NSC NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	Narodowy Standard Cyberbezpieczeństwa		
Nazwa standardu	Symbol	Wersja	Data wydania
MAPOWANIE ŚRODKÓW BEZPIECZEŃSTWA: NSC 800-53 WER. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 WER. 2	**NSC 800-53 MAP**	1.0	15/07/2021

MAPOWANIE ŚRODKÓW BEZPIECZEŃSTWA: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2

PEŁNOMOCNIK RZĄDU DS. CYBERBEZPIECZEŃSTWA
Warszawa 2021

WPROWADZENIE

Tabele mapowania zawarte w niniejszym dodatku dostarczają organizacjom ogólnych wskazówek dotyczących zabezpieczeń NSC 800-53 wer. 2[1] w odniesieniu do normy PN-ISO/IEC 27001:2013[2], *Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania*[3]. Norma PN-ISO/IEC 27001 może być stosowana we wszystkich typach organizacji i określa wymagania dotyczące ustanawiania, wdrażania, eksploatacji, monitorowania, przeglądów, utrzymywania i doskonalenia udokumentowanego systemu zarządzania bezpieczeństwem informacji (*ang. Information Security Management System - ISMS*) w kontekście ryzyka biznesowego. Specjalna publikacja NIST 800-39 zawierająca wytyczne dotyczące zarządzania ryzykiem na poziomie organizacyjnym, poziomie misji/procesu biznesowego oraz na poziomie systemu informacyjnego, jest zgodna z normą PN-ISO/IEC 27001 i dostarcza dodatkowych szczegółów wdrożeniowych dla podmiotów publicznych i ich kontrahentów.

Mapowanie zabezpieczeń określonych w NSC 800-53 do wymagań i zabezpieczeń określonych w PN-ISO/IEC 27001 odzwierciedla, czy wdrożenie środka bezpieczeństwa z NSC 800-53 spełnia intencje odwzorowanego wymagania bezpieczeństwa lub zabezpieczenia z PN-ISO/IEC 27001 i odwrotnie, czy implementacja wymagania bezpieczeństwa lub zabezpieczenia z PN-ISO/IEC 27001 spełnia intencje odwzorowanego zabezpieczenia z NSC 800-53. Warunkiem pomyślnego spełnienia kryteriów mapowania jest to, że wdrożenie mapowanych zabezpieczeń powinno skutkować równoważną postawą w zakresie bezpieczeństwa informacji. Organizacje nie powinny jednak zakładać równoważności wymagań bezpieczeństwa i zabezpieczeń wyłącznie

[1] Dalej: NSC 800-53.

[2] Dalej: PN-ISO/IEC 27001

[3] Norma ISO/IEC 27001 została opublikowana w październiku 2013 r. przez Międzynarodową Organizację Normalizacyjną (ISO) i Międzynarodową Komisję Elektrotechniczną (IEC). Na jej podstawie, Prezes Polskiego Komitetu Normalizacyjnego zatwierdził w dniu 25.11.2014 r. PN- ISO/IEC 27001.

na podstawie tabel odwzorowań, ponieważ w analizie odwzorowań zawsze istnieje pewien stopień subiektywności, bowiem odwzorowania nie zawsze są jeden do jednego i mogą nie być całkowicie równoważne. Implementacje specyficzne dla danej organizacji mogą również odgrywać rolę w równoważności stosowanych zabezpieczeń. Poniższe przykłady ilustrują niektóre z problemów związanych z mapowaniem:

- ***Przykład 1.*** Planowanie awaryjne opisane w NSC 800-53 i zarządzanie ciągłością działania zawarte w PN-ISO/IEC 27001 zostały uznane funkcjonalnie za podobne, ale nie takie same.
- ***Przykład 2.*** W niektórych przypadkach podobne tematy są poruszane w dwóch zestawach zabezpieczeń, ale zapewniają inny kontekst, perspektywę lub zakres. NSC 800-53 odnosi się do zabezpieczeń przepływu informacji w szerokim zakresie pod względem zatwierdzonych zezwoleń na kontrolowanie dostępu między obiektami źródłowymi i docelowymi, podczas gdy PN-ISO/IEC 27001 zajmuje się przepływem informacji w bardziej wąskim zakresie, ponieważ ma zastosowanie do połączonych domen sieciowych.
- ***Przykład 3.*** Zabezpieczenie A.6.1.1 „Role i odpowiedzialność za bezpieczeństwo informacji”, zawarte w PN-ISO/IEC 27001 określa, że „odpowiedzialność za bezpieczeństwo informacji powinna być określona i przypisana”, podczas gdy zabezpieczenie rodziny PM-10 – „Proces autoryzacji” NSC 800-53, które jest mapowane na A.6.1.1, składa się z trzech odrębnych części. Część b. PM-10 wymaga wyznaczenia "osób do pełnienia określonych ról i obowiązków...". Jeśli A.6.1.1 jest mapowana do PM-10 bez żadnych dodatkowych informacji, organizacje mogą założyć, że jeśli zabezpieczenie A.6.1.1 jest wdrożone (tj. wszystkie obowiązki są zdefiniowane i przydzielone), to intencje PM-10 są również w pełni spełnione. Może to jednak nie odpowiadać rzeczywistości, ponieważ części a. i c. PM-10 mogły nie zostać

uwzględnione. W celu rozwiązania i wyjaśnienia mapowania zabezpieczeńe, w przypadku gdy wymóg bezpieczeństwa lub środek bezpieczeństwa w prawej kolumnie tabel 1 i 2 nie spełniają w pełni intencji wymogu bezpieczeństwa lub zabezpieczenia w lewej kolumnie tabel 1 i 2, zabezpieczenie lub cały zestaw wymienionych zabezpieczeń w prawej kolumnie jest oznaczony gwiazdką (*).

- ***Przykład 4.*** Mechanizmy ochrony prywatności zostały włączone do zestawu zabezpieczeń NSC 800-53, wer.2, aby spełnić wymagania dotyczące prywatności przy przetwarzaniu informacji umożliwiających identyfikację osób (*ang. personal identifiable information - PII*) I dlatego są uwzględnione w tabeli mapowania; jednakże norma PN-ISO/IEC 27001 nie odnosi się konkretnie do prywatności poza korzyściami wynikającymi z utrzymania bezpieczeństwa PII. Użytkownicy tej tabeli mogą założyć, że mechanizmy zabezpieczające PN-ISO/IEC 27001 nie spełniają wymogów ochrony prywatności w odniesieniu do przetwarzania PII.

