					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P35					Naziv dokumenta: **Politika sigurnosti za IoT / OT**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 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	
GDPR EU	Članci 5, 25, 32	
Direktiva EU NIS2	Članci 21, 23	
Uredba EU DORA	Članci 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Svrha

1.1 Ova politika utvrđuje obvezne zahtjeve informacijske sigurnosti za uvođenje, rad, praćenje i stavljanje izvan uporabe sustava Interneta stvari (IoT) i operativne tehnologije (OT) unutar organizacije.

1.2 Njome se osigurava da su takvi sustavi integrirani u širi sustav upravljanja kibernetičkom sigurnošću organizacije te zaštićeni od kompromitacije, zlouporabe ili operativne sabotaže.

1.3 Cilj ove politike jest uspostaviti snažne tehničke, organizacijske i proceduralne kontrole radi zaštite IoT/OT sustava povezanih s fizičkom infrastrukturom, proizvodnim procesima i sigurnosno kritičnim okruženjima.

1.4 Ova politika podupire regulatorne i ugovorne obveze u području kibernetičke sigurnosti, fizičke sigurnosti, zaštite okoliša i kontinuiteta poslovanja.

2. Opseg

2.1 Ova politika primjenjuje se na sve IoT i OT sustave, neovisno o tome jesu li u vlasništvu organizacije, unajmljeni ili ih osiguravaju treće strane, a koji se koriste u operativnim, administrativnim ili produkcijskim okruženjima organizacije.

2.2 Obuhvaćeni sustavi uključuju, ali nisu ograničeni na:

2.2.1 IoT uređaje kao što su senzori okoliša, sustavi kontrole pristupa, pametna rasvjeta, oprema za nadzor i nosivi uređaji

2.2.2 OT platforme kao što su programabilni logički kontroleri (PLC), SCADA sustavi, distribuirani upravljački sustavi (DCS), sučelja čovjek-stroj (HMI), sučelja sustava za upravljanje proizvodnjom (MES) i terenski kontroleri

2.2.3 industrijske upravljačke mreže ili imovinu u oblaku koja prati fizičke operacije

2.3 Ova politika obuhvaća:

2.3.1 sva okruženja (lokalna, rubna, upravljana iz oblaka)

2.3.2 sve dionike (interne korisnike, integratore, dobavljače trećih strana, ugovorne izvođače)

2.3.3 sve faze životnog ciklusa (projektiranje, nabavu, uvođenje, rad, stavljanje izvan pogona)

3. Ciljevi

3.1 Zaštititi IoT i OT infrastrukturu od unutarnjih i vanjskih kibernetičkih prijetnji, uključujući uskraćivanje usluge, neovlašteni pristup, širenje ucjenjivačkog softvera i neovlaštenu izmjenu firmvera.

3.2 Osigurati da IoT/OT platforme ne postanu vektori napada preko IT-OT poveznice niti ugroze sigurnosno kritične sustave.

3.3 Primijeniti načela ugrađene sigurnosti i obrane u dubini tijekom cijelog životnog ciklusa tih tehnologija.

3.4 Omogućiti pouzdanu, sigurnu i revizijski sljedivu integraciju IoT i OT platformi u centar za sigurnosne operacije (SOC) organizacije i planove odgovora na incidente.

3.5 Osigurati da su sva uvođenja usklađena s kontrolama norme ISO/IEC 27001 i primjenjivim sektorskim smjernicama (npr. IEC 62443, ISO 27019, NIST SP 800-82).

