					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P35S					Titolo del documento: **Politica di sicurezza dell'Internet delle cose (IoT) e della tecnologia operativa (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**

Allineamento a standard e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 6.1, 6.2, 8	
ISO/IEC 27002:2022	Controlli 5.23, 5.31	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
GDPR UE	Articolo 32	
NIS2 UE	Articolo 21(2)(a), (d), (f)	
DORA UE	Articolo 9(2), 10(1)	

1. Finalità

1.1. La presente politica definisce le regole obbligatorie per l'utilizzo e la gestione sicuri dei sistemi dell'Internet delle cose (IoT) e della tecnologia operativa (OT) all'interno dell'organizzazione. Tali dispositivi possono includere sensori intelligenti, telecamere di sicurezza, macchine di produzione, controllori HVAC o qualsiasi sistema industriale connesso alla rete.

1.2. Le finalità della presente politica sono:

1.2.1. Proteggere le operazioni fisiche e digitali da interruzioni o manipolazioni dovute a dispositivi connessi non adeguatamente protetti

1.2.2. Garantire l'implementazione, il monitoraggio e la manutenzione sicuri dei sistemi dell'Internet delle cose (IoT) e della tecnologia operativa (OT)

1.2.3. Assicurare la conformità alla ISO/IEC 27001:2022, alla Direttiva NIS2 e ai relativi quadri normativi

1.2.4. Fornire controlli pratici, applicabili e verificabili per le piccole e medie imprese (PMI) che operano in ambienti d'ufficio, di magazzino o di produzione

2. Ambito di applicazione

2.1. La presente politica si applica a tutte le persone coinvolte nella pianificazione, installazione, configurazione, utilizzo, supporto o dismissione di dispositivi IoT o OT. Ciò include:

2.1.1. dipendenti, collaboratori esterni o tirocinanti con accesso fisico o remoto ai dispositivi

2.1.2. fornitori terzi o tecnici dell'assistenza che installano o mantengono sistemi connessi

2.1.3. Direttore generale (GM) o personale responsabile della supervisione delle politiche di sicurezza

2.2. La politica si applica a:

2.2.1. dispositivi IoT quali serrature intelligenti, sistemi di sorveglianza, contatori intelligenti o stampanti

2.2.2. sistemi OT, inclusi controllori logici programmabili (PLC), pannelli di controllo e acquisizione dati (SCADA) o gateway industriali

2.2.3. hardware di supporto, applicazioni di gestione e reti di comunicazione utilizzati da tali sistemi

2.3. La presente politica si applica a tutte le sedi di lavoro: ambienti d'ufficio, siti remoti, aree produttive e piattaforme cloud che si interfacciano con tali dispositivi.

3. Obiettivi

3.1. Implementazione sicura: garantire che tutti i sistemi IoT/OT siano configurati in modo sicuro prima della loro introduzione nell'ambiente operativo.

3.2. Limitazione dell'esposizione: prevenire l'accesso non autorizzato, l'uso improprio o la compromissione dei dispositivi connessi mediante l'applicazione del controllo degli accessi e della segmentazione e dell'isolamento della rete.

3.3. Monitoraggio continuo: mantenere visibilità sulle operazioni IoT/OT mediante registrazione delle attività e monitoraggio di comportamenti anomali.

3.4. Responsabilità dei fornitori: garantire che i fornitori terzi adottino pratiche sicure di installazione, configurazione e manutenzione.

3.5. Conformità normativa: dimostrare il pieno allineamento agli standard applicabili quali ISO 27001, GDPR (ove siano trattati dati personali) e NIS2 ai fini della resilienza delle infrastrutture critiche.

4. Ruoli e responsabilità

4.1. Direttore generale (GM)

4.1.1. Ha la responsabilità complessiva della sicurezza dei sistemi IoT e OT

4.1.2. Approva la presente politica e ne garantisce l'applicazione in tutte le aree di lavoro

4.1.3. Verifica che fornitori e collaboratori esterni adottino pratiche sicure di installazione, configurazione iniziale e manutenzione

4.1.4. Autorizza l'accesso alla rete per ogni sistema IoT/OT

4.2. Dipendente designato o responsabile operativo (ove nominato)

4.2.1. Supervisiona l'inventario degli asset, la collocazione e la configurazione dei dispositivi IoT/OT

4.2.2. Registra la posizione di ciascun dispositivo, l'assegnazione di rete e la documentazione di supporto

4.2.3. Garantisce che qualsiasi modifica, ad esempio aggiornamenti del firmware o sostituzioni di dispositivi, sia documentata

[... 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. Riesame annuale

9.1.1. La presente politica deve essere riesaminata almeno una volta all'anno dal Direttore generale (GM)

9.1.2. Il riesame deve valutare se la politica resti efficace, copra le tipologie correnti di dispositivi e sia allineata a nuovi rischi o tecnologie

