					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P35					Tytuł dokumentu: **Polityka bezpieczeństwa IoT / OT**							
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	
ISO/IEC 27002:2022	Środki kontrolne 5.7, 5.23, 5.27, 5.31, 5.36	
NIST SP 800-53 Rev.5	SC-7, SI-4, CM-2, AC-6, PL-8	
RODO	Artykuły 5, 25, 32	
Dyrektywa NIS2	Artykuły 21, 23	
Rozporządzenie DORA	Artykuły 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Cel

1.1 Niniejsza polityka ustanawia obowiązkowe wymagania bezpieczeństwa informacji dotyczące wdrażania, eksploatacji, monitorowania i wycofywania z eksploatacji systemów Internetu rzeczy (IoT) oraz technologii operacyjnej (OT) w organizacji.

1.2 Zapewnia ona, że systemy te są zintegrowane z szerszym systemem zarządzania cyberbezpieczeństwem organizacji oraz chronione przed naruszeniem, niewłaściwym użyciem lub sabotażem operacyjnym.

1.3 Celem polityki jest egzekwowanie silnych zabezpieczeń technicznych, organizacyjnych i proceduralnych w celu ochrony systemów IoT/OT współpracujących z infrastrukturą fizyczną, procesami produkcyjnymi i środowiskami krytycznymi dla bezpieczeństwa.

1.4 Wspiera ona realizację obowiązków regulacyjnych i umownych w obszarach cyberbezpieczeństwa, bezpieczeństwa, kontroli środowiskowej i ciągłości działania.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich systemów IoT i OT — niezależnie od tego, czy stanowią własność organizacji, są leasingowane, czy dostarczane przez strony trzecie — wykorzystywanych w środowiskach operacyjnych, administracyjnych lub produkcyjnych organizacji.

2.2 Systemy objęte zakresem obejmują między innymi:

2.2.1 urządzenia IoT, takie jak czujniki środowiskowe, systemy kontroli dostępu, inteligentne oświetlenie, sprzęt dozorowy oraz urządzenia ubieralne

2.2.2 platformy technologii operacyjnej, takie jak sterowniki PLC, systemy SCADA, rozproszone systemy sterowania, panele HMI, interfejsy systemów realizacji produkcji (MES) oraz sterowniki polowe

2.2.3 sieci sterowania przemysłowego lub zasoby połączone z chmurą monitorujące operacje fizyczne

2.3 Polityka obejmuje:

2.3.1 wszystkie środowiska (infrastruktura lokalna, brzegowa, zarządzana z chmury)

2.3.2 wszystkich interesariuszy (użytkowników wewnętrznych, integratorów, zewnętrznych dostawców, wykonawców)

2.3.3 wszystkie fazy cyklu życia (projektowanie, zakupy, wdrażanie, eksploatacja, wycofywanie z eksploatacji)

3. Cele

3.1 Zabezpieczenie infrastruktury IoT i OT przed wewnętrznymi i zewnętrznymi zagrożeniami cyberbezpieczeństwa, w tym atakami typu denial of service, nieuprawnionym dostępem, rozprzestrzenianiem ransomware oraz manipulacją oprogramowaniem układowym.

3.2 Zapewnienie, że platformy IoT/OT nie staną się wektorem ataków pomiędzy środowiskami IT i OT ani źródłem naruszenia systemów krytycznych dla bezpieczeństwa.

3.3 Stosowanie zasad bezpieczeństwa już na etapie projektowania oraz obrony wielowarstwowej w całym cyklu życia tych technologii.

3.4 Umożliwienie niezawodnej, bezpiecznej i audytowalnej integracji platform IoT i OT z centrum operacji bezpieczeństwa (SOC) organizacji oraz planami reagowania na incydenty.

3.5 Zapewnienie, że wszystkie wdrożenia są zgodne ze środkami kontrolnymi ISO/IEC 27001 oraz mającymi zastosowanie wytycznymi sektorowymi (np. IEC 62443, ISO/IEC 27019, NIST SP 800-82).

