					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P35S					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 s normami a právními předpisy

Norma / právní předpis	Kapitola / článek	Komentář
ISO/IEC 27001:2022	Kapitoly 6.1, 6.2, 8	
ISO/IEC 27002:2022	Opatření 5.23, 5	
GDPR / obecné nařízení o ochraně osobních údajů	Článek 32	
směrnice NIS2	Článek 21 odst. 2 písm. a), d), f)	
nařízení DORA	Článek 9 odst. 2, 10 odst. 1	

1. Účel

1.1. Tato politika stanoví závazná pravidla pro bezpečné používání a správu zařízení internetu věcí (IoT) a systémů provozních technologií (OT) v organizaci. Tato zařízení mohou zahrnovat chytré senzory, bezpečnostní kamery, výrobní stroje, řídicí jednotky HVAC nebo jakékoli průmyslové systémy připojené k síti.

1.2. Účelem této politiky je:

1.2.1. chránit fyzický i digitální provoz před narušením nebo manipulací prostřednictvím nedostatečně zabezpečených připojených zařízení,

1.2.2. prosazovat bezpečné nasazení, monitorování a údržbu systémů IoT a OT,

1.2.3. zajistit soulad s ISO/IEC 27001:2022, směrnicí NIS2 a souvisejícími regulačními rámci,

1.2.4. stanovit praktická a vymahatelná opatření pro SME působící v kancelářském, skladovém nebo výrobním prostředí.

2. Rozsah

2.1. Tato politika se vztahuje na všechny osoby zapojené do plánování, instalace, konfigurace, používání, podpory nebo likvidace zařízení IoT nebo OT. To zahrnuje:

2.1.1. zaměstnance, smluvní pracovníky nebo stážisty s fyzickým nebo vzdáleným přístupem k zařízením,

2.1.2. dodavatele třetích stran nebo servisní techniky provádějící instalaci nebo údržbu připojených systémů,

2.1.3. generálního ředitele nebo pracovníky odpovědné za dohled nad bezpečnostními politikami.

2.2. Politika se vztahuje na:

2.2.1. zařízení IoT, jako jsou chytré zámky, sledovací systémy, chytré měřiče nebo tiskárny,

2.2.2. systémy provozních technologií (OT), včetně PLC (programmable logic controllers), panelů SCADA nebo průmyslových bran,

2.2.3. podpůrný hardware, aplikace pro správu a komunikační sítě používané těmito systémy.

2.3. Tato politika se uplatňuje na všech pracovištích: v kancelářském prostředí, na vzdálených lokalitách, ve výrobních provozech a na cloudových platformách propojených s těmito zařízeními.

3. Cíle

3.1. Bezpečné nasazení: zajistit, aby všechny systémy IoT/OT byly před zavedením do provozního prostředí bezpečně nakonfigurovány.

3.2. Omezení expozice: předcházet neoprávněnému přístupu, zneužití nebo převzetí kontroly nad připojenými zařízeními prostřednictvím důsledného řízení přístupu a segmentace sítě.

3.3. Průběžné monitorování: zajistit přehled o provozu IoT/OT prostřednictvím protokolování činností a monitorování neobvyklého chování.

3.4. Odpovědnost dodavatelů: zajistit, aby poskytovatelé třetích stran dodržovali bezpečné postupy instalace, konfigurace a údržby.

3.5. Regulační soulad: doložit soulad s příslušnými normami, jako jsou ISO 27001, GDPR / obecné nařízení o ochraně osobních údajů (pokud jsou shromažďovány osobní údaje) a směrnice NIS2 pro odolnost kritické infrastruktury.

4. Role a odpovědnosti

4.1. Generální ředitel (GM)

4.1.1. nese celkovou odpovědnost za zabezpečení systémů IoT a OT,

4.1.2. schvaluje tuto politiku a zajišťuje její uplatňování ve všech pracovních prostorách,

4.1.3. ověřuje, že dodavatelé a smluvní pracovníci dodržují bezpečné postupy konfigurace a údržby,

4.1.4. schvaluje síťový přístup pro každý systém IoT/OT.

4.2. Určený zaměstnanec nebo provozní manažer (je-li určen)

4.2.1. odpovídá za dohled nad evidencí, umístěním a konfigurací zařízení IoT/OT,

4.2.2. zaznamenává umístění každého zařízení, jeho přiřazení do sítě a související dokumentaci,

4.2.3. zajišťuje, aby všechny změny, například aktualizace firmwaru nebo výměny zařízení, byly zdokumentovány.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1. Roční přezkum

9.1.1. Tato politika musí být nejméně jednou ročně přezkoumána GM.

9.1.2. Přezkum musí posoudit, zda politika zůstává účinná, zda pokrývá aktuální typy zařízení a zda odpovídá novým rizikům nebo technologiím.

