					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P35					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 standarde și reglementări

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauza 8	
ISO/IEC 27002:2022	Controalele 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	
GDPR	Articolele 5, 25, 32	
Directiva UE NIS2	Articolele 21, 23	
Regulamentul UE DORA	Articolele 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Scop

1.1 Prezenta politică stabilește cerințele obligatorii de securitate a informației pentru implementarea, operarea, monitorizarea și scoaterea din uz a sistemelor din Internetul obiectelor (IoT) și a sistemelor de tehnologie operațională (OT) din cadrul organizației.

1.2 Aceasta asigură integrarea acestor sisteme în cadrul general de management al securității cibernetice al organizației și protejarea lor împotriva compromiterii, utilizării necorespunzătoare sau sabotajului operațional.

1.3 Politica are ca obiectiv impunerea unor controale tehnice, organizaționale și procedurale solide pentru protejarea sistemelor IoT/OT care interacționează cu infrastructura fizică, procesele de producție și mediile critice pentru siguranță.

1.4 Aceasta sprijină obligațiile de reglementare și contractuale din domeniile securității cibernetice, siguranței, controlului de mediu și continuității activității.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică tuturor sistemelor IoT și OT — indiferent dacă sunt deținute de companie, închiriate sau furnizate de terți — utilizate în mediile operaționale, administrative sau de producție ale organizației.

2.2 Sistemele vizate includ, fără a se limita la:

2.2.1 dispozitive IoT, precum senzori de mediu, sisteme de control al accesului, iluminat inteligent, echipamente de supraveghere și dispozitive purtabile

2.2.2 platforme de tehnologie operațională, precum PLC-uri, sisteme de control și achiziție de date (SCADA), sisteme de control distribuit (DCS), panouri de interfață om-mașină (HMI), interfețe ale sistemului de execuție a producției (MES) și controlere de câmp

2.2.3 rețele de control industrial sau active conectate la cloud care monitorizează operațiuni fizice

2.3 Politica acoperă:

2.3.1 toate mediile (on-premises, edge, gestionate din cloud)

2.3.2 toate părțile interesate (utilizatori interni, integratori, furnizori terți, contractori)

2.3.3 toate etapele ciclului de viață (proiectare, achiziție, implementare, operare, dezafectare)

3. Obiective

3.1 Protejarea infrastructurii IoT și OT împotriva amenințărilor de securitate cibernetică interne și externe, inclusiv atacuri de tip denial-of-service, acces neautorizat, propagarea ransomware-ului și alterarea firmware-ului.

3.2 Asigurarea faptului că platformele IoT/OT nu devin vectori pentru atacuri de tip punte IT-OT și nu compromit sistemele critice pentru siguranță.

3.3 Aplicarea principiilor de securitate prin proiectare și apărare în profunzime pe întreg ciclul de viață al acestor tehnologii.

3.4 Asigurarea unei integrări fiabile, securizate și verificabile a platformelor IoT și OT în centrul operațional de securitate (SOC) al organizației și în planurile de răspuns la incidente.

3.5 Asigurarea faptului că toate implementările sunt aliniate la controalele ISO/IEC 27001 și la ghidurile sectoriale aplicabile (de exemplu, IEC 62443, ISO 27019, NIST SP 800-82).

4. Roluri și responsabilități

4.1 Directorul de securitate a informațiilor (CISO) / responsabilul cu securitatea

4.1.1 Definește politicile și standardele tehnice pentru securitatea cibernetică IoT/OT

4.1.2 Supraveghează evaluările de risc, validarea controalelor și coordonarea interdepartamentală

4.2 Ingineri OT / manageri de facilități și de uzină

4.2.1 Validează configurațiile sistemelor de tehnologie operațională și asigură respectarea politicii în zonele de producție

4.2.2 Mențin măsurile de protecție fizică și logică pentru integritatea și siguranța mediilor OT

[... 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 Prezenta politică trebuie revizuită cel puțin anual și actualizată pe baza:

9.1.1 schimbărilor în arhitectura sistemelor OT sau IoT, a furnizorilor ori a platformelor

9.1.2 actualizărilor majore de reglementare (de exemplu, revizuiri ale DORA, NIS2, directive sectoriale)

9.1.3 apariției unor noi vulnerabilități sau tipare de amenințări în sistemele de control

9.1.4 constatărilor rezultate din audituri interne sau externe, teste de penetrare ori exerciții de tip red team

9.2 CISO, responsabilul de securitate OT și șefii de departamente relevante sunt responsabili de inițierea în comun a procesului de revizuire.

9.3 Revizuirile intermediare trebuie declanșate după:

9.3.1 orice incident legat de IoT/OT care conduce la defectarea sistemului sau la pierderea datelor

9.3.2 introducerea unor echipamente noi majore, a unui software de monitorizare sau a unor platforme de firmware

9.3.3 integrarea unor capabilități inteligente de edge computing sau de automatizare îmbunătățită prin IA la nivel de teren

9.4 Toate modificările politicii trebuie:

9.4.1 să fie documentate în istoricul versiunilor și în registrul modificărilor de politică

9.4.2 să fie comunicate tuturor utilizatorilor, furnizorilor și operatorilor IT/OT afectați

9.4.3 să fie reaprobate de managementul executiv

10. Politici conexe și corelări

10.1 Prezenta politică funcționează împreună cu următoarele politici de securitate a informației și este susținută de acestea:

10.1.1 P1 – Politica de securitate a informației: stabilește principiile de bază de securitate care se extind și asupra securității sistemelor IoT și OT.

