					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P21					Název dokumentu: **Politika zabezpečení sítí**							
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	Článek/ustanovení	Komentář
ISO/IEC 27001:2022	Kapitola 8	N/A
ISO/IEC 27002:2022	Opatření 8.20-8	N/A
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	N/A
GDPR	Článek 32	N/A
směrnice NIS2	Článek 21 odst. 2 písm. d)	N/A
nařízení DORA	Článek 9	N/A
COBIT 2019	DSS01.03, DSS05.01, MEA	N/A

1. Účel

1.1 Účelem této politiky je stanovit požadavky organizace na ochranu jejích interních a externích sítí před neoprávněným přístupem, narušením služeb, odposlechem dat a zneužitím.

1.2 Zajišťuje, aby byla veškerá síťová infrastruktura, včetně fyzické, virtuální, cloudové a provozované v hybridním režimu, chráněna prostřednictvím vícevrstvé ochrany, jako jsou segmentace, uplatňování pravidel firewallu, bezpečné směrování a centralizované monitorování.

1.3 Tato politika uplatňuje požadavky ISO/IEC 27001 kapitoly 8.1 a opatření přílohy A 8.20 až 8.22 a zajišťuje soulad s příslušnými právními a regulačními povinnostmi podle GDPR článku 32, směrnice NIS2 článku 21 a nařízení DORA článku 9.

2. Rozsah

2.1 Tato politika se vztahuje na všechny sítě a související komponenty infrastruktury, včetně:

2.1.1 směrovačů, přepínačů, bezdrátových přístupových bodů a firewallů,

2.1.2 cloudových virtuálních sítí (např. AWS VPC, Azure VNet), koncentrátorů VPN a systémů SD-WAN,

2.1.3 interních LAN, demilitarizovaných zón (DMZ), cest vzdáleného přístupu a propojení mezi lokalitami nebo s třetími stranami,

2.1.4 podpůrných systémů, jako jsou DNS, DHCP, proxy servery a monitorovací zařízení.

2.2 Tato politika je závazná pro veškerý personál a poskytovatele služeb třetích stran, kteří spravují, konfigurují, monitorují nebo jinak pracují se sítěmi organizace, a to jak v on-premise infrastruktuře, tak v cloudu.

2.3 Všechny systémy a aplikace připojené k sítím organizace, bez ohledu na umístění nebo vlastnictví, musí splňovat tyto požadavky na zabezpečení sítí.

3. Cíle

3.1 Zajistit důvěrnost, integritu a dostupnost (CIA) dat přenášených po sítích prostřednictvím silného řízení přístupu, bezpečného směrování a monitorování.

3.2 Předcházet neoprávněnému přístupu, laterálnímu pohybu a zneužití síťových zdrojů prosazováním segmentace, zonace a ochrany perimetru.

3.3 Udržovat konzistentní konfigurace sítí založené na osvědčených postupech v odvětví a informacích o hrozbách s cílem bránit se proti vyvíjejícím se kybernetickým hrozbám.

3.4 Zabezpečit externí komunikaci, cloudovou konektivitu a vzdálený přístup pomocí šifrovaných komunikačních kanálů, silné autentizace a ověřování koncových bodů.

3.5 Zajistit viditelnost síťových aktivit prostřednictvím centralizovaného protokolování, inspekce provozu v reálném čase a automatizovaných upozornění.

3.6 Zajistit soulad s právními předpisy sladěním všech síťových operací s požadavky ISO/IEC 27001:2022, GDPR, směrnice NIS2, nařízení DORA a COBIT 2019.

4. Role a odpovědnosti

4.1 ředitel informační bezpečnosti (CISO)

4.1.1 Odpovídá za tuto politiku a zajišťuje její přezkum a sladění se širší strategií kybernetické bezpečnosti organizace.

4.1.2 Schvaluje modely segmentace sítě, sady pravidel firewallu pro citlivé systémy a žádosti o výjimku.

4.2 manažer zabezpečení sítí / vedoucí bezpečnosti infrastruktury

4.2.1 Řídí architekturu ochrany sítí, včetně firewallů, systémů detekce a prevence průniků (IDS/IPS), VPN a bezpečného směrování.

4.2.2 Odpovídá za segmentaci sítě, přiřazování VLAN, zonaci provozu a externí konektivitu.

4.2.3 Zajišťuje průběžný přezkum filtrování příchozího a odchozího provozu a uplatňování principů Zero Trust napříč síťovými vrstvami.

