					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P21S					Názov dokumentu: **Politika bezpečnosti sietí**							
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	Kontrola 8	-
NIST SP 800-53 Rev. 5	AC-4, SC-7	-
Nariadenie EÚ GDPR	Článok 32	-
Smernica EÚ NIS2	Články 21(2)(d), (e)	-
Nariadenie EÚ DORA	Články 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Účel

1.1. Účelom tejto politiky je zabezpečiť, aby bola všetka interná a externá sieťová komunikácia chránená pred neoprávneným prístupom, manipuláciou, odpočúvaním a zneužitím prostredníctvom jasne definovaných bezpečnostných kontrol.

1.2. Táto politika stanovuje pravidlá pre bezpečný návrh, používanie a správu sieťovej infraštruktúry vrátane smerovačov, bezdrôtových prístupových bodov, pripojení vzdialeného prístupu a segmentovaných sietí.

1.3. Jej cieľom je minimalizovať vystavenie hrozbám z internetu, zabezpečiť dôvernosť údajov prenášaných cez interné a externé siete a zachovať dostupnosť kritických služieb.

1.4. Táto politika podporuje certifikáciu podľa ISO/IEC 27001:2022 a priamo prispieva k plneniu zákonných a regulačných povinností podľa GDPR, NIS2 a DORA, pričom poskytuje technické uistenie zákazníkom a audítorom.

2. Rozsah

2.1. Táto politika sa vzťahuje na všetky súčasti IT siete organizácie vrátane:

2.1.1. káblovej a bezdrôtovej infraštruktúry na pracoviskách,

2.1.2. smerovačov, prepínačov, prístupových bodov, firewallov a brán,

2.1.3. pripojení vzdialeného prístupu vrátane VPN, RDP a cloudových tunelov,

2.1.4. aplikácií v cloudovom prostredí prístupných z interných alebo externých sietí,

2.1.5. zariadení pripojených do siete zamestnancami, zmluvnými dodávateľmi alebo hosťami.

2.2. Táto politika upravuje fyzické aj logické segmenty siete vrátane hosťovských zón, zariadení IoT a back-office systémov.

2.3. Politika sa vzťahuje na všetky osoby s prístupom do siete organizácie vrátane:

2.3.1. interných zamestnancov,

2.3.2. pracovníkov na diaľku a zamestnancov v hybridnom režime,

2.3.3. externých dodávateľov, konzultantov a poskytovateľov služieb,

2.3.4. hostí využívajúcich dočasný prístup k Wi-Fi.

3. Ciele

3.1. Zabezpečiť ochranu siete organizácie pred neoprávneným prístupom a externými kybernetickými hrozbami.

3.2. Uplatňovať primeranú segmentáciu medzi dôveryhodnými a nedôveryhodnými sieťami (napr. hosťovská Wi-Fi, prístup dodávateľov).

3.3. Umožniť bezpečné vzdialené pripojenie bez ohrozenia interných systémov.

3.4. Predchádzať šíreniu malvéru a exfiltrácii údajov prostredníctvom sieťových kanálov.

3.5. Zabezpečiť monitorovanie, upozorňovanie a auditovanie sieťovej aktivity na podporu detekcie incidentov a preukazovania súladu.

3.6. Zabezpečiť, aby sa do interných sietí mohli pripájať len schválené a zabezpečené zariadenia.

3.7. Plniť povinnosti podľa ISO 27001, GDPR a súvisiacich rámcov kybernetickej bezpečnosti.

4. Roly a zodpovednosti

4.1. Generálny manažér (GM)

4.1.1. Je vlastníkom tejto politiky a zabezpečuje pridelenie primeraných zdrojov na bezpečný návrh a správu siete.

4.1.2. Preskúmava výnimky z bezpečnostných kontrol siete a schvaľuje dohody o sieťovom prístupe dodávateľov.

4.1.3. Preskúmava incidenty alebo auditné zistenia súvisiace s bezpečnostnými slabinami siete.

4.2. Poskytovateľ IT podpory / interná IT funkcia

4.2.1. Implementuje, konfiguruje a udržiava všetky firewally, smerovače, prepínače a bezdrôtové kontroléry.

4.2.2. Riadi segmentáciu medzi internými, hosťovskými a externými sieťami.

4.2.3. Monitoruje logy a upozornenia na pokusy o neoprávnený prístup alebo sieťové anomálie.

4.2.4. Zabezpečuje bezpečné a včasné uplatňovanie aktualizácií firmvéru a konfigurácie.

[... 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 najmenej raz ročne preskúmať Generálny manažér (GM) spolu s poskytovateľom IT podpory a koordinátorom ochrany údajov.

