					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P21					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	N/A
ISO/IEC 27002:2022	8.20–8. kontroll	N/A
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	N/A
GDPR	32. cikk	N/A
NIS2 irányelv	21. cikk (2) bekezdés d) pont	N/A
DORA rendelet	9. cikk	N/A
COBIT 2019	DSS01.03, DSS05.01, MEA	N/A

1. Cél

1.1 Jelen szabályzat célja a szervezet belső és külső hálózatainak védelmére vonatkozó követelmények meghatározása a jogosulatlan hozzáféréssel, szolgáltatáskimaradással, adatlehallgatással és visszaélésszerű használattal szemben.

1.2 A szabályzat biztosítja, hogy valamennyi hálózati infrastruktúra – beleértve a fizikai, virtuális, felhőalapú és hibrid környezeteket – rétegezett védelmi kontrollokkal, így szegmentálással, tűzfalszabályok érvényesítésével, biztonságos útvonalválasztással és központi felügyelettel védett legyen.

1.3 Jelen szabályzat érvényesíti az ISO/IEC 27001 8.1 pontjának és az A. melléklet 8.20–8.22 kontrolljainak követelményeit, továbbá biztosítja a GDPR 32. cikke, a NIS2 irányelv 21. cikke és a DORA rendelet 9. cikke szerinti releváns jogi és szabályozási kötelezettségek teljesítését.

2. Hatály

2.1 Jelen szabályzat valamennyi hálózatra és kapcsolódó infrastruktúra-elemre kiterjed, ideértve különösen az alábbiakat:

2.1.1 útválasztók, kapcsolók, vezeték nélküli hozzáférési pontok és tűzfalak

2.1.2 felhőalapú virtuális hálózatok (pl. AWS VPC, Azure VNET), VPN-koncentrátorok és SD-WAN rendszerek

2.1.3 belső LAN-ok, demilitarizált zónák (DMZ), távoli hozzáférési útvonalak, valamint telephelyek közötti vagy harmadik félhez kapcsolódó összeköttetések

2.1.4 támogató rendszerek, így különösen DNS, DHCP, proxykiszolgálók és felügyeleti eszközök

2.2 A szabályzat kötelező érvényű valamennyi munkavállaló és külső szolgáltató számára, akik a szervezeti hálózatokat kezelik, konfigurálják, felügyelik vagy azokhoz kapcsolódnak, függetlenül attól, hogy a környezet helyszíni vagy felhőalapú.

2.3 A szervezet hálózataihoz csatlakozó valamennyi rendszernek és alkalmazásnak – elhelyezkedéstől vagy tulajdonjogtól függetlenül – meg kell felelnie a jelen hálózatbiztonsági követelményeknek.

3. Célkitűzések

3.1 A hálózatokon továbbított adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása erős hozzáférés-szabályozással, biztonságos útvonalválasztással és folyamatos felügyelettel.

3.2 A jogosulatlan hozzáférés, az oldalirányú mozgás és a hálózati erőforrásokkal való visszaélés megelőzése szegmentálás, zónabesorolás és peremvédelem alkalmazásával.

3.3 Az iparági legjobb gyakorlatokkal és fenyegetési információkkal összhangban álló, egységes hálózati konfigurációk fenntartása a változó kibertámadások elleni védelem érdekében.

3.4 A külső kommunikáció, a felhőkapcsolatok és a távoli hozzáférés védelme titkosított kommunikációs csatornákkal, szigorú hitelesítéssel és végpontellenőrzéssel.

3.5 A hálózati tevékenységek átláthatóságának biztosítása központi naplózással, valós idejű forgalomelemzéssel és automatizált riasztásokkal.

3.6 A jogszabályi megfelelés biztosítása azáltal, hogy valamennyi hálózati művelet összhangban áll az ISO/IEC 27001:2022, a GDPR, a NIS2, a DORA és a COBIT 2019 követelményeivel.

4. Szerepkörök és felelősségi körök

4.1 Információbiztonsági vezető

4.1.1 A szabályzat tulajdonosa, és biztosítja annak rendszeres felülvizsgálatát, valamint a szervezet átfogó kiberbiztonsági stratégiájával való összhangját.

4.1.2 Jóváhagyja a hálózati szegmentálási modelleket, az érzékeny rendszerekre vonatkozó tűzfalszabály-készleteket és a kivételkérelmeket.

4.2 Hálózatbiztonsági vezető / infrastruktúravédelmi vezető

4.2.1 Irányítja a hálózatvédelmi architektúrát, beleértve a tűzfalakat, a behatolásészlelő/-megelőző rendszereket (IDS/IPS), a VPN-eket és a biztonságos útvonalválasztást.