10.1.2 P3 – Politica de utilizare acceptabilă: definește restricțiile privind utilizarea personală și utilizarea neautorizată a dispozitivelor, inclusiv în mediile operaționale.

10.1.3 P6 – Politica de management al riscurilor: ghidează evaluarea, acceptarea și atenuarea riscurilor asociate sistemelor încorporate și sistemelor de control.

10.1.4 P12 – Politica de management al activelor: asigură inventarierea formală a tuturor sistemelor IoT și OT și alocarea unor proprietari responsabili.

10.1.5 P20 – Politica privind protecția punctelor terminale / malware: se aplică controlerelor conectate, gateway-urilor inteligente și sistemelor edge din producție.

10.1.6 P22 – Politica de jurnalizare și monitorizare: se extinde asupra procedurilor de colectare și revizuire a jurnalelor pentru mediile OT.

10.1.7 P30 – Politica de răspuns la incidente: reglementează direct modul în care încălcările, anomaliile sau defectările de sistem IoT/OT trebuie escaladate și gestionate.

10.1.8 P33 – Politica de monitorizare a auditului și conformității: furnizează mecanisme de asigurare pentru validarea conformității continue cu prezenta politică.

11. Standarde și cadre de referință

11.1 Prezenta politică este aliniată la standarde și cadre de reglementare recunoscute la nivel internațional, care asigură securitatea, reziliența și conformitatea sistemelor din Internetul obiectelor (IoT) și a sistemelor de tehnologie operațională (OT) în medii industriale, de producție și corporative.

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

11.2.1 Controlul 5.7 – Informații privind amenințările: fundamentează monitorizarea mediilor OT și identificarea vulnerabilităților specifice IoT.

11.2.2 Controlul 5.23 – Securitatea informației pentru utilizarea serviciilor cloud: se aplică atunci când dispozitivele IoT interacționează cu platforme cloud pentru telemetrie, control sau analiză.

11.2.3 Controlul 5.27 – Principii de arhitectură și inginerie a sistemelor securizate: guvernează principiile de securitate prin proiectare pentru sistemele încorporate și rețelele de control.

11.2.4 Controlul 5.31 – Securitatea în procesele de dezvoltare și suport: impune validarea software-ului/firmware-ului, controale privind patch-urile și cerințele aplicabile furnizorilor în implementările OT.

11.2.5 Controlul 5.36 – Conformitatea cu cerințele legale, statutare, de reglementare și contractuale: asigură conformitatea activelor OT cu cerințele privind siguranța, mediul și reglementările aplicabile.

11.2.6 Aceste controale stabilesc împreună bune practici recunoscute în industrie pentru securizarea sistemelor IoT/OT pe întreg ciclul lor de viață, inclusiv proiectarea arhitecturii, implementarea securizată, aplicarea patch-urilor, detectarea anomaliilor și conformitatea cu cerințele sectoriale.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Protecția perimetrului: asigură că rețelele OT sunt segmentate și protejate împotriva accesului neautorizat.

11.3.2 SI-4 – Monitorizarea sistemelor: impune implementarea unor mecanisme de monitorizare continuă și de detectare a anomaliilor în mediile ICS.

11.3.3 CM-2 – Configurație de referință: impune controlul configurației și hardening-ul dispozitivelor pentru platformele IoT/OT.

11.3.4 AC-6 – Principiul privilegiului minim: se aplică accesului utilizatorilor și intervențiilor la distanță ale furnizorilor asupra sistemelor de control încorporate.

11.3.5 PL-8 – Arhitecturi de securitate și confidențialitate: guvernează planificarea integrării securizate a sistemelor, în special pentru proiectele de modernizare OT.

11.4 GDPR (UE) 2016/679

11.4.1 Articolul 5 – Principii privind prelucrarea datelor cu caracter personal: se aplică platformelor IoT care prelucrează date provenite din senzori sau date comportamentale asociate persoanelor.

11.4.2 Articolul 25 – Protecția datelor începând cu momentul conceperii și în mod implicit: impune măsuri de protecție a vieții private integrate în proiectarea produselor IoT și a firmware-ului.

11.4.3 Articolul 32 – Securitatea prelucrării: impune criptarea, controlul accesului și comunicații securizate pentru transmiterea datelor de pe dispozitive inteligente.

11.5 Directiva UE NIS2 (2022/2555)

11.5.1 Articolele 21 și 23: impun obligații de securitate entităților esențiale și importante care utilizează sisteme OT. Acestea includ evaluarea riscurilor, raportarea incidentelor și validarea lanțului de aprovizionare pentru furnizorii IoT/OT și integritatea firmware-ului.

11.6 Regulamentul UE DORA (2022/2554)

11.6.1 Articolul 9 – Managementul riscurilor TIC: impune integrarea securizată a sistemelor încorporate și a tehnologiilor OT în programul de guvernanță a riscurilor TIC.

11.6.2 Articolul 10 – Cerințe de securitate TIC: impune măsuri de protecție pentru platformele OT interconectate utilizate în medii financiare și de servicii critice.

11.7 COBIT 2019

11.7.1 DSS05.01 – Protecție împotriva malware-ului: include detectarea și răspunsul la amenințări specifice ICS și la campaniile malware care vizează IoT.

11.7.2 BAI09.01 – Stabilirea și menținerea cerințelor de securitate: corespunde furnizării și operării securizate a infrastructurilor inteligente sau încorporate.

11.7.3 APO13.02 – Stabilirea și menținerea unui plan de securitate a informației: impune includerea sistemelor OT și a vulnerabilităților acestora în strategia de securitate cibernetică la nivelul întregii organizații.