					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P38					Tytuł dokumentu: **Polityka bezpiecznej komunikacji i uwierzytelniania wieloskładnikowego**							
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	5.30, 5.31, 8.24	
ISO/IEC 27002:2022	5.15, 5.17, 5.18, 8.24, 8.28	
NIST SP 800-53 Rev.5	IA-2, IA-3, IA-5, IA-8, SC-12, SC-13, SC-31	
RODO	Art. 32 ust. 1 lit. b	
Dyrektywa NIS2	Art. 21 ust. 2 lit. j	
Rozporządzenie DORA	Art. 9 ust. 2 lit. d, Art. 11	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Cel

1.1 Niniejsza polityka określa wymagania dotyczące stosowania uwierzytelniania wieloskładnikowego lub rozwiązań ciągłego uwierzytelniania przy dostępie do systemów, zgodnie z art. 21 ust. 2 lit. j Dyrektywy NIS2.

1.2 Niniejsza polityka ustanawia środki kontrolne dotyczące bezpiecznej komunikacji głosowej, wideo, tekstowej oraz komunikacji awaryjnej w celu ochrony poufności i integralności informacji.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich mechanizmów uwierzytelniania oraz systemów komunikacji (połączeń głosowych, wideokonferencji, komunikatorów i systemów powiadamiania awaryjnego) wykorzystywanych przez organizację.

2.2 Obejmuje wszystkich pracowników i współpracowników oraz wszelkie strony trzecie korzystające z kanałów komunikacji organizacji lub uzyskujące dostęp do jej sieci i systemów informacyjnych.

3. Cele

3.1 Należy zapewnić, aby dostęp do systemów uzyskiwali wyłącznie użytkownicy poddani odpowiedniemu uwierzytelnieniu, co ogranicza ryzyko nieuprawnionego dostępu poprzez wdrożenie uwierzytelniania wieloskładnikowego.

3.2 Należy zapewnić, aby komunikacja wewnętrzna i awaryjna była realizowana z wykorzystaniem bezpiecznych metod, takich jak szyfrowane kanały, co zapobiega podsłuchowi lub manipulacji.

3.3 Należy spełnić wymagania Dyrektywy NIS2 w zakresie silnego uwierzytelniania i bezpiecznej komunikacji, wzmacniając ogólną cyberodporność organizacji.

4. Role i odpowiedzialności

4.1 Dyrektor ds. Bezpieczeństwa Informacji (CISO) / zespoły IT i bezpieczeństwa informacji: definiują i utrzymują mechanizmy uwierzytelniania wieloskładnikowego oraz narzędzia bezpiecznej komunikacji; zapewniają techniczne egzekwowanie postanowień niniejszej polityki.

4.2 Administratorzy IT: wdrażają uwierzytelnianie wieloskładnikowe dla odpowiednich systemów i konfigurują zatwierdzone platformy bezpiecznej komunikacji; monitorują zgodność.

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

9. Monitorowanie i audyt

9.1 Zespoły IT i bezpieczeństwa informacji muszą stale monitorować dzienniki uwierzytelniania pod kątem prób logowania z użyciem pojedynczego składnika uwierzytelniającego lub anomalii związanych z niepowodzeniami uwierzytelniania wieloskładnikowego. Dzienniki systemów bezpiecznej komunikacji, tam gdzie ma to zastosowanie, muszą być monitorowane pod kątem prób nieuprawnionego dostępu lub zmian konfiguracji.

9.2 Funkcja audytu wewnętrznego / zgodności corocznie przeprowadza przegląd przestrzegania wymagań dotyczących wdrożenia uwierzytelniania wieloskładnikowego, w tym potwierdza, że wszystkie systemy krytyczne wymuszają uwierzytelnianie wieloskładnikowe, oraz weryfikuje, że do komunikacji wrażliwej wykorzystywane są wyłącznie zatwierdzone bezpieczne kanały. Ustalenia są przekazywane kierownictwu wraz z rekomendacjami.

10. Przegląd i utrzymanie

10.1 Niniejsza polityka podlega przeglądowi co najmniej raz w roku oraz po każdym istotnym incydencie bezpieczeństwa lub nowo zidentyfikowanym ryzyku związanym z uwierzytelnianiem lub komunikacją (np. nowych wektorach zagrożeń wymierzonych w uwierzytelnianie wieloskładnikowe lub wykryciu korzystania z niezabezpieczonych kanałów komunikacji).

10.2 Aktualizacje są wprowadzane w razie potrzeby, aby uwzględnić rozwój technologii (np. wdrożenie bardziej odpornych rozwiązań ciągłego uwierzytelniania) lub zapewnić zgodność ze zaktualizowanymi wytycznymi regulacyjnymi, takimi jak przyszłe zalecenia ENISA dotyczące bezpiecznej komunikacji.

11. Powiązane polityki i zależności

11.1 P01 – P01 Polityka bezpieczeństwa informacji. Określa wymagania organizacyjne dotyczące zabezpieczeń uwierzytelniania i komunikacji.

11.2 P04 – Polityka kontroli dostępu. Ustanawia nadzór nad dostępem, który w ramach P38 jest wspierany przez uwierzytelnianie wieloskładnikowe.

11.3 P11 – Polityka zarządzania kontami użytkowników i uprawnieniami. Łączy uwierzytelnianie wieloskładnikowe z cyklem życia dostępu uprzywilejowanego.

11.4 P18 – Polityka zabezpieczeń kryptograficznych. Określa zatwierdzone metody kryptograficzne oraz zarządzanie kluczami dla bezpiecznej komunikacji.

11.5 P21 – Polityka bezpieczeństwa sieci. Zabezpiecza kanały transmisji wykorzystywane przez komunikację głosową, wideo i komunikatory.

11.6 P22 – Polityka logowania i monitorowania. Obejmuje monitorowanie zdarzeń uwierzytelniania oraz korzystania z bezpiecznych kanałów.

11.7 P32 – Polityka ciągłości działania i odtwarzania po awarii. Zabezpiecza komunikację awaryjną podczas sytuacji kryzysowych.

11.8 P08 – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji. Obejmuje szkolenia użytkowników dotyczące uwierzytelniania wieloskładnikowego i higieny korzystania z kanałów komunikacji.

12. Odniesienia

12.1 Dyrektywa NIS2 (UE 2022/2555), art. 21 ust. 2 lit. j (stosowanie uwierzytelniania wieloskładnikowego i zabezpieczonej komunikacji)

12.2 Rozporządzenie wykonawcze Komisji (UE) 2024/2690, załącznik, sekcja 11 (wymagania dotyczące kontroli dostępu, w tym uwierzytelnianie wieloskładnikowe dla kont uprzywilejowanych)

12.3 ISO/IEC 27001:2022 oraz ISO/IEC 27002: