					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P35					Název dokumentu: **Politika zabezpečení IoT / OT**							
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Standard		Postup		Formulář		Registr		Jiné	

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu se standardy a právními předpisy

Standard/právní předpis	Kapitola/článek	Komentář
ISO/IEC 27001:2022	Kapitola 8	
ISO/IEC 27002:2022	Opatření 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	Články 5, 25, 32	
směrnice NIS2	Články 21, 23	
nařízení DORA	Články 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Účel

1.1 Tato politika stanoví závazné požadavky na informační bezpečnost při nasazení, provozu, monitorování a vyřazování systémů internetu věcí (IoT) a provozních technologií (OT) v organizaci.

1.2 Zajišťuje, aby tyto systémy byly začleněny do širšího systému řízení kybernetické bezpečnosti organizace a chráněny před kompromitací, zneužitím nebo provozní sabotáží.

1.3 Cílem této politiky je prosazovat účinná technická, organizační a procesní opatření na ochranu systémů IoT/OT propojených s fyzickou infrastrukturou, výrobními procesy a bezpečnostně kritickými prostředími.

1.4 Podporuje plnění regulatorních a smluvních povinností v oblasti kybernetické bezpečnosti, bezpečnosti, environmentálního řízení a kontinuity činností.

2. Rozsah

2.1 Tato politika se vztahuje na všechny systémy IoT a OT, ať již vlastněné organizací, pronajaté nebo poskytované třetí stranou, které jsou používány v provozních, administrativních nebo výrobních prostředích organizace.

2.2 Mezi zahrnuté systémy patří mimo jiné:

2.2.1 zařízení IoT, jako jsou environmentální senzory, systémy řízení přístupu, inteligentní osvětlení, sledovací zařízení a nositelná zařízení

2.2.2 platformy OT, jako jsou PLC, systémy SCADA, DCS, panely HMI, rozhraní systémů MES a polní řídicí jednotky

2.2.3 průmyslové řídicí sítě nebo aktiva připojená ke cloudovým službám, která monitorují fyzický provoz

2.3 Tato politika se vztahuje na:

2.3.1 všechna prostředí (on-premise, edge, spravovaná z cloudu)

2.3.2 všechny zainteresované strany (interní uživatelé, systémoví integrátoři, dodavatelé třetích stran, smluvní pracovníci)

2.3.3 všechny fáze životního cyklu (návrh, pořízení, nasazení, provoz, vyřazení z provozu)

3. Cíle

3.1 Zabezpečit infrastrukturu IoT a OT proti interním i externím kybernetickým hrozbám, včetně útoků typu denial-of-service, neoprávněného přístupu, šíření ransomwaru a manipulace s firmwarem.

3.2 Zajistit, aby se platformy IoT/OT nestaly vektorem útoku prostřednictvím propojení mezi IT a OT ani neohrozily bezpečnostně kritické systémy.

3.3 Uplatňovat principy security by design a vícevrstvé ochrany v celém životním cyklu těchto technologií.

3.4 Umožnit spolehlivou, bezpečnou a auditovatelnou integraci platforem IoT a OT do bezpečnostního dohledového centra (SOC) organizace a do plánů reakce na incidenty.

3.5 Zajistit, aby všechna nasazení byla v souladu s opatřeními ISO/IEC 27001 a příslušnými oborovými doporučeními (např. IEC 62443, ISO 27019, NIST SP 800-82).

4. Role a odpovědnosti

4.1 ředitel informační bezpečnosti (CISO) / vedoucí bezpečnosti

4.1.1 definuje politiky a technické standardy pro kybernetickou bezpečnost IoT/OT

4.1.2 dohlíží na hodnocení rizik, ověřování kontrol a meziútvarovou koordinaci

4.2 inženýři provozních technologií (OT) / manažeři správy budov a provozu

4.2.1 ověřují konfigurace systémů OT a zajišťují dodržování politiky ve výrobních prostorech

4.2.2 udržují fyzická a logická ochranná opatření pro zajištění integrity a bezpečnosti OT

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Požadavky na přezkoumávání a aktualizaci

9.1 Tato politika musí být přezkoumána nejméně jednou ročně a aktualizována na základě:

9.1.1 změn v architektuře systémů OT nebo IoT, dodavatelích nebo platformách

9.1.2 zásadních regulatorních aktualizací (např. změn nařízení DORA, směrnice NIS2, oborových směrnic)

9.1.3 výskytu nových zranitelností nebo vzorců hrozeb v řídicích systémech

9.1.4 zjištění z interních nebo externích auditů, penetračních testů nebo cvičení red teamu

9.2 CISO, vedoucí bezpečnosti OT a příslušní vedoucí oddělení odpovídají za společné zahájení procesu přezkumu.

9.3 Mimořádné přezkumy musí být zahájeny po:

9.3.1 jakémkoli incidentu souvisejícím s IoT/OT, který vedl k výpadku systému nebo ztrátě dat

9.3.2 zavedení významného nového vybavení, monitorovacího softwaru nebo platforem firmwaru

9.3.3 integraci inteligentních edge computing řešení nebo automatizace rozšířené o AI na úrovni provozu

9.4 Všechny změny politiky musí být:

9.4.1 zdokumentovány v historii verzí a registru změn politik

9.4.2 oznámeny všem dotčeným uživatelům, dodavatelům a operátorům IT/OT

9.4.3 znovu schváleny výkonným vedením

10. Související politiky a vazby

10.1 Tato politika se uplatňuje společně s následujícími politikami informační bezpečnosti a je jimi podporována:

10.1.1 P1 – Politika informační bezpečnosti: Stanoví základní bezpečnostní principy, které se vztahují i na zabezpečení systémů IoT a OT.

