC 200, Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200.
- NSC 800-18, Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych – na podstawie NIST SP 800-18.
- 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 informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37.

- NSC 800-39, Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39.
- NSC 800-53, Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53.
- NSC 800-53A, Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A.
- NSC 800-53B, Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B.
- NSC 800-60, Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informacyjnego – 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.

W oparciu o te publikacje można stosunkowo łatwo zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę.

Cykl zarządzania bezpieczeństwem informacji bazujący na publikacjach NIST wykorzystuje następujące dokumenty:



## Cykl zarządzania bezpieczeństwem informacji

---

## WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował szereg standardów i wytycznych w celu zapewnienia jednolitego podejścia do problematyki bezpieczeństwa informacji i systemów informacyjnych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji i systemów informacyjnych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością działalności i majątku organizacji, osób fizycznych 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. Dzięki jednolitemu podejściu do zarządzania ryzykiem ułatwia także wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznym i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi, które zostały opracowane przez inne organizacje (m. in. ISO<sup>1</sup>), 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 dopuszczone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejściem do zagadnień związanych z bezpieczeństwem informacji i systemów informacyjnych 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

---

<sup>1</sup> International Organization for Standardization (ISO) - Międzynarodowa Organizacja Normalizacyjna – organizacja pozarządowa zrzeszająca krajowe organizacje normalizacyjne.

podmioty przy opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania.

Podmioty, urządzenia lub materiały prezentowane są w niniejszym dokumencie w celu odpowiedniego opisanie procedury lub koncepcji eksperymentalnej. Celem ich wskazania nie jest nakłanianie do korzystania z ww. podmiotów, urządzeń lub materiałów lub ich poparcie. Wskazanie ich nie ma również na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w danej dziedzinie.

W niniejszej publikacji mogą znajdować się odniesienia do innych opracowywanych przez nas publikacji. Informacje tu zawarte, 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 powinny obowiązywać dotychczasowe wymagania, wytyczne i procedury, jeśli takie istnieją. W ramach planowanych przez Państwa prac zalecamy śledzenie naszych prac publikacyjnych.

Aktualne informacje o prowadzonych przez nas pracach dostępne są pod adresem:



[Narodowe Standardy Cyberbezpieczeństwa](#)

Jesteśmy również otwarci na wszelkie Państwa sugestie, które pomogą nam w dalszych pracach nad standardami cyberbezpieczeństwa i zachęcamy do kontaktu.



[+48222455922](tel:+48222455922)



[sekretariat.dc@kprm.gov.pl](mailto:sekretariat.dc@kprm.gov.pl)

Niniejszy publikacja NSC 200, ***Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie publikacji FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*.

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

**Uwaga:**

W standardzie NSC 200 wer. 2.0 przywoływany jest standard NSC 800-53 wer. 2.0 (bazujący na publikacji NIST SP 800-53 rev. 5) oraz standard NSC 800-53B (bazujący na publikacji NIST SP 800-53B).

## SPIS TREŚCI

Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych.....	1
Preambuła.....	2
Cykl zarządzania bezpieczeństwem informacji .....	4
Wspólne fundamenty bezpieczeństwa i ochrony prywatności.....	5
Spis treści .....	8
Wprowadzenie .....	9
1. Cel.....	11
2. Poziomy wpływ zakłócenia na system informacyjny .....	12
3. Minimalne wymagania bezpieczeństwa.....	14
4. Wybór zabezpieczeń.....	20
Załącznik A Słownik i akronimy .....	22
Załącznik B Referencje .....	23



## WPROWADZENIE

Opracowane zostały standardy w zakresie: (I) kategoryzacji bezpieczeństwa informacji i systemów informacyjnych w oparciu o cele zapewnienia odpowiedniego poziomu bezpieczeństwa informacji w zależności od zakresu poziomów ryzyka; oraz (II) minimalnych wymagań bezpieczeństwa dla informacji i systemów informacyjnych w każdej z tych kategorii.<sup>2</sup>

Niniejszy standard dotyczy specyfikacji minimalnych wymagań bezpieczeństwa informacji i systemów informacyjnych w sektorze publicznym. Określa minimalne wymagania bezpieczeństwa systemów informacyjnych w siedemnastu obszarach związanych z bezpieczeństwem. Organizacje powinny spełniać minimalne wymagania bezpieczeństwa określone w niniejszym dokumencie poprzez stosowanie środków bezpieczeństwa zgodnie ze standardem NSC 800-53.