W kilku przypadkach wymaganie lub środek bezpieczeństwa PN-ISO/IEC 27001 może być bezpośrednio przyporządkowana tylko do zabezpieczenia rozszerzonego zawartego w NSC 800-53. W takich przypadkach stosowne zabezpieczenie rozszerzone jest wyszczególnione w Tabeli 2, wskazując, że odpowiednie wymaganie lub zabezpieczenie określone w PN-ISO/IEC 27001 spełnia jedynie intencje określonego zabezpieczenia rozszerzonego i nie odnosi się do powiązanego zabezpieczenia podstawowego z NSC 800-53 lub jakiegokolwiek innego zabezpieczenia rozszerzonego w ramach tego zabezpieczenia podstawowego. Jeśli nie określono żadnego zabezpieczenia rozszerzonego, wymaganie lub zabezpieczenie PN-ISO/IEC 27001 jest odpowiednia tylko dla zabezpieczenia bazoweego z NSC 800-53.

Zabezpieczenia PN-ISO/IEC 27002 nie zostały uwzględnione w analizie mapowania, ponieważ norma ma charakter informacyjny, a nie normatywny.

TABELA 1: MAPOWANIE ŚRODKÓW BEZPIECZEŃSTWA: NSC 800-53 WER. 2 – PN-ISO/IEC 27001

Tabela 1 zawiera mapowanie zabezpieczeń zawartych w NSC 800-53 z zabezpieczeniami zawartymi w PN-ISO/IEC 27001. Przed zastosowaniem mapowania z tabeli 1 należy zapoznać się z wyjaśnieniami zawartymi we Wprowadzeniu.

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
AC-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AC-2	ZARZĄDZANIE KONTAMI	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6
AC-3	EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3
AC-4	EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI	A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
AC-5	ROZDZIAŁ OBOWIĄZKÓW	A.6.1.2
AC-6	ZASADA WIEDZY KONIECZNEJ	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5
AC-7	NIEUDANE PRÓBY LOGOWANIA	A.9.4.2
AC-8	POWIADOMIENIE O ZASADACH UŻYCIA SYSTEMU	A.9.4.2

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
AC-9	POWIADOMIENIE O POPRZEDNIM ZALOGOWANIU	A.9.4.2
AC-10	KONTROLA ILOŚCI RÓWNOCZESNYCH SESJI	Brak
AC-11	BLOKADA URZĄDZENIA	A.11.2.8, A.11.2.9
AC-12	ZAKOŃCZENIE SESJI	Brak
AC-13	NADZÓR I PRZEGLĄD KONTROLI DOSTĘPU (włączone do AC-2 i AU-6)	---
AC-14	DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIENIA	Brak
AC-15	ZNAKOWANIE AUTOMATYCZNE (włączone do AC-2 i AU-6)	---
AC-16	ATRYBUTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI	Brak
AC-17	DOSTĘP ZDALNY	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
AC-18	DOSTĘP BEZPRZEWODOWY	A.6.2.1, A.13.1.1, A.13.2.1

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
AC-19	KONTROLA DOSTĘPU DO URZĄDZEŃ PRZENOŚNYCH	A.6.2.1, A.11.1.5, A.11.2.6, A.13.2.1
AC-20	WYKORZYSTANIE SYSTEMÓW ZEWNĘTRZNYCH	A.11.2.6, A.13.1.1, A.13.2.1
AC-21	UDOSTĘPNIANIE INFORMACJI	Brak
AC-22	TREŚCI PUBLICZNIE DOSTĘPNE	Brak
AC-23	OCHRONA PRZED PRZESZUKIWANIEM DANYCH	Brak
AC-24	PRZYZNAWANIE PRAW DOSTĘPU	A.9.4.1*
AC-25	MONITOR REFERENCYJNY	Brak
AT-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AT-2	SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA	7.3, A.7.2.2, A.12.2.1
AT-3	SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH	A.7.2.2*
AT-4	DOKUMENTACJA SZKOLENIOWA	Brak

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
AT-5	UTRZYMYWANIE KONTAKTÓW Z ZESPOŁAMI I STOWARZYSZENIAMI SPECJALIZUJĄCYMI SIĘ W CYBERBEZPIECZEŃSTWIE (włączone do PM-15)	---
AT-6	INFORMACJE ZWROTNE O SZKOLENIACH	Brak
AU-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AU-2	AUDYT ZDARZEŃ	Brak
AU-3	ZAWARTOŚĆ REJESTRÓW AUDYTU	A.12.4.1*
AU-4	POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU	A.12.1.3
AU-5	REAKCJA NA BŁĘDY PROCESÓW AUDYTU	Brak
AU-6	PRZEGLĄD ZAPISÓW AUDYTU, ANALIZA I RAPORTOWANIE	A.12.4.1, A.16.1.2, A.16.1.4
AU-7	REDUKCJA AUDYTÓW I SPORZĄDZANIE RAPORTÓW	Brak

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
AU-8	ZNACZNIKI CZASU	A.12.4.4
AU-9	OCHRONA INFORMACJI AUDYTOWYCH	A.12.4.2, A.12.4.3, A.18.1.3
AU-10	NIEZAPRZECZALNOŚĆ	Brak
AU-11	RETENCJA ZAPISÓW AUDYTU	A.12.4.1, A.16.1.7
AU-12	TWORZENIE ZAPISÓW AUDYTU	A.12.4.1, A.12.4.3
AU-13	MONITOROWANIE UJAWNIANIA INFORMACJI	Brak
AU-14	AUDYT SESJI	A.12.4.1*
AU-15	ZDOLNOŚĆ DO ALTERNATYWNEGO AUDYTU (włączone do AU-5(5))	---
AU-16	AUDYT MIĘDZYORGANIZACYJNY	Brak
CA-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CA-2	OCENA ZABEZPIECZEŃ	A.14.2.8, A.18.2.2, A.18.2.3
CA-3	WYMIANA INFORMACJI	A.13.1.2, A.13.2.1, A.13.2.2

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
CA-4	CERTYFIKACJA BEZPIECZEŃSTWA (włączone do CA-2)	---
CA-5	PLAN I ETAPY DZIAŁANIA	8.3, 9.2, 10.1*
CA-6	AUTORYZACJA	9.3*
CA-7	CIĄGŁE MONITOROWANIE	9.1, 9.2, A.18.2.2, A.18.2.3*.
CA-8	BADANIE PENETRACYJNE	Brak
CA-9	POŁĄCZENIA WEWNĘTRZSYSTEMOWE	Brak
CM-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CM-2	KONFIGURACJA BAZOWA	Brak
CM-3	ZABEZPIECZANIE ZMIAN KONFIGURACJI	8.1, A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
CM-4	ANALIZY WPŁYWU	A.14.2.3
CM-5	OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1
CM-6	USTAWIENIA KONFIGURACYJNE	Brak

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
CM-7	ZASADA MINIMALNEJ FUNKCJONALNOŚCI	A.12.5.1*
CM-8	INWENTARYZACJA KOMPONENTÓW SYSTEMU	A.8.1.1, A.8.1.2
CM-9	PLAN ZARZĄDZANIA KONFIGURACJĄ	A.6.1.1*
CM-10	OGRANICZENIA W UŻYCIU OPROGRAMOWANIA	A.18.1.2
CM-11	OPROGRAMOWANIE ZAINSTALOWANE PRZEZ UŻYTKOWNIKA	A.12.5.1, A.12.6.2
CM-12	POŁOŻENIE (LOKACJA) INFORMACJI	Brak
CM-13	MAPOWANIE DZIAŁAŃ NA DANYCH	Brak
CM-14	PODPISYWANIE KOMPONENTÓW	Brak
CP-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CP-2	PLAN CIĄGŁOŚCI DZIAŁANIA	7.5.1, 7.5.2, 7.5.3, A.6.1.1, A.17.1.1, A.17.2.1
CP-3	SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA	A.7.2.2*