4. Uloge i odgovornosti

4.1 glavni službenik za informacijsku sigurnost (CISO) / voditelj informacijske sigurnosti

4.1.1 Definira politike i tehničke standarde kibernetičke sigurnosti za IoT/OT sustave

4.1.2 Nadgleda procjene rizika, provjeru kontrola i međufunkcionalnu koordinaciju

4.2 OT inženjeri / voditelji objekata i postrojenja

4.2.1 Provode provjeru konfiguracija OT sustava i osiguravaju usklađenost s politikom u produkcijskim područjima

4.2.2 Održavaju fizičke i logičke zaštitne mjere radi očuvanja cjelovitosti i sigurnosti OT sustava

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Ova politika mora se pregledati najmanje jednom godišnje i ažurirati na temelju:

9.1.1 promjena u arhitekturi, dobavljačima ili platformama OT ili IoT sustava

9.1.2 značajnih regulatornih promjena (npr. izmjene Uredbe EU DORA, Direktive EU NIS2 ili sektorskih direktiva)

9.1.3 pojave novih ranjivosti ili obrazaca prijetnji u upravljačkim sustavima

9.1.4 nalaza unutarnjih ili vanjskih revizija, penetracijskih testova ili vježbi crvenog tima

9.2 CISO, voditelj sigurnosti OT-a i relevantni voditelji odjela zajednički su odgovorni za pokretanje postupka pregleda.

9.3 Izvanredni pregledi moraju se pokrenuti nakon:

9.3.1 bilo kojeg incidenta povezanog s IoT/OT-om koji je rezultirao kvarom sustava ili gubitkom podataka

9.3.2 uvođenja značajne nove opreme, softvera za praćenje ili platformi firmvera

9.3.3 integracije pametnog rubnog računalstva ili automatizacije unaprijeđene umjetnom inteligencijom na terenskoj razini

9.4 Sve promjene politike moraju biti:

9.4.1 dokumentirane u povijesti verzija i registru promjena politike

9.4.2 priopćene svim pogođenim korisnicima, dobavljačima i IT/OT operaterima

9.4.3 ponovno odobrene od strane izvršnog rukovodstva

10. Povezane politike i poveznice

10.1 Ova politika primjenjuje se zajedno sa sljedećim politikama informacijske sigurnosti i na njih se oslanja:

10.1.1 P1 – Politika informacijske sigurnosti: utvrđuje temeljna sigurnosna načela koja se primjenjuju i na sigurnost IoT i OT sustava.

10.1.2 P3 – Politika prihvatljive uporabe: definira ograničenja osobne uporabe i uporabe neovlaštenih uređaja, uključujući operativna okruženja.

10.1.3 P6 – Politika upravljanja rizicima: usmjerava procjenu, prihvaćanje i ublažavanje rizika povezanih s ugrađenim i upravljačkim sustavima.

10.1.4 P12 – Politika upravljanja imovinom: osigurava da su svi IoT i OT sustavi formalno evidentirani i da imaju dodijeljene odgovorne vlasnike.

10.1.5 P20 – Politika zaštite krajnjih točaka / zaštite od zlonamjernog softvera: primjenjuje se na povezane kontrolere, pametne pristupnike i rubne sustave u proizvodnji.

10.1.6 P22 – Politika bilježenja i praćenja: primjenjuje se i na postupke prikupljanja i pregleda dnevničkih zapisa u OT okruženjima.

10.1.7 P30 – Politika odgovora na incidente: izravno uređuje kako se povrede, anomalije ili kvarovi sustava povezani s IoT/OT-om moraju eskalirati i njima upravljati.

10.1.8 P33 – Politika praćenja revizije i usklađenosti: osigurava mehanizme potvrde za provjeru trajne usklađenosti s ovom politikom.

11. Referentni standardi i okviri

11.1 Ova politika usklađena je s međunarodno priznatim standardima i regulatornim okvirima koji osiguravaju sigurnost, otpornost i usklađenost sustava Interneta stvari (IoT) i operativne tehnologije (OT) u industrijskim, proizvodnim i poslovnim okruženjima.

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

11.2.1 Kontrola 5.7 – obavještajni podaci o prijetnjama: usmjerava praćenje OT okruženja i identifikaciju ranjivosti specifičnih za IoT.