4.2.2 Felügyeli a hálózati szegmentálást, a VLAN-hozzárendeléseket, a forgalmi zónák kialakítását és a külső kapcsolódásokat.

4.2.3 Biztosítja a bejövő és kimenő forgalom szűrésének folyamatos felülvizsgálatát, valamint a Zero Trust elvek érvényesítését a hálózati rétegek között.

[... 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 Jelen szabályzatot a hálózatbiztonsági vezetőnek évente felül kell vizsgálnia az információbiztonsági vezetővel együttműködésben, és szükség esetén frissítenie kell az alábbiak alapján:

9.1.1 kialakuló kockázatok (pl. új támadási technikák, protokollsérülékenységek)

9.1.2 az infrastruktúrát érintő változások (pl. felhőmigrációk, SD-WAN bevezetések)

9.1.3 a hálózatvédelemre hatással lévő jogszabályi vagy szabványváltozások

9.1.4 auditmegállapítások, incidens-trendek vagy a kontrollok által okozott teljesítményromlás

9.2 Felülvizsgálatot kell kezdeményezni az alábbi esetekben is:

9.2.1 jelentős hálózati architektúraváltozások

9.2.2 új tűzfal-, VPN- vagy felhőhálózati platformok bevezetése

9.2.3 kulcsfontosságú vagyonelemek vagy megbízható zónák kivonása

9.3 A frissítéseket az IBIR dokumentumkezelési nyilvántartásában kell rögzíteni, és az alábbiak részére kell kommunikálni:

9.3.1 infrastruktúra- és hálózatüzemeltetés

9.3.2 SOC és biztonságmérnöki csapatok

9.3.3 olyan alkalmazási csapatok, amelyek rendszerei hálózati adatfolyamoktól függenek

9.3.4 valamennyi aktív összeköttetéssel rendelkező külső beszállító

9.4 A szabályzat minden korábbi verzióját biztonságosan archiválni kell, változáselőzményi megjegyzésekkel ellátva az auditálhatóság és a változások visszakövethetőségének biztosítása érdekében.

10. Kapcsolódó szabályzatok és összefüggések

10.1 P1 – Információbiztonsági szabályzat. Meghatározza az alapvető biztonsági elveket, és előírja a rétegezett védelmet, beleértve a hálózatalapú hozzáférési és fenyegetéskezelési kontrollokat is.

10.2 P4 – Hozzáférés-szabályozási szabályzat. Biztosítja, hogy a hálózati szegmentálás összhangban álljon a felhasználói szerepkörökkel, a legkisebb jogosultság elvével és a hozzáférés-kiosztási szabályokkal.

10.3 P5 – Változáskezelési szabályzat. Dokumentált és auditálható folyamaton keresztül szabályozza a tűzfalmódosításokat, a VPN-szabályok módosítását és az útválasztási változásokat.

10.4 P12 – Eszközkezelési szabályzat. Támogatja a hálózatra kapcsolt rendszerek azonosítását és osztályozását, és biztosítja, hogy minden csatlakoztatott eszközt a szabályzatban meghatározott hatály szerint kezeljenek.

10.5 P22 – Naplózási és felügyeleti szabályzat. Szabályozza a hálózati naplók – ideértve a tűzfaleseményeket, a hozzáférési kísérleteket és az anomáliaészleléseket – gyűjtését, korrelációját és megőrzését.

10.6 P30 – Incidenskezelési szabályzat. Meghatározza az eszkalációs, elszigetelési és felszámolási eljárásokat a hálózaton terjedő fenyegetések vagy behatolások – például DDoS, oldalirányú mozgás vagy jogosulatlan hozzáférés – kezelésére.

11. Hivatkozott szabványok és keretrendszerek

11.1 Jelen szabályzat összhangban áll azokkal a nemzetközi szabványokkal és szabályozói követelményekkel, amelyek meghatározzák a biztonságos hálózati működést, a szegmentálást, a peremvédelmet és a biztonságos távoli hozzáférést.

11.2 ISO/IEC 27001

11.2.1 8.1 pont – Működéstervezés és -szabályozás: előírja, hogy a technikai kontrollokat, beleértve a hálózatvédelmi intézkedéseket is, be kell építeni a működési folyamatokba.

11.3 ISO/IEC 27002:2022

11.3.1 8.20–8. kontrollok. Iránymutatást adnak a hálózatok védelmére, a szolgáltatások szegmentálására, valamint a hálózati szolgáltatások hozzáférés-szabályozással és felügyelettel történő védelmére.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 – Peremvédelem: előírja a peremvédelmi kontrollokat, a szegmentálást és a biztonságos összekapcsolásokat.

11.4.2 AC-4 – Információáramlás kikényszerítése: támogatja a zónakezelést és a szabályalapú forgalomkorlátozásokat.

11.4.3