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
CP-4	TESTOWANIE PLANU AWARYJNEGO	A.17.1.3
CP-5	AKTUALIZACJA PLANU CIĄGŁOŚCI DZIAŁANIA (włączone do CP-2)	---
CP-6	ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII	A.11.1.4, A.17.1.2, A.17.2.1
CP-7	ZAPASOWE MIEJSCE PRZETWARZANIA	A.11.1.4, A.17.1.2, A.17.2.1
CP-8	USŁUGI TELEKOMUNIKACYJNE	A.11.2.2, A.17.1.2
CP-9	KOPIA ZAPASOWA	A.12.3.1, A.17.1.2, A.18.1.3
CP-10	ODZYSKIWANIE I ODTWARZANIE SYSTEMU	A.17.1.2
CP-11	ALTERNATYWNE PROTOKOŁY KOMUNIKACJI	A.17.1.2*
CP-12	TRYB BEZPIECZNY	Brak
CP-13	ALTERNATYWNE MECHANIZMY BEZPIECZEŃSTWA	A.17.1.2*
IA-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
IA-2	IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI)	A.9.2.1
IA-3	IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA	Brak
IA-4	ZARZĄDZANIE IDENTYFIKATOREM	A.9.2.1
IA-5	ZARZĄDZANIE METODAMI UWIERZYTELNIANIA	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3
IA-6	OCHRONA PROCESU UWIERZYTELNIANIA	A.9.4.2
IA-7	MODUŁ KRYPTOGRAFICZNY UWIERZYTELNIANIE	A.18.1.5
IA-8	IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI)	A.9.2.1
IA-9	IDENTYFIKACJA I UWIERZYTELNIANIE USŁUG	Brak
IA-10	UWIERZYTELNIANIE ADAPTACYJNE	Brak
IA-11	PONOWNE UWIERZYTELNIENIE	Brak
IA-12	POTWIERDZENIE TOŻSAMOŚCI	Brak

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
IR-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1 A.18.1.1, A.18.2.2
IR-2	SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY	A.7.2.2*
IR-3	TESTOWANIE REAGOWANIA NA INCYDENTY	Brak
IR-4	OBSŁUGA INCYDENTÓW	A.16.1.4, A.16.1.5, A.16.1.6
IR-5	MONITOROWANIE INCYDENTÓW	Brak
IR-6	ZGŁASZANIE INCYDENTÓW	A.6.1.3, A.16.1.2
IR-7	WSPARCIE REAGOWANIA NA INCYDENTY	Brak
IR-8	PLAN REAGOWANIA NA INCYDENTY	7.5.1, 7.5.2, 7.5.3, A.16.1.1
IR-9	REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI	Brak
IR-10	ZINTEGROWANY ZESPÓŁ DS. ANALIZY BEZPIECZEŃSTWA INFORMACJI (włączone do IR-4(11))	---

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
MA-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
MA-2	NADZÓR NAD UTRZYMANIEM	A.11.2.4*, A.11.2.5*.
MA-3	NARZĘDZIA UTRZYMANIOWE	Brak
MA-4	UTRZYMANIE ZDALNE	Brak
MA-5	PERSONEL UTZRYMANIOWY	Brak
MA-6	TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI	A.11.2.4
MA-7	KONSERWACJA W TERENIE	Brak
MP-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
MP-2	DOSTĘP DO NOŚNIKÓW DANYCH	A.8.2.3, A.8.3.1, A.11.2.9
MP-3	OZNAKOWANIE NOŚNIKÓW DANYCH	A.8.2.2
MP-4	PRZECHOWYWANIE NOŚNIKÓW DANYCH	A.8.2.3, A.8.3.1, A.11.2.9
MP-5	TRANSPORT NOŚNIKÓW DANYCH	A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.5, A.11.2.6
MP-6	SANITYZACJA NOŚNIKÓW DANYCH	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
MP-7	UŻYWANIE NOŚNIKÓW DANYCH	A.8.2.3, A.8.3.1
MP-8	DEKLASYFIKACJA NOŚNIKÓW DANYCH	Brak
PE-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PE-2	ZEZWOLENIA NA DOSTĘP FIZYCZNY	A.11.1.2*
PE-3	KONTROLA DOSTĘPU FIZYCZNEGO	A.11.1.1, A.11.1.2, A.11.1.3
PE-4	KONTROLA DOSTĘPU DO MEDIUM TRANSMISYJNEGO	A.11.1.2, A.11.2.3
PE-5	KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA	A.11.1.2, A.11.1.3
PE-6	MONITOROWANIE DOSTĘPU FIZYCZNEGO	Brak
PE-7	KONTROLA GOŚCI (włączone do PE-2 i PE-3)	---
PE-8	REJESTRY DOSTĘPU GOŚCI	Brak
PE-9	WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE	A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
PE-10	WYŁĄCZENIE AWARYJNE	A.11.2.2*
PE-11	ZASILANIE AWARYJNE	A.11.2.2
PE-12	OŚWIETLENIE AWARYJNE	A.11.2.2*
PE-13	OCHRONA PRZECIWPOŻAROWA	A.11.1.4, A.11.2.1
PE-14	ZABEZPIECZENIA ŚRODOWISKOWE	A.11.1.4, A.11.2.1, A.11.2.2
PE-15	OCHRONA PRZED ZALANIEM	A.11.1.4, A.11.2.1, A.11.2.2
PE-16	DOSTAWA I USUWANIE	A.8.2.3, A.11.1.6, A.11.2.5
PE-17	ZAPASOWE MIEJSCE PRACY	A.6.2.2, A.11.2.6, A.13.2.1
PE-18	LOKALIZACJA KOMPONENTÓW SYSTEMU	A.8.2.3, A.11.1.4, A.11.2.1
PE-19	ULOT INFORMACJI / ELEKTROMAGNETYCZNA EMISJA UJAWNIAJĄCA	A.11.1.4, A.11.2.1
PE-20	MONITOROWANIE I ŚLEDZENIE ZASOBÓW	A.8.2.3*
PE-21	OCHRONA PRZED IMPULSEM ELEKTROMAGNETYCZNYM	Brak
PE-22	ZNAKOWANIE KOMPONENTÓW	A.8.2.2

