					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P35S					Naziv dokumenta: **Politika sigurnosti za internet stvari (IoT) i operativnu tehnologiju (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**

Usklađenost sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 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	
GDPR EU	Članak 32	
Direktiva EU NIS2	Članak 21(2)(a), (d), (f)	
Uredba EU DORA	Članak 9(2), 10(1)	

1. Svrha

1.1. Ova politika propisuje obvezna pravila za sigurno korištenje i upravljanje sustavima interneta stvari (IoT) i operativne tehnologije (OT) unutar organizacije. Ti sustavi mogu uključivati pametne senzore, sigurnosne kamere, proizvodne strojeve, HVAC kontrolere ili bilo koje industrijske sustave povezane na mrežu.

1.2. Svrha ove politike je:

1.2.1. zaštititi fizičke i digitalne operacije od prekida ili manipulacije putem nedovoljno zaštićenih povezanih uređaja

1.2.2. osigurati sigurnu uspostavu, nadzor i održavanje IoT i OT sustava

1.2.3. osigurati usklađenost s normom ISO/IEC 27001:2022, Direktivom NIS2 i povezanim regulatornim okvirima

1.2.4. uspostaviti praktične i provedive kontrole za SME organizacije koje posluju u uredskim, skladišnim ili proizvodnim okruženjima

2. Područje primjene

2.1. Ova politika primjenjuje se na sve osobe uključene u planiranje, instalaciju, konfiguraciju, korištenje, podršku ili zbrinjavanje IoT ili OT uređaja. To uključuje:

2.1.1. zaposlenike, ugovorne izvođače ili vježbenike s fizičkim ili udaljenim pristupom uređajima

2.1.2. vanjske dobavljače ili servisne tehničare koji instaliraju ili održavaju povezane sustave

2.1.3. glavnog direktora ili osoblje odgovorno za nadzor sigurnosnih politika

2.2. Ova politika obuhvaća:

2.2.1. IoT uređaje kao što su pametne brave, oprema za nadzor, pametna brojila ili pisači

2.2.2. OT sustave, uključujući programabilne logičke kontrolere (PLC), SCADA panele ili industrijske pristupnike

2.2.3. pripadajući hardver, aplikacije za upravljanje i komunikacijske mreže koje ti sustavi koriste

2.3. Ova politika primjenjuje se na svim lokacijama rada: u uredskim okruženjima, na udaljenim lokacijama, u proizvodnim pogonima i na platformama u oblaku koje su povezane s tim uređajima.

3. Ciljevi

3.1. Sigurna uspostava: osigurati da su svi IoT/OT sustavi sigurno konfigurirani prije uvođenja u operativno okruženje.

3.2. Ograničavanje izloženosti: spriječiti neovlašteni pristup, zlouporabu ili preuzimanje kontrole nad povezanim uređajima provedbom snažnih kontrola pristupa i segmentacije mreže.

3.3. Kontinuirani nadzor: održavati vidljivost nad radom IoT/OT sustava evidentiranjem aktivnosti i praćenjem neuobičajenog ponašanja.

3.4. Odgovornost dobavljača: osigurati da vanjski pružatelji usluga primjenjuju sigurne prakse instalacije, konfiguracije i održavanja.

3.5. Usklađenost s regulatornim zahtjevima: dokazati potpunu usklađenost s primjenjivim standardima kao što su ISO 27001, GDPR EU (ako se prikupljaju osobni podaci) i NIS2 za otpornost kritične infrastrukture.

4. Uloge i odgovornosti

4.1. glavni direktor (GM)

4.1.1. snosi ukupnu odgovornost za sigurnost IoT i OT sustava

4.1.2. odobrava ovu politiku i osigurava njezinu primjenu u svim područjima rada

4.1.3. provjerava primjenjuju li dobavljači i ugovorni izvođači sigurne prakse uspostave i održavanja

4.1.4. odobrava mrežni pristup za svaki IoT/OT sustav

4.2. imenovani zaposlenik ili voditelj operacija (ako je određen)

4.2.1. nadzire popis imovine, smještaj i konfiguraciju IoT/OT uređaja

4.2.2. evidentira lokaciju svakog uređaja, mrežnu dodjelu i pripadajuću dokumentaciju podrške

4.2.3. osigurava da se sve promjene (npr. ažuriranja firmvera ili zamjene uređaja) dokumentiraju

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

9. Zahtjevi za pregled i ažuriranje

9.1. godišnji pregled

9.1.1. ovu politiku GM mora pregledati najmanje jednom godišnje

9.1.2. pregled mora ocijeniti ostaje li politika djelotvorna, obuhvaća li aktualne vrste uređaja te je li usklađena s novim rizicima i tehnologijama

9.2. ažuriranja potaknuta događajem

9.2.1. ažuriranja politike moraju se pokrenuti i kada:

9.2.2. se uvedu nove vrste IoT ili OT sustava

9.2.3. dobavljači izdaju sigurnosne biltene ili obavijesti o kraju životnog vijeka

