					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P21S					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**

Nota prawna (prawa autorskie i ograniczenia użytkowania)

(C) 2025 Clarysec LLC. All rights reserved.

Niniejszy dokument stanowi własność intelektualną spółki Clarysec LLC. Żadna część tego dokumentu nie może być kopiowana, ponownie wykorzystywana, rozpowszechniana ani modyfikowana do celów komercyjnych lub wdrożeniowych bez uprzedniej wyraźnej pisemnej zgody.
Nieuprawnione użycie jest surowo zabronione i może skutkować podjęciem kroków prawnych.
W sprawach licencjonowania prosimy o kontakt: info@clarysec.com

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 8	-
ISO/IEC 27002:2022	Środek kontrolny 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
RODO	Artykuł 32	-
Dyrektywa NIS2	Artykuły 21(2)(d), (e)	-
Rozporządzenie DORA	Artykuły 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Cel

1.1. Celem niniejszej polityki jest zapewnienie ochrony całej wewnętrznej i zewnętrznej komunikacji sieciowej przed nieuprawnionym dostępem, manipulacją, podsłuchem oraz niewłaściwym wykorzystaniem poprzez wdrożenie jasno określonych środków bezpieczeństwa.

1.2. Polityka ustanawia zasady bezpiecznego projektowania, użytkowania i zarządzania infrastrukturą sieciową, w tym routerami, bezprzewodowymi punktami dostępowymi, połączeniami dostępu zdalnego oraz sieciami segmentowanymi.

1.3. Jej celem jest minimalizacja ekspozycji na zagrożenia internetowe, zapewnienie poufności danych przesyłanych przez sieci wewnętrzne i zewnętrzne oraz utrzymanie dostępności usług krytycznych.

1.4. Niniejsza polityka wspiera certyfikację ISO/IEC 27001:2022 i bezpośrednio przyczynia się do spełnienia obowiązków prawnych i regulacyjnych wynikających z RODO, NIS2 oraz DORA, a także stanowi techniczne potwierdzenie stosowanych zabezpieczeń dla klientów i audytorów.

2. Zakres

2.1. Niniejsza polityka ma zastosowanie do wszystkich komponentów sieci IT organizacji, w tym:

2.1.1. infrastruktury przewodowej i bezprzewodowej w lokalizacjach biurowych,

2.1.2. routerów, przełączników, punktów dostępowych, zapór sieciowych i bram,

2.1.3. połączeń dostępu zdalnego, w tym VPN, RDP oraz tuneli do chmury obliczeniowej,

2.1.4. aplikacji chmurowych, do których uzyskuje się dostęp z sieci wewnętrznych lub zewnętrznych,

2.1.5. urządzeń podłączonych do sieci przez pracowników, kontrahentów lub gości.

2.2. Niniejsza polityka reguluje zarówno fizyczne, jak i logiczne segmenty sieci, w tym strefy gościnne, urządzenia Internetu rzeczy (IoT) oraz systemy zaplecza administracyjnego.

2.3. Polityka obejmuje cały personel posiadający dostęp do sieci organizacji, w tym:

2.3.1. pracowników wewnętrznych,

2.3.2. pracowników zdalnych i personel pracujący hybrydowo,

2.3.3. zewnętrznych dostawców, konsultantów i usługodawców,

2.3.4. gości korzystających z tymczasowego dostępu Wi-Fi.

3. Cele

3.1. Zapewnienie ochrony sieci organizacji przed nieuprawnionym dostępem i zewnętrznymi zagrożeniami cybernetycznymi.

3.2. Zapewnienie właściwej segmentacji pomiędzy sieciami zaufanymi i niezaufanymi (np. gościnne Wi-Fi, dostęp dostawców).

3.3. Umożliwienie bezpiecznej łączności zdalnej bez narażania systemów wewnętrznych.

3.4. Zapobieganie rozprzestrzenianiu się złośliwego oprogramowania i eksfiltracji danych przez kanały sieciowe.

3.5. Zapewnienie monitorowania, alertowania i audytowalności aktywności sieciowej na potrzeby wykrywania incydentów i zgodności.

3.6. Zapewnienie, że do sieci wewnętrznych mogą być podłączane wyłącznie zatwierdzone i odpowiednio zabezpieczone urządzenia.

3.7. Spełnienie wymagań wynikających z ISO/IEC 27001, RODO oraz powiązanych ram cyberbezpieczeństwa.

4. Role i odpowiedzialności

4.1. Dyrektor Generalny (GM)

4.1.1. Jest właścicielem niniejszej polityki i zapewnia przydzielenie odpowiednich zasobów na potrzeby bezpiecznego projektowania i zarządzania siecią.

4.1.2. Dokonuje przeglądu odstępstw od środków bezpieczeństwa sieci oraz zatwierdza ustalenia dotyczące dostępu sieciowego dostawców.

4.1.3. Dokonuje przeglądu incydentów lub ustaleń audytowych związanych ze słabościami w obszarze bezpieczeństwa sieci.

4.2. Dostawca wsparcia IT / wewnętrzna funkcja IT

4.2.1. Wdraża, konfiguruje i utrzymuje wszystkie zapory sieciowe, routery, przełączniki oraz kontrolery sieci bezprzewodowej.