10.1.2 P3 – Zásady přípustného užívání: Vymezují omezení týkající se používání osobních a neoprávněných zařízení, včetně provozních prostředí.

10.1.3 P6 – Politika řízení rizik: Upravuje posuzování, akceptaci a zmírňování rizik souvisejících s vestavěnými a řídicími systémy.

10.1.4 P12 – Politika správy aktiv: Zajišťuje, aby všechny systémy IoT a OT byly formálně evidovány a měly přidělené odpovědné vlastníky.

10.1.5 P20 – Politika ochrany koncových bodů / malwaru: Vztahuje se na připojené řídicí jednotky, inteligentní brány a edge systémy ve výrobě.

10.1.6 P22 – Politika protokolování a monitorování: Rozšiřuje se na postupy sběru logů a jejich přezkumu v prostředích OT.

10.1.7 P30 – Politika reakce na incidenty: Přímo upravuje, jak musí být porušení, anomálie nebo selhání systémů IoT/OT eskalována a řízena.

10.1.8 P33 – Politika monitorování auditu a souladu: Poskytuje mechanismy zajištění k ověření průběžného souladu s touto politikou.

11. Referenční standardy a rámce

11.1 Tato politika je v souladu s mezinárodně uznávanými standardy a regulatorními rámci, které zajišťují bezpečnost, odolnost a soulad systémů internetu věcí (IoT) a provozních technologií (OT) v průmyslových, výrobních a podnikových prostředích.

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

11.2.1 Opatření 5.7 – Threat Intelligence: Podporuje monitorování prostředí OT a identifikaci zranitelností specifických pro IoT.

11.2.2 Opatření 5.23 – Bezpečnost informací při využívání cloudových služeb: Uplatňuje se v případech, kdy zařízení IoT komunikují s cloudovými platformami za účelem telemetrie, řízení nebo analytiky.

11.2.3 Opatření 5.27 – Principy bezpečné architektury a inženýrství systémů: Řídí uplatňování principů security by design u vestavěných systémů a řídicích sítí.

11.2.4 Opatření 5.31 – Bezpečnost ve vývojových a podpůrných procesech: Prosazuje validaci softwaru/firmwaru, řízení záplat a požadavky na dodavatele v nasazeních OT.

11.2.5 Opatření 5.36 – Soulad s právními a smluvními požadavky: Zajišťuje soulad aktiv OT s požadavky na bezpečnost, ochranu životního prostředí a regulatorními povinnostmi.

11.2.6 Tato opatření společně stanovují osvědčené postupy pro zabezpečení systémů IoT/OT v celém jejich životním cyklu, včetně návrhu architektury, bezpečného nasazení, záplatování, detekce anomálií a souladu s oborovými požadavky.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Ochrana perimetru: Zajišťuje segmentaci sítí OT a jejich ochranu před neoprávněným přístupem.

11.3.2 SI-4 – Monitorování systémů: Vyžaduje zavedení mechanismů průběžného monitorování a detekce anomálií v prostředích ICS.

11.3.3 CM-2 – Výchozí konfigurace: Ukládá řízení konfigurace a hardening zařízení a platforem IoT/OT.

11.3.4 AC-6 – zásada minimálních oprávnění: Uplatňuje se na přístup uživatelů a vzdálený servis vestavěných řídicích systémů dodavatelem.

11.3.5 PL-8 – Architektury bezpečnosti a ochrany soukromí: Řídí plánování bezpečné integrace systémů, zejména u projektů modernizace OT.

11.4 GDPR (2016/679)

11.4.1 Článek 5 – Zásady zpracování osobních údajů: Uplatňuje se na platformy IoT zpracovávající data ze senzorů nebo behaviorální data vztahující se k fyzickým osobám.

11.4.2 Článek 25 – Ochrana osobních údajů již od návrhu a ve výchozím nastavení: Vyžaduje začlenění ochranných opatření na ochranu soukromí do návrhu produktů IoT a firmwaru.

11.4.3 Článek 32 – Zabezpečení zpracování: Vyžaduje šifrování, řízení přístupu a bezpečnou komunikaci při přenosu dat inteligentních zařízení.

11.5 směrnice NIS2 (2022/2555)

11.5.1 Články 21 a 23: Ukládají bezpečnostní povinnosti základním a důležitým subjektům využívajícím systémy OT. Ty zahrnují hodnocení rizik, hlášení incidentů a ověřování dodavatelského řetězce dodavatelů IoT/OT i integrity firmwaru.

11.6 nařízení DORA (2022/2554)

11.6.1 Článek 9 – Řízení rizik v oblasti ICT: Vyžaduje bezpečnou integraci vestavěných systémů a technologií OT do programu správy a řízení ICT rizik.

11.6.2 Článek 10 – Požadavky na bezpečnost ICT: Ukládá ochranná opatření pro propojené platformy OT používané ve finančních a kritických službách.

11.7 COBIT 2019

11.7.1 DSS05.01 – Ochrana proti malwaru: Zahrnuje detekci a reakci na hrozby specifické pro ICS a kampaně malwaru zaměřené na IoT.

11.7.2 BAI09.01 – Stanovení a udržování bezpečnostních požadavků: Mapuje se na bezpečné zřizování a provoz inteligentní nebo vestavěné infrastruktury.

11.7.3 APO13.02 – Stanovení a udržování plánu bezpečnosti informací: Vyžaduje zahrnutí systémů OT a jejich zranitelností do celopodnikové strategie kybernetické bezpečnosti.