					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P35					Titolo del documento: **Politica di sicurezza IoT / OT**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineata a norme e regolamenti, ove applicabile

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	
ISO/IEC 27002:2022	Controlli 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 UE	Articoli 5, 25, 32	
Direttiva UE NIS2	Articoli 21, 23	
Regolamento UE DORA	Articoli 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Finalità

1.1 La presente politica stabilisce i requisiti obbligatori di sicurezza delle informazioni per la distribuzione, l'esercizio, il monitoraggio e la dismissione dei sistemi Internet of Things (IoT) e dei sistemi di tecnologia operativa (OT) all'interno dell'organizzazione.

1.2 Garantisce che tali sistemi siano integrati nel più ampio sistema di gestione della cibersicurezza dell'organizzazione e protetti da compromissioni, usi impropri o sabotaggi della produzione.

1.3 La politica ha l'obiettivo di applicare controlli tecnici, organizzativi e procedurali robusti per proteggere i sistemi IoT/OT che interagiscono con infrastrutture fisiche, processi produttivi e ambienti critici per la sicurezza.

1.4 Supporta gli obblighi normativi e contrattuali in materia di cibersicurezza, sicurezza, controllo ambientale e continuità operativa.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i sistemi IoT e OT, di proprietà aziendale, in leasing o forniti da terze parti, utilizzati negli ambienti operativi, amministrativi o produttivi dell'organizzazione.

2.2 I sistemi coperti includono, a titolo esemplificativo e non esaustivo:

2.2.1 dispositivi IoT quali sensori ambientali, sistemi di controllo degli accessi, illuminazione intelligente, apparecchiature di sorveglianza e dispositivi indossabili

2.2.2 piattaforme OT quali PLC, SCADA, DCS, pannelli HMI, interfacce del Manufacturing Execution System (MES) e controllori di campo

2.2.3 reti di controllo industriale o asset connessi al cloud che monitorano operazioni fisiche

2.3 La politica copre:

2.3.1 tutti gli ambienti (on-premise, edge, gestiti in cloud)

2.3.2 tutte le parti interessate (utenti interni, integratori, fornitori terzi, appaltatori e prestatori di servizi terzi)

2.3.3 tutte le fasi del ciclo di vita (progettazione, approvvigionamento, distribuzione, esercizio, dismissione)

3. Obiettivi

3.1 Proteggere l’infrastruttura IoT e OT dalle minacce di cibersicurezza interne ed esterne, inclusi attacchi di denial-of-service, accessi non autorizzati, propagazione di ransomware e manomissione del firmware.

3.2 Garantire che le piattaforme IoT/OT non diventino vettori di attacco tra IT e OT né compromettano sistemi critici per la sicurezza.

3.3 Applicare i principi di sicurezza by design e di difesa in profondità lungo tutto il ciclo di vita di tali tecnologie.

3.4 Consentire l’integrazione affidabile, sicura e verificabile delle piattaforme IoT e OT nel Security Operations Center (SOC) dell’organizzazione e nei piani di risposta agli incidenti.

3.5 Garantire che tutte le distribuzioni siano allineate ai controlli ISO/IEC 27001 e alle linee guida settoriali applicabili (ad es. IEC 62443, ISO 27019, NIST SP 800-82).

4. Ruoli e responsabilità

4.1 Responsabile della sicurezza delle informazioni (CISO) / Responsabile della sicurezza

4.1.1 Definisce politiche e standard tecnici per la cibersicurezza IoT/OT

4.1.2 Supervisiona le valutazioni del rischio, la convalida dei controlli e il coordinamento interfunzionale

4.2 Ingegneri OT / Responsabili di strutture e impianti

4.2.1 Convalidano le configurazioni dei sistemi OT e garantiscono la conformità alle politiche nelle aree produttive

4.2.2 Mantengono misure di sicurezza fisiche e logiche per l’integrità e la sicurezza dei sistemi OT

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Requisiti di riesame e aggiornamento

9.1 La presente politica deve essere riesaminata almeno annualmente e aggiornata sulla base di:

9.1.1 modifiche dell’architettura, dei fornitori o delle piattaforme dei sistemi OT o IoT

9.1.2 aggiornamenti normativi rilevanti (ad es. revisioni di DORA, NIS2, direttive settoriali)

9.1.3 emersione di nuove vulnerabilità o nuovi schemi di minaccia nei sistemi di controllo

9.1.4 risultanze di audit interni o esterni, test di penetrazione o esercitazioni di red team

9.2 Il Responsabile della sicurezza delle informazioni (CISO), il Responsabile della sicurezza OT e i responsabili dei dipartimenti interessati sono responsabili dell’avvio congiunto del processo di riesame.

9.3 Devono essere attivati riesami intermedi dopo:

9.3.1 qualsiasi incidente correlato a IoT/OT che comporti guasto del sistema o perdita di dati

9.3.2 introduzione di nuove apparecchiature rilevanti, software di monitoraggio o piattaforme firmware

9.3.3 integrazione di edge computing intelligente o automazione potenziata dall’IA a livello di campo

9.4 Tutte le modifiche alle politiche devono essere:

9.4.1 documentate nella cronologia delle versioni e nel registro delle modifiche alle politiche

9.4.2 comunicate a tutti gli utenti, fornitori e operatori IT/OT interessati

9.4.3 nuovamente approvate dalla Direzione esecutiva

10. Politiche correlate e collegamenti

10.1 La presente politica opera congiuntamente ed è supportata dalle seguenti politiche di sicurezza delle informazioni:

10.1.1 P1 – Politica per la sicurezza delle informazioni: stabilisce i principi fondamentali di sicurezza che si estendono alla sicurezza dei sistemi IoT e OT.