4.2.2. Zarządza segmentacją pomiędzy sieciami wewnętrznymi, gościnnymi i zewnętrznymi.

4.2.3. Monitoruje logi i alerty pod kątem prób nieuprawnionego dostępu lub anomalii sieciowych.

4.2.4. Zapewnia bezpieczne i terminowe wdrażanie aktualizacji oprogramowania układowego oraz zmian konfiguracyjnych.

[... 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. Coroczny przegląd

9.1.1. Niniejsza polityka musi być przeglądana co najmniej raz w roku przez Dyrektora Generalnego wspólnie z dostawcą wsparcia IT i Koordynatorem ds. prywatności.

9.2. Przesłanki przeglądu międzyokresowego

9.2.1. Przegląd polityki musi być również uruchamiany w przypadku:

9.2.1.1. istotnych zmian architektury sieci (np. nowych systemów VPN lub zapór sieciowych),

9.2.1.2. incydentu związanego z siecią (np. włamania, rozprzestrzenienia ransomware lub eksfiltracji danych),

9.2.1.3. zmian prawnych, regulacyjnych lub w ramach odniesienia wpływających na ochronę sieci,

9.2.1.4. nowych platform dostawców wymagających alternatywnych metod dostępu lub protokołów.

9.3. Zarządzanie wersjami i dokumentacją

9.3.1. Zmiany w polityce muszą być rejestrowane wraz z numerem wersji, datą oraz podsumowaniem zmian.

9.3.2. Poprzednie wersje muszą być archiwizowane przez okres nie krótszy niż 3 lata.

9.3.3. Aktualizacje muszą być komunikowane pracownikom, których dotyczą, wraz z wymaganym potwierdzeniem zapoznania się, jeżeli wprowadzane są istotne zmiany w wymaganych zachowaniach.

10. Powiązane polityki i zależności

10.1. Niniejsza polityka musi być stosowana łącznie z następującymi politykami bezpieczeństwa dla SME:

10.1.1. P9S – Polityka pracy zdalnej: określa bezpieczne metody dostępu zdalnego, wymagania dotyczące VPN oraz ochronę punktów końcowych dla użytkowników pracujących poza lokalizacją.

10.1.2. P12S – Polityka zarządzania aktywami: zapewnia, że wszystkie systemy podłączone do sieci są zidentyfikowane, skategoryzowane i ewidencjonowane wraz z aktualnym statusem bezpieczeństwa.

10.1.3. P17S – Polityka ochrony danych i prywatności: zapewnia, że segmentacja sieci, środki kontroli dostępu i rejestrowanie wspierają zasady prywatności i ochrony danych wynikające z RODO.

10.1.4. P22S – Polityka rejestrowania i monitorowania: określa wymagania dotyczące gromadzenia i przeglądu logów z urządzeń sieciowych, połączeń zdalnych oraz kontrolerów sieci bezprzewodowej.

10.1.5. P30S – Polityka reagowania na incydenty: definiuje wymagane działania w odpowiedzi na naruszenia sieci, próby nieuprawnionego dostępu lub rozprzestrzenianie się złośliwego oprogramowania przez sieci wewnętrzne.

11. Normy i ramy odniesienia

11.1. ISO/IEC 27001

11.1.1. Klauzula 8.1 – wymaga wdrożenia środków kontroli zapewniających bezpieczne i odporne operacje, w tym w obszarze sieci.

11.2. ISO/IEC 27002

11.2.1. Środek kontrolny 8.20 – zawiera wytyczne techniczne i proceduralne dotyczące zabezpieczania dostępu sieciowego, segmentacji i monitorowania.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – wymaga kontroli przepływu informacji w sieciach i między systemami.

11.3.2. SC-7 – wymaga ochrony granic, bezpiecznego routingu i segmentacji sieci w celu ograniczenia ryzyka nieuprawnionego dostępu.

11.4. RODO

11.4.1. Artykuł 32 – wymaga zastosowania odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poufności, integralności i dostępności systemów i usług sieciowych przetwarzających dane osobowe.

11.5. Dyrektywa UE NIS2

11.5.1. Artykuł 21(2)(d) – wymaga technicznych środków opartych na ryzyku, w tym bezpieczeństwa sieci i kontroli dostępu.

11.5.2. Artykuł 21(2)(e) – wymaga segmentacji i izolacji systemów, aby zapobiegać rozprzestrzenianiu się incydentów cybernetycznych.

11.6. Rozporządzenie DORA

11.6.1. Artykuł 9 – wymaga wdrożenia środków kontroli w zakresie zarządzania ryzykiem ICT, w tym dotyczących bezpiecznych sieci i komunikacji.

11.6.2. Artykuł 10 – wymaga, aby strategie odporności cyfrowej obejmowały ochronę infrastruktury sieciowej i łączności zdalnej.

11.7. COBIT 2019

11.7.1. DSS05.02 – wymaga skutecznej ochrony infrastruktury IT i środowisk sieciowych przed zagrożeniami wewnętrznymi i zewnętrznymi.

11.7.2. APO13.01 – wymaga strategii zarządzania ryzykiem obejmujących segmentację sieci i monitorowanie jako element ograniczania zagrożeń.