[... 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 každoročně přezkoumána manažerem zabezpečení sítí ve spolupráci s CISO a aktualizována na základě:

9.1.1 nově vznikajících rizik (např. nové techniky útoků, zranitelnosti protokolů),

9.1.2 změn infrastruktury (např. migrace do cloudu, nasazení SD-WAN),

9.1.3 regulatorních aktualizací nebo aktualizací norem ovlivňujících ochranu sítí,

9.1.4 zjištění z auditů, trendů incidentů nebo snížení výkonnosti způsobeného opatřeními.

9.2 Přezkum musí být zahájen také při:

9.2.1 zásadních změnách architektury sítě,

9.2.2 implementaci nových platforem firewallu, VPN nebo cloudových síťových platforem,

9.2.3 vyřazení klíčových aktiv nebo důvěryhodných zón z provozu.

9.3 Aktualizace musí být zaznamenány v registru řízení dokumentace ISMS a rozeslány:

9.3.1 týmům infrastruktury a síťového provozu,

9.3.2 týmům SOC a bezpečnostního inženýrství,

9.3.3 aplikačním týmům se systémovými závislostmi na síťových tocích,

9.3.4 všem dodavatelům třetích stran s aktivní konektivitou.

9.4 Všechny předchozí verze politiky musí být bezpečně archivovány s poznámkami k historii změn, aby byla zachována auditovatelnost a dohledatelnost změn.

10. Související politiky a vazby

10.1 P1 - P01 Politika informační bezpečnosti. Stanoví základní bezpečnostní zásady a ukládá vícevrstvou ochranu včetně síťově založeného řízení přístupu a opatření proti hrozbám.

10.2 P4 - Politika řízení přístupu. Zajišťuje, aby byla segmentace sítě uplatňována v souladu s rolemi uživatelů, zásadou minimálních oprávnění a pravidly zřizování přístupu.

10.3 P5 - Politika řízení změn. Upravuje změny firewallu, úpravy pravidel VPN a změny směrování prostřednictvím dokumentovaného a auditovatelného procesu.

10.4 P12 - Politika správy aktiv. Podporuje identifikaci a klasifikaci síťových systémů a zajišťuje, že všechna připojená aktiva jsou spravována v rozsahu stanoveném politikou.

10.5 P22 - Politika protokolování a monitorování. Upravuje sběr, korelaci a uchovávání síťových logů, včetně událostí firewallu, pokusů o přístup a detekovaných anomálií.

10.6 P30 - Politika reakce na incidenty. Definuje eskalaci, zamezení šíření a eradikaci v reakci na hrozby nebo průniky šířené po síti, jako jsou DDoS, laterální pohyb nebo neoprávněný přístup.

11. Referenční normy a rámce

11.1 Tato politika je v souladu s mezinárodními normami a regulačními požadavky, které stanovují bezpečný provoz sítí, segmentaci, ochranu perimetru a bezpečný vzdálený přístup.

11.2 ISO/IEC 27001

11.2.1 Kapitola 8.1 – Operativní plánování a řízení: Vyžaduje, aby technická opatření, včetně síťových ochranných mechanismů, byla začleněna do provozních procesů.

11.3 ISO/IEC 27002:2022

11.3.1 Opatření 8.20-8: Poskytuje pokyny pro ochranu sítí, segmentaci služeb a zabezpečení síťových služeb prostřednictvím řízení přístupu a monitorování.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - Ochrana perimetru: Vyžaduje perimetrické kontroly, segmentaci a bezpečná propojení.

11.4.2 AC-4 - Vynucování toku informací: Podporuje zonaci a omezení provozu na základě pravidel.

11.4.3 SC-32 - Rozdělení informačních systémů: Podporuje logické oddělení informačních systémů.

11.5 GDPR (2016/679)

11.5.1 Článek 32 - Zabezpečení zpracování: Vyžaduje technická opatření, jako jsou firewally a segmentace, k ochraně osobních údajů.

11.6 směrnice NIS2 (2022/2555)

11.6.1 Článek 21 odst. 2 písm. d): Vyžaduje účinné zabezpečení sítí a informačních systémů, ochranu perimetru, bezpečnou konfiguraci a opatření pro oddělení.

11.7 nařízení DORA (2022/2554)

11.7.1 Článek 9 - Řízení rizik v oblasti ICT: Ukládá finančním subjektům chránit sítě a propojení před neoprávněným přístupem, únikem dat a provozním narušením.

11.8 COBIT 2019

11.8.1 DSS01.03 - Monitorování infrastruktury: Vyžaduje proaktivní řízení stavu sítě a konektivity.

11.8.2 DSS05.01 - Ochrana proti malwaru: Zahrnuje segmentaci a ochranu perimetru za účelem minimalizace šíření.

11.8.3 MEA03 - Monitorování, vyhodnocování a posuzování souladu: Posiluje uplatňování síťové politiky a posuzování souladu.