					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P21S					Dokumentum címe: **Hálózatbiztonsági szabályzat**							
Verzió: 1.0		Hatálybalépés dátuma: 01.01.2025			A dokumentum tulajdonosa:							
X	Szabályzat		Szabvány		Eljárás		Űrlap		Nyilvántartás		Egyéb	

Felülvizsgálati előzmények				
Felülvizsgálat száma	**Felülvizsgálat dátuma**	**Változások**	**Felülvizsgálta**	**A folyamat tulajdonosa**

Jóváhagyások			
Név	**Beosztás**	**Dátum**	**Aláírás**

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	8. pont	-
ISO/IEC 27002:2022	8. kontroll	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
GDPR	32. cikk	-
NIS2 irányelv	21. cikk (2) bekezdés d), e) pont	-
DORA-rendelet	9., 10. cikk	-
COBIT 2019	DSS05.02, APO13	-

1. Cél

1.1. Jelen szabályzat célja annak biztosítása, hogy valamennyi belső és külső hálózati kommunikáció egyértelműen meghatározott biztonsági kontrollokkal legyen védve a jogosulatlan hozzáféréssel, módosítással, lehallgatással és visszaélésszerű használattal szemben.

1.2. A szabályzat meghatározza a hálózati infrastruktúra biztonságos tervezésére, használatára és üzemeltetésére vonatkozó szabályokat, ideértve az útválasztókat, a vezeték nélküli hozzáférési pontokat, a távoli hozzáférési kapcsolatokat és a szegmentált hálózatokat.

1.3. Célja az internetalapú fenyegetéseknek való kitettség minimalizálása, a belső és külső hálózatokon továbbított adatok bizalmasságának biztosítása, valamint a kritikus szolgáltatások rendelkezésre állásának fenntartása.

1.4. Jelen szabályzat támogatja az ISO/IEC 27001:2022 szerinti tanúsítást, és közvetlenül hozzájárul a GDPR, a NIS2 irányelv és a DORA-rendelet szerinti jogi és szabályozási kötelezettségek teljesítéséhez, továbbá technikai bizonyosságot nyújt az ügyfelek és az auditorok számára.

2. Hatály

2.1. Jelen szabályzat a szervezet informatikai hálózatának valamennyi elemére kiterjed, beleértve az alábbiakat:

2.1.1. Az irodai helyszíneken működő vezetékes és vezeték nélküli infrastruktúra

2.1.2. Útválasztók, kapcsolók, hozzáférési pontok, tűzfalak és átjárók

2.1.3. Távoli hozzáférési kapcsolatok, beleértve a VPN-eket, az RDP-t és a felhőalapú titkosított alagutakat

2.1.4. Belső vagy külső hálózatokról elért felhőalapú alkalmazások

2.1.5. A hálózathoz munkavállalók, vállalkozók vagy vendégek által csatlakoztatott eszközök

2.2. Jelen szabályzat a fizikai és logikai hálózati szegmensekre egyaránt vonatkozik, beleértve a vendéghálózatokat, az IoT-eszközöket és a háttérirodai rendszereket.

2.3. A szabályzat a szervezet hálózatához hozzáféréssel rendelkező valamennyi személyre kiterjed, beleértve az alábbiakat:

2.3.1. Belső munkavállalók

2.3.2. Távmunkában vagy hibrid munkarendben dolgozó munkatársak

2.3.3. Külső beszállítók, tanácsadók és szolgáltatók

2.3.4. Ideiglenes Wi-Fi-hozzáférést használó vendégek

3. Célkitűzések

3.1. A szervezet hálózatának védelme a jogosulatlan hozzáféréssel és a külső kibertámadásokkal szemben

3.2. A megbízható és nem megbízható hálózatok közötti megfelelő szegmentálás érvényesítése (pl. vendég-Wi-Fi, beszállítói hozzáférés)

3.3. Biztonságos távoli kapcsolódás biztosítása a belső rendszerek veszélyeztetése nélkül

3.4. A kártékony kód terjedésének és az adatkivitelnek a megelőzése hálózati csatornákon keresztül

3.5. A hálózati tevékenységek nyomon követésének, riasztásának és auditálhatóságának biztosítása az incidensek észlelése és a megfelelés támogatása érdekében

3.6. Annak biztosítása, hogy a belső hálózatokhoz kizárólag jóváhagyott és megfelelően védett eszközök csatlakozhassanak

3.7. Az ISO 27001, a GDPR és a kapcsolódó kiberbiztonsági keretrendszerek szerinti kötelezettségek teljesítése

4. Szerepkörök és felelősségi körök

4.1. Ügyvezető

4.1.1. A szabályzat tulajdonosa, és biztosítja, hogy megfelelő erőforrások álljanak rendelkezésre a biztonságos hálózattervezéshez és hálózatüzemeltetéshez.

4.1.2. Felülvizsgálja a hálózatbiztonsági kontrollok alóli kivételeket, és jóváhagyja a beszállítói hálózati hozzáférésre vonatkozó megállapodásokat.

4.1.3. Felülvizsgálja a hálózatbiztonsági gyengeségekkel kapcsolatos incidenseket és auditmegállapításokat.

4.2. Informatikai támogatás / belső informatikai szerepkör

4.2.1. Bevezeti, konfigurálja és karbantartja valamennyi tűzfalat, útválasztót, kapcsolót és vezeték nélküli vezérlőt.

4.2.2. Kezeli a belső, vendég- és külső hálózatok közötti szegmentálást.

4.2.3. Figyelemmel kíséri a naplókat és riasztásokat a jogosulatlan hozzáférési kísérletek vagy hálózati rendellenességek azonosítása érdekében.