Stosowanie środków bezpieczeństwa określonych w standardzie NSC 800-53 i wymaganych przez ten standard stanowi aktualny stan praktycznych zabezpieczeń i środków zaradczych dla systemów informacyjnych. Zabezpieczenia te będą poddawane przeglądowi przez Kolegium ds. Cyberbezpieczeństwa co najmniej raz w roku oraz w razie potrzeby zmieniane i rozszerzane w celu odzwierciedlenia: (I) doświadczenia zdobytego podczas korzystania z zabezpieczeń; (II) zmieniających się wymagań w zakresie bezpieczeństwa informacji; oraz (III) nowych, dostępnych technologii bezpieczeństwa. Oczekuje się, że minimalne mechanizmy zabezpieczeń określone dla systemów informacyjnych podlegających niskim, umiarkowanym i wysokim wpływom zakłócenia, również będą się zmieniać w miarę zmian w czasie, a poziom bezpieczeństwa i należytej staranności w zakresie ograniczania ryzyka w organizacjach będzie wzrastał.

---

<sup>2</sup> Zdefiniowany zgodnie ze standardem NSC 800-53B zestaw minimalnych zabezpieczeń / zabezpieczeń bazowych (*ang. Security control baselines*) systemu informacyjnego o niskim, umiarkowanym lub o dużym wpływie zakłócenia na atrybuty bezpieczeństwa informacji (poufność, integralność, dostępność). Ustanowiony w wyniku podjętych działań planowania strategicznego bezpieczeństwa informacji w celu określenia jednej lub kilku kategoryzacji zabezpieczeń (określanych zgodnie ze standardem NSC 199). Ten zestaw zabezpieczeń jest początkowym zbiorem środków bezpieczeństwa wybranym dla określonego systemu informacyjnego po określeniu kategoryzacji zabezpieczeń systemu.

Proponowane uzupełnienia, usunięcia lub modyfikacje zabezpieczeń oraz zmiany minimalnych środków bezpieczeństwa określonych w standardzie NSC 800-53 przejdą rygorystyczny, publiczny proces przeglądu w celu uzyskania informacji zwrotnych dla sektora podmiotów publicznych oraz do wypracowania konsensusu w sprawie zmian.

## 1. CEL

Kompleksowe podejście do spraw związanych z cyberbezpieczeństwem opiera się na trzech fundamentach:

1. Standardach, które wykorzystywane będą przez podmioty publiczne w celu kategoryzacji wszelkich informacji i systemów informacyjnych będących w posiadaniu lub utrzymywanych przez lub w imieniu każdego z tych podmiotów, na podstawie celów zapewniania stosownych poziomów bezpieczeństwa zgodnie z oszacowanym zakresem poziomów ryzyka.
2. Wytycznych zawierających rekomendacje, co do rodzajów informacji i systemów informacyjnych, mających zostać uwzględnionymi w każdej z kategorii.
3. Minimalnych wymaganiach bezpieczeństwa informacji (tj. zarządczych, operacyjnych i technicznych mechanizmów zabezpieczeń) odnoszących się do informacji i systemów informacyjnych w każdej z tych kategorii.

