					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P35S					Naslov dokumenta: **Politika varnosti IoT/OT**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzule 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontrole 5.23, 5	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
Uredba EU GDPR	Člen 32	
Direktiva EU NIS2	Člen 21(2)(a), (d), (f)	
Uredba EU DORA	Člen 9(2), 10(1)	

1. Namen

1.1. Ta politika določa obvezna pravila za varno uporabo in upravljanje naprav interneta stvari (IoT) ter sistemov operativne tehnologije (OT) v organizaciji. Te naprave lahko vključujejo pametne senzorje, varnostne kamere, proizvodne stroje, krmilnike HVAC ali druge industrijske sisteme, povezane v omrežje.

1.2. Namen te politike je:

1.2.1. zaščititi fizične in digitalne operacije pred motnjami ali manipulacijo prek neustrezno zavarovanih povezanih naprav;

1.2.2. zagotoviti varno uvajanje, spremljanje in vzdrževanje sistemov IoT in OT;

1.2.3. zagotoviti skladnost z ISO/IEC 27001:2022, Direktivo NIS2 in povezanimi regulativnimi okviri;

1.2.4. določiti praktične in izvršljive kontrole za MSP, ki delujejo v pisarniških, skladiščnih ali proizvodnih okoljih.

2. Področje uporabe

2.1. Ta politika velja za vse posameznike, vključene v načrtovanje, namestitev, konfiguracijo, uporabo, podporo ali odstranitev naprav IoT ali OT. To vključuje:

2.1.1. zaposlene, pogodbene izvajalce ali praktikante s fizičnim ali oddaljenim dostopom do naprav;

2.1.2. zunanje dobavitelje ali servisne tehnike, ki nameščajo ali vzdržujejo povezane sisteme;

2.1.3. generalnega direktorja ali osebje, odgovorno za nadzor nad varnostnimi politikami.

2.2. Politika zajema:

2.2.1. naprave IoT, kot so pametne ključavnice, nadzorni sistemi, pametni števci ali tiskalniki;

2.2.2. sisteme operativne tehnologije (OT), vključno s PLC-ji (programirljivimi logičnimi krmilniki), paneli sistema za nadzor, vodenje in zbiranje podatkov (SCADA) ali industrijskimi prehodi;

2.2.3. podporno strojno opremo, aplikacije za upravljanje in komunikacijska omrežja, ki jih ti sistemi uporabljajo.

2.3. Ta politika velja na vseh delovnih lokacijah: v pisarniških okoljih, na oddaljenih lokacijah, v proizvodnih prostorih in na oblačnih platformah, ki se povezujejo s temi napravami.

3. Cilji

3.1. Varno uvajanje: zagotoviti, da so vsi sistemi IoT/OT varno konfigurirani, preden se uvedejo v operativno okolje.

3.2. Omejitev izpostavljenosti: preprečiti nepooblaščen dostop, neustrezno uporabo ali prevzem povezanih naprav z uvedbo močnih kontrol dostopa in segmentacije omrežja.

3.3. Stalno spremljanje: ohranjati pregled nad delovanjem IoT/OT z beleženjem dejavnosti in spremljanjem neobičajnega vedenja.

3.4. Odgovornost dobaviteljev: zagotoviti, da zunanji ponudniki upoštevajo varne prakse namestitve, konfiguracije in vzdrževanja.

3.5. Regulativna skladnost: izkazovati popolno skladnost z veljavnimi standardi, kot so ISO 27001, GDPR (če se zbirajo osebni podatki) in NIS2 za odpornost kritične infrastrukture.

4. Vloge in odgovornosti

4.1. Generalni direktor (GM)

4.1.1. nosi celovito odgovornost za varnost sistemov IoT in OT;

4.1.2. odobri to politiko in zagotovi njeno izvajanje na vseh delovnih področjih;

4.1.3. preveri, ali dobavitelji in pogodbeni izvajalci upoštevajo varne prakse vzpostavitve in vzdrževanja;

4.1.4. odobri omrežni dostop za vsak sistem IoT/OT.

4.2. Imenovani zaposleni ali vodja operacij (če je določen)

4.2.1. nadzira popis, namestitev in konfiguracijo naprav IoT/OT;

4.2.2. evidentira lokacijo posamezne naprave, omrežno dodelitev in podporno dokumentacijo;

4.2.3. zagotovi, da so vse spremembe (npr. posodobitve vdelane programske opreme ali zamenjave naprav) dokumentirane.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Zahteve za pregled in posodobitev

9.1. Letni pregled

9.1.1. To politiko mora GM pregledati najmanj enkrat letno.

9.1.2. Pregled mora oceniti, ali politika ostaja učinkovita, ali zajema aktualne vrste naprav in ali je usklajena z novimi tveganji ali tehnologijami.

9.2. Posodobitve na podlagi sprožilcev

9.2.1. Posodobitev politike je treba začeti tudi, kadar:

9.2.2. se uvedejo nove vrste sistemov IoT ali OT;

9.2.3. dobavitelji izdajo varnostna opozorila ali obvestila o koncu življenjske dobe;

9.2.4. incident ali presoja pokaže vrzeli v kontrolah IoT/OT;

9.2.5. novi zakoni ali standardi določijo dodatne zahteve.

