					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P21					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	N/A
ISO/IEC 27002:2022	Kontroly 8.20-8.22	N/A
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	N/A
Nariadenie EÚ GDPR	Článok 32	N/A
Smernica EÚ NIS2	Článok 21(2)(d)	N/A
Nariadenie EÚ DORA	Článok 9	N/A
COBIT 2019	DSS01.03, DSS05.01, MEA03	N/A

1. Účel

1.1 Účelom tejto politiky je stanoviť požiadavky organizácie na ochranu jej interných a externých sietí pred neoprávneným prístupom, prerušením služieb, zachytávaním údajov a zneužitím.

1.2 Zabezpečuje, aby bola všetka sieťová infraštruktúra vrátane fyzickej, virtuálnej, cloudovej a hybridnej infraštruktúry chránená prostredníctvom vrstvených kontrol, ako sú segmentácia, presadzovanie pravidiel firewallov, bezpečné smerovanie a centralizované monitorovanie.

1.3 Táto politika uplatňuje požiadavky ISO/IEC 27001, kapitoly 8.1, a kontrol prílohy A 8.20 až 8.22 a zabezpečuje súlad s príslušnými zákonnými a regulačnými povinnosťami podľa článku 32 GDPR, článku 21 smernice NIS2 a článku 9 nariadenia DORA.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky siete a súvisiace komponenty infraštruktúry vrátane:

2.1.1 smerovačov, prepínačov, bezdrôtových prístupových bodov a firewallov,

2.1.2 cloudových virtuálnych sietí (napr. AWS VPC, Azure VNet), koncentrátorov VPN a systémov SD-WAN,

2.1.3 interných sietí LAN, demilitarizovaných zón (DMZ), ciest vzdialeného prístupu a prepojení medzi lokalitami alebo s tretími stranami,

2.1.4 podporných systémov, ako sú DNS, DHCP, proxy servery a monitorovacie zariadenia.

2.2 Táto politika je záväzná pre všetkých pracovníkov a poskytovateľov služieb tretích strán, ktorí spravujú, konfigurujú, monitorujú siete organizácie alebo sa k nim pripájajú, či už v priestoroch organizácie alebo v cloudovom prostredí.

2.3 Všetky systémy a aplikácie pripojené k sieťam organizácie bez ohľadu na umiestnenie alebo vlastníctvo musia spĺňať tieto požiadavky na bezpečnosť sietí.

3. Ciele

3.1 Zabezpečiť dôvernosť, integritu a dostupnosť údajov prenášaných cez siete prostredníctvom silného riadenia prístupu, bezpečného smerovania a monitorovania.

3.2 Predchádzať neoprávnenému prístupu, laterálnemu pohybu a zneužitiu sieťových zdrojov uplatňovaním segmentácie, zónovania a ochrany hraníc siete.

3.3 Udržiavať konzistentné sieťové konfigurácie založené na odvetvových osvedčených postupoch a spravodajstve o hrozbách na ochranu pred vyvíjajúcimi sa kybernetickými hrozbami.

3.4 Zabezpečiť externú komunikáciu, cloudovú konektivitu a vzdialený prístup pomocou šifrovaných komunikačných kanálov, silnej autentifikácie a overovania koncových bodov.

3.5 Zabezpečiť viditeľnosť sieťových aktivít prostredníctvom centralizovaného logovania, inšpekcie sieťovej prevádzky v reálnom čase a automatizovaného upozorňovania.

3.6 Zabezpečiť súlad zosúladením všetkých sieťových operácií s požiadavkami ISO/IEC 27001:2022, GDPR, NIS2, DORA a COBIT 2019.

4. Roly a zodpovednosti

4.1 riaditeľ informačnej bezpečnosti (CISO)

4.1.1 Zodpovedá za túto politiku a zabezpečuje jej preskúmanie a zosúladenie so širšou stratégiou kybernetickej bezpečnosti organizácie.

4.1.2 Schvaľuje modely segmentácie sietí, súbory pravidiel firewallov pre citlivé systémy a žiadosti o výnimku.

4.2 manažér bezpečnosti sietí / vedúci bezpečnosti infraštruktúry

4.2.1 Riadi architektúru ochrany sietí vrátane firewallov, systémov detekcie a prevencie prienikov (IDS/IPS), VPN a bezpečného smerovania.

4.2.2 Zodpovedá za segmentáciu sietí, priradenie VLAN, zónovanie prevádzky a externú konektivitu.

4.2.3 Zabezpečuje priebežné preskúmavanie filtrovania vstupnej a výstupnej prevádzky a uplatňovanie princípov Zero Trust naprieč sieťovými vrstvami.

[... 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 každoročne preskúmaná manažérom bezpečnosti sietí v spolupráci s CISO a aktualizovaná na základe:

9.1.1 nových hrozieb (napr. nové techniky útokov, zraniteľnosti protokolov),

9.1.2 zmien infraštruktúry (napr. migrácie do cloudového prostredia, nasadenie SD-WAN),

9.1.3 aktualizácií predpisov alebo noriem ovplyvňujúcich ochranu sietí,

9.1.4 auditných zistení, trendov incidentov alebo zhoršenia výkonnosti spôsobeného kontrolami.