Standard NSC 199, Standardy kategoryzacji bezpieczeństwa, jest jednym ze standardów odnoszących się do pierwszego z powyższych fundamentów – wypracowania standardów kategoryzacji informacji i systemów informacyjnych. Standard NSC 200, drugi ze standardów bezpieczeństwa odnoszących się do pierwszego z powyższych fundamentów, określa minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych oraz proces wyboru środków bezpieczeństwa niezbędny do zapewnienia minimalnych wymogów bezpieczeństwa zgodnie z oszacowanym zakresem poziomów ryzyka. Standard ten będzie wspierać rozwój, wdrażanie i funkcjonowanie bezpieczniejszych systemów informacyjnych poprzez ustanowienie minimalnych poziomów należytej staranności w zakresie bezpieczeństwa informacji i ułatwienie bardziej spójnego, porównywalnego i powtarzalnego podejścia do wyboru i określania zabezpieczeń systemów informacyjnych spełniających minimalne wymagania bezpieczeństwa.

## 2. POZIOMY WPŁYWU ZAKŁÓCENIA NA SYSTEM INFORMACYJNY

Standard NSC 199 definiuje trzy poziomy potencjalnego wpływu zakłócenia na organizacje i osoby fizyczne powodującego naruszenie bezpieczeństwa (tj. utratę poufności, integralności lub dostępności). Stosowanie tych definicji musi być dokonywane w kontekście danej organizacji.

*Potencjalny wpływ jest NISKI*, jeżeli można oczekiwać **ograniczonego** negatywnego wpływu utraty poufności, integralności lub dostępności na działalność organizacji, jej zasoby lub osoby fizyczne.

*Potencjalny wpływ jest UMIARKOWANY*, jeżeli można oczekiwać **poważnego** negatywnego wpływu utraty poufności, integralności lub dostępności na działalność organizacji, jej zasoby lub osoby fizyczne.

*Potencjalny wpływ jest WYSOKI*, jeżeli można oczekiwać **drastycznie lub katastrofalnie** negatywnego wpływu utraty poufności, integralności lub dostępności na działalność organizacji, jej zasoby lub osoby fizyczne.

Określenie kategorii bezpieczeństwa systemu informacyjnego wymaga pogłębionej analizy, jak również musi uwzględniać kategorie bezpieczeństwa wszystkich rodzajów informacji przetwarzanych w systemie informacyjnym. W przypadku systemu informacyjnego, potencjalne wartości wpływu przypisane do stosownych atrybutów bezpieczeństwa (poufności, integralności, dostępności) są to najwyższe wartości<sup>3</sup> (*ang. high water mark*) spośród tych atrybutów, które zostały określone dla poszczególnych rodzajów informacji przetwarzanych w danym systemie informacyjnym.

Uogólniona formuła wyrażania kategorii bezpieczeństwa (KB) dla systemu informacyjnego przedstawiona została poniżej:

---

<sup>3</sup> Stosowana jest koncepcja najwyższej wartości, ponieważ istnieją znaczące zależności pomiędzy atrybutami bezpieczeństwa, takimi jak poufność, integralność i dostępność. W większości przypadków naruszenie jednego z atrybutów bezpieczeństwa ostatecznie wpływa również na pozostałe atrybuty bezpieczeństwa. W związku z tym środki bezpieczeństwa nie są kategoryzowane według atrybutów bezpieczeństwa. Natomiast są grupowane w zabezpieczenia bazowe mające na celu zapewnienia ogólnej zdolności ochrony poszczególnych klas systemów w oparciu o poziom wpływu na te systemy.

**KB** system informacyjny = {(poufność, wpływ), (integralność, wpływ),  
(dostępność, wpływ)},

gdzie dopuszczalne wartości potencjalnego wpływu to NISKI,  
UMIARKOWANY, oraz WYSOKI.

Ponieważ potencjalne wartości wpływu na atrybuty bezpieczeństwa (poufność, integralność i dostępność) mogą nie zawsze być takie same dla danego systemu informacyjnego, do określenia ogólnego poziomu oddziaływania na system informacyjny należy zastosować koncepcję najwyższej wartości spośród tych kategorii bezpieczeństwa, które zostały określone dla poszczególnych rodzajów informacji przetwarzanych w tym systemie informacyjnym.

