					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P35S					Titlul documentului: **Politica de securitate IoT/OT**							
Versiunea: 1.0		Data intrării în vigoare: 01.01.2025			Proprietarul documentului:							
X	Politică		Standard		Procedură		Formular		Registru		Altul	

Istoricul reviziilor				
Numărul reviziei	**Data reviziei**	**Modificări**	**Revizuit de**	**Proprietarul procesului**

Aprobări			
Nume	**Funcție**	**Data**	**Semnătură**

Aliniată la standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauzele 6.1, 6.2, 8	
ISO/IEC 27002:2022	Controalele 5.23, 5	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
GDPR	Articolul 32	
Directiva NIS2	Articolul 21(2)(a), (d), (f)	
Regulamentul DORA	Articolul 9(2), 10(1)	

1. Scop

1.1. Prezenta politică stabilește regulile obligatorii pentru utilizarea și administrarea în condiții de securitate a sistemelor din Internetul obiectelor (IoT) și a sistemelor de tehnologie operațională (OT) din cadrul organizației. Acestea pot include senzori inteligenți, camere de supraveghere, echipamente de producție, controlere HVAC sau orice alte sisteme industriale conectate la rețea.

1.2. Scopul acestei politici este de a:

1.2.1. Proteja operațiunile fizice și digitale împotriva întreruperii sau manipulării prin intermediul dispozitivelor conectate insuficient securizate

1.2.2. Impune implementarea, monitorizarea și mentenanța în condiții de siguranță a sistemelor IoT și OT

1.2.3. Asigura conformitatea cu ISO/IEC 27001:2022, Directiva NIS2 și cadrele de reglementare conexe

1.2.4. Furniza controale practice, aplicabile și verificabile pentru IMM-uri care operează în medii de birou, depozit sau producție

2. Domeniu de aplicare

2.1. Această politică se aplică tuturor persoanelor implicate în planificarea, instalarea, configurarea, utilizarea, suportul sau scoaterea din uz a dispozitivelor IoT sau OT. Aceasta include:

2.1.1. Angajați, contractori sau stagiari care au acces fizic sau acces la distanță la dispozitive

2.1.2. Furnizori terți sau tehnicieni de service care instalează sau întrețin sisteme conectate

2.1.3. Directorul general sau membri ai personalului responsabili de supravegherea politicilor de securitate

2.2. Politica acoperă:

2.2.1. Dispozitive IoT precum încuietori inteligente, echipamente de supraveghere, contoare inteligente sau imprimante

2.2.2. Sisteme OT, inclusiv PLC-uri (controlere logice programabile), panouri SCADA sau gateway-uri industriale

2.2.3. Echipamentele-suport, aplicațiile de administrare și rețelele de comunicații utilizate de aceste sisteme

2.3. Această politică se aplică în toate locațiile de lucru: medii de birou, locații la distanță, zone de producție și platforme cloud care interfațează cu aceste dispozitive.

3. Obiective

3.1. Implementare securizată: se asigură că toate sistemele IoT/OT sunt configurate în mod securizat înainte de introducerea lor în mediul operațional.

3.2. Limitarea expunerii: se previne accesul neautorizat, utilizarea abuzivă sau compromiterea dispozitivelor conectate prin aplicarea unor controale de acces robuste și a segmentării rețelei.

3.3. Monitorizare continuă: se menține vizibilitatea asupra operațiunilor IoT/OT prin jurnalizarea activităților și monitorizarea comportamentelor neobișnuite.

3.4. Responsabilizarea furnizorilor: se asigură că furnizorii terți respectă practici securizate de instalare, configurare și mentenanță.

3.5. Conformitate cu reglementările: se demonstrează alinierea deplină la standardele aplicabile, precum ISO 27001, GDPR (dacă sunt colectate date cu caracter personal) și NIS2 pentru reziliența infrastructurilor critice.

4. Roluri și responsabilități

4.1. Director general (GM)

4.1.1. Deține responsabilitatea generală pentru securitatea sistemelor IoT și OT

4.1.2. Aprobă această politică și asigură aplicarea acesteia în toate zonele de lucru

4.1.3. Verifică faptul că furnizorii și contractorii respectă practici securizate de instalare și mentenanță

4.1.4. Autorizează accesul la rețea pentru orice sistem IoT/OT

4.2. Angajat desemnat sau manager operațional (dacă este desemnat)

4.2.1. Supraveghează inventarul, amplasarea și configurarea dispozitivelor IoT/OT

4.2.2. Înregistrează locația fiecărui dispozitiv, alocarea în rețea și documentația-suport

4.2.3. Se asigură că orice modificări (de exemplu, actualizări de firmware sau înlocuiri de dispozitive) sunt documentate

[... Secțiunile 4.3–8 nu sunt incluse în această previzualizare. Achiziționați documentul complet pentru a accesa conținutul integral. ...]