9.2. Spúšťače priebežného preskúmania

9.2.1. Preskúmanie politiky sa musí vykonať aj pri:

9.2.1.1. významných zmenách architektúry siete (napr. nové systémy VPN alebo firewallov),

9.2.1.2. incidente súvisiacom so sieťou (napr. prienik, šírenie ransomvéru alebo exfiltrácia údajov),

9.2.1.3. právnych, regulačných alebo rámcových zmenách ovplyvňujúcich ochranu siete,

9.2.1.4. nových platformách dodávateľov vyžadujúcich alternatívne metódy alebo protokoly prístupu.

9.3. Riadenie verzií a dokumentácia

9.3.1. Revízie politiky musia byť zaznamenané s číslom verzie, dátumom a súhrnom zmien.

9.3.2. Predchádzajúce verzie sa musia archivovať najmenej 3 roky.

9.3.3. Aktualizácie musia byť oznámené dotknutým zamestnancom; ak sa zavádzajú významné zmeny správania, vyžaduje sa potvrdenie oboznámenia sa s politikou.

10. Súvisiace politiky a väzby

10.1. Táto politika sa musí implementovať spolu s nasledujúcimi bezpečnostnými politikami MSP:

10.1.1. P9S – Politika práce na diaľku: uplatňuje bezpečné metódy vzdialeného prístupu, požiadavky na VPN a ochranu koncových zariadení pre používateľov mimo pracoviska.

10.1.2. P12S – Politika správy aktív: zabezpečuje, aby všetky systémy pripojené do siete boli identifikované, kategorizované a sledované s aktuálnym stavom bezpečnosti.

10.1.3. P17S – Politika ochrany údajov a súkromia: zabezpečuje, aby sieťová segmentácia, riadenie prístupu a logovanie podporovali zásady súkromia a ochrany údajov podľa GDPR.

10.1.4. P22S – Politika logovania a monitorovania: špecifikuje požiadavky na zaznamenávanie a preskúmavanie logov zo sieťových zariadení, vzdialených pripojení a bezdrôtových kontrolérov.

10.1.5. P30S – Politika reakcie na incidenty: definuje požadované kroky pri reakcii na narušenia siete, pokusy o neoprávnený prístup alebo šírenie malvéru cez interné siete.

11. Referenčné normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 8 – Vyžaduje implementáciu kontrol na zabezpečenie bezpečnej a odolnej prevádzky vrátane sietí.

11.2. ISO/IEC 27002

11.2.1. Kontrola 8.20 – Poskytuje technické a procesné usmernenia na zabezpečenie sieťového prístupu, segmentácie a monitorovania.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-4 – Vyžaduje riadenie toku informácií v rámci sietí a medzi systémami.

11.3.2. SC-7 – Vyžaduje ochranu hraníc, bezpečné smerovanie a sieťovú segmentáciu na zníženie rizika neoprávneného prístupu.

11.4. Nariadenie EÚ GDPR

11.4.1. Článok 32 – Vyžaduje primerané technické a organizačné opatrenia na zabezpečenie dôvernosti, integrity a dostupnosti sieťovo prepojených systémov a služieb, ktoré spracúvajú osobné údaje.

11.5. Smernica EÚ NIS2

11.5.1. Článok 21(2)(d) – Vyžaduje technické opatrenia založené na riziku vrátane bezpečnosti sietí a riadenia prístupu.

11.5.2. Článok 21(2)(e) – Vyžaduje segmentáciu a izoláciu systémov na zabránenie šírenia kybernetických incidentov.

11.6. Nariadenie EÚ DORA

11.6.1. Článok 9 – Vyžaduje, aby organizácie zaviedli kontroly riadenia rizík IKT vrátane kontrol bezpečných sietí a komunikácie.

11.6.2. Článok 10 – Vyžaduje, aby stratégie digitálnej odolnosti zahŕňali ochranu sieťovej infraštruktúry a vzdialeného pripojenia.

11.7. COBIT 2019

11.7.1. DSS05.02 – Vyžaduje účinnú ochranu IT infraštruktúry a sieťových prostredí pred internými a externými hrozbami.

11.7.2. APO13.01 – Vyžaduje stratégie riadenia rizík, ktoré zahŕňajú sieťovú segmentáciu a monitorovanie ako súčasť zmierňovania hrozieb.