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
PE-23	LOKALIZACJA OBIEKTU	A.11.1.4, A.11.2.1
PL-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PL-2	PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI	7.5.1, 7.5.2, 7.5.3, 10.1, A.14.1.1
PL-3	AKTUALIZACJA PLANU BEZPIECZEŃSTWA SYSTEMU (włączone do PL-2)	---
PL-4	ZASADY POSTĘPOWANIA	A.7.1.2, A.7.2.1, A.8.1.3
PL-5	OCENA WPŁYWU NA PRYWATNOŚĆ (włączone do RA-8)	---
PL-6	PLANOWANIE DZIAŁALNOŚCI ZWIĄZANEJ Z BEZPIECZEŃSTWEM (włączone do PL-2)	---
PL-7	KONCEPCJA BEZPIECZEŃSTWA DZIAŁAŃ OPERACYJNYCH	8.1, A.14.1.1
PL-8	ARCHITEKTURA BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI	A.14.1.1*
PL-9	ZARZĄDZANIE CENTRALNE	Brak

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
PL-10	WYBÓR ZABEZPIECZEŃ BAZOWYCH	Brak
PL-11	DOSTOSOWYWANIE ZABEZPIECZEŃ BAZOWYCH	Brak
PM-1	PLAN PROGRAMU BEZPIECZEŃSTWA INFORMACJI	4.1, 4.2, 4.3, 4.4, 5.2, 5.3, 6.1.1, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3, 8.1, 9.3, 10.2, A.5.1.1, A.5.1.2, A.6.1.1, A.18.1.1, A.18.2.2
PM-2	ROLE KIEROWNICZE PROGRAMU BEZPIECZEŃSTWA INFORMACJI	5.1, 5.3, A.6.1.1
PM-3	ZASOBY W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI I OCHRONY PRYWATNOŚCI	5.1, 6.2, 7.1
PM-4	PLAN DZIAŁANIA I ETAPY WPROWADZANIA ZABEZPIECZEŃ	6.1.1, 6.2, 7.5.1, 7.5.2, 7.5.3, 8.3, 9.2, 9.3, 10.1
PM-5	INWENTARYZACJA SYSTEMU	Brak
PM-6	MIARY WYDAJNOŚCI	5.3, 6.1.1, 6.2, 9.1,
PM-7	STRUKTURA ORGANIZACYJNA	Brak
PM-8	PLAN INFRASTRUKTURY KRYTYCZNEJ	Brak
PM-9	STRATEGIA ZARZĄDZANIA RYZYKIEM	4.3, 4.4, 6.1.1, 6.1.2, 6.2, 7.5.1, 7.5.2, 7.5.3, 9.3, 10.2

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
PM-10	PROCES AUTORYZACJI	9.3, A.6.1.1*
PM-11	DEFINICJA MISJI I PROCESU BIZNESOWEGO	4.1
PM-12	ZAGROŻENIA WEWNĘTRZNE	Brak
PM-13	PESONEL BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI	7.2, A.7.2.2*
PM-14	TESTOWANIE, SZKOLENIA I MONITOROWANIE	6.2*
PM-15	GRUPY I STOWARZYSZENIA ZAJMUJĄCE SIĘ BEZPIECZEŃSTWEM I OCHRONĄ PRYWATNOŚCI	7.4, A.6.1.4
PM-16	OSTRZEGANIE O ZAGROŻENIACH	Brak
PM-17	OCHRONA NADZOROWANYCH INFORMACJI JAWNYCH PRZETWARZANYCH W SYSTEMACH ZEWNĘTRZNYCH	Brak
PM-18	PLAN PROGRAMU OCHRONY PRYWATNOŚCI	Brak
PM-19	ROLE KIEROWNICZE PROGRAMU OCHRONY PRYWATNOŚCI	Brak

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
PM-20	ROZPOWSZECHNIANIE INFORMACJI O PROGRAMIE OCHRONY PRYWATNOŚCI	Brak
PM-21	REJESTROWANIE UJAWNIEŃ	Brak
PM-22	ZARZĄDZANIE JAKOŚCIĄ DANYCH OSOBOWYCH	Brak
PM-23	ORGAN ZARZĄDZANIA DANYMI	Brak
PM-24	RADA DS. INTEGRALNOŚCI DANYCH	Brak
PM-25	MINIMALIZACJA DANYCH OSOBOWYCH WYKORZYSTYWANYCH W TESTACH, SZKOLENIACH I BADANIACH	Brak
PM-26	ZARZĄDZANIE SKARGAMI	Brak
PM-27	SPRAWOZDAWCZOŚĆ W ZAKRESIE OCHRONY PRYWATNOŚCI	Brak
PM-28	OPRACOWYWANIE RAM RYZYKA	4.3, 6.1.2, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3
PM-29	ROLE KIEROWNICZE PROGRAMU ZARZĄDZANIA RYZYKIEM	5.1, 5.3, 9.2, A.6.1.1

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
PM-30	STRATEGIA ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW	4.4, 6.2, 7.5.1, 7.5.2, 7.5.3, 10.2*
PM-31	STRATEGIA CIĄGŁEGO MONITORINGU	4.4, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3, 9.1, 10.1, 10.2
PM-32	PRZEZNACZENIE	Brak
PS-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PS-2	OKREŚLANIE RYZYKA DLA STANOWISKA PRACY	Brak
PS-3	DOBÓR PERSONELU	A.7.1.1
PS-4	ZAKOŃCZENIE ZATRUDNIENIA	A.7.3.1, A.8.1.4
PS-5	OBSADZENIE LUB PRZENIESIENIE STANOWISKA	A.7.3.1, A.8.1.4
PS-6	UMOWY DOSTĘPU / WSPÓŁPRACY	A.7.1.2, A.7.2.1, A.13.2.4
PS-7	BEZPIECZEŃSTWO OSOBOWE STRON TRZECICH	A.6.1.1, A.7.2.1*.
PS-8	SANKCJE PERSONALNE	7.3, A.7.2.3
PS-9	OPISY STANOWISK PRACY	A.6.1.1

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
PT-1	POLITYKA I PROCEDURY	Brak
PT-2	UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH	Brak
PT-3	CELE PRZETWARZANIA DANYCH OSOBOWYCH	Brak
PT-4	ZGODY	Brak
PT-5	INFORMACJA O OCHRONIE PRYWATNOŚCI	Brak
PT-6	SYSTEM ZAWIADOMIEŃ O REJESTRACH	Brak
PT-7	SZCZEGÓŁOWE KATEGORIE DANYCH OSOBOWYCH	Brak
PT-8	WYMAGANIA DOTYCZĄCE ZGODNOŚCI PRZY PRZETWARZANIU KOMPUTEROWOWYM	Brak
RA-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
RA-2	KATEGORYZACJA BEZPIECZEŃSTWA	A.8.2.1
RA-3	SZACOWANIE RYZYKA	6.1.2, 8.2, A.12.6.1*