9.2. Aktualizace na základě spouštěcích událostí

9.2.1. Aktualizace politiky musí být zahájeny také tehdy, pokud:

9.2.2. jsou zavedeny nové typy systémů IoT nebo OT,

9.2.3. dodavatelé vydají bezpečnostní bulletiny nebo oznámení o ukončení životního cyklu,

9.2.4. incident nebo audit identifikuje mezery v kontrolách IoT/OT,

9.2.5. nové právní předpisy nebo normy uloží další požadavky.

9.3. Dokumentace a správa verzí

9.3.1. Všechny aktualizace musí být zdokumentovány, včetně data, čísla verze a souhrnu změn.

9.3.2. GM musí uchovávat historické verze politiky pro účely auditu.

9.4. Komunikace změn

9.4.1. Jakékoli aktualizace politiky musí být sdíleny se všemi relevantními pracovníky a dodavateli.

9.4.2. Aktualizované verze musí být zpřístupněny prostřednictvím sdílených složek nebo tištěných materiálů v místech instalace nebo řídicích centrech.

10. Související politiky a vazby

10.1. Tato politika musí být implementována v souladu s následujícími souvisejícími politikami SME:

10.1.1. P4S – Politika řízení přístupu: uplatňuje řízení přihlášení na úrovni zařízení, používání silných hesel a postupy oprávněného přístupu pro platformy IoT a OT,

10.1.2. P9S – Politika práce na dálku: zabraňuje používání vzdáleného přístupu k řídicím panelům IoT/OT prostřednictvím nezabezpečených nebo neschválených kanálů,

10.1.3. P17S – Politika ochrany dat a soukromí: uplatní se, pokud zařízení IoT (např. bezpečnostní kamery) zpracovávají nebo zaznamenávají osobní údaje, a zajišťuje soulad s GDPR,

10.1.4. P30S – Politika reakce na incidenty: stanoví postupy pro detekci, hlášení a řešení incidentů IoT nebo OT, včetně podezření na manipulaci nebo provozní selhání,

10.1.5. P36S – Politika sociálních médií a externí komunikace: zajišťuje, aby žádné informace o zařízeních ani topologii sítě nebyly externě sdíleny bez schválení.

10.2. Každá související politika posiluje uplatňování a praktické používání této politiky tím, že poskytuje cílené procesní pokyny.

11. Referenční normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 6.1 – Identifikace a ošetření rizik: vyžaduje, aby byla rizika související se systémy IoT a OT systematicky hodnocena a zmírňována.

11.1.2. Kapitola 8.1 – Provozní plánování a řízení: zajišťuje bezpečné provozní řízení připojených zařízení.

11.2. ISO/IEC 27002

11.2.1. Opatření 5.23 – Bezpečnost informací při používání provozních technologií: vymezuje bezpečné používání OT ve fyzickém i digitálním prostředí.

11.2.2. Opatření 5.31 – Bezpečná konfigurace informačních systémů: vyžaduje hardening zařízení IoT/OT a vyloučení nezabezpečených výchozích nastavení.

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – Integrita softwaru, firmwaru a informací: vyžaduje ověření integrity firmwaru a aktualizací.

11.3.2. CM-7 – princip nejmenší funkčnosti: zařízení nesmí mít povoleny nevyužívané nebo nezabezpečené funkce.

11.3.3. AC-6 – zásada minimálních oprávnění: přístup k zařízením musí být omezen pouze na oprávněné uživatele.

11.3.4. PE-20 – monitorování aktiv: fyzické a provozní monitorování aktiv IoT a OT.

11.3.5. SC-7 – Ochrana perimetru: segmentace a řízení síťové komunikace připojených systémů.

11.4. GDPR / obecné nařízení o ochraně osobních údajů (2016/679)

11.4.1. Článek 32 – Zabezpečení zpracování: pokud jsou zpracovávány osobní údaje (např. prostřednictvím sledovacích kamer), musí organizace zavést odpovídající technická a organizační opatření (TOM) k zabezpečení takového zpracování.

11.5. směrnice NIS2 (2022/2555)

11.5.1. Článek 21 odst. 2 písm. a) – opatření řízení rizik.

11.5.2. Článek 21 odst. 2 písm. d) – bezpečná konfigurace a používání zařízení.

11.5.3. Článek 21 odst. 2 písm. f) – bezpečnost dodavatelského řetězce a systémů.

11.6. nařízení DORA (2022/2554)

11.6.1. Článek 9 odst. 2 – rozsah řízení rizik v oblasti ICT: zahrnuje průmyslová a vestavěná zařízení používaná v provozním prostředí.

11.6.2. Článek 10 odst. 1 – kontinuita ICT: vyžaduje, aby konfigurace zařízení podporovaly odolnost a činnosti obnovy.

11.7. COBIT 2019

11.7.1. DSS01 – řízení provozu: vztahuje se na dohled nad technologickým provozem, včetně fyzických zařízení.

11.7.2. DSS05 – řízení bezpečnostních služeb: zajišťuje, aby připojené systémy byly řádně monitorovány a chráněny.

11.7.3. APO13 – řízení bezpečnosti: posiluje politiky pro ochranu provozních aktiv v prostředí SME.