W związku z tym, system o *niskim* wpływie jest systemem informacyjnym, w którym wpływ na wszystkie trzy atrybuty bezpieczeństwa jest *niski*.

System o *umiarkowanym* wpływie jest systemem informacyjnym, w którym wpływ, na co najmniej jeden z atrybutów bezpieczeństwa jest *umiarkowany* i żaden atrybut bezpieczeństwa nie podlega wpływowi większemu niż *umiarkowany*.

System o *wysokim* wpływie jest systemem informacyjnym, w którym wpływ, na co najmniej jeden atrybut bezpieczeństwa, jest *wysoki*.

Określenie poziomów oddziaływania systemu informacyjnego musi zostać osiągnięte przed określeniem minimalnych wymogów bezpieczeństwa i wyborem odpowiednich środków bezpieczeństwa systemów informacyjnych.

### 3. MINIMALNE WYMAGANIA BEZPIECZEŃSTWA

Minimalne wymagania bezpieczeństwa obejmują dwadzieścia obszarów związanych z bezpieczeństwem w odniesieniu do ochrony poufności, integralności i dostępności systemów informacyjnych oraz informacji przetwarzanych, przechowywanych i przekazywanych przez te systemy. Obszary związane z bezpieczeństwem obejmują: (I) kontrolę dostępu; (II) uświadamianie i szkolenia; (III) audyt i rozliczalność; (IV) ocenę, autoryzację i monitorowanie ; (V) zarządzanie konfiguracją; (VI) planowanie awaryjne / ciągłość działania; (VII) identyfikację i uwierzytelnienie; (VIII) reagowanie na incydenty; (IX) utrzymanie i wsparcie; (X) ochronę nośników danych; (XI) ochronę fizyczną i środowiskową; (XII) planowanie; (XIII) programy zarządzania; (XIV) bezpieczeństwo osobowe; (XV) przejrzystość przetwarzania danych osobowych; (XVI) ocenę ryzyka; (XVII) nabywanie systemu i usług; (XVIII) ochronę systemów i sieci telekomunikacyjnych; (XIX) integralność systemu i informacji; oraz (XX) zarządzanie ryzykiem w łańcuchu dostaw. Dwadzieścia obszarów reprezentuje szeroko zakrojony, zrównoważony program bezpieczeństwa informacji, który dotyczy zarządzania, operacyjnych i technicznych aspektów ochrony informacji i systemów informacyjnych.

Zasady i procedury odgrywają ważną rolę w skutecznym wdrażaniu programów bezpieczeństwa informacji w całej organizacji i stanowią o sukcesie wynikającym ze stosowania środków bezpieczeństwa w celu ochrony informacji i systemów informacyjnych. W związku z tym, organizacje powinny opracować i propagować formalne, udokumentowane zasady i procedury regulujące minimalne wymogi bezpieczeństwa określone w niniejszym standardzie i powinny zapewnić ich skuteczne wdrożenie.

#### SPECYFIKACJE DOTYCZĄCE MINIMALNYCH WYMAGAŃ BEZPIECZEŃSTWA

**Kontrola dostępu** (*ang. Access Control - AC*): Organizacje powinny ograniczyć dostęp do systemu informacyjnego do autoryzowanych użytkowników, procesów działających w imieniu autoryzowanych użytkowników lub urządzeń (w tym innych systemów informacyjnych) oraz do typów transakcji i funkcji, które upoważnieni użytkownicy mogą wykonywać.

**Uświadamianie i szkolenia** (*ang. Awareness and Training - AT*): Organizacje powinny:

(I) zapewnić, aby menedżerowie i użytkownicy organizacyjnych systemów informacyjnych byli informowani o zagrożeniach bezpieczeństwa związanych z ich działalnością oraz o obowiązujących przepisach prawa, zarządzeniach wykonawczych, dyrektywach, zasadach, standardach, instrukcjach, przepisach lub procedurach związanych z bezpieczeństwem organizacyjnych systemów informacyjnych; oraz  
(II) zapewnić, aby personel organizacyjny był odpowiednio przeszkolony w zakresie wykonywania powierzonych mu zadań i obowiązków związanych z bezpieczeństwem informacji.