9.2.4. incident ili revizija utvrdi nedostatke u IoT/OT kontrolama

9.2.5. novi zakoni ili standardi uvedu dodatne zahtjeve

9.3. dokumentiranje i upravljanje verzijama

9.3.1. sva ažuriranja moraju biti dokumentirana, uključujući datum, broj verzije i sažetak promjena

9.3.2. GM mora zadržati povijesne verzije politike za potrebe revizije

9.4. obavještavanje o promjenama

9.4.1. svako ažuriranje politike mora se podijeliti sa svim relevantnim zaposlenicima i dobavljačima

9.4.2. ažurirane verzije moraju biti dostupne putem zajedničkih mapa ili u tiskanom obliku na lokacijama instalacije ili u upravljačkim centrima

10. Povezane politike i poveznice

10.1. Ova politika mora se provoditi usklađeno sa sljedećim povezanim SME politikama:

10.1.1. P4S – Politika kontrole pristupa: propisuje kontrole prijave na razini uređaja, korištenje snažnih lozinki i postupke ovlaštenog pristupa za IoT i OT platforme

10.1.2. P9S – Politika rada na daljinu: sprječava korištenje udaljenog pristupa upravljačkim nadzornim pločama IoT/OT sustava putem nesigurnih ili neodobrenih kanala

10.1.3. P17S – Politika zaštite podataka i privatnosti: primjenjuje se ako IoT uređaji (npr. sigurnosne kamere) obrađuju ili snimaju osobne podatke, čime se osigurava usklađenost s GDPR-om

10.1.4. P30S – Politika odgovora na incidente: definira postupke za otkrivanje, prijavljivanje i rješavanje IoT ili OT incidenata, uključujući sumnju na neovlaštenu izmjenu ili operativni kvar

10.1.5. P36S – Politika društvenih mreža i vanjskih komunikacija: osigurava da se podaci o uređajima ili mrežnom rasporedu ne dijele izvan organizacije bez odobrenja

10.2. Svaka povezana politika jača primjenu i praktičnu uporabu ove politike pružanjem ciljano usmjerenih proceduralnih smjernica.

11. Referentni standardi i okviri

11.1. ISO/IEC 27001

11.1.1. Točka 6.1 – identifikacija i obrada rizika: zahtijeva da se rizici povezani s IoT i OT sustavima sustavno procjenjuju i ublažavaju

11.1.2. Točka 8.1 – operativno planiranje i kontrola: osigurava sigurnu operativnu kontrolu nad povezanim uređajima

11.2. ISO/IEC 27002

11.2.1. Kontrola 5.23 – sigurnost informacija pri korištenju operativne tehnologije: definira sigurno korištenje OT-a u fizičkim i digitalnim okruženjima

11.2.2. Kontrola 5.31 – sigurna konfiguracija informacijskih sustava: zahtijeva sigurnosno očvrsnute postavke za IoT/OT uređaje i izbjegavanje nesigurnih zadanih postavki

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – cjelovitost softvera, firmvera i informacija: zahtijeva provjeru cjelovitosti firmvera i ažuriranja

11.3.2. CM-7 – minimalna funkcionalnost: uređaji ne smiju imati omogućene neiskorištene ili nesigurne funkcije

11.3.3. AC-6 – načelo najmanjih privilegija: pristup uređajima mora biti ograničen isključivo na ovlaštene korisnike

11.3.4. PE-20 – praćenje imovine: fizičko i operativno praćenje IoT i OT imovine

11.3.5. SC-7 – zaštita granica sustava: segmentacija i kontrola mrežnih komunikacija za povezane sustave

11.4. GDPR EU (2016/679)

11.4.1. Članak 32 – sigurnost obrade: ako se prikupljaju osobni podaci (npr. putem sigurnosnih kamera), organizacija mora primijeniti odgovarajuće tehničke i organizacijske mjere za zaštitu takve obrade

11.5. Direktiva EU NIS2 (2022/2555)

11.5.1. Članak 21(2)(a) – mjere upravljanja rizicima

11.5.2. Članak 21(2)(d) – sigurna konfiguracija i korištenje uređaja

11.5.3. Članak 21(2)(f) – sigurnost opskrbnog lanca i sustava

11.6. Uredba EU DORA (2022/2554)

11.6.1. Članak 9(2) – opseg upravljanja IKT rizicima: uključuje industrijske i ugrađene uređaje koji se koriste u operativnim okruženjima

11.6.2. Članak 10(1) – kontinuitet IKT-a: zahtijeva da konfiguracije uređaja podržavaju otpornost i postupke oporavka

11.7. COBIT 2019

11.7.1. DSS01 – upravljanje operacijama: primjenjuje se na nadzor tehnoloških operacija, uključujući fizičke uređaje

11.7.2. DSS05 – upravljanje sigurnosnim uslugama: osigurava da se povezani sustavi pravilno nadziru i štite

11.7.3. APO13 – upravljanje sigurnošću: jača politike za zaštitu operativne imovine u SME organizacijama