					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P35					Názov dokumentu: **Politika bezpečnosti IoT / OT**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8	
ISO/IEC 27002:2022	Kontroly 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	
Nariadenie EÚ GDPR	Články 5, 25, 32	
Smernica EÚ NIS2	Články 21, 23	
Nariadenie EÚ DORA	Články 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13	

1. Účel

1.1 Táto politika stanovuje záväzné požiadavky informačnej bezpečnosti na nasadenie, prevádzku, monitorovanie a vyradenie systémov internetu vecí (IoT) a systémov prevádzkových technológií (OT) v organizácii.

1.2 Zabezpečuje, aby tieto systémy boli integrované do širšieho systému riadenia kybernetickej bezpečnosti organizácie a chránené pred kompromitáciou, zneužitím alebo narušením prevádzky.

1.3 Cieľom politiky je uplatňovať silné technické, organizačné a procesné kontroly na ochranu systémov IoT/OT, ktoré sú prepojené s fyzickou infraštruktúrou, výrobnými procesmi a bezpečnostne kritickými prostrediami.

1.4 Podporuje plnenie zákonných a zmluvných povinností v oblastiach kybernetickej bezpečnosti, bezpečnosti, kontroly prostredia a kontinuity činností.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky systémy IoT a OT používané v prevádzkových, administratívnych alebo výrobných prostrediach organizácie bez ohľadu na to, či sú vo vlastníctve spoločnosti, prenajaté alebo poskytnuté treťou stranou.

2.2 Medzi zahrnuté systémy patria okrem iného:

2.2.1 zariadenia IoT, ako sú senzory prostredia, systémy riadenia prístupu, inteligentné osvetlenie, sledovacie zariadenia a nositeľné zariadenia

2.2.2 platformy OT, ako sú PLC, SCADA, DCS, operátorské panely HMI, rozhrania systémov riadenia výroby (MES) a poľné riadiace jednotky

2.2.3 priemyselné riadiace siete alebo aktíva pripojené ku cloudu monitorujúce fyzické operácie

2.3 Politika sa vzťahuje na:

2.3.1 všetky prostredia (v priestoroch organizácie, na okraji siete, spravované v cloude)

2.3.2 všetky zainteresované strany (interní používatelia, integrátori, dodávatelia tretích strán, zmluvní dodávatelia)

2.3.3 všetky fázy životného cyklu (návrh, obstarávanie, nasadenie, prevádzka, vyradenie)

3. Ciele

3.1 Zabezpečiť infraštruktúru IoT a OT pred internými a externými kybernetickými hrozbami vrátane útokov odmietnutia služby, neoprávneného prístupu, šírenia ransomvéru a manipulácie s firmvérom.

3.2 Zabezpečiť, aby sa platformy IoT/OT nestali vektorom útoku prostredníctvom premostenia medzi IT a OT ani neohrozili bezpečnostne kritické systémy.

3.3 Uplatňovať princípy bezpečnosti už od návrhu a obrany do hĺbky počas celého životného cyklu týchto technológií.

3.4 Umožniť spoľahlivú, bezpečnú a overiteľnú integráciu platforiem IoT a OT do centra bezpečnostných operácií (SOC) organizácie a do plánov reakcie na incidenty.

3.5 Zabezpečiť, aby všetky nasadenia boli v súlade s kontrolami ISO/IEC 27001 a príslušnými sektorovými usmerneniami (napr. IEC 62443, ISO 27019, NIST SP 800-82).