**Audyt i rozliczalność** (*ang. Audit and Accountability - AU*): Organizacje powinny:

(I) tworzyć, chronić i przechowywać rejestry audytu systemu informacyjnego w zakresie niezbędnym do umożliwienia monitorowania, analizy, badania i zgłaszania bezprawnych, nieautoryzowanych lub nieodpowiednich działań systemu informacyjnego; oraz (II) zapewnić, aby działania poszczególnych użytkowników systemu informacyjnego mogły być jednoznacznie powiązane z tymi użytkownikami, tak, aby mogli oni zostać pociągnięci do odpowiedzialności za swoje działania.

**Ocena, autoryzacja i monitorowanie** (*ang. Certification, Accreditation, and Security Assessments - CA*): Organizacje powinny: (I) okresowo oceniać środki bezpieczeństwa w systemach informacyjnych organizacji, w celu ustalenia, czy zabezpieczenia są skuteczne w ich stosowaniu; (II) opracowywać i wdrażać plany działania mające na celu wyeliminowanie niedociągnięć oraz zmniejszenie lub wyeliminowanie luk w zabezpieczeniach organizacyjnych systemów informacyjnych; (III) autoryzować działanie organizacyjnych systemów informacyjnych i wszelkich powiązanych połączeń systemów informacyjnych; oraz (IV) na bieżąco monitorować środki bezpieczeństwa systemu informacyjnego w celu zapewnienia ciągłej skuteczności zabezpieczeń.

**Zarządzanie konfiguracją** (*ang. Configuration Management - CM*): Organizacje powinny:

(I) ustanowić i utrzymywać podstawowe konfiguracje i wykazy organizacyjnych systemów informacyjnych (w tym sprzętu, oprogramowania, oprogramowania układowego i dokumentacji) w odpowiednich cyklach życia rozwoju systemu; oraz

(II) ustanowić i egzekwować ustawienia konfiguracji zabezpieczeń dla produktów technologii informacyjnych stosowanych w organizacyjnych systemach informacyjnych.

**Planowanie awaryjne / ciągłość działania** (*ang. Contingency Planning - CP*): Organizacje powinny ustanawiać, utrzymywać i skutecznie wdrażać plany reagowania w sytuacjach awaryjnych. Do tych działań należą: tworzenie kopii zapasowych danych i odzyskiwanie ich po awarii dla organizacyjnych systemów informacyjnych. Ma to zapewnić dostępność krytycznych zasobów informacyjnych i ciągłość operacji w sytuacjach awaryjnych.

**Identyfikacja i uwierzytelnianie** (*ang. Identification and Authentication - IA*): Organizacje powinny identyfikować użytkowników systemu informacyjnego, procesy działające w imieniu użytkowników lub urzędzenia oraz uwierzytelniać (lub weryfikować) tożsamości tych użytkowników, procesów lub urzędzeń, jako wymóg zasadniczy umożliwiający dostęp do organizacyjnych systemów informacyjnych.

**Reagowanie na incydenty** (*ang. Incident Response - IR*): Organizacje powinny:

(I) ustanowić operacyjną zdolność obsługi incydentów dla organizacyjnych systemów informacyjnych, która obejmuje odpowiednie przygotowanie, wykrywanie, analizę, powstrzymywanie, odzyskiwanie i działania związane z reagowaniem na potrzeby użytkownika; oraz (II) śledzić, dokumentować i zgłaszać incydenty odpowiednim organom.

**Utrzymanie i wsparcie** (*ang. Maintenance - MA*): Organizacje powinny:

(I) przeprowadzać okresową i terminową obsługę organizacyjnych systemów informacyjnych; oraz (II) zapewniać skuteczne zabezpieczenia narzędzi, technik, mechanizmów i personelu wykorzystywanego do przeprowadzania konserwacji systemu informacyjnego.

