| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem zadajte názov registrovanej právnickej osoby | | | | | | | |
| Číslo dokumentu:<br>P35S | | | | | Názov dokumentu:<br>**Politika bezpečnosti IoT / OT** | | | | | | | |
| Verzia:<br>1.0 | | Dátum nadobudnutia účinnosti:<br>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 | Kapitoly 6.1, 6.2, 8 | |
| ISO/IEC 27002:2022 | Kontroly 5.23, 5.31 | |
| NIST SP 800-53 Rev.5 | SI-7, CM-7, AC-6, PE-20, SC-7 | |
| Nariadenie EÚ GDPR | Článok 32 | |
| Smernica EÚ NIS2 | Článok 21(2)(a), (d), (f) | |
| Nariadenie EÚ DORA | Článok 9(2), 10(1) | |

**1. Účel**

1.1. Táto politika stanovuje záväzné pravidlá pre bezpečné používanie a správu zariadení internetu vecí (IoT) a systémov prevádzkových technológií (OT) v rámci organizácie. Tieto zariadenia môžu zahŕňať inteligentné snímače, bezpečnostné kamery, výrobné stroje, riadiace jednotky HVAC alebo akékoľvek priemyselné systémy pripojené k sieti.

**1.2. Účelom tejto politiky je:**

1.2.1. chrániť fyzickú aj digitálnu prevádzku pred prerušením alebo manipuláciou prostredníctvom nedostatočne zabezpečených pripojených zariadení,

1.2.2. zabezpečiť bezpečné nasadenie, monitorovanie a údržbu systémov IoT a OT,

1.2.3. zabezpečiť súlad s ISO/IEC 27001:2022, smernicou EÚ NIS2 a súvisiacimi regulačnými rámcami,

1.2.4. poskytovať praktické a vynútiteľné bezpečnostné opatrenia pre MSP pôsobiace v kancelárskom, skladovom alebo výrobnom prostredí.

**2. Rozsah**

**2.1. Táto politika sa vzťahuje na všetky osoby zapojené do plánovania, inštalácie, konfigurácie, používania, podpory alebo vyradenia zariadení IoT alebo OT. Zahŕňa najmä:**

2.1.1. zamestnancov, zmluvných pracovníkov alebo stážistov s fyzickým alebo vzdialeným prístupom k zariadeniam,

2.1.2. dodávateľov tretích strán alebo servisných technikov, ktorí inštalujú alebo udržiavajú pripojené systémy,

2.1.3. generálneho manažéra (GM) alebo pracovníkov zodpovedných za dohľad nad bezpečnostnými politikami.

**2.2. Politika sa vzťahuje na:**

2.2.1. zariadenia IoT, ako sú inteligentné zámky, kamerové systémy, inteligentné merače alebo tlačiarne,

2.2.2. systémy OT vrátane programovateľných logických automatov (PLC), panelov SCADA alebo priemyselných brán,

2.2.3. podporný hardvér, aplikácie na správu a komunikačné siete používané týmito systémami.

2.3. Táto politika sa uplatňuje na všetkých pracoviskách vrátane kancelárskych priestorov, vzdialených lokalít, výrobných prevádzok a cloudových platforiem prepojených s týmito zariadeniami.

**3. Ciele**

3.1. Bezpečné nasadenie: zabezpečiť, aby boli všetky systémy IoT/OT bezpečne nakonfigurované pred ich zavedením do prevádzkového prostredia.

3.2. Obmedzenie vystavenia riziku: predchádzať neoprávnenému prístupu, zneužitiu alebo prevzatiu kontroly nad pripojenými zariadeniami prostredníctvom dôsledného riadenia prístupu a segmentácie siete.

3.3. Nepretržité monitorovanie: udržiavať prehľad o prevádzke prostredia IoT/OT prostredníctvom protokolovania aktivít a monitorovania neobvyklého správania.

3.4. Zodpovednosť dodávateľov: zabezpečiť, aby externí poskytovatelia dodržiavali bezpečné postupy inštalácie, konfigurácie a údržby.

3.5. Súlad s požiadavkami: preukázať úplný súlad s uplatniteľnými normami, ako sú ISO 27001, GDPR (ak sa spracúvajú osobné údaje) a smernica EÚ NIS2 v oblasti odolnosti kritickej infraštruktúry.

## 4. Roly a zodpovednosti

### 4.1. Generálny manažér (GM)

4.1.1. nesie celkovú zodpovednosť za bezpečnosť systémov IoT a OT,

4.1.2. schvaľuje túto politiku a zabezpečuje jej uplatňovanie vo všetkých pracovných priestoroch,

4.1.3. overuje, že dodávatelia a zmluvní pracovníci dodržiavajú bezpečné postupy inštalácie a údržby,

4.1.4. schvaľuje sieťový prístup pre každý systém IoT/OT.

### 4.2. Určený zamestnanec alebo prevádzkový manažér (ak je určený)

4.2.1. vykonáva dohľad nad evidenciou, umiestnením a konfiguráciou zariadení IoT/OT,

4.2.2. zaznamenáva umiestnenie každého zariadenia, jeho sieťové priradenie a podpornú dokumentáciu,

4.2.3. zabezpečuje zdokumentovanie každej zmeny, napríklad aktualizácie firmvéru alebo výmeny zariadenia.

[ ... 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. Ročné preskúmanie

9.1.1. Túto politiku musí GM preskúmať najmenej raz ročne.

9.1.2. Preskúmanie musí posúdiť, či politika zostáva účinná, pokrýva aktuálne typy zariadení a je zosúladená s novými rizikami alebo technológiami.