10.1.2 P3 – Politica di uso accettabile: definisce le restrizioni sull'uso personale e non autorizzato dei dispositivi, anche negli ambienti operativi.

10.1.3 P6 – Politica di gestione del rischio: disciplina la valutazione, l'accettazione e la mitigazione dei rischi relativi ai sistemi embedded e di controllo.

10.1.4 P12 – Politica di gestione degli asset: garantisce che tutti i sistemi IoT e OT siano formalmente inventariati e assegnati a responsabili designati.

10.1.5 P20 – Politica di protezione degli endpoint / Politica malware: si applica ai controllori connessi, ai gateway intelligenti e ai sistemi edge in produzione.

10.1.6 P22 – Politica di registrazione e monitoraggio: si estende alle procedure di acquisizione e riesame dei log per gli ambienti OT.

10.1.7 P30 – Politica di risposta agli incidenti: disciplina direttamente le modalità con cui violazioni, anomalie o guasti dei sistemi IoT/OT devono essere portati in escalation e gestiti.

10.1.8 P33 – Politica di monitoraggio di audit e conformità: fornisce meccanismi di assurance per convalidare la conformità continuativa alla presente politica.

11. Norme e quadri di riferimento

11.1 La presente politica è allineata a norme internazionalmente riconosciute e quadri normativi che assicurano la sicurezza, la resilienza e la conformità dei sistemi Internet of Things (IoT) e dei sistemi di tecnologia operativa (OT) in ambienti industriali, produttivi e aziendali.

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

11.2.1 Controllo 5.7 – Threat intelligence: supporta il monitoraggio degli ambienti OT e l'identificazione delle vulnerabilità specifiche dell'IoT.

11.2.2 Controllo 5.23 – Sicurezza delle informazioni per l'uso dei servizi cloud: si applica quando i dispositivi IoT si interfacciano con piattaforme cloud per telemetria, controllo o analisi.

11.2.3 Controllo 5.27 – Architettura di sistema sicura e principi di ingegneria: disciplina i principi di progettazione sicura per i sistemi embedded e le reti di controllo.

11.2.4 Controllo 5.31 – Sicurezza nei processi di sviluppo e supporto: impone convalida di software e firmware, controlli sulle patch e requisiti per i fornitori nelle distribuzioni OT.

11.2.5 Controllo 5.36 – Conformità ai requisiti legali e contrattuali: garantisce la conformità degli asset OT ai requisiti di sicurezza, ambientali e normativi.

11.2.6 Nel loro complesso, questi controlli definiscono buone pratiche per proteggere i sistemi IoT/OT lungo tutto il ciclo di vita, inclusi progettazione dell'architettura, distribuzione sicura, applicazione delle patch, rilevazione delle anomalie e conformità ai requisiti settoriali.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Protezione dei confini: garantisce che le reti OT siano segmentate e protette dall'accesso non autorizzato.

11.3.2 SI-4 – Monitoraggio dei sistemi: richiede l'implementazione di meccanismi di monitoraggio continuo e rilevamento delle anomalie negli ambienti ICS.

11.3.3 CM-2 – Configurazione di baseline: impone il controllo della configurazione e l'hardening dei dispositivi delle piattaforme IoT/OT.

11.3.4 AC-6 – Privilegio minimo: si applica all'accesso degli utenti e alle attività di assistenza remota dei fornitori sui sistemi di controllo embedded.

11.3.5 PL-8 – Architetture di sicurezza e privacy: disciplina la pianificazione dell'integrazione sicura dei sistemi, in particolare per i progetti di modernizzazione OT.

11.4 GDPR UE (2016/679)

11.4.1 Articolo 5 – Principi applicabili al trattamento dei dati personali: si applica alle piattaforme IoT che trattano dati basati su sensori o dati comportamentali riferibili a persone fisiche.

11.4.2 Articolo 25 – Protezione dei dati fin dalla progettazione e per impostazione predefinita: richiede misure di tutela della privacy integrate nella progettazione dei prodotti IoT e del firmware.

11.4.3 Articolo 32 – Sicurezza del trattamento: impone cifratura, controllo degli accessi e comunicazioni sicure per la trasmissione dei dati dei dispositivi intelligenti.

11.5 Direttiva UE NIS2 (2022/2555)

11.5.1 Articoli 21 e 23: impongono obblighi di sicurezza agli enti essenziali e importanti che utilizzano sistemi OT. Tali obblighi includono valutazione del rischio, segnalazione degli incidenti e convalida della catena di fornitura dei fornitori IoT/OT e dell'integrità del firmware.

11.6 Regolamento UE DORA (2022/2554)

11.6.1 Articolo 9 – Gestione del rischio ICT: richiede l'integrazione sicura dei sistemi embedded e delle tecnologie OT nel programma di governance del rischio ICT.

11.6.2 Articolo 10 – Requisiti di sicurezza ICT: impone misure di protezione per le piattaforme OT interconnesse utilizzate in ambienti finanziari e di servizi critici.

11.7 COBIT 2019

11.7.1 DSS05.01 – Protezione dal malware: include rilevamento e risposta alle minacce specifiche ICS e alle campagne malware IoT.

11.7.2 BAI09.01 – Definire e mantenere i requisiti di sicurezza: si collega al provisioning sicuro e all'esercizio di infrastrutture intelligenti o embedded.

11.7.3 APO13.02 – Definire e mantenere un piano per la sicurezza delle informazioni: richiede l'inclusione dei sistemi OT e delle relative vulnerabilità nella strategia aziendale di cibersicurezza.