9. Cerințe de revizuire și actualizare

9.1. Revizuire anuală

9.1.1. Această politică trebuie revizuită cel puțin o dată pe an de către GM

9.1.2. Revizuirea trebuie să evalueze dacă politica rămâne eficace, acoperă tipurile actuale de dispozitive și este aliniată la riscuri sau tehnologii noi

9.2. Actualizări declanșate de evenimente

9.2.1. Actualizările politicii trebuie inițiate și atunci când:

9.2.2. Sunt introduse tipuri noi de sisteme IoT sau OT

9.2.3. Furnizorii emit informări de securitate sau notificări privind sfârșitul ciclului de viață

9.2.4. Un incident sau un audit identifică lacune în controalele IoT/OT

9.2.5. Legi sau standarde noi impun cerințe suplimentare

9.3. Documentare și controlul versiunilor

9.3.1. Toate actualizările trebuie documentate, inclusiv data, numărul versiunii și rezumatul modificărilor

9.3.2. GM trebuie să păstreze versiunile istorice ale politicii în scop de audit

9.4. Comunicarea modificărilor

9.4.1. Orice actualizare a politicii trebuie comunicată tuturor membrilor relevanți ai personalului și furnizorilor

9.4.2. Versiunile actualizate trebuie puse la dispoziție prin foldere partajate sau materiale tipărite la locurile de instalare ori în centrele de control

10. Politici conexe și interdependențe

10.1. Această politică trebuie implementată în aliniere cu următoarele politici SME conexe:

10.1.1. P4S – Politica de control al accesului: impune controale de autentificare la nivel de dispozitiv, utilizarea de parole puternice și proceduri de acces autorizat pentru platformele IoT și OT

10.1.2. P9S – Politica de telemuncă: previne utilizarea accesului la distanță la consolele de administrare IoT/OT prin canale nesecurizate sau neaprobate

10.1.3. P17S – Politica de protecție a datelor și confidențialitate: se aplică dacă dispozitivele IoT (de exemplu, camerele de supraveghere) prelucrează sau înregistrează date cu caracter personal, asigurând conformitatea cu GDPR

10.1.4. P30S – Politica de răspuns la incidente: definește procedurile pentru detectarea, raportarea și soluționarea incidentelor IoT sau OT, inclusiv a suspiciunilor de manipulare sau de defecțiune operațională

10.1.5. P36S – Politica privind rețelele sociale și comunicațiile externe: asigură că informațiile despre dispozitive sau arhitectura rețelei nu sunt partajate extern fără aprobare

10.2. Fiecare politică conexă consolidează aplicarea și utilizarea practică a prezentei politici prin furnizarea de orientări procedurale specifice.

11. Standarde și cadre de referință

11.1. ISO/IEC 27001

11.1.1. Clauza 6.1 – Identificarea și tratarea riscurilor: impune ca riscurile aferente sistemelor IoT și OT să fie evaluate și diminuate în mod sistematic

11.1.2. Clauza 8.1 – Planificare și control operațional: asigură control operațional securizat asupra dispozitivelor conectate

11.2. ISO/IEC 27002

11.2.1. Controlul 5.23 – Securitatea informației pentru utilizarea tehnologiei operaționale: definește utilizarea securizată a OT în medii fizice și digitale

11.2.2. Controlul 5.31 – Configurarea securizată a sistemelor informatice: impune configurații întărite pentru dispozitivele IoT/OT și evitarea setărilor implicite nesigure

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – Integritatea software-ului, firmware-ului și informațiilor: impune validarea integrității firmware-ului și a actualizărilor

11.3.2. CM-7 – Funcționalitate minimă: dispozitivele nu trebuie să aibă activate funcții neutilizate sau nesecurizate

11.3.3. AC-6 – Principiul privilegiului minim: accesul la dispozitive trebuie limitat exclusiv la utilizatorii autorizați

11.3.4. PE-20 – Monitorizarea activelor: monitorizarea fizică și operațională a activelor IoT și OT

11.3.5. SC-7 – Protecția perimetrului: segmentarea și controlul comunicațiilor de rețea pentru sistemele conectate

11.4. GDPR (UE) 2016/679

11.4.1. Articolul 32 – Securitatea prelucrării: dacă sunt captate date cu caracter personal (de exemplu, prin camere de supraveghere), organizația trebuie să implementeze măsuri tehnice și organizatorice adecvate pentru securizarea unei astfel de prelucrări

11.5. Directiva NIS2 (UE) 2022/2555

11.5.1. Articolul 21(2)(a) – Măsuri de management al riscurilor

11.5.2. Articolul 21(2)(d) – Configurarea și utilizarea securizată a dispozitivelor

11.5.3. Articolul 21(2)(f) – Securitatea lanțului de aprovizionare și a sistemelor

11.6. Regulamentul DORA (UE) 2022/2554

11.6.1. Articolul 9(2) – Domeniul de aplicare al managementului riscurilor TIC: include dispozitive industriale și sisteme integrate utilizate în medii operaționale

11.6.2. Articolul 10(1) – Continuitate TIC: impune ca configurațiile dispozitivelor să susțină reziliența și operațiunile de recuperare

11.7. COBIT 2019

11.7.1. DSS01 – Manage Operations: se aplică supravegherii operațiunilor tehnologice, inclusiv a dispozitivelor fizice

11.7.2. DSS05 – Manage Security Services: asigură monitorizarea și protejarea corespunzătoare a sistemelor conectate

11.7.3. APO13 – Manage Security: consolidează politicile pentru protejarea activelor operaționale în cadrul IMM-urilor