| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vnesite naziv registrirane pravne osebe | | | | | | | |
| Številka dokumenta:<br>P35 | | | | | Naslov dokumenta:<br>**Politika varnosti IoT/OT** | | | | | | | |
| Različica:<br>1.0 | | Datum začetka veljavnosti:<br>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 | Klavzula 8 | |
| ISO/IEC 27002:2022 | Kontrole 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 | |
| Uredba EU GDPR | Členi 5, 25, 32 | |
| Direktiva EU NIS2 | Člena 21, 23 | |
| Uredba EU DORA | Člena 9, 10 | |
| COBIT 2019 | DSS05.01, BAI09.01, APO13.02 | |

**1. Namen**

1.1 Ta politika določa obvezne zahteve informacijske varnosti za uvajanje, delovanje, spremljanje in izločitev iz uporabe sistemov interneta stvari (IoT) in sistemov operativne tehnologije (OT) v organizaciji.

1.2 Zagotavlja, da so takšni sistemi vključeni v širši sistem upravljanja kibernetske varnosti organizacije ter zaščiteni pred ogrožanjem, zlorabo in operativno sabotažo.

1.3 Namen politike je vzpostaviti močne tehnične, organizacijske in procesne kontrole za zaščito sistemov IoT/OT, ki so povezani s fizično infrastrukturo, proizvodnimi procesi in varnostno kritičnimi okolji.

1.4 Politika podpira regulatorne in pogodbene obveznosti na področjih kibernetske varnosti, varnosti, okoljskega nadzora in neprekinjenega poslovanja.

**2. Področje uporabe**

2.1 Ta politika velja za vse sisteme IoT in OT, ne glede na to, ali so v lasti podjetja, v najemu ali jih zagotavljajo tretje osebe, ki se uporabljajo v operativnih, administrativnih ali proizvodnih okoljih organizacije.

**2.2 Zajeti sistemi med drugim vključujejo:**

2.2.1 naprave interneta stvari, kot so okoljski senzorji, sistemi za nadzor dostopa, pametna razsvetljava, nadzorna oprema in nosljive naprave,

2.2.2 platforme OT, kot so PLC-ji, sistemi za nadzor, vodenje in zajem podatkov (SCADA), porazdeljeni krmilni sistemi (DCS), vmesniki človek–stroj (HMI), vmesniki proizvodnega izvršilnega sistema (MES) in terenski krmilniki,

2.2.3 industrijska krmilna omrežja ali z oblakom povezani viri, ki spremljajo fizične operacije.

**2.3 Politika zajema:**

2.3.1 vsa okolja (v lastnih prostorih, na robu omrežja, v oblaku),

2.3.2 vse deležnike (notranje uporabnike, integratorje, dobavitelje tretjih oseb, pogodbene izvajalce),

2.3.3 vse faze življenjskega cikla (načrtovanje, nabava, uvajanje, delovanje, izločitev iz uporabe).

**3. Cilji**

3.1 Zaščititi infrastrukturo IoT in OT pred notranjimi in zunanjimi kibernetskimi grožnjami, vključno z napadi za zavrnitev storitve, nepooblaščenim dostopom, širjenjem izsiljevalske programske opreme in posegi v vdelano programsko opremo.

3.2 Zagotoviti, da platforme IoT/OT ne postanejo vektorji napadov prek povezave IT-OT ali sredstvo za ogrožanje varnostno kritičnih sistemov.

3.3 Uveljavljati načela varnosti že v zasnovi in večplastne obrambe skozi celoten življenjski cikel teh tehnologij.

3.4 Omogočiti zanesljivo, varno in revizijsko sledljivo integracijo platform IoT in OT v center za varnostne operacije (SOC) organizacije in načrte odzivanja na incidente.

3.5 Zagotoviti, da so vse uvedbe usklajene s kontrolami standarda ISO/IEC 27001 in veljavnimi sektorskimi smernicami (npr. IEC 62443, ISO 27019, NIST SP 800-82).