**Ochrona nośników danych** (*ang. Media Protection - MP*): Organizacje powinny:

(I) chronić nośniki systemowe, zarówno papierowe, jak i cyfrowe; (II) zezwolić na dostęp do informacji o nośnikach systemu informacyjnego tylko upoważnionym



użytkownikom; oraz (III) przeprowadzać sanityzację lub niszczyć nośniki systemu informacyjnego przed utylizacją lub dopuszczeniem do ponownego użycia.

**Ochrona fizyczna i środowiskowa** (*ang. Physical and Environmental Protection - PE*):

Organizacje powinny: (i) ograniczyć fizyczny dostęp do systemów informacyjnych, sprzętu i odpowiednich środowisk operacyjnych tylko do upoważnionych osób; (II) chronić fizyczne instalacje i infrastrukturę wsparcia systemów informacyjnych; (III) zapewnić narzędzia wsparcia dla systemów informacyjnych; (IV) chronić systemy informacyjne przed zagrożeniami środowiskowymi; oraz (V) zapewnić odpowiednie zabezpieczenia środowiskowe w obiektach zawierających systemy informacyjne.

**Planowanie** (*ang. Planning - PL*): Organizacje powinny opracowywać, dokumentować, okresowo aktualizować i wdrażać plany bezpieczeństwa dla organizacyjnych systemów informacyjnych, które opisują mechanizmy zabezpieczeń obowiązujące lub planowane dla systemów informacyjnych oraz reguły zachowania osób uzyskujących dostęp do systemów informacyjnych.

**Programy zarządzania** (*ang. Program Management - PM*): Organizacje powinny:

(I) opracowywać i rozpowszechniać plan programu bezpieczeństwa informacji (*ang. Information Security Program Plan*)<sup>4</sup>; (II) przeglądać i aktualizować plan programu bezpieczeństwa informacji; (III) chronić plan bezpieczeństwa informacji przed nieautoryzowanym ujawnieniem i modyfikacją.

**Bezpieczeństwo osobowe** (*ang. Personnel Security - PS*): Organizacje powinny:

(I) zapewnić, aby osoby zajmujące odpowiedzialne stanowiska w organizacjach (w tym zewnętrzni dostawcy usług) były godne zaufania i spełniały ustalone kryteria bezpieczeństwa dla tych stanowisk; (II) zapewnić ochronę informacji i systemów informacyjnych organizacji w trakcie i po działaniach personalnych, takich jak rozwiązania umowy o pracę (współpracy) i zmiana zajmowanych stanowisk; oraz (III) stosować formalne sankcje za brak przestrzegania przez personel zasad i procedur bezpieczeństwa organizacyjnego.

---

<sup>4</sup> Patrz: NSC 800-53, NSC 7298.

**Przejrzystość przetwarzania danych osobowych** (*ang. Personally Identifiable Information Processing and Transparency - PT*): Organizacje powinny: (I) opracowywać polityki i procedury w zakresie przejrzystości przetwarzania danych osobowych; (II) opracowywać programy bezpieczeństwa i ochrony prywatności uwzględniające polityki i procedury przejrzystości przetwarzania danych osobowych; (III) aktualizować polityki i procedury dotyczące przejrzystości przetwarzania danych osobowych w oparciu o zaistniałe zdarzenia obejmujące wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

**Ocena ryzyka** (*ang. Risk Assessment - RA*): Organizacje powinny okresowo oceniać ryzyko odnoszące się do operacji organizacyjnych (w tym misji, funkcji, wizerunku lub reputacji), zasobów organizacyjnych i osób fizycznych, wynikających z działania organizacyjnych systemów informacyjnych i związanego z nimi przetwarzania, przechowywania lub przekazywania informacji organizacyjnych.