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
RA-4	AKTUALIZACJA SZACOWANIA RYZYKA (włączone do RA-3)	---
RA-5	MONITOROWANIE I SKANOWANIE PODATNOŚCI	A.12.6.1*
RA-6	TECHNICZNE ZABEZPIECZENIE PRZED PODGLĄDEM I PODSŁUCHEM	Brak
RA-7	REAKCJA NA RYZYKO	6.1.3, 8.3, 10.1
RA-8	OCENY WPŁYWU NA PRYWATNOŚĆ	Brak
RA-9	ANALIZA KRYTYCZNOŚCI	A.15.2.2*
RA-10	WYSZUKIWANIE ZAGROŻEŃ	Brak
SA-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 8.1, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SA-2	PRZYDZIAŁ ZASOBÓW	Brak
SA-3	CYKL ŻYCIA SYSTEMU	A.6.1.1, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.6
SA-4	PROCES NABYCIA	8.1, A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2
SA-5	DOKUMENTACJA SYSTEMU	7.5.1, 7.5.2, 7.5.3, A.12.1.1*

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
SA-6	OGRANICZENIA W UŻYCIU OPROGRAMOWANIA (włączone do CM-10 i SI-7)	---
SA-7	OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA (włączone do CM-11 i SI-7)	---
SA-8	ZASADY INŻYNIERII BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI	A.14.2.5
SA-9	USŁUGI SYSTEMU ZEWNĘTRZNEGO	A.6.1.1, A.6.1.5, A.7.2.1, A.13.1.2, A.13.2.2, A.15.2.1, A.15.2.2
SA-10	ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA	A.12.1.2, A.14.2.2, A.14.2.4, A.14.2.7
SA-11	TESTOWANIE I OCENA PRZEZ DEWELOPERA	A.14.2.7, A.14.2.8
SA-12	BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW (włączone do kategorii SR)	---
SA-13	WIARYGODNOŚĆ (włączone do SA-8)	---

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
SA-14	ANALIZA KRYTYCZNOŚCI (włączone do RA-9)	---
SA-15	PROCES ROZWOJU, STANDARDY I NARZĘDZIA	A.6.1.5, A.14.2.1
SA-16	SZKOLENIA PROWADZONE PRZEZ DEWELOPERA	Brak
SA-17	ARCHITEKTURA ORAZ PROJEKT BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI DEWELOPERA	A.14.2.1, A.14.2.5
SA-18	ODPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI (włączone do SR-9)	---
SA-19	AUTENTYCZNOŚĆ KOMPONENTÓW (włączone do SR-11)	---
SA-20	NIESTANDARDOWA (NA ZAMÓWIENIE) ROZBUDOWA KOMPONENTÓW KRYTYCZNYCH	Brak
SA-21	DOBÓR DEWELOPERÓW	A.7.1.1

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
SA-22	KOMPONENTY SYSTEMU BEZ WSPARCIA	Brak
SA-23	SPECJALIZACJA	Brak
SC-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SC-2	ROZDZIELENIE FUNKCJONALNOŚCI SYSTEMU I UŻYTKOWNIKA	Brak
SC-3	IZOLACJA FUNKCJI BEZPIECZEŃSTWA	Brak
SC-4	INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH SYSTEMOWYCH	Brak
SC-5	OCHRONA PRZED BLOKADĄ USŁUG (DoS)	Brak
SC-6	DOSTĘPNOŚĆ ZASOBÓW	Brak
SC-7	OCHRONA POŁĄCZEŃ BRZEGOWYCH	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3
SC-8	POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
SC-9	POUFNOŚĆ TRANSMISJI (włączone do SC-7(18))	---

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
SC-10	ZAKOŃCZENIE POŁĄCZENIA SIECIOWEGO	A.13.1.1
SC-11	ZAUFANA ŚCIEŻKA KOMUNIKACYJNA	Brak
SC-12	GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI	A.10.1.2
SC-13	OCHRONA KRYPTOGRAFICZNA	A.10.1.1, A.14.1.2, A.14.1.3, A.18.1.5
SC-14	OCHRONA DOSTĘPU PUBLICZNEGO (włączone do AC-2, AC-3, AC-5, SI-3, SI-4, SI-5, SI-7, SI-10)	---
SC-15	WSPÓŁPRACUJĄCE URZĄDZENIA I APLIKACJE	A.13.2.1*
SC-16	TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI	Brak
SC-17	CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO	A.10.1.2
SC-18	KOD MOBILNY	Brak

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
SC-19	PROTOKÓŁ TRANSMISJI PAKIETOWEJ (VOIP) (uwzględnione w zabezpieczeniach innych protokołów)	Brak
SC-20	BEZPIECZEŃSTWO NAZW DOMEN / ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA)	Brak
SC-21	BEZPIECZEŃSTWO NAZW DOMEN / USŁUGA USTALANIA ADRESU IP	Brak
SC-22	ARCHITEKTURA NAZW DOMEN / ADRESÓW IP / ZAMAWIANIE USŁUGI DNS	Brak
SC-23	AUTENTYCZNOŚĆ SESJI	Brak
SC-24	PRZEJŚCIE DO OKREŚLONEGO STANU SYSTEMU PO BŁĘDZIE	Brak
SC-25	THIN NODES / TERMINALOWE STACJE ROBOCZE	Brak
SC-26	WABIKI	Brak
SC-27	WIELOPLATFORMOWOŚĆ APLIKACJI	Brak

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
SC-28	OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU	A.8.2.3*
SC-29	HETEROGENICZNOŚĆ SYSTEMU	Brak
SC-30	MASKOWANIE I DEZINFORMACJA	Brak
SC-31	ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI	Brak
SC-32	DZIELENIE SYSTEMU NA PARTYCJE	Brak
SC-33	INTEGRALNOŚĆ TRANSMISJI (włączone do SC-8)	---
SC-34	NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE	Brak
SC-35	ZEWNĘTRZNA IDENTYFIKACJA ZŁOŚLIWEGO KODU	Brak
SC-36	PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE	Brak
SC-37	KANAŁY POZAPASMOWE	Brak
SC-38	BEZPIECZEŃSTWO OPERACJI	A.12.x

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
SC-39	IZOLACJA PROCESÓW	Brak
SC-40	OCHRONA ŁĄCZA BEZPRZEWODOWEGO	Brak
SC-41	DOSTĘP DO PORTÓW I URZĄDZEŃ WEJŚCIA / WYJŚCIA	Brak
SC-42	CZUJNIKI	A.11.1.5*
SC-43	OGRANICZENIA UŻYCIA	Brak
SC-44	KOMORY DETONACYJNE	Brak
SC-45	SYNCHRONIZACJA CZASU SYSTEMOWEGO	Brak
SC-46	EGZEKWOWANIE POLITYKI MIĘDZYDOMENOWEJ	Brak
SC-47	ALTERNATYWNE ŚCIEŻKI KOMUNIKACYJNE	Brak
SC-48	ROZMIWSZCZENIE CZUJNIKÓW	Brak
SC-49	EGZEKWOWANIE SEPARACJI SPRZĘTOWEJ / POLITYKA EGZEKWOWANIA	Brak

