					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P21					Tytuł dokumentu: **Polityka bezpieczeństwa sieci**							
Wersja: 1.0		Data wejścia w życie: 01.01.2025			Właściciel dokumentu:							
X	Polityka		Standard		Procedura		Formularz		Rejestr		Inne	

Historia zmian				
Numer zmiany	**Data zmiany**	**Zmiany**	**Przegląd wykonał**	**Właściciel procesu**

Zatwierdzenia			
Imię i nazwisko	**Stanowisko**	**Data**	**Podpis**

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 8	N/D
ISO/IEC 27002:2022	Zabezpieczenia 8.20-8.22	N/D
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	N/D
RODO	Artykuł 32	N/D
Dyrektywa NIS2	Artykuł 21(2)(d)	N/D
Rozporządzenie DORA	Artykuł 9	N/D
COBIT 2019	DSS01.03, DSS05.01, MEA03	N/D

1. Cel

1.1 Celem niniejszej polityki jest określenie wymagań organizacji dotyczących ochrony sieci wewnętrznych i zewnętrznych przed nieuprawnionym dostępem, zakłóceniem usług, przechwyceniem danych oraz niewłaściwym wykorzystaniem.

1.2 Polityka zapewnia, że cała infrastruktura sieciowa — w tym fizyczna, wirtualna, chmurowa i hybrydowa — jest chroniona za pomocą warstwowych zabezpieczeń, takich jak segmentacja, egzekwowanie reguł zapór sieciowych, bezpieczny routing oraz scentralizowane monitorowanie.

1.3 Niniejsza polityka zapewnia stosowanie wymagań ISO/IEC 27001, klauzuli 8.1, oraz zabezpieczeń załącznika A od 8.20 do 8.22, a także zgodność z mającymi zastosowanie obowiązkami prawnymi i regulacyjnymi wynikającymi z art. 32 RODO, art. 21 dyrektywy NIS2 oraz art. 9 rozporządzenia DORA.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich sieci oraz powiązanych komponentów infrastruktury, w tym:

2.1.1 routerów, przełączników, bezprzewodowych punktów dostępowych oraz zapór sieciowych;

2.1.2 sieci wirtualnych w chmurze (np. AWS VPC, Azure VNet), koncentratorów VPN oraz systemów SD-WAN;

2.1.3 wewnętrznych sieci LAN, stref zdemilitaryzowanych (DMZ), ścieżek dostępu zdalnego oraz połączeń między lokalizacjami lub ze stronami trzecimi;

2.1.4 systemów wspierających, takich jak DNS, DHCP, serwery proxy oraz urządzenia monitorujące.

2.2 Polityka jest wiążąca dla całego personelu oraz dostawców zewnętrznych, którzy zarządzają sieciami organizacji, konfigurują je, monitorują lub integrują się z nimi, niezależnie od tego, czy działają w infrastrukturze lokalnej, czy w chmurze.

2.3 Wszystkie systemy i aplikacje podłączone do sieci organizacji — niezależnie od lokalizacji lub własności — muszą spełniać wymagania bezpieczeństwa sieci określone w niniejszej polityce.

3. Cele

3.1 Zapewnienie poufności, integralności i dostępności (CIA) danych przesyłanych przez sieci poprzez stosowanie silnych mechanizmów kontroli dostępu, bezpiecznego routingu i monitorowania.

3.2 Zapobieganie nieuprawnionemu dostępowi, ruchowi bocznemu oraz wykorzystaniu zasobów sieciowych poprzez egzekwowanie segmentacji, strefowania i ochrony granic sieci.

3.3 Utrzymywanie spójnych konfiguracji sieciowych opartych na standardach branżowych i danych wywiadowczych o zagrożeniach w celu ochrony przed ewoluującymi cyberzagrożeniami.

3.4 Zabezpieczenie komunikacji zewnętrznej, łączności chmurowej oraz dostępu zdalnego z wykorzystaniem szyfrowanych kanałów, silnego uwierzytelniania oraz walidacji punktów końcowych.

3.5 Zapewnienie widoczności aktywności sieciowej poprzez scentralizowane rejestrowanie, inspekcję ruchu w czasie rzeczywistym oraz automatyczne alerty.

3.6 Zapewnienie zgodności regulacyjnej poprzez dostosowanie wszystkich operacji sieciowych do wymagań norm ISO/IEC 27001:2022, RODO, NIS2, DORA oraz COBIT 2019.

4. Role i odpowiedzialności

4.1 Dyrektor ds. Bezpieczeństwa Informacji (CISO)

4.1.1 Jest właścicielem niniejszej polityki oraz zapewnia jej przegląd i zgodność z nadrzędną strategią cyberbezpieczeństwa organizacji.

4.1.2 Zatwierdza modele segmentacji sieci, zbiory reguł zapór sieciowych dla systemów wrażliwych oraz wnioski o odstępstwo.

4.2 Menedżer Bezpieczeństwa Sieci / Kierownik ds. Bezpieczeństwa Infrastruktury

4.2.1 Zarządza architekturą zabezpieczeń sieci, w tym zaporami sieciowymi, systemami wykrywania i zapobiegania włamaniom (IDS/IPS), sieciami VPN oraz bezpiecznym routingiem.

4.2.2 Nadzoruje segmentację sieci, przypisania VLAN, strefowanie ruchu oraz łączność zewnętrzną.

4.2.3 Zapewnia ciągły przegląd filtrowania ruchu przychodzącego i wychodzącego oraz stosowanie modelu Zero Trust we wszystkich warstwach sieci.