**Nabywanie systemu i usług** (*ang. System and Services Acquisition - SA*): Organizacje powinny: (I) alokować wystarczające zasoby, zapewniające odpowiednią ochronę organizacyjnych systemów informacyjnych; (II) stosować procesy cyklu życia rozwoju systemu, które uwzględniają względy bezpieczeństwa informacji; (III) stosować ograniczenia dotyczące używania oprogramowania i instalacji; oraz (IV) zapewnić, aby dostawcy zewnętrzni stosowali adekwatne środki bezpieczeństwa w celu ochrony informacji, aplikacji i/lub usług zleconych przez organizację.

**Ochrona systemów i sieci telekomunikacyjnych** (*ang. System and Communications Protection - SC*): Organizacje powinny: (I) monitorować, kontrolować i chronić komunikację organizacyjną (tj. informacje przekazywane lub odbierane przez organizacyjne systemy informacyjne) na zewnętrznych granicach i kluczowych granicach wewnętrznych systemów informacyjnych; oraz (II) stosować projekty architektoniczne, techniki tworzenia oprogramowania i zasady inżynierii systemów, które promują skuteczne bezpieczeństwo informacji przetwarzanych w organizacyjnych systemach informacyjnych.

**Integralność systemu i informacji** (*ang. System and Information Integrity - SI*):

Organizacje powinny: (I) w odpowiednim czasie identyfikować, zgłaszać i korygować błędy informacji i systemów informacyjnych; (II) zapewnić ochronę przed złośliwym kodem w stosownych lokalizacjach w ramach organizacyjnych systemów informacyjnych; oraz (III) monitorować ostrzeżenia i porady systemu informacyjnego oraz w odpowiedzi na to podejmować odpowiednie działania.

**Zarządzanie ryzykiem w łańcuchu dostaw** (*ang. Supply Chain Risk Management - SR*):

Strategia zarządzania ryzykiem uwzględnia koszty, harmonogram, wyniki i kwestie dotyczące łańcucha dostaw powiązane z projektowaniem, rozwojem, pozyskiwaniem, wdrażaniem, eksploatacją, utrzymaniem i utylizacją systemów organizacyjnych. Proces zarządzania ryzykiem jest następnie stosowany w celu bieżącego zarządzania ryzykiem.

Organizacje powinny: (I) opracowywać polityki i procedury w zakresie zarządzania ryzykiem w łańcuchu dostaw; (II) opracowywać programy bezpieczeństwa i ochrony prywatności uwzględniające polityki i procedury zarządzania ryzykiem w łańcuchu dostaw; (III) aktualizować polityki i procedury zarządzania ryzykiem w łańcuchu dostaw w oparciu o zaistniałe zdarzenia obejmujące wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

## 4. WYBÓR ZABEZPIECZEŃ

Organizacje powinny spełniać minimalne wymagania bezpieczeństwa określone w niniejszym standardzie, stosując odpowiednie środki bezpieczeństwa opisane w standardzie NSC 800-53. Proces wyboru odpowiednich zabezpieczeń i wymagań mających na celu osiągnięcie przez systemy informacyjne organizacji adekwatnego poziomu bezpieczeństwa jest wieloaspektową, opartą na szacowaniu ryzyka działalnością obejmującą personel zarządzający i operacyjny w organizacji.

Kategoryzacja zabezpieczeń organizacyjnych informacji i systemów, zgodnie z wymogami standardu NSC 199, jest pierwszym krokiem w procesie zarządzania ryzykiem.<sup>5</sup> Po procesie kategoryzacji zabezpieczeń organizacje powinny wybrać odpowiedni zestaw środków bezpieczeństwa dla swoich systemów informacyjnych, które spełniają minimalne wymagania bezpieczeństwa określone w niniejszym standardzie. Wybrany zestaw zabezpieczeń powinien zawierać jeden z trzech odpowiednio dostosowanych bazowych minimalnych środków bezpieczeństwa opisanych w publikacji NSC 800-53, które są skojarzone z oszacowanymi poziomami wpływu na organizacyjny system informacyjny, określonymi podczas procesu kategoryzacji zabezpieczeń.

