					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P21S					Název dokumentu: **Politika zabezpečení sítě**							
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**

Právní upozornění (autorská práva a omezení užití)

(C) 2025 Clarysec LLC. All rights reserved.

Tento dokument je duševním vlastnictvím společnosti Clarysec LLC. Žádná jeho část nesmí být kopírována, znovu použita, distribuována ani upravována pro komerční nebo implementační účely bez výslovného písemného souhlasu.

Neoprávněné použití je přísně zakázáno a může vést k právním krokům.

V případě licencování kontaktujte: info@clarysec.com

V souladu s normami a právními předpisy

Norma/právní předpis	Článek/ustanovení	Komentář
ISO/IEC 27001:2022	Kapitola 8	-
ISO/IEC 27002:2022	Opatření 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
GDPR	Článek 32	-
směrnice NIS2	Články 21(2)(d), (e)	-
nařízení DORA	Články 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Účel

1.1. Účelem této politiky je zajistit, aby veškerá interní i externí síťová komunikace byla chráněna před neoprávněným přístupem, manipulací, odposlechem nebo zneužitím prostřednictvím jasně definovaných bezpečnostních opatření.

1.2. Tato politika stanoví pravidla pro bezpečný návrh, používání a správu síťové infrastruktury, včetně směrovačů, bezdrátových přístupových bodů, připojení pro vzdálený přístup a segmentovaných sítí.

1.3. Cílem je minimalizovat vystavení internetovým hrozbám, zajistit důvěrnost dat přenášených v interních i externích sítích a zachovat dostupnost kritických služeb.

1.4. Tato politika podporuje certifikaci podle ISO/IEC 27001:2022 a přímo přispívá k plnění právních a regulačních povinností podle GDPR, směrnice NIS2 a nařízení DORA a současně poskytuje technické ujištění zákazníkům a auditorům.

2. Rozsah

2.1. Tato politika se vztahuje na všechny součásti IT sítě organizace, včetně:

2.1.1. kabelové a bezdrátové infrastruktury v kancelářských lokalitách,

2.1.2. směrovačů, přepínačů, přístupových bodů, firewallů a bran,

2.1.3. připojení pro vzdálený přístup, včetně VPN, RDP a cloudových tunelů,

2.1.4. cloudových aplikací přístupných z interních nebo externích sítí,

2.1.5. zařízení připojených k síti zaměstnanci, smluvními pracovníky nebo hosty.

2.2. Tato politika upravuje fyzické i logické síťové segmenty, včetně hostovských zón, zařízení IoT a back-office systémů.

2.3. Tato politika se vztahuje na veškerý personál s přístupem k síti organizace, včetně:

2.3.1. interních zaměstnanců,

2.3.2. pracovníků na dálku a pracovníků v hybridním režimu,

2.3.3. externích dodavatelů, konzultantů a poskytovatelů služeb,

2.3.4. hostů využívajících dočasný přístup k Wi-Fi.

3. Cíle

3.1. Zajistit ochranu sítě organizace před neoprávněným přístupem a externími kybernetickými hrozbami.

3.2. Prosazovat odpovídající segmentaci mezi důvěryhodnými a nedůvěryhodnými sítěmi (např. hostovská Wi-Fi, přístup dodavatelů).

3.3. Umožnit bezpečné vzdálené připojení bez ohrožení interních systémů.

3.4. Předcházet šíření malwaru a exfiltraci dat prostřednictvím síťových kanálů.

3.5. Zajistit monitorování, upozorňování a auditovatelnost síťových aktivit na podporu detekce incidentů a souladu.

3.6. Zajistit, aby k interním sítím byla připojována pouze schválená a zabezpečená zařízení.

3.7. Plnit požadavky podle ISO 27001, GDPR a souvisejících rámců kybernetické bezpečnosti.

4. Role a odpovědnosti

4.1. generální ředitel

4.1.1. Je vlastníkem této politiky a zajišťuje přidělení odpovídajících zdrojů pro bezpečný návrh a správu sítě.

4.1.2. Přezkoumává výjimky z bezpečnostních opatření pro síť a schvaluje dohody o síťovém přístupu dodavatelů.

4.1.3. Přezkoumává incidenty nebo zjištění auditu související se slabinami v zabezpečení sítě.

4.2. externí poskytovatel IT služeb / interní IT funkce

4.2.1. Implementuje, konfiguruje a udržuje všechny firewally, směrovače, přepínače a řadiče bezdrátové sítě.

4.2.2. Řídí segmentaci mezi interními, hostovskými a externími sítěmi.

