					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P35S					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	Klauzule 6.1, 6.2, 8	
ISO/IEC 27002:2022	Środki kontrolne 5.23, 5	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
RODO	Artykuł 32	
Dyrektywa NIS2	Artykuł 21(2)(a), (d), (f)	
Rozporządzenie DORA	Artykuł 9(2), 10(1)	

1. Cel

1.1. Niniejsza polityka określa obowiązkowe zasady bezpiecznego użytkowania i zarządzania urządzeniami Internetu Rzeczy (IoT) oraz technologii operacyjnej (OT) w organizacji. Do urządzeń tych mogą należeć inteligentne czujniki, kamery bezpieczeństwa, maszyny produkcyjne, sterowniki HVAC oraz wszelkie przemysłowe systemy podłączone do sieci.

1.2. Celem niniejszej polityki jest:

1.2.1. ochrona procesów fizycznych i cyfrowych przed zakłóceniem lub manipulacją za pośrednictwem niewłaściwie zabezpieczonych urządzeń podłączonych do sieci

1.2.2. zapewnienie bezpiecznego wdrażania, monitorowania i utrzymania systemów IoT i OT

1.2.3. zapewnienie zgodności z ISO/IEC 27001:2022, Dyrektywą NIS2 oraz powiązanymi ramami regulacyjnymi

1.2.4. ustanowienie praktycznych i egzekwowalnych zabezpieczeń dla MŚP działających w środowiskach biurowych, magazynowych lub produkcyjnych

2. Zakres

2.1. Niniejsza polityka ma zastosowanie do wszystkich osób zaangażowanych w planowanie, instalację, konfigurację, użytkowanie, wsparcie lub wycofanie z eksploatacji urządzeń IoT lub OT. Obejmuje to:

2.1.1. pracowników, wykonawców i stażystów posiadających dostęp fizyczny lub zdalny do urządzeń

2.1.2. zewnętrznych dostawców i techników serwisowych instalujących lub utrzymujących systemy podłączone do sieci

2.1.3. Dyrektora Generalnego oraz personel odpowiedzialny za nadzór nad politykami bezpieczeństwa

2.2. Polityka obejmuje:

2.2.1. urządzenia IoT, takie jak inteligentne zamki, systemy dozorowe, inteligentne liczniki lub drukarki

2.2.2. systemy OT, w tym programowalne sterowniki logiczne (PLC), panele SCADA oraz przemysłowe bramy sieciowe

2.2.3. wspierający sprzęt, aplikacje zarządzające i sieci komunikacyjne wykorzystywane przez te systemy

2.3. Niniejsza polityka obowiązuje we wszystkich lokalizacjach pracy: w środowiskach biurowych, lokalizacjach zdalnych, na halach produkcyjnych oraz na platformach chmurowych współpracujących z tymi urządzeniami.

3. Cele

3.1. Bezpieczne wdrożenie: zapewnienie, że wszystkie systemy IoT/OT są bezpiecznie skonfigurowane przed wprowadzeniem do środowiska operacyjnego.

3.2. Ograniczenie ekspozycji: zapobieganie nieuprawnionemu dostępowi, niewłaściwemu użyciu lub przejęciu urządzeń podłączonych do sieci poprzez stosowanie silnych mechanizmów kontroli dostępu i segmentacji sieci.

3.3. Ciągłe monitorowanie: utrzymanie widoczności działań w obszarze IoT/OT poprzez rejestrowanie aktywności i monitorowanie nietypowych zachowań.

3.4. Odpowiedzialność dostawców: zapewnienie, że podmioty zewnętrzne stosują bezpieczne praktyki instalacji, konfiguracji i utrzymania.

3.5. Zgodność regulacyjna: wykazanie pełnej zgodności z mającymi zastosowanie normami, takimi jak ISO 27001, RODO (jeżeli gromadzone są dane osobowe) oraz NIS2 w zakresie odporności infrastruktury krytycznej.

4. Role i odpowiedzialności

4.1. Dyrektor Generalny (GM)

4.1.1. ponosi ogólną odpowiedzialność za bezpieczeństwo systemów IoT i OT

4.1.2. zatwierdza niniejszą politykę i zapewnia jej stosowanie we wszystkich obszarach działalności

4.1.3. weryfikuje, czy dostawcy i wykonawcy stosują bezpieczne praktyki konfiguracji i utrzymania

4.1.4. autoryzuje dostęp sieciowy dla każdego systemu IoT/OT

4.2. Wyznaczony pracownik lub kierownik operacyjny (jeżeli został wyznaczony)

4.2.1. nadzoruje inwentaryzację, rozmieszczenie i konfigurację urządzeń IoT/OT

4.2.2. rejestruje lokalizację każdego urządzenia, przypisanie sieciowe oraz dokumentację wsparcia

4.2.3. zapewnia, że wszelkie zmiany (np. aktualizacje firmware lub wymiana urządzeń) są dokumentowane

[... 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 przez GM co najmniej raz w roku

9.1.2. Przegląd musi oceniać, czy polityka pozostaje skuteczna, obejmuje aktualne typy urządzeń i odpowiada nowym ryzykom lub technologiom

9.2. Aktualizacje inicjowane zdarzeniem

9.2.1. Aktualizacja polityki musi zostać również uruchomiona, gdy:

9.2.2. wprowadzane są nowe typy systemów IoT lub OT

9.2.3. dostawcy publikują komunikaty bezpieczeństwa lub powiadomienia o zakończeniu cyklu życia