11.2.2 Kontrola 5.23 – informacijska sigurnost pri uporabi usluga u oblaku: primjenjuje se kada se IoT uređaji povezuju s platformama u oblaku radi telemetrije, upravljanja ili analitike.

11.2.3 Kontrola 5.27 – načela sigurne arhitekture i inženjerstva sustava: uređuje načela ugrađene sigurnosti za ugrađene sustave i upravljačke mreže.

11.2.4 Kontrola 5.31 – sigurnost u procesima razvoja i podrške: nalaže provjeru softvera i firmvera, kontrole zakrpavanja i zahtjeve prema dobavljačima u OT uvođenjima.

11.2.5 Kontrola 5.36 – usklađenost sa zakonskim i ugovornim zahtjevima: osigurava usklađenost OT imovine sa zahtjevima sigurnosti, zaštite okoliša i regulatornim obvezama.

11.2.6 Ove kontrole zajedno uspostavljaju dobre prakse za zaštitu IoT/OT sustava tijekom cijelog životnog ciklusa, uključujući projektiranje arhitekture, sigurno uvođenje, zakrpavanje, otkrivanje anomalija i usklađenost sa sektorskim zahtjevima.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – zaštita granica sustava: osigurava da su OT mreže segmentirane i zaštićene od neovlaštenog pristupa.

11.3.2 SI-4 – praćenje sustava: zahtijeva provedbu kontinuiranog praćenja i mehanizama za otkrivanje anomalija u ICS okruženjima.

11.3.3 CM-2 – polazna konfiguracija: nalaže upravljanje konfiguracijom i otvrdnjavanje uređaja na IoT/OT platformama.

11.3.4 AC-6 – načelo najmanjih privilegija: primjenjuje se na pristup korisnika i udaljeno servisiranje ugrađenih upravljačkih sustava od strane dobavljača.

11.3.5 PL-8 – sigurnosne arhitekture i arhitekture privatnosti: uređuje planiranje sigurne integracije sustava, osobito za projekte modernizacije OT-a.

11.4 GDPR EU (2016/679)

11.4.1 Članak 5 – načela obrade osobnih podataka: primjenjuje se na IoT platforme koje obrađuju podatke sa senzora ili podatke o ponašanju povezane s pojedincima.

11.4.2 Članak 25 – zaštita podataka kroz dizajn i zadane postavke: zahtijeva mjere zaštite privatnosti ugrađene u dizajn IoT proizvoda i firmvera.

11.4.3 Članak 32 – sigurnost obrade: nalaže šifriranje, kontrole pristupa i sigurnu komunikaciju za prijenos podataka pametnih uređaja.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članci 21 i 23: nameću sigurnosne obveze ključnim i važnim subjektima koji koriste OT sustave. To uključuje procjenu rizika, prijavljivanje incidenata i provjeru opskrbnog lanca dobavljača IoT/OT rješenja te integriteta firmvera.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Članak 9 – upravljanje IKT rizicima: zahtijeva sigurnu integraciju ugrađenih sustava i OT tehnologija u program upravljanja IKT rizicima.

11.6.2 Članak 10 – zahtjevi IKT sigurnosti: nalaže zaštitne mjere za međusobno povezane OT platforme koje se koriste u financijskim i kritičnim uslužnim okruženjima.

11.7 COBIT 2019

11.7.1 DSS05.01 – zaštita od zlonamjernog softvera: uključuje otkrivanje i odgovor na prijetnje specifične za ICS i kampanje zlonamjernog softvera usmjerene na IoT.

11.7.2 BAI09.01 – uspostava i održavanje sigurnosnih zahtjeva: povezuje se sa sigurnom dodjelom i radom pametne ili ugrađene infrastrukture.

11.7.3 APO13.02 – uspostava i održavanje plana informacijske sigurnosti: zahtijeva uključivanje OT sustava i njihovih ranjivosti u strategiju kibernetičke sigurnosti na razini cijele organizacije.