4. Roly a zodpovednosti

4.1 riaditeľ informačnej bezpečnosti (CISO) / vedúci bezpečnosti

4.1.1 Definuje politiky a technické štandardy kybernetickej bezpečnosti pre IoT/OT.

4.1.2 Vykonáva dohľad nad posúdeniami rizík, validáciou kontrol a medziodborovou koordináciou.

4.2 OT inžinieri / manažéri správy budov / riaditelia závodov

4.2.1 Validujú konfigurácie systémov OT a zabezpečujú dodržiavanie tejto politiky vo výrobných priestoroch.

4.2.2 Udržiavajú fyzické a logické bezpečnostné opatrenia na zachovanie integrity a bezpečnosti prostredí OT.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1 Táto politika musí byť preskúmaná najmenej raz ročne a aktualizovaná na základe:

9.1.1 zmien architektúry systémov OT alebo IoT, dodávateľov alebo platforiem

9.1.2 významných regulačných aktualizácií (napr. revízie DORA, NIS2, sektorových smerníc)

9.1.3 výskytu nových zraniteľností alebo vzorcov hrozieb v riadiacich systémoch

9.1.4 zistení z interných alebo externých auditov, penetračných testov alebo cvičení red teamu

9.2 CISO, vedúci bezpečnosti OT a príslušní vedúci oddelení spoločne zodpovedajú za iniciovanie procesu preskúmania.

9.3 Mimoriadne preskúmania musia byť vykonané po:

9.3.1 akomkoľvek incidente súvisiacom s IoT/OT, ktorý viedol k zlyhaniu systému alebo strate údajov

9.3.2 zavedení významného nového zariadenia, monitorovacieho softvéru alebo platformy firmvéru

9.3.3 integrácii inteligentného edge computingu alebo automatizácie rozšírenej o AI na úrovni poľa

9.4 Všetky zmeny politík musia byť:

9.4.1 zdokumentované v histórii verzií a registri zmien politík

9.4.2 oznámené všetkým dotknutým používateľom, dodávateľom a operátorom IT/OT

9.4.3 opätovne schválené výkonným manažmentom

10. Súvisiace politiky a väzby

10.1 Táto politika sa uplatňuje spolu s nasledujúcimi politikami informačnej bezpečnosti a je nimi podporovaná:

10.1.1 P1 – Politika informačnej bezpečnosti: stanovuje základné princípy bezpečnosti, ktoré sa vzťahujú aj na bezpečnosť systémov IoT a OT.

10.1.2 P3 – Politika prijateľného používania: definuje obmedzenia týkajúce sa osobného a neoprávneného používania zariadení vrátane prevádzkových prostredí.

10.1.3 P6 – Politika riadenia rizík: usmerňuje posudzovanie, akceptáciu a zmierňovanie rizík súvisiacich s vloženými a riadiacimi systémami.

10.1.4 P12 – Politika správy aktív: zabezpečuje, aby všetky systémy IoT a OT boli formálne evidované v inventári a mali priradených zodpovedných vlastníkov.

10.1.5 P20 – Politika ochrany koncových bodov / ochrany pred malvérom: vzťahuje sa na pripojené riadiace jednotky, inteligentné brány a okrajové systémy vo výrobe.

10.1.6 P22 – Politika logovania a monitorovania: vzťahuje sa aj na postupy zachytávania a preskúmania logov v prostrediach OT.

10.1.7 P30 – Politika reakcie na incidenty: priamo upravuje, ako sa musia eskalovať a riadiť porušenia, anomálie alebo zlyhania systémov IoT/OT.

10.1.8 P33 – Politika monitorovania auditu a súladu: poskytuje mechanizmy uistenia na validáciu priebežného súladu s touto politikou.

11. Referenčné normy a rámce

11.1 Táto politika je zosúladená s medzinárodne uznávanými normami a regulačnými rámcami, ktoré zabezpečujú bezpečnosť, odolnosť a súlad systémov internetu vecí (IoT) a systémov prevádzkových technológií (OT) v priemyselných, výrobných a podnikových prostrediach.

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

11.2.1 Kontrola 5.7 – Spravodajstvo o hrozbách: podporuje monitorovanie prostredí OT a identifikáciu zraniteľností špecifických pre IoT.

11.2.2 Kontrola 5.23 – Informačná bezpečnosť pri používaní cloudových služieb: uplatňuje sa, keď sú zariadenia IoT prepojené s cloudovými platformami na telemetriu, riadenie alebo analytiku.