9.2.4. incydent lub audyt identyfikuje luki w zabezpieczeniach IoT/OT

9.2.5. nowe przepisy prawa lub normy nakładają dodatkowe wymagania

9.3. Dokumentowanie i kontrola wersji

9.3.1. Wszystkie aktualizacje muszą być dokumentowane, w tym z podaniem daty, numeru wersji oraz podsumowania zmian

9.3.2. GM musi przechowywać historyczne wersje polityki do celów audytowych

9.4. Komunikowanie zmian

9.4.1. Wszelkie aktualizacje polityki muszą być przekazywane wszystkim właściwym pracownikom i dostawcom

9.4.2. Zaktualizowane wersje muszą być dostępne we współdzielonych folderach lub w materiałach drukowanych w miejscach instalacji albo centrach sterowania

10. Powiązane polityki i zależności

10.1. Niniejsza polityka musi być wdrożona zgodnie z następującymi powiązanymi politykami MŚP:

10.1.1. P4S – Polityka kontroli dostępu: określa mechanizmy kontroli logowania na poziomie urządzenia, stosowanie silnych haseł oraz procedury autoryzowanego dostępu do platform IoT i OT

10.1.2. P9S – Polityka pracy zdalnej: zapobiega wykorzystywaniu dostępu zdalnego do konsol IoT/OT przez niezabezpieczone lub niezatwierdzone kanały

10.1.3. P17S – Polityka ochrony danych i prywatności: ma zastosowanie, jeżeli urządzenia IoT (np. kamery bezpieczeństwa) przetwarzają lub rejestrują dane osobowe, zapewniając zgodność z RODO

10.1.4. P30S – Polityka reagowania na incydenty: określa procedury wykrywania, zgłaszania i obsługi incydentów IoT lub OT, w tym podejrzeń manipulacji lub awarii operacyjnej

10.1.5. P36S – Polityka mediów społecznościowych i komunikacji zewnętrznej: zapewnia, że informacje o urządzeniach lub topologii sieci nie są udostępniane na zewnątrz bez zatwierdzenia

10.2. Każda polityka powiązana wzmacnia stosowanie i praktyczne wykorzystanie niniejszej polityki poprzez ukierunkowane wytyczne proceduralne.

11. Normy i ramy odniesienia

11.1. ISO/IEC 27001

11.1.1. Klauzula 6.1 – Identyfikacja ryzyka i postępowanie z ryzykiem: wymaga, aby ryzyka związane z systemami IoT i OT były systematycznie oceniane i ograniczane

11.1.2. Klauzula 8.1 – Planowanie operacyjne i nadzór: zapewnia bezpieczny nadzór operacyjny nad urządzeniami podłączonymi do sieci

11.2. ISO/IEC 27002

11.2.1. Środek kontrolny 5.23 – Bezpieczeństwo informacji przy korzystaniu z technologii operacyjnej: określa bezpieczne korzystanie z OT w środowiskach fizycznych i cyfrowych

11.2.2. Środek kontrolny 5.31 – Bezpieczna konfiguracja systemów informacyjnych: wymaga utwardzonych konfiguracji urządzeń IoT/OT oraz unikania niezabezpieczonych ustawień domyślnych

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – Integralność oprogramowania, firmware i informacji: wymaga walidacji integralności firmware oraz aktualizacji

11.3.2. CM-7 – Zasada minimalnej funkcjonalności: urządzenia nie mogą mieć włączonych nieużywanych lub niezabezpieczonych funkcji

11.3.3. AC-6 – Zasada najmniejszych uprawnień: dostęp do urządzeń musi być ograniczony wyłącznie do autoryzowanych użytkowników

11.3.4. PE-20 – Monitorowanie aktywów: monitorowanie fizyczne i operacyjne aktywów IoT i OT

11.3.5. SC-7 – Ochrona granic: segmentacja i kontrola komunikacji sieciowej dla systemów podłączonych do sieci

11.4. RODO (2016/679)

11.4.1. Artykuł 32 – Bezpieczeństwo przetwarzania: jeżeli pozyskiwane są dane osobowe (np. z kamer dozorowych), organizacja musi wdrożyć odpowiednie środki techniczne i organizacyjne w celu zabezpieczenia takiego przetwarzania

11.5. Dyrektywa NIS2 (2022/2555)

11.5.1. Artykuł 21(2)(a) – Środki zarządzania ryzykiem

11.5.2. Artykuł 21(2)(d) – Bezpieczna konfiguracja i użytkowanie urządzeń

11.5.3. Artykuł 21(2)(f) – Bezpieczeństwo łańcucha dostaw i systemów

11.6. Rozporządzenie DORA (2022/2554)

11.6.1. Artykuł 9(2) – Zakres zarządzania ryzykiem ICT: obejmuje urządzenia przemysłowe i wbudowane wykorzystywane w środowiskach operacyjnych

11.6.2. Artykuł 10(1) – Ciągłość ICT: wymaga, aby konfiguracje urządzeń wspierały odporność i odtwarzanie

11.7. COBIT 2019

11.7.1. DSS01 – Zarządzanie operacjami: odnosi się do nadzoru nad operacjami technologicznymi, w tym nad urządzeniami fizycznymi

11.7.2. DSS05 – Zarządzanie usługami bezpieczeństwa: zapewnia właściwe monitorowanie i ochronę systemów podłączonych do sieci

11.7.3. APO13 – Zarządzanie bezpieczeństwem: wzmacnia polityki ochrony aktywów operacyjnych w MŚP