4.2.3. Monitoruje logy a upozornění na pokusy o neoprávněný přístup nebo síťové anomálie.

4.2.4. Zajišťuje bezpečné a včasné provádění aktualizací firmwaru a konfigurací.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1. Každoroční přezkum

9.1.1. Tato politika musí být nejméně jednou ročně přezkoumána generálním ředitelem společně s externím poskytovatelem IT služeb a koordinátorem ochrany soukromí.

9.2. Spouštěče průběžného přezkumu

9.2.1. Přezkum politiky musí být zahájen také při:

9.2.1.1. zásadních změnách síťové architektury (např. nové systémy VPN nebo firewallů),

9.2.1.2. incidentu souvisejícím se sítí (např. průniku, šíření ransomwaru nebo exfiltraci dat),

9.2.1.3. změnách právních předpisů, regulačních požadavků nebo rámců ovlivňujících ochranu sítě,

9.2.1.4. zavedení nových dodavatelských platforem vyžadujících alternativní metody přístupu nebo protokoly.

9.3. Správa verzí a dokumentace

9.3.1. Změny politiky musí být zaznamenány s číslem verze, datem a souhrnem změn.

9.3.2. Předchozí verze musí být archivovány po dobu nejméně 3 let.

9.3.3. Aktualizace musí být oznámeny dotčeným zaměstnancům a při zavedení významných změn chování musí být vyžadováno potvrzení seznámení.

10. Související politiky a vazby

10.1. Tato politika musí být implementována společně s následujícími bezpečnostními politikami SME:

10.1.1. P9S – Politika práce na dálku: stanoví požadavky na bezpečné metody vzdáleného přístupu, VPN a ochranu koncových stanic pro uživatele mimo pracoviště.

10.1.2. P12S – Politika správy aktiv: zajišťuje, že všechny systémy připojené k síti jsou identifikovány, kategorizovány a sledovány s aktuálním stavem zabezpečení.

10.1.3. P17S – Politika ochrany dat a soukromí: zajišťuje, že segmentace sítě, řízení přístupu a protokolování podporují zásady ochrany soukromí a ochrany dat podle GDPR.

10.1.4. P22S – Politika protokolování a monitorování: stanoví požadavky na zaznamenávání a přezkoumávání logů ze síťových zařízení, vzdálených připojení a řadičů bezdrátové sítě.

10.1.5. P30S – Politika reakce na incidenty: vymezuje požadované kroky při reakci na porušení bezpečnosti sítě, pokusy o neoprávněný přístup nebo šíření malwaru prostřednictvím interních sítí.

11. Referenční normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 8 – Vyžaduje implementaci opatření k zajištění bezpečného a odolného provozu, včetně sítí.

11.2. ISO/IEC 27002

11.2.1. Opatření 8.20 – Poskytuje technické a procesní pokyny pro zabezpečení síťového přístupu, segmentace a monitorování.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – Vyžaduje řízení toku informací v sítích a mezi systémy.

11.3.2. SC-7 – Vyžaduje ochranu perimetru, bezpečné směrování a segmentaci sítě ke snížení rizika neoprávněného přístupu.

11.4. GDPR

11.4.1. Článek 32 – Vyžaduje přiměřená technická a organizační opatření k zajištění důvěrnosti, integrity a dostupnosti síťově propojených systémů a služeb, které zpracovávají osobní údaje.

11.5. směrnice NIS2

11.5.1. Článek 21(2)(d) – Vyžaduje technická opatření založená na rizicích, včetně zabezpečení sítě a řízení přístupu.

11.5.2. Článek 21(2)(e) – Vyžaduje segmentaci a izolaci systémů, aby se zabránilo šíření kybernetických incidentů.

11.6. nařízení DORA

11.6.1. Článek 9 – Vyžaduje, aby organizace zavedly opatření řízení rizik v oblasti ICT, včetně opatření pro bezpečné sítě a komunikaci.

11.6.2. Článek 10 – Vyžaduje, aby strategie digitální odolnosti zahrnovaly ochranu síťové infrastruktury a vzdáleného připojení.

11.7. COBIT 2019

11.7.1. DSS05.02 – Vyžaduje účinnou ochranu IT infrastruktury a síťových prostředí před interními i externími hrozbami.

11.7.2. APO13.01 – Vyžaduje strategie řízení rizik, které zahrnují segmentaci sítě a monitorování jako součást zmírňování hrozeb.