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
SC-50	EGZEKWOWANIE SEPARACJI PROGRAMOWEJ / POLITYKA EGZEKWOWANIA	Brak
SC-51	OCHRONA SPRZĘTOWA	Brak
SI-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SI-2	USUWANIE USTEREK	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
SI-3	ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM	A.12.2.1
SI-4	MONITOROWANIE SYSTEMU	Brak
SI-5	ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY	A.6.1.4*
SI-6	WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI	Brak
SI-7	APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI	Brak
SI-8	OCHRONA PRZED SPAMEM	Brak

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
SI-9	OGRANICZENIA WPROWADZANIA INFORMACJI (włączone do AC-2, AC-3, AC-5, AC-6)	---
SI-10	WERYFIKACJA WPROWADZANYCH INFORMACJI	Brak
SI-11	OBSŁUGA BŁĘDÓW	Brak
SI-12	ZARZĄDZANIE I RETENCJA DANYCH	Brak
SI-13	PRZEWIDYWANIE AWARII	Brak
SI-14	ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT)	Brak
SI-15	FILTROWANIE INFORMACJI WYJŚCIOWYCH	Brak
SI-16	OCHRONA PAMIĘCI	Brak
SI-17	PROCEDURY TESTOWANIA AWARYJNEGO „FAIL-SAFE”	Brak
SI-18	OPERACJE SPRAWDZAJĄCE JAKOŚĆ DANYCH OSOBOWYCH	Brak

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
SI-19	DE-IDENTYFIKACJA	Brak
SI-20	SKAŻENIE	Brak
SI-21	ODŚWIEŻANIE INFORMACJI	Brak
SI-22	RÓŻNICOWANIE INFORMACJI	Brak
SI-23	FRAGMENTACJA INFORMACJI	Brak
SR-1	POLITYKA I PROCEDURY	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.15.1.1, A.18.1.1, A.18.2.2
SR-2	PLAN ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW	A.14.2.7*
SR-3	ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW	A.15.1.2, A.15.1.3*.
SR-4	POCHODZENIE	A.14.2.7*
SR-5	STRATEGIE, NARZĘDZIA I METODY NABYCIA	A.15.1.3
SR-6	OCENY I RECENZJE DOSTAWCÓW	A.15.2.1
SR-7	BEZPIECZEŃSTWO OPERACJI W RAMACH ŁAŃCUCHA DOSTAW	A.15.2.2*

ZABEZPIECZENIA NSC 800-53		**ZABEZPIECZENIA PN-ISO/IEC 27001** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
SR-8	UMOWY DOTYCZĄCE POWIADOMIEŃ	Brak
SR-9	ODPORNOŚĆ NA MANIPULACJE I WYKRYWANIE SABOTAŻU	Brak
SR-10	KONTROLA SYSTEMÓW / KOMPONENTÓW	Brak
SR-11	AUTENTYCZNOŚĆ KOMPONENTU	Brak
SR-12	USUWANIE KOMPONENTÓW	Brak

TABELA 2: MAPOWANIE ŚRODKÓW BEZPIECZEŃSTWA: PN-ISO/IEC 27001 – NSC 800-53

Tabela 2 zawiera mapowanie wymagań i zabezpieczeń zawartych w PN-ISO/IEC 27001 z zabezpieczeniami zawartymi w NSC 800-53. Przed zastosowaniem mapowania z tabeli 2 należy zapoznać się z wyjaśnieniami zawartymi we Wprowadzeniu.

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
Wymagania PN-ISO/IEC 27001	
4. Kontekst organizacji	
4.1 Zrozumienie organizacji i jej kontekstu	PM-1, PM-11
4.2 Zrozumienie potrzeb i oczekiwań zainteresowanych stron	PM-1
4.3 Określanie zakresu systemu zarządzania bezpieczeństwem informacji	PM-1, PM-9, PM-28
4.4 System zarządzania bezpieczeństwem informacji	PM-1, PM-9, PM-30, PM-31
5. Przywództwo	
5.1 Przywództwo i zaangażowanie	PM-2, PM-3, PM-29

[4] Nazwy wymagań i zabezpieczeń pochodzą z Polskiej Normy PN-ISO/IEC-27001.

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
5.2 Polityka	Wszystkie zabezpieczenia XX-1
5.3 Role, odpowiedzialność i uprawnienia	Wszystkie zabezpieczenia XX-1, PM-2, PM-6, PM-29
6. Planowanie	
6.1 Działania odnoszące sie do ryzyk i szans	
6.1.1 Postanowienia ogólne	PM-1, PM-4, PM-6, PM-9
6.1.2 Szacowanie ryzyka w bezpieczeństwie informacji	PM-9, PM-28, RA-3
6.1.3 Postępowanie z ryzykiem w bezpieczeństwie informacji	RA-7
6.2 Cele bezpieczeństwa informacji I planowanie ich osiągnięcia	PM-1, PM-3, PM-4, PM-6, PM-9, PM-14, PM-28, PM-30, PM-31
7. Wsparcie	
7.1 Zasoby	PM-3
7.2 Kompetencje	PM-13

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
7.3 Uświadamianie	AT-2, PS-8
7.4 Komunikacja	PM-1, PM-15, PM-28, PM-31
7.5 Udokumentowane informacje	
7.5.1 Postanowienia ogólne	Wszystkie zabezpieczenia XX-1, CP-2, IR-8, PL-2, PM-4, PM-9, PM-28, PM-30, PM-31, SA-5
7.5.2 Opracowywanie i aktualizacja	Wszystkie zabezpieczenia XX-1, CP-2, IR-8, PL-2, PM-4, PM-9, PM-28, PM-30, PM-31, SA-5
7.5.3 Nadzór nad udokumentowanymi informacjami	Wszystkie zabezpieczenia XX-1, CP-2, IR-8, PL-2, PM-4, PM-9, PM-28, PM-30, PM-31, SA-5
8. Działania operacyjne	
8.1 Planowanie i nadzór nad działaniami operacyjnymi	CM-3, PL-7, PM-1, SA-1, SA-4
8.2 Szacowanie ryzyka w bezpieczeństwie informacji	RA-3
8.3 Postępowanie z ryzykiem w bezpieczeństwie informacji	CA-5, PM-4, RA-7

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
9. Ocena wyników	
9.1 Monitorowanie, pomiary, analiza i ocena	CA-1, CA-7, PM-6, PM-31
9.2 Audyt wewnętrzny	CA-1, CA-2, CA-5, CA-7, PM-4
9.3 Przegląd zarządzania	CA-6, PM-1, PM-4, PM-9, PM-10, PM-29
10. Doskonalenie	
10.1 Niezgodność i działania korygujące	CA-5, PL-2, PM-4, PM-31, RA-7
10.2 Ciągłe doskonalenie	PM-1, PM-9, PM-30, PM-31
Zabezpieczenia PN-ISO/IEC 27001	
A.5 Polityki bezpieczeństwa informacji	
A.5.1 Kierunki bezpieczeństwa informacji określane przez kierownictwo	
A.5.1.1 Polityki bezpieczeństwa informacji	Wszystkie zabezpieczenia XX-1