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Wymagania dotyczące przeglądu i aktualizacji

9.1 Niniejsza polityka podlega corocznemu przeglądowi przez Menedżera Bezpieczeństwa Sieci we współpracy z CISO oraz aktualizacji na podstawie:

9.1.1 pojawiających się zagrożeń (np. nowych technik ataku, podatności protokołów);

9.1.2 zmian w infrastrukturze (np. migracji do chmury, wdrożeń SD-WAN);

9.1.3 aktualizacji regulacyjnych lub zmian w normach mających wpływ na zabezpieczenia sieci;

9.1.4 ustaleń audytowych, trendów incydentów lub pogorszenia wydajności spowodowanego przez zabezpieczenia.

9.2 Przeglądy muszą być również inicjowane przez:

9.2.1 istotne zmiany architektury sieci;

9.2.2 wdrożenie nowych platform zapór sieciowych, VPN lub sieci chmurowych;

9.2.3 wycofanie z eksploatacji kluczowych aktywów lub stref zaufanych.

9.3 Aktualizacje muszą być rejestrowane w Rejestrze dokumentów SZBI i przekazywane do:

9.3.1 zespołów infrastruktury i operacji sieciowych;

9.3.2 zespołów SOC i inżynierii bezpieczeństwa;

9.3.3 zespołów aplikacyjnych zależnych od przepływów sieciowych;

9.3.4 wszystkich dostawców zewnętrznych posiadających aktywną łączność międzyśrodowiskową.

9.4 Wszystkie poprzednie wersje polityki muszą być archiwizowane w sposób bezpieczny wraz z adnotacjami historii zmian, aby zachować ścieżkę audytu i identyfikowalność zmian.

10. Powiązane polityki i odniesienia

10.1 P1 - Polityka bezpieczeństwa informacji. Ustanawia podstawowe zasady bezpieczeństwa i wymaga stosowania ochrony warstwowej, w tym kontroli dostępu i mechanizmów ochrony przed zagrożeniami opartych na sieci.

10.2 P4 - Polityka kontroli dostępu. Zapewnia, że segmentacja sieci jest egzekwowana zgodnie z rolami użytkowników, zasadą najmniejszych uprawnień oraz zasadami nadawania uprawnień dostępu.

10.3 P5 - Polityka zarządzania zmianami. Reguluje modyfikacje zapór sieciowych, zmiany reguł VPN oraz zmiany routingu w udokumentowanym procesie podlegającym kontroli audytowej.

10.4 P12 - Polityka zarządzania aktywami. Wspiera identyfikację i klasyfikację systemów sieciowych oraz zapewnia, że wszystkie podłączone aktywa są zarządzane zgodnie z zakresem określonym w polityce.

10.5 P22 - Polityka rejestrowania i monitorowania. Reguluje gromadzenie, korelację i przechowywanie logów sieciowych, w tym zdarzeń zapór sieciowych, prób dostępu i wykrytych anomalii.

10.6 P30 - Polityka reagowania na incydenty. Określa procedury eskalacji, odizolowania i eliminacji w odpowiedzi na zagrożenia lub włamania przenoszone siecią, takie jak DDoS, ruch boczny lub nieuprawniony dostęp.

11. Normy i ramy odniesienia

11.1 Niniejsza polityka jest zgodna z międzynarodowymi normami oraz wymogami regulacyjnymi określającymi bezpieczne operacje sieciowe, segmentację, ochronę granic oraz bezpieczny dostęp zdalny.

11.2 ISO/IEC 27001

11.2.1 Klauzula 8.1 - Planowanie operacyjne i nadzór: wymaga, aby zabezpieczenia techniczne, w tym zabezpieczenia sieciowe, były wbudowane w procesy operacyjne.

11.3 ISO/IEC 27002:2022

11.3.1 Zabezpieczenia 8.20-8.22. Zawierają wytyczne dotyczące ochrony sieci, segmentacji usług oraz zabezpieczania usług sieciowych za pomocą mechanizmów kontroli dostępu i monitorowania.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - Ochrona granic: wymaga stosowania kontroli brzegowych, segmentacji i bezpiecznych połączeń między systemami.

11.4.2 AC-4 - Egzekwowanie przepływu informacji: wspiera strefowanie i ograniczenia ruchu oparte na regułach.

11.4.3 SC-32 - Podział systemów informatycznych: promuje logiczne rozdzielenie systemów informatycznych.

11.5 RODO (2016/679)

11.5.1 Artykuł 32 - Bezpieczeństwo przetwarzania: wymaga stosowania środków technicznych — takich jak zapory sieciowe i segmentacja — w celu ochrony danych osobowych.

11.6 Dyrektywa UE NIS2 (2022/2555)

11.6.1 Artykuł 21(2)(d): wymaga skutecznego bezpieczeństwa sieci i systemów informacyjnych, ochrony granic, bezpiecznej konfiguracji oraz kontroli separacji.

11.7 Rozporządzenie DORA (2022/2554)

11.7.1 Artykuł 9 - Zarządzanie ryzykiem ICT: nakłada na podmioty finansowe obowiązek ochrony sieci i połączeń wzajemnych przed nieuprawnionym dostępem, wyciekiem danych i zakłóceniami operacyjnymi.

11.8 COBIT 2019

11.8.1 DSS01.03 - Monitorowanie infrastruktury: wymaga proaktywnej kontroli stanu infrastruktury sieciowej i łączności.

11.8.2 DSS05.01 - Ochrona przed złośliwym oprogramowaniem: obejmuje segmentację i kontrolę granic w celu ograniczenia rozprzestrzeniania się zagrożeń.

11.8.3 MEA03 - Monitorowanie, ocena i zgodność: wzmacnia stosowanie polityki sieciowej oraz oceny zgodności.