4.2.4. Biztosítja, hogy a firmware- és konfigurációfrissítések biztonságosan és időben telepítésre kerüljenek.

[... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ...]

9. Felülvizsgálati és frissítési követelmények

9.1. Éves felülvizsgálat

9.1.1. Jelen szabályzatot legalább évente egyszer felül kell vizsgálnia az ügyvezetőnek az informatikai támogatást nyújtó szolgáltatóval és az adatvédelmi koordinátorral együtt.

9.2. Soron kívüli felülvizsgálat kiváltó okai

9.2.1. A szabályzat felülvizsgálatát az alábbi esetekben is el kell végezni:

9.2.1.1. A hálózati architektúrát érintő jelentős változások esetén (pl. új VPN- vagy tűzfalrendszerek)

9.2.1.2. Hálózattal kapcsolatos incidens esetén (pl. behatolás, zsarolóvírus terjedése vagy adatkivitel)

9.2.1.3. A hálózat védelmét érintő jogi, szabályozási vagy keretrendszerbeli változások esetén

9.2.1.4. Olyan új beszállítói platformok bevezetése esetén, amelyek eltérő hozzáférési módszereket vagy protokollokat igényelnek

9.3. Verziókezelés és dokumentálás

9.3.1. A szabályzat módosításait verziószámmal, dátummal és a változások összefoglalásával kell rögzíteni.

9.3.2. A korábbi verziókat legalább 3 évig archiválni kell.

9.3.3. A frissítésekről tájékoztatni kell az érintett munkavállalókat, és kötelező tudomásulvételt kell előírni, ha a módosítás jelentős magatartásbeli változást vezet be.

10. Kapcsolódó szabályzatok és összefüggések

10.1. Jelen szabályzatot az alábbi KKV-biztonsági szabályzatokkal együtt kell alkalmazni:

10.1.1. P9S – Távmunka-szabályzat: meghatározza a biztonságos távoli hozzáférési módszereket, a VPN-követelményeket és a telephelyen kívül dolgozó felhasználók végpontvédelmi követelményeit.

10.1.2. P12S – Eszközkezelési szabályzat: biztosítja, hogy minden hálózatra csatlakozó rendszer azonosított, kategorizált és nyomon követett legyen naprakész biztonsági állapottal.

10.1.3. P17S – Adatvédelmi és magánszféra-védelmi szabályzat: biztosítja, hogy a hálózati szegmentálás, a hozzáférés-szabályozás és a naplózás támogassa a GDPR szerinti adatvédelmi elveket.

10.1.4. P22S – Naplózási és felügyeleti szabályzat: meghatározza a hálózati eszközökből, távoli kapcsolatokból és vezeték nélküli vezérlőkből származó naplók rögzítésére és felülvizsgálatára vonatkozó követelményeket.

10.1.5. P30S – Incidenskezelési szabályzat: meghatározza a szükséges intézkedéseket hálózati adatsértések, jogosulatlan hozzáférési kísérletek vagy a belső hálózatokon keresztül terjedő kártékony kód esetén.

11. Hivatkozott szabványok és keretrendszerek

11.1. ISO/IEC 27001

11.1.1. 8.1. pont – Előírja a kontrollok bevezetését a biztonságos és reziliens működés biztosítására, beleértve a hálózatokat is.

11.2. ISO/IEC 27002

11.2.1. 8.20 kontroll – Technikai és eljárási iránymutatást ad a hálózati hozzáférés, a szegmentálás és a nyomon követés védelméhez.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – Előírja az információáramlás szabályozását a hálózatokon belül és a rendszerek között.

11.3.2. SC-7 – Előírja a határvédelem, a biztonságos útválasztás és a hálózati szegmentálás alkalmazását a jogosulatlan hozzáférés kockázatának csökkentése érdekében.

11.4. GDPR

11.4.1. 32. cikk – Megfelelő technikai és szervezési intézkedéseket ír elő a személyes adatokat kezelő hálózatba kapcsolt rendszerek és szolgáltatások bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítására.

11.5. NIS2 irányelv

11.5.1. 21. cikk (2) bekezdés d) pont – Kockázatalapú technikai intézkedéseket ír elő, beleértve a hálózatbiztonságot és a hozzáférés-szabályozást.

11.5.2. 21. cikk (2) bekezdés e) pont – Előírja a rendszerek szegmentálását és elkülönítését a biztonsági incidensek továbbterjedésének megelőzésére.

11.6. DORA-rendelet

11.6.1. 9. cikk – Előírja, hogy a szervezetek IKT-kockázatkezelési kontrollokat vezessenek be, beleértve a biztonságos hálózatokra és kommunikációra vonatkozó kontrollokat is.

11.6.2. 10. cikk – Előírja, hogy a digitális reziliencia-stratégiák terjedjenek ki a hálózati infrastruktúra és a távoli kapcsolódás védelmére.

11.7. COBIT 2019

11.7.1. DSS05.02 – Előírja az IT-infrastruktúra és a hálózati környezetek hatékony védelmét a belső és külső fenyegetésekkel szemben.

11.7.2. APO13.01 – Előírja olyan kockázatkezelési stratégiák alkalmazását, amelyek a fenyegetések mérséklésének részeként magukban foglalják a hálózati szegmentálást és a nyomon követést.