4. Role i odpowiedzialności

4.1 Dyrektor ds. bezpieczeństwa informacji (CISO) / kierownik ds. bezpieczeństwa

4.1.1 Określa polityki i standardy techniczne w zakresie cyberbezpieczeństwa IoT/OT.

4.1.2 Nadzoruje oceny ryzyka, walidację zabezpieczeń oraz koordynację międzydziałową.

4.2 Inżynierowie OT / kierownicy obiektów i zakładów

4.2.1 Walidują konfiguracje systemów OT i egzekwują zgodność z polityką w obszarach produkcyjnych.

4.2.2 Utrzymują zabezpieczenia fizyczne i logiczne zapewniające integralność i bezpieczeństwo środowiska OT.

[... 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 musi być poddawana przeglądowi co najmniej raz w roku i aktualizowana na podstawie:

9.1.1 zmian w architekturze systemów OT lub IoT, zmian dostawców lub platform

9.1.2 istotnych zmian regulacyjnych (np. aktualizacji DORA, NIS2, dyrektyw sektorowych)

9.1.3 pojawienia się nowych podatności lub wzorców zagrożeń w systemach sterowania

9.1.4 ustaleń z audytów wewnętrznych lub zewnętrznych, testów penetracyjnych lub ćwiczeń red team

9.2 CISO, kierownik ds. bezpieczeństwa OT oraz właściwi kierownicy działów odpowiadają za wspólne inicjowanie procesu przeglądu.

9.3 Przeglądy doraźne muszą być uruchamiane po:

9.3.1 każdym incydencie związanym z IoT/OT skutkującym awarią systemu lub utratą danych

9.3.2 wdrożeniu istotnego nowego wyposażenia, oprogramowania monitorującego lub platform oprogramowania układowego

9.3.3 integracji inteligentnych rozwiązań przetwarzania brzegowego lub automatyzacji wspomaganej przez AI na poziomie polowym

9.4 Wszystkie zmiany polityki muszą być:

9.4.1 udokumentowane w historii wersji i rejestrze zmian polityki

9.4.2 zakomunikowane wszystkim użytkownikom, dostawcom i operatorom IT/OT, których dotyczą

9.4.3 ponownie zatwierdzone przez kierownictwo wykonawcze

10. Powiązane polityki i odniesienia

10.1 Niniejsza polityka funkcjonuje łącznie z następującymi politykami bezpieczeństwa informacji i jest przez nie wspierana:

10.1.1 P1 – Polityka bezpieczeństwa informacji: ustanawia podstawowe zasady bezpieczeństwa mające zastosowanie również do bezpieczeństwa systemów IoT i OT.

10.1.2 P3 – Polityka dopuszczalnego użytkowania: określa ograniczenia dotyczące użytkowania prywatnych i nieautoryzowanych urządzeń, w tym w środowiskach operacyjnych.

10.1.3 P6 – Polityka zarządzania ryzykiem: określa zasady oceny, akceptacji i ograniczania ryzyk związanych z systemami wbudowanymi i systemami sterowania.

10.1.4 P12 – Polityka zarządzania aktywami: zapewnia, że wszystkie systemy IoT i OT są formalnie ujmowane w inwentarzu i mają przypisanych odpowiedzialnych właścicieli.

10.1.5 P20 – Polityka ochrony punktów końcowych / ochrony przed złośliwym oprogramowaniem: ma zastosowanie do podłączonych kontrolerów, inteligentnych bram i systemów brzegowych w produkcji.

10.1.6 P22 – Polityka rejestrowania i monitorowania: obejmuje również procedury gromadzenia i przeglądu logów dla środowisk OT.

10.1.7 P30 – Polityka reagowania na incydenty: bezpośrednio reguluje sposób eskalacji i obsługi naruszeń, anomalii lub awarii systemów IoT/OT.

10.1.8 P33 – Polityka monitorowania audytu i zgodności: zapewnia mechanizmy potwierdzające bieżącą zgodność z niniejszą polityką.

11. Normy i ramy odniesienia

11.1 Niniejsza polityka jest zgodna z uznanymi międzynarodowo normami i ramami regulacyjnymi zapewniającymi bezpieczeństwo, odporność i zgodność systemów Internetu rzeczy (IoT) oraz technologii operacyjnej (OT) w środowiskach przemysłowych, produkcyjnych i korporacyjnych.

11.2 ISO/IEC 27002:2022 – Środki kontrolne 5.7, 5.23, 5.27, 5.31, 5.36

11.2.1 Środek kontrolny 5.7 – Threat intelligence: wspiera monitorowanie środowisk OT oraz identyfikację podatności specyficznych dla IoT.