- W przypadku systemów informacyjnych o niskim wpływie, organizacje powinny co najmniej stosować odpowiednio dostosowane zabezpieczenia bazowe<sup>6</sup> (*ang. security control baselines*) zdefiniowane w standardzie NSC 800-53B, jako *Niski poziom wpływu na atrybuty bezpieczeństwa informacji*. Organizacje powinny mieć pewność, że minimalne wymagania zapewnione przez zastosowanie zabezpieczeń *Poziomu Niskiego*, są wystarczające.
- W przypadku systemów informacyjnych o umiarkowanym wpływie, organizacje powinny co najmniej stosować odpowiednio dostosowane zabezpieczenia

---

<sup>5</sup> Kategoryzacja bezpieczeństwa musi być dokonana w aspekcie działalności całego przedsiębiorstwa z udziałem kluczowych urzędników / pracowników organizacyjnych, w tym między innymi pełniących role: CIO, SAISO, AO, właścicieli systemów informacyjnych i właścicieli informacji (definicje ról – patrz publikacje NSC 800-37, NSC 7298).

<sup>6</sup> W potocznym języku technicznym – „bejslajny”.

bazowe zdefiniowane w standardzie NSC 800-53B jako *Umiarkowany poziom wpływu na atrybuty bezpieczeństwa informacji*. Organizacje powinny mieć pewność, że minimalne wymagania zapewnione przez zastosowanie zabezpieczeń *Poziomu Umiarkowanego*, są wystarczające.

- W przypadku systemów informacyjnych o wysokim wpływie, organizacje powinny co najmniej stosować odpowiednio dostosowane zabezpieczenia bazowe) zdefiniowane w standardzie NSC 800-53B jako *Wysoki poziom wpływu na atrybuty bezpieczeństwa informacji*. Organizacje powinny mieć pewność, że minimalne wymagania zapewnione przez zastosowanie zabezpieczeń *Poziomu Wysokiego*, są wystarczające.

Organizacje powinny stosować wszystkie mechanizmy zabezpieczeń w odpowiednich planach podstawowych zabezpieczeń, chyba, że określone wyjątki są zastosowane na podstawie wyników szacowania ryzyka dotyczących dostosowywania lub pominięcia zabezpieczeń opisanych w publikacji NSC 800-53. Aby zapewnić opłacalne, oparte na ryzyku podejście do osiągnięcia odpowiedniego bezpieczeństwa w całej organizacji, podstawowe działania w zakresie dostosowywania środków bezpieczeństwa powinny być koordynowane i zatwierdzone przez odpowiedni personel organizacyjny (np. dyrektorów ds. informacji, wyższy personel zajmujący się bezpieczeństwem informacji, personel zatwierdzający lub przez upoważnionych wyznaczonych przedstawicieli). Wynikowy zestaw zabezpieczeń musi być udokumentowany w planie bezpieczeństwa systemu informacyjnego.

## ZAŁĄCZNIK A SŁOWNIK I AKRONIMY

PATRZ: NSC 7298, SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA

---

## ZAŁĄCZNIK B REFERENCJE

### NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA<sup>7</sup>

NSC 199	Standardy kategoryzacji bezpieczeństwa
NSC 800-18	Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych – na podstawie NIST SP 800-18
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych 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: <a href="#">SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations   CSRC (nist.gov)</a>
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60

---

<sup>7</sup> [Narodowe Standardy Cyberbezpieczeństwa](#)

**PUBLIKACJE ANGLOJĘZYCZNE<sup>8</sup>**

FIPS 199      *Standards for Security Categorization of Federal Information and Information Systems, February 2004*

NIST SP 800-18      *Guide for Developing Security Plans for Federal Information Systems, February 2006*

NIST SP 800-53      *Security and Privacy Controls for Information Systems and Organizations, September 2020*

NIST SP 800-60      *Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004*

---

<sup>8</sup> Referencje zostały podane w celach uzupełniających dla osób zainteresowanych.