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.5.1.2 Przegląd polityk bezpieczeństwa informacji	Wszystkie zabezpieczenia XX-1
A.6 Organizacja bezpieczeństwa informacji	
A.6.1 Organizacja wewnętrzna	
A.6.1.1 Role i odpowiedzialność za bezpieczeństwo informacji	Wszystkie zabezpieczenia XX-1, CM-9, CP-2, PS-7, PS-9, SA-3, SA-9, PM-2, PM-10
A.6.1.2 Rozdzielanie obowiązków	AC-5
A.6.1.3 Kontakty z organami władzy	IR-6
A.6.1.4 Kontakty z grupami zainteresowanych specjalistów	SI-5, PM-15
A.6.1.5 Bezpieczeństwo informacji w zarządzaniu projektami	SA-3, SA-9, SA-15
A.6.2 Urządzenia mobilne i telepraca	
A.6.2.1 Polityka stosowania urządzeń mobilnych	AC-17, AC-18, AC-19
A.6.2.2 Telepraca	AC-3, AC-17, PE-17

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.7 Bezpieczeństwo zasobów ludzkich	
A.7.1 Przed zatrudnieniem	
A.7.1.1 Postępowanie sprawdzające	PS-3, SA-21
A.7.1.2 Warunki zatrudnienia	PL-4, PS-6
A.7.2 Podczas zatrudnienia	
A.7.2.1 Odpowiedzialność kierownictwa	PL-4, PS-6, PS-7, SA-9
A.7.2.2 Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	AT-2, AT-3, CP-3, IR-2, PM-13
A.7.2.3 Postępowanie dyscyplinarne	PS-8
A.7.3 Zakończenie i zmiana zatrudnienia	
A.7.3.1 Zakończenie zatrudnienia lub zmiana zakresu obowiązków	PS-4, PS-5
A.8 Zarządzanie aktywami	
A.8.1 Odpowiedzialność za aktywa	

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.8.1.1 Inwentaryzacja aktywów	CM-8
A.8.1.2 Własność aktywów	CM-8
A.8.1.3 Akceptowalne użycie aktywów	PL-4
A.8.1.4 Zwrot aktywów	PS-4, PS-5
A.8.2 Klasyfikacja informacji	
A.8.2.1 Klasyfikowanie informacji	RA-2
A.8.2.2 Oznaczanie informacji	MP-3, PE-22
A.8.2.3 Postępowanie z aktywami	MP-2, MP-4, MP-5, MP-6, MP-7, PE-16, PE-18, PE- 20, SC-8, SC-28
A.8.3 Postępowanie z nośnikami	
A.8.3.1 Zarządzanie nośnikami wymiennymi	MP-2, MP-4, MP-5, MP-6, MP-7
A.8.3.2 Wycofywanie nośników	MP-6
A.8.3.3 Przekazywanie nośników	MP-5

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.9 Kontrola dostępu	
A.9.1 Polityka kontroli dostępu	
A.9.1.1 Access control policy	AC-1
A.9.1.2 Dostęp do sieci i usług sieciowych	AC-3, AC-6
A.9.2 Zarządzenie dostępem użytkowników	
A.9.2.1 Rejestrowanie i wyrejestrowywanie użytkowników	AC-2, IA-2, IA-4, IA-5, IA-8
A.9.2.2 Przydzielanie dostępu użytkownikom	AC-2
A.9.2.3 Zarządzanie prawami uprzywilejowanego dostępu	AC-2, AC-3, AC-6, CM-5
A.9.2.4 Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	IA-5
A.9.2.5 Przegląd praw dostępu użytkowników	AC-2

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.9.2.6 Odbieranie lub dostosowywanie praw dostępu	AC-2
A.9.3 Odpowiedzialność użytkowników	
A.9.3.1 Stosowanie poufnych informacji uwierzytelniających	IA-5
A.9.4 Kontrola dostępu do systemów i aplikacji	
A.9.4.1 Ograniczanie dostępu do informacji	AC-3, AC-24
A.9.4.2 Procedury bezpiecznego logowania	AC-7, AC-8, AC-9, IA-6
A.9.4.3 System zarządzania hasłami	IA-5
A.9.4.4 Użycie uprzywilejowanych programów narzędziowych	AC-3, AC-6
A.9.4.5 Kontrola dostępu do kodów źródłowych programów	AC-3, AC-6, CM-5
A.10 Kryptografia	
A.10.1 Zabezpieczenia kryptograficzne	

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.10.1.1 Polityka stosowania zabezpieczeń kryptograficznych	SC-13
A.10.1.2 Zarządzanie kluczami	SC-12, SC-17
A.11 Bezpieczeństwo fizyczne i środowiskowe	
A.11.1 Obszary bezpieczne	
A.11.1.1 Fizyczna granica obszaru bezpiecznego	PE-3*
A.11.1.2 Fizyczne zabezpieczenie wejść	PE-2, PE-3, PE-4, PE-5
A.11.1.3 Zabezpieczenie biur, pomieszczeń i obiektów	PE-3, PE-5
A.11.1.4 Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	CP-6, CP-7, PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23
A.11.1.5 Praca w obszarach bezpiecznych	AC-19(4), SC-42*.
A.11.1.6 Obszary dostaw i załadunku	PE-16
A.11.2 Sprzęt	

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.11.2.1 Lokalizacja i ochrona sprzętu	PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23
A.11.2.2 Systemy wspomagające	CP-8, PE-9, PE-10, PE-11, PE-12, PE-14, PE-15
A.11.2.3 Bezpieczeństwo okablowania	PE-4, PE-9
A.11.2.4 Konserwacja sprzętu	MA-2, MA-6
A.11.2.5 Wynoszenie aktywów	MA-2, MP-5, PE-16
A.11.2.6 Bezpieczeństwo sprzętu i aktywów poza siedzibą	AC-19, AC-20, MP-5, PE-17
A.11.2.7 Bezpieczne zbywanie lub przekazywanie do ponownego użycia	MP-6
A.11.2.8 Pozostawianie sprzętu użytkownika bez opieki	AC-11
A.11.2.9 Polityka czystego biurka i czystego ekranu	AC-11, MP-2, MP-4
A.12 Bezpieczna eksploatacja	
A.12.1 Procedury eksploatacyjne i odpowiedzialność	

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.12.1.1 Dokumentowanie procedur eksploatacyjnych	Wszystkie zabezpieczenia XX-1, SA-5
A.12.1.2 Zarządzanie zmianami	CM-3, CM-5, SA-10
A.12.1.3 Zarządzanie pojemnością	AU-4, CP-2(2), SC-5(2)
A.12.1.4 Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	CM-4(1), CM-5*.
A.12.2 Ochrona przed szkodliwym oprogramowaniem	
A.12.2.1 Zabezpieczenia przed szkodliwym oprogramowaniem	AT-2, SI-3
A.12.3 Kopie zapasowe	
A.12.3.1 Zapasowe kopie informacji	CP-9
A.12.4 Rejestrowanie zdarzeń i monitorowanie	
A.12.4.1 Rejestrowanie zdarzeń	AU-3, AU-6, AU-11, AU-12, AU-14
A.12.4.2 Ochrona informacji w dziennikach zdarzeń	AU-9