**4. Vloge in odgovornosti**

**4.1 Vodja informacijske varnosti (CISO) / vodja varnosti**

4.1.1 Določa politike in tehnične standarde za kibernetsko varnost IoT/OT.

4.1.2 Nadzira ocenjevanje tveganj, preverjanje kontrol in medoddelčno usklajevanje.

**4.2 Inženirji operativne tehnologije / vodje objektov in obratov**

4.2.1 Preverjajo konfiguracije sistemov OT in zagotavljajo skladnost s to politiko v proizvodnih območjih.

4.2.2 Vzdržujejo fizične in logične varnostne ukrepe za celovitost in varnost okolij OT.

[ ... 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 Ta politika mora biti pregledana najmanj enkrat letno in posodobljena na podlagi:**

9.1.1 sprememb arhitekture sistemov OT ali IoT, dobaviteljev ali platform,

9.1.2 večjih regulatornih sprememb (npr. sprememb DORA, NIS2 ali sektorskih direktiv),

9.1.3 pojava novih ranljivosti ali vzorcev groženj v krmilnih sistemih,

9.1.4 ugotovitev notranjih ali zunanjih presoj, penetracijskih testov ali vaj rdeče ekipe.

9.2 Vodja informacijske varnosti, vodja varnosti OT in vodje zadevnih oddelkov so skupaj odgovorni za začetek postopka pregleda.

**9.3 Vmesni pregledi se morajo sprožiti po:**

9.3.1 vsakem incidentu, povezanem z IoT/OT, ki povzroči odpoved sistema ali izgubo podatkov,

9.3.2 uvedbi pomembne nove opreme, programske opreme za spremljanje ali platform vdelane programske opreme,

9.3.3 integraciji pametnega robnega računalništva ali avtomatizacije na terenski ravni, podprte z umetno inteligenco.

**9.4 Vse spremembe politike morajo biti:**

9.4.1 dokumentirane v evidenci različic in registru sprememb politike,

9.4.2 sporočene vsem zadevnim uporabnikom, dobaviteljem in operaterjem IT/OT,

9.4.3 ponovno odobrene s strani najvišjega vodstva.

**10. Povezane politike in povezave**

**10.1 Ta politika se uporablja skupaj z naslednjimi politikami informacijske varnosti in je z njimi podprta:**

10.1.1 P1 – Politika informacijske varnosti: določa temeljna načela varnosti, ki veljajo tudi za varnost sistemov IoT in OT.

10.1.2 P3 – Politika sprejemljive uporabe (AUP): določa omejitve glede osebne in nepooblaščene uporabe naprav, tudi v operativnih okoljih.

10.1.3 P6 – Politika upravljanja tveganj: usmerja presojo, sprejem in zmanjševanje tveganj, povezanih z vdelanimi in krmilnimi sistemi.

10.1.4 P12 – Politika upravljanja sredstev: zagotavlja, da so vsi sistemi IoT in OT formalno evidentirani v popisu in imajo določene odgovorne lastnike.

10.1.5 P20 – Politika zaščite končnih točk / zaščite pred zlonamerno programsko opremo: velja za povezane krmilnike, pametne prehode in robne sisteme v proizvodnji.

10.1.6 P22 – Politika beleženja in spremljanja: velja tudi za zajemanje dnevnikov in postopke njihovega pregleda v okoljih OT.

10.1.7 P30 – Politika odzivanja na incidente: neposredno določa, kako je treba eskalirati in upravljati kršitve, anomalije ali odpovedi sistemov IoT/OT.

10.1.8 P33 – Politika spremljanja presoj in skladnosti: zagotavlja mehanizme za potrditev stalne skladnosti s to politiko.

## 11. Referenčni standardi in okviri

11.1 Ta politika je usklajena z mednarodno priznanimi standardi in regulatornimi okviri, ki zagotavljajo varnost, odpornost in skladnost sistemov interneta stvari (IoT) in sistemov operativne tehnologije (OT) v industrijskih, proizvodnih in korporativnih okoljih.

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

11.2.1 Kontrola 5.7 – Obveščevalni podatki o grožnjah: podpira spremljanje okolij OT in prepoznavanje ranljivosti, značilnih za IoT.