### 9.2. Aktualizácie na základe spúšťacích udalostí

9.2.1. Aktualizácie politiky sa musia iniciovať aj vtedy, keď:

9.2.2. sa zavedú nové typy systémov IoT alebo OT,

9.2.3. dodávatelia vydajú bezpečnostné upozornenia alebo oznámenia o ukončení podpory,

9.2.4. incident alebo audit identifikuje medzery v kontrolách IoT/OT,

9.2.5. nové právne predpisy alebo normy zavedú ďalšie požiadavky.

### 9.3. Dokumentácia a riadenie verzií

9.3.1. Všetky aktualizácie musia byť zdokumentované vrátane dátumu, čísla verzie a súhrnu zmien.

9.3.2. GM musí uchovávať historické verzie politiky na účely auditu.

### 9.4. Komunikácia zmien

9.4.1. Každá aktualizácia politiky musí byť oznámená všetkým relevantným zamestnancom a dodávateľom.

9.4.2. Aktualizované verzie musia byť sprístupnené prostredníctvom zdieľaných priečinkov alebo tlačených materiálov v miestach inštalácie alebo v riadiacich centrách.

## 10. Súvisiace politiky a väzby

### 10.1. Táto politika sa musí uplatňovať v súlade s nasledujúcimi súvisiacimi politikami MSP:

10.1.1. P4S – Politika riadenia prístupu: uplatňuje kontroly prihlasovania na úrovni zariadení, používanie silných hesiel a postupy autorizovaného prístupu pre platformy IoT a OT,

10.1.2. P9S – Politika práce na diaľku: zabraňuje používaniu vzdialeného prístupu k panelom IoT/OT prostredníctvom nezabezpečených alebo neschválených kanálov,

10.1.3. P17S – Politika ochrany údajov a súkromia: uplatňuje sa, ak zariadenia IoT, napríklad bezpečnostné kamery, spracúvajú alebo zaznamenávajú osobné údaje, a zabezpečuje súlad s GDPR,

10.1.4. P30S – Politika reakcie na incidenty: definuje postupy na detekciu, nahlasovanie a riešenie incidentov IoT alebo OT vrátane podozrenia na manipuláciu alebo prevádzkové zlyhanie,

10.1.5. P36S – Politika sociálnych médií a externej komunikácie: zabezpečuje, aby sa informácie o zariadeniach alebo topológii siete nezdieľali externe bez schválenia.

10.2. Každá súvisiaca politika posilňuje uplatňovanie a praktické používanie tejto politiky tým, že poskytuje cielené procedurálne usmernenia.

## 11. Referenčné normy a rámce

### 11.1. ISO/IEC 27001

11.1.1. Kapitola 6.1 – identifikácia rizík a ošetrenie rizík: vyžaduje, aby boli riziká súvisiace so systémami IoT a OT systematicky posudzované a zmierňované.

11.1.2. Kapitola 8.1 – prevádzkové plánovanie a riadenie: zabezpečuje bezpečné prevádzkové riadenie pripojených zariadení.

### 11.2. ISO/IEC 27002

11.2.1. Kontrola 5.23 – informačná bezpečnosť pri používaní systémov prevádzkových technológií (OT): definuje bezpečné používanie OT vo fyzickom aj digitálnom prostredí.

11.2.2. Kontrola 5.31 – bezpečná konfigurácia informačných systémov: vyžaduje hardening zariadení IoT/OT a predchádzanie nezabezpečeným predvoleným nastaveniam.

### 11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – integrita softvéru, firmvéru a informácií: vyžaduje overovanie integrity firmvéru a aktualizácií.

11.3.2. CM-7 – zásada minimálnej funkčnosti: zariadenia nesmú mať povolené nevyužívané alebo nezabezpečené funkcie.

11.3.3. AC-6 – zásada minimálnych oprávnení: prístup k zariadeniam musí byť obmedzený iba na autorizovaných používateľov.

11.3.4. PE-20 – monitorovanie aktív: fyzické a prevádzkové monitorovanie aktív IoT a OT.

11.3.5. SC-7 – ochrana hraníc: segmentácia a riadenie sieťovej komunikácie pre pripojené systémy.

### 11.4. Nariadenie EÚ GDPR (2016/679)

11.4.1. Článok 32 – bezpečnosť spracúvania: ak sa zachytávajú osobné údaje, napríklad prostredníctvom bezpečnostných kamier, organizácia musí zaviesť primerané technické a organizačné opatrenia (TOM) na zabezpečenie takéhoto spracúvania.

### 11.5. Smernica EÚ NIS2 (2022/2555)

11.5.1. Článok 21(2)(a) – opatrenia riadenia rizík,

11.5.2. Článok 21(2)(d) – bezpečná konfigurácia a používanie zariadení,

11.5.3. Článok 21(2)(f) – bezpečnosť dodávateľského reťazca a systémov.

**11.6. Nariadenie EÚ DORA (2022/2554)**

11.6.1. Článok 9(2) – rozsah riadenia IKT rizík: zahŕňa priemyselné a vstavané zariadenia používané v prevádzkových prostrediach.

11.6.2. Článok 10(1) – kontinuita IKT: vyžaduje, aby konfigurácie zariadení podporovali odolnosť a činnosti obnovy.

**11.7. COBIT 2019**

11.7.1. DSS01 – riadenie prevádzky: vzťahuje sa na dohľad nad technologickou prevádzkou vrátane fyzických zariadení.

11.7.2. DSS05 – riadenie bezpečnostných služieb: zabezpečuje, aby boli pripojené systémy primerane monitorované a chránené.

11.7.3. APO13 – riadenie bezpečnosti: posilňuje politiky na ochranu prevádzkových aktív v prostredí MSP.