9.3. Dokumentacija in nadzor različic

9.3.1. Vse posodobitve morajo biti dokumentirane, vključno z datumom, številko različice in povzetkom sprememb.

9.3.2. GM mora zaradi potreb revizije hraniti zgodovinske različice politike.

9.4. Obveščanje o spremembah

9.4.1. O vseh posodobitvah politike je treba obvestiti vse relevantne zaposlene in dobavitelje.

9.4.2. Posodobljene različice morajo biti dostopne prek deljenih map ali tiskanega gradiva na mestih namestitve ali v nadzornih centrih.

10. Povezane politike in povezave

10.1. To politiko je treba izvajati usklajeno z naslednjimi povezanimi politikami za MSP:

10.1.1. P4S – Politika nadzora dostopa: določa kontrole prijave na ravni naprav, uporabo močnih gesel in postopke za odobren dostop do platform IoT in OT;

10.1.2. P9S – Politika dela na daljavo: preprečuje uporabo oddaljenega dostopa do nadzornih plošč IoT/OT prek nevarnih ali neodobrenih kanalov;

10.1.3. P17S – Politika varstva podatkov in zasebnosti: uporablja se, če naprave IoT (npr. varnostne kamere) obdelujejo ali snemajo osebne podatke, in zagotavlja skladnost z GDPR;

10.1.4. P30S – Politika odzivanja na incidente: določa postopke za odkrivanje, prijavo in obravnavo incidentov IoT ali OT, vključno s sumom poseganja ali operativne odpovedi;

10.1.5. P36S – Politika družbenih medijev in zunanjega komuniciranja: zagotavlja, da se podatki o napravah ali razporeditvi omrežja ne delijo navzven brez odobritve.

10.2. Vsaka povezana politika krepi izvajanje in praktično uporabo te politike z usmerjenimi postopkovnimi navodili.

11. Referenčni standardi in okviri

11.1. ISO/IEC 27001

11.1.1. Klavzula 6.1 – identifikacija tveganj in obravnava tveganj: zahteva, da se tveganja, povezana s sistemi IoT in OT, sistematično ocenijo in zmanjšujejo.

11.1.2. Klavzula 8.1 – operativno načrtovanje in nadzor: zagotavlja varen operativni nadzor nad povezanimi napravami.

11.2. ISO/IEC 27002

11.2.1. Kontrola 5.23 – informacijska varnost pri uporabi sistemov operativne tehnologije (OT): določa varno uporabo OT v fizičnih in digitalnih okoljih.

11.2.2. Kontrola 5.31 – varna konfiguracija informacijskih sistemov: zahteva varnostno utrjevanje nastavitev naprav IoT/OT in izogibanje nevarnim privzetim nastavitvam.

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – celovitost programske opreme, vdelane programske opreme in informacij: zahteva preverjanje celovitosti vdelane programske opreme in posodobitev.

11.3.2. CM-7 – načelo najmanjše funkcionalnosti: naprave ne smejo imeti omogočenih neuporabljenih ali nevarnih funkcij.

11.3.3. AC-6 – načelo najmanjših privilegijev: dostop do naprav mora biti omejen izključno na pooblaščene uporabnike.

11.3.4. PE-20 – spremljanje sredstev: fizično in operativno spremljanje sredstev IoT in OT.

11.3.5. SC-7 – zaščita omrežnih meja: segmentacija in nadzor omrežnih komunikacij za povezane sisteme.

11.4. Uredba EU GDPR (2016/679)

11.4.1. Člen 32 – Varnost obdelave: če se zajemajo osebni podatki (npr. prek nadzornih kamer), mora organizacija uvesti ustrezne tehnične in organizacijske ukrepe za zavarovanje takšne obdelave.

11.5. Direktiva EU NIS2 (2022/2555)

11.5.1. Člen 21(2)(a) – ukrepi za obvladovanje tveganj;

11.5.2. Člen 21(2)(d) – varna konfiguracija in uporaba naprav;

11.5.3. Člen 21(2)(f) – varnost dobavne verige in sistemov.

11.6. Uredba EU DORA (2022/2554)

11.6.1. Člen 9(2) – področje upravljanja tveganj IKT: vključuje industrijske in vdelane naprave, ki se uporabljajo v operativnih okoljih.

11.6.2. Člen 10(1) – neprekinjeno izvajanje IKT: zahteva, da konfiguracije naprav podpirajo odpornost in postopke obnovitve.

11.7. COBIT 2019

11.7.1. DSS01 – upravljanje operacij: uporablja se za nadzor tehnoloških operacij, vključno s fizičnimi napravami.

11.7.2. DSS05 – upravljanje varnostnih storitev: zagotavlja, da se povezani sistemi ustrezno spremljajo in varujejo.

11.7.3. APO13 – upravljanje varnosti: krepi politike za zaščito operativnih sredstev v MSP.