11.2.2 Środek kontrolny 5.23 – Bezpieczeństwo informacji przy korzystaniu z usług chmurowych: ma zastosowanie, gdy urządzenia IoT współpracują z platformami chmurowymi na potrzeby telemetrii, sterowania lub analityki.

11.2.3 Środek kontrolny 5.27 – Bezpieczna architektura systemów i zasady inżynierskie: reguluje zasady bezpieczeństwa w fazie projektowania dla systemów wbudowanych i sieci sterowania.

11.2.4 Środek kontrolny 5.31 – Bezpieczeństwo w procesach rozwoju i wsparcia: egzekwuje walidację oprogramowania i oprogramowania układowego, kontrolę poprawek oraz wymagania wobec dostawców we wdrożeniach OT.

11.2.5 Środek kontrolny 5.36 – Zgodność z wymaganiami prawnymi, ustawowymi, regulacyjnymi i umownymi: zapewnia zgodność zasobów OT z wymogami bezpieczeństwa, środowiskowymi i regulacyjnymi.

11.2.6 Środki te łącznie ustanawiają dobre praktyki zabezpieczania systemów IoT/OT w całym ich cyklu życia, w tym w zakresie projektowania architektury, bezpiecznego wdrażania, wdrażania poprawek, wykrywania anomalii i zgodności z wymaganiami sektorowymi.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Ochrona granic: zapewnia segmentację sieci OT i ich ochronę przed nieuprawnionym dostępem.

11.3.2 SI-4 – Monitorowanie systemu: wymaga wdrożenia mechanizmów ciągłego monitorowania i wykrywania anomalii w środowiskach ICS.

11.3.3 CM-2 – Konfiguracja bazowa: nakazuje kontrolę konfiguracji oraz utwardzanie urządzeń i platform IoT/OT.

11.3.4 AC-6 – Najmniejsze uprawnienia: ma zastosowanie do dostępu użytkowników oraz zdalnego serwisowania przez dostawców systemów sterowania wbudowanego.

11.3.5 PL-8 – Architektury bezpieczeństwa i prywatności: reguluje planowanie bezpiecznej integracji systemów, zwłaszcza w projektach modernizacji OT.

11.4 RODO (2016/679)

11.4.1 Artykuł 5 – Zasady dotyczące przetwarzania danych osobowych: ma zastosowanie do platform IoT przetwarzających dane z czujników lub dane behawioralne powiązane z osobami fizycznymi.

11.4.2 Artykuł 25 – Ochrona danych w fazie projektowania i domyślna ochrona danych: wymaga uwzględnienia zabezpieczeń prywatności w projekcie produktów IoT i oprogramowania układowego.

11.4.3 Artykuł 32 – Bezpieczeństwo przetwarzania: wymaga szyfrowania, kontroli dostępu i bezpiecznej komunikacji przy transmisji danych urządzeń inteligentnych.

11.5 Dyrektywa NIS2 (2022/2555)

11.5.1 Artykuły 21 i 23: nakładają obowiązki bezpieczeństwa na podmioty kluczowe i ważne wykorzystujące systemy OT. Obejmują one ocenę ryzyka, zgłaszanie incydentów oraz walidację łańcucha dostaw dostawców IoT/OT i integralności oprogramowania układowego.

11.6 Rozporządzenie DORA (2022/2554)

11.6.1 Artykuł 9 – Zarządzanie ryzykiem ICT: wymaga bezpiecznej integracji systemów wbudowanych i technologii OT w ramach programu ładu korporacyjnego w zakresie ryzyka ICT.

11.6.2 Artykuł 10 – Wymagania bezpieczeństwa ICT: nakazuje stosowanie środków ochrony dla połączonych platform OT używanych w środowiskach usług finansowych i usług krytycznych.

11.7 COBIT 2019

11.7.1 DSS05.01 – Ochrona przed złośliwym oprogramowaniem: obejmuje wykrywanie i reagowanie na zagrożenia specyficzne dla ICS oraz kampanie złośliwego oprogramowania wymierzone w IoT.

11.7.2 BAI09.01 – Ustanowienie i utrzymanie wymagań bezpieczeństwa: odpowiada bezpiecznemu wdrażaniu oraz eksploatacji infrastruktury inteligentnej lub wbudowanej.

11.7.3 APO13.02 – Ustanowienie i utrzymanie planu bezpieczeństwa informacji: wymaga uwzględnienia systemów OT oraz ich podatności w strategii cyberbezpieczeństwa obejmującej całą organizację.