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.12.4.3 Rejestrowanie działań administratorów i operatorów	AU-9, AU-12
A.12.4.4 Synchronizacja zegarów	AU-8
A.12.5 Nadzór nad oprogramowaniem produkcyjnym	
A.12.5.1 Instalacja oprogramowania w systemach produkcyjnych	CM-5, CM-7(4), CM-7(5), CM-11
A.12.6 Zarządzanie podatnościami technicznymi	
A.12.6.1 Zarządzanie podatnościami technicznymi	RA-3, RA-5, SI-2, SI-5
A.12.6.2 Ograniczenia w instalowaniu oprogramowania	CM-11
A.12.7 Rozważania dotyczące audytu systemów informacyjnych	
A.12.7.1 Zabezpieczenia audytu systemów informacyjnych	AU-5*
A.13 Bezpieczeństwo komunikacji	

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.13.1 Zarządzanie bezpieczeństwem sieci	
A.13.1.1 Zabezpieczenia sieci	AC-3, AC-17, AC-18, AC-20, SC-7, SC-8, SC-10
A.13.1.2 Bezpieczeństwo usług sieciowych	CA-3, SA-9
A.13.1.3 Rozdzielanie sieci	AC-4, SC-7
A.13.2 Przesyłanie informacji	
A.13.2.1 Polityki i procedury przesyłania informacji	AC-4, AC-17, AC-18, AC-19, AC-20, CA-3, PE-17, SC-7, SC-8, SC-15
A.13.2.2 Porozumienia dotyczące przesyłania informacji	CA-3, PS-6, SA-9
A.13.2.3 Wiadomości elektroniczne	SC-8
A.13.2.4 Umowy o zachowaniu poufności	PS-6
A.14 Pozyskiwanie, rozwój i utrzymanie systemów	

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.14.1 Wymagania związane z bezpieczeństwem systemów informacyjnych	
A.14.1.1 Analiza i specyfikacja wymagań bezpieczeństwa informacji	PL-2, PL-7, PL-8, SA-3, SA-4
A.14.1.2 Zabezpieczanie usług aplikacyjnych w sieciach publicznych	AC-3, AC-4, AC-17, SC-8, SC-13
A.14.1.3 Ochrona transakcji usług aplikacyjnych	AC-3, AC-4, SC-7, SC-8, SC-13
A.14.2 Bezpieczeństwo w procesach rozwoju i wsparcia	
A.14.2.1 Polityka bezpieczeństwa prac rozwojowych	SA-3, SA-15, SA-17
A.14.2.2 Procedury kontroli zmian w systemach	CM-3, SA-10, SI-2
A.14.2.3 Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	CM-3, CM-4, SI-2
A.14.2.4 Ograniczenia dotyczące zmian w pakietach oprogramowania	CM-3, SA-10

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.14.2.5 Zasady projektowania bezpiecznych systemów	SA-8
A.14.2.6 Bezpieczne środowisko rozwojowe	SA-3*
A.14.2.7 Prace rozwojowe zlecane podmiotom zewnętrznym	SA-4, SA-10, SA-11, SA-15, SR-2, SR-4
A.14.2.8 Testowanie bezpieczeństwa systemów	CA-2, SA-11
A.14.2.9 Testy akceptacyjne systemów	SA-4, SR-5(2)
A.14.3 Dane testowe	
A.14.3.1 Ochrona danych testowych	SA-15(9)*.
A.15 Relacje z dostawcami	
A.15.1 Bezpieczeństwo informacji w relacjach z dostawcami	
A.15.1.1 Polityka bezpieczeństwa informacji w relacjach z dostawcami	SR-1
A.15.1.2 Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami	SA-4, SR-3

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.15.1.3 Łańcuch dostaw technologii informacyjnych I telekomunikacyjnych	SR-3, SR-5
A.15.2 Zarządzanie usługami świadczonymi przez dostawców	
A.15.2.1 Monitorowanie i przegląd usług świadczonych przez dostawców	SA-9, SR-6
A.15.2.2 Zarządzenie zmianami w usługach świadczonych przez dostawców	RA-9, SA-9, SR-7
A.16 Zarządzanie incydentami związanymi z bezpieczeństwem informacji	
A.16.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami	
A.16.1.1 Odpowiedzialność i procedury	IR-8
A.16.1.2 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	AU-6, IR-6
A.16.1.3 Zgłaszanie słabości związanych z bezpieczeństwem informacji	SI-2

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.16.1.4 Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji	AU-6, IR-4
A.16.1.5 Reagowanie na incydenty związane z bezpieczeństwem informacji	IR-4
A.16.1.6 Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	IR-4
A.16.1.7 Gromadzenie materiału dowodowego	AU-4, AU-9, AU-10(3), AU-11*
A.17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania	
A.17.1 Ciągłość bezpieczeństwa informacji	
A.17.1.1 Planowanie ciągłości bezpieczeństwa informacji	CP-2
A.17.1.2 Wdrożenie ciągłości bezpieczeństwa informacji	CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13
A.17.1.3 Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji	CP-4

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.17.2 Nadmiarowość	
A.17.2.1 Dostępność środków przetwarzania informacji	CP-2,CP-6, CP-7
A.18 Zgodność	
A.18.1 Zgodność z wymaganiami prawnymi i umownymi	
A.18.1.1 Określenie stosownych wymagań prawnych i umownych	Wszystkie zabezpieczenia XX-1
A.18.1.2 Prawa własności intelektualnej	CM-10
A.18.1.3 Ochrona zapisów	AC-3, AC-23, AU-9, AU-10, CP-9, SC-8, SC-8(1), SC-13, SC-28, SC-28(1)
A.18.1.4 Prywatność i ochrona danych identyfikujących osobę	Dodatek J Kontrola prywatności
A.18.1.5 Regulacje dotyczące zabezpieczeń kryptograficznych	IA-7, SC-12, SC-13, SC-17
A.18.2 **Przeglądy bezpieczeństwa informacji**	

WYMAGANIA I ZABEZPIECZENIA PN-ISO/IEC 27001[4]	**ZABEZPIECZENIA NSC 800-53** *Uwaga: Gwiazdka (*) wskazuje, że zabezpieczenie PN-ISO/IEC nie spełnia w pełni intencji zabepieczenia zawartego w NSC 800-53*
A.18.2.1 Niezależny przegląd bezpieczeństwa informacji	CA-2(1), SA-11(3)
A.18.2.2 Zgodność z politykami bezpieczeństwa i standardami	Wszystkie Zabezpieczenia XX-1, CA-2
A.18.2.3 Sprawdzanie zgodności technicznej	CA-2