9.2. Aggiornamenti basati su eventi attivanti

9.2.1. Gli aggiornamenti della politica devono essere avviati anche quando:

9.2.2. vengono introdotte nuove tipologie di sistemi IoT o OT

9.2.3. i fornitori emettono avvisi di sicurezza o comunicazioni di fine vita

9.2.4. un incidente o un audit individua lacune nei controlli IoT/OT

9.2.5. nuove leggi o norme impongono requisiti aggiuntivi

9.3. Documentazione e controllo delle versioni

9.3.1. Tutti gli aggiornamenti devono essere documentati, inclusi data, numero di versione e sintesi delle modifiche

9.3.2. Il Direttore generale (GM) deve conservare le versioni storiche della politica ai fini di audit

9.4. Comunicazione delle modifiche

9.4.1. Qualsiasi aggiornamento della politica deve essere condiviso con tutto il personale e i fornitori interessati

9.4.2. Le versioni aggiornate devono essere rese accessibili tramite unità condivise o materiali stampati presso i siti di installazione o i centri di controllo

10. Politiche correlate e collegamenti

10.1. La presente politica deve essere applicata in coerenza con le seguenti politiche PMI correlate:

10.1.1. P4S – Politica di controllo degli accessi: definisce controlli di accesso a livello di dispositivo, uso di password robuste e procedure di accesso autorizzato per le piattaforme IoT e OT

10.1.2. P9S – Politica di lavoro da remoto: vieta l'uso di accessi remoti alle dashboard IoT/OT tramite canali non sicuri o non approvati

10.1.3. P17S – Politica di protezione dei dati e della privacy: si applica quando i dispositivi IoT, ad esempio telecamere di sicurezza, trattano o registrano dati personali, garantendo la conformità al GDPR

10.1.4. P30S – Politica di risposta agli incidenti (P30): definisce le procedure per rilevare, segnalare e risolvere incidenti IoT o OT, incluse sospette manomissioni o guasti operativi

10.1.5. P36S – Politica sui social media e sulle comunicazioni esterne: garantisce che nessuna informazione sui dispositivi o sulla configurazione della rete sia condivisa all'esterno senza approvazione

10.2. Ciascuna politica correlata rafforza l'applicazione e l'utilizzo operativo della presente politica fornendo indicazioni procedurali mirate.

11. Standard e quadri di riferimento

11.1. ISO/IEC 27001

11.1.1. Clausola 6.1 – Identificazione e trattamento del rischio: richiede che i rischi relativi ai sistemi IoT e OT siano valutati e mitigati in modo sistematico

11.1.2. Clausola 8.1 – Pianificazione e controllo operativi: garantisce il controllo operativo sicuro dei dispositivi connessi

11.2. ISO/IEC 27002

11.2.1. Controllo 5.23 – Sicurezza delle informazioni per l'uso della tecnologia operativa: definisce l'uso sicuro dell'OT negli ambienti fisici e digitali

11.2.2. Controllo 5.31 – Configurazione sicura dei sistemi informativi: richiede configurazioni sicure per i dispositivi IoT/OT ed evita impostazioni predefinite non sicure

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – Integrità di software, firmware e informazioni: richiede la validazione dell'integrità del firmware e degli aggiornamenti

11.3.2. CM-7 – Principio di minima funzionalità: i dispositivi non devono avere funzionalità inutilizzate o non sicure abilitate

11.3.3. AC-6 – Principio del privilegio minimo: l'accesso ai dispositivi deve essere limitato ai soli utenti autorizzati

11.3.4. PE-20 – Monitoraggio degli asset: monitoraggio fisico e operativo degli asset IoT e OT

11.3.5. SC-7 – Protezione dei confini: segmentazione e controllo delle comunicazioni di rete per i sistemi connessi

11.4. GDPR UE (2016/679)

11.4.1. Articolo 32 – Sicurezza del trattamento: se vengono acquisiti dati personali, ad esempio tramite telecamere di sorveglianza, l'organizzazione deve attuare misure tecniche e organizzative (TOM) adeguate per proteggere tale trattamento

11.5. Direttiva UE NIS2 (2022/2555)

11.5.1. Articolo 21(2)(a) – Misure di gestione del rischio

11.5.2. Articolo 21(2)(d) – Configurazione e uso sicuri dei dispositivi

11.5.3. Articolo 21(2)(f) – Sicurezza della catena di fornitura e dei sistemi

11.6. DORA UE (2022/2554)

11.6.1. Articolo 9(2) – Ambito di applicazione della gestione del rischio ICT: include dispositivi industriali e sistemi embedded utilizzati negli ambienti operativi

11.6.2. Articolo 10(1) – Continuità ICT: richiede che le configurazioni dei dispositivi supportino resilienza e operazioni di ripristino

11.7. COBIT 2019

11.7.1. DSS01 – Gestire le operazioni: si applica alla supervisione delle operazioni tecnologiche, inclusi i dispositivi fisici

11.7.2. DSS05 – Garantire i servizi di sicurezza: assicura che i sistemi connessi siano adeguatamente monitorati e protetti

11.7.3. APO13 – Gestire la sicurezza: rafforza le politiche per la protezione degli asset operativi nelle piccole e medie imprese (PMI)