11.2.3 Kontrola 5.27 – Bezpečná architektúra systémov a princípy inžinierstva: upravuje princípy bezpečnosti už od návrhu pre vstavané systémy a riadiace siete.

11.2.4 Kontrola 5.31 – Bezpečnosť v procesoch vývoja a podpory: vyžaduje validáciu softvéru/firmvéru, kontrolu záplat a požiadavky na dodávateľov pri nasadeniach OT.

11.2.5 Kontrola 5.36 – Súlad so zákonnými a zmluvnými požiadavkami: zabezpečuje súlad aktív OT s požiadavkami na bezpečnosť, ochranu životného prostredia a regulačnými požiadavkami.

11.2.6 Tieto kontroly spoločne stanovujú osvedčené postupy na zabezpečenie systémov IoT/OT počas celého ich životného cyklu vrátane návrhu architektúry, bezpečného nasadenia, záplatovania, detekcie anomálií a súladu so sektorovými požiadavkami.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Ochrana hraníc: zabezpečuje, aby siete OT boli segmentované a chránené pred neoprávneným prístupom.

11.3.2 SI-4 – Monitorovanie systémov: vyžaduje zavedenie mechanizmov nepretržitého monitorovania a detekcie anomálií v prostrediach ICS.

11.3.3 CM-2 – Referenčná konfigurácia: vyžaduje riadenie konfigurácie a hardening zariadení a platforiem IoT/OT.

11.3.4 AC-6 – Zásada minimálnych oprávnení: vzťahuje sa na používateľské prístupy a vzdialený servis vstavaných riadiacich systémov dodávateľom.

11.3.5 PL-8 – Architektúra bezpečnosti a ochrany súkromia: upravuje plánovanie bezpečnej integrácie systémov, najmä pri projektoch modernizácie OT.

11.4 Nariadenie EÚ GDPR (2016/679)

11.4.1 Článok 5 – Zásady spracúvania osobných údajov: uplatňuje sa na platformy IoT spracúvajúce údaje zo senzorov alebo behaviorálne údaje viazané na jednotlivcov.

11.4.2 Článok 25 – Ochrana údajov už v štádiu návrhu a štandardná ochrana údajov: vyžaduje zavedenie opatrení na ochranu súkromia v návrhu produktov IoT a firmvéru.

11.4.3 Článok 32 – Bezpečnosť spracúvania: vyžaduje šifrovanie, riadenie prístupu a bezpečnú komunikáciu pri prenose údajov z inteligentných zariadení.

11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Články 21 a 23: ukladajú bezpečnostné povinnosti základným a dôležitým subjektom používajúcim systémy OT. Zahŕňajú posúdenie rizík, nahlasovanie incidentov a validáciu dodávateľského reťazca dodávateľov IoT/OT a integrity firmvéru.

11.6 Nariadenie EÚ DORA (2022/2554)

11.6.1 Článok 9 – Riadenie rizík IKT: vyžaduje bezpečnú integráciu vstavaných systémov a technológií OT do programu správy a riadenia rizík IKT.

11.6.2 Článok 10 – Požiadavky na bezpečnosť IKT: vyžaduje ochranné opatrenia pre prepojené platformy OT používané vo finančnom sektore a v prostrediach kritických služieb.

11.7 COBIT 2019

11.7.1 DSS05.01 – Ochrana pred malvérom: zahŕňa detekciu a reakciu na hrozby špecifické pre ICS a kampane malvéru zamerané na IoT.

11.7.2 BAI09.01 – Stanovenie a udržiavanie bezpečnostných požiadaviek: nadväzuje na bezpečné zriaďovanie a prevádzku inteligentnej alebo vstavanej infraštruktúry.

11.7.3 APO13.02 – Stanovenie a udržiavanie plánu informačnej bezpečnosti: vyžaduje zahrnutie systémov OT a ich zraniteľností do celoorganizačnej stratégie kybernetickej bezpečnosti.