9.2 Preskúmania musia byť vykonané aj pri:

9.2.1 významných zmenách architektúry siete,

9.2.2 implementácii nových firewallov, VPN alebo cloudových sieťových platforiem,

9.2.3 vyradení kľúčových aktív alebo dôveryhodných zón.

9.3 Aktualizácie musia byť zaznamenané v registri riadenia dokumentácie ISMS a oznámené:

9.3.1 tímom infraštruktúry a sieťovej prevádzky,

9.3.2 tímom SOC a bezpečnostného inžinierstva,

9.3.3 aplikačným tímom so systémovými závislosťami od sieťových tokov,

9.3.4 všetkým dodávateľom tretích strán s aktívnou konektivitou.

9.4 Všetky predchádzajúce verzie politiky musia byť bezpečne archivované spolu s poznámkami o histórii zmien, aby sa zachovala auditovateľnosť a sledovateľnosť zmien.

10. Súvisiace politiky a väzby

10.1 P1 - Politika informačnej bezpečnosti. Stanovuje základné princípy bezpečnosti a vyžaduje vrstvené ochranné opatrenia vrátane sieťového riadenia prístupu a kontrol hrozieb.

10.2 P4 - Politika riadenia prístupu. Zabezpečuje, aby sa sieťová segmentácia uplatňovala v súlade s používateľskými rolami, zásadou minimálnych oprávnení a pravidlami zriaďovania prístupu.

10.3 P5 - Politika riadenia zmien. Upravuje zmeny firewallov, úpravy pravidiel VPN a zmeny smerovania prostredníctvom zdokumentovaného procesu vhodného na audit.

10.4 P12 - Politika správy aktív. Podporuje identifikáciu a klasifikáciu sieťových systémov a zabezpečuje, aby všetky pripojené aktíva boli spravované v rozsahu definovanom politikou.

10.5 P22 - Politika logovania a monitorovania. Upravuje zber, koreláciu a uchovávanie sieťových logov vrátane udalostí firewallov, pokusov o prístup a detekcie anomálií.

10.6 P30 - Politika reakcie na incidenty. Definuje postupy eskalácie, zamedzenia šírenia a eradikácie v reakcii na sieťové hrozby alebo prieniky, ako sú DDoS, laterálny pohyb alebo neoprávnený prístup.

11. Referenčné normy a rámce

11.1 Táto politika je zosúladená s medzinárodnými normami a regulačnými požiadavkami, ktoré definujú bezpečnú prevádzku sietí, segmentáciu, ochranu perimetra a bezpečný vzdialený prístup.

11.2 ISO/IEC 27001

11.2.1 Kapitola 8.1 - Prevádzkové plánovanie a riadenie: Vyžaduje, aby technické kontroly vrátane sieťových ochranných opatrení boli začlenené do prevádzkových procesov.

11.3 ISO/IEC 27002:2022

11.3.1 Kontroly 8.20-8.22. Poskytujú usmernenia na ochranu sietí, segmentáciu služieb a zabezpečenie sieťových služieb prostredníctvom riadenia prístupu a monitorovania.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - Ochrana hraníc: Vyžaduje perimetrické kontroly, segmentáciu a bezpečné prepojenia.

11.4.2 AC-4 - Vynucovanie tokov informácií: Podporuje zónovanie a obmedzenia prevádzky na základe pravidiel.

11.4.3 SC-32 - Rozdelenie informačných systémov: Podporuje logické oddelenie informačných systémov.

11.5 Nariadenie EÚ GDPR (2016/679)

11.5.1 Článok 32 - Bezpečnosť spracúvania: Vyžaduje technické opatrenia, ako sú firewally a segmentácia, na ochranu osobných údajov.

11.6 Smernica EÚ NIS2 (2022/2555)

11.6.1 Článok 21(2)(d): Vyžaduje účinnú bezpečnosť sietí a informačných systémov, ochranu perimetra, bezpečnú konfiguráciu a kontroly oddelenia.

11.7 Nariadenie EÚ DORA (2022/2554)

11.7.1 Článok 9 - Riadenie rizík IKT: Ukladá finančným subjektom povinnosť chrániť siete a prepojenia pred neoprávneným prístupom, únikmi údajov a prevádzkovým narušením.

11.8 COBIT 2019

11.8.1 DSS01.03 - Monitorovanie infraštruktúry: Vyžaduje proaktívnu kontrolu stavu siete a konektivity.

11.8.2 DSS05.01 - Ochrana pred malvérom: Zahŕňa segmentáciu a ochranu hraníc s cieľom minimalizovať šírenie.

11.8.3 MEA03 - Monitorovanie, hodnotenie a posudzovanie súladu: Posilňuje uplatňovanie sieťovej politiky a posúdenia súladu.