11.2.2 Kontrola 5.23 – Informacijska varnost pri uporabi storitev v oblaku: velja, kadar se naprave IoT povezujejo z oblačnimi platformami za telemetrijo, krmiljenje ali analitiko.

11.2.3 Kontrola 5.27 – Načela varne arhitekture in inženiringa sistemov: določa načela varnosti že v zasnovi za vdelane sisteme in krmilna omrežja.

11.2.4 Kontrola 5.31 – Varnost v razvojnih in podpornih procesih: zahteva preverjanje programske in vdelane opreme, kontrole popravkov ter zahteve do dobaviteljev pri uvedbah OT.

11.2.5 Kontrola 5.36 – Skladnost s pravnimi in pogodbenimi zahtevami: zagotavlja skladnost sredstev OT z zahtevami glede varnosti, okolja in regulative.

11.2.6 Te kontrole skupaj določajo dobre prakse za zaščito sistemov IoT/OT skozi celoten njihov življenjski cikel, vključno z načrtovanjem arhitekture, varnim uvajanjem, nameščanjem popravkov, zaznavanjem anomalij in skladnostjo s sektorskimi zahtevami.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Zaščita meja: zagotavlja, da so omrežja OT segmentirana in zaščitena pred nepooblaščenim dostopom.

11.3.2 SI-4 – Spremljanje sistemov: zahteva uvedbo mehanizmov neprekinjenega spremljanja in zaznavanja anomalij v okoljih ICS.

11.3.3 CM-2 – Osnovna konfiguracija: zahteva nadzor konfiguracij in varnostno utrjevanje platform IoT/OT.

11.3.4 AC-6 – Načelo najmanjših privilegijev: velja za uporabniški dostop in oddaljeno servisiranje vdelanih krmilnih sistemov s strani dobaviteljev.

11.3.5 PL-8 – Arhitekture varnosti in zasebnosti: določa načrtovanje varne integracije sistemov, zlasti pri projektih modernizacije OT.

### 11.4 Uredba EU GDPR (2016/679)

11.4.1 Člen 5 – Načela v zvezi z obdelavo osebnih podatkov: velja za platforme IoT, ki obdelujejo senzorske ali vedenjske podatke, povezane s posamezniki.

11.4.2 Člen 25 – Varstvo podatkov že v fazi načrtovanja in privzeto: zahteva varovala zasebnosti, vključena v zasnovo izdelkov IoT in vdelane programske opreme.

11.4.3 Člen 32 – Varnost obdelave: zahteva šifriranje, nadzor dostopa in varne komunikacije pri prenosu podatkov pametnih naprav.

**11.5 Direktiva EU NIS2 (2022/2555)**

11.5.1 Člena 21 in 23: nalagata varnostne obveznosti bistvenim in pomembnim subjektom, ki uporabljajo sisteme OT. To vključuje ocenjevanje tveganj, poročanje o incidentih in preverjanje dobavne verige dobaviteljev IoT/OT ter celovitosti vdelane programske opreme.

**11.6 Uredba EU DORA (2022/2554)**

11.6.1 Člen 9 – Upravljanje tveganj IKT: zahteva varno integracijo vdelanih sistemov in tehnologij OT v program upravljanja tveganj IKT.

11.6.2 Člen 10 – Varnostne zahteve IKT: določa zaščitne ukrepe za medsebojno povezane platforme OT, ki se uporabljajo v finančnih in kritičnih storitvenih okoljih.

**11.7 COBIT 2019**

11.7.1 DSS05.01 – Zaščita pred zlonamerno programsko opremo: vključuje zaznavanje in odzivanje na grožnje, značilne za ICS, ter kampanje zlonamerne programske opreme, usmerjene v IoT.

11.7.2 BAI09.01 – Določitev in vzdrževanje varnostnih zahtev: preslika se na varno zagotavljanje in delovanje pametne ali vdelane infrastrukture.

11.7.3 APO13.02 – Določitev in vzdrževanje načrta informacijske varnosti: zahteva vključitev sistemov OT in njihovih ranljivosti v celovito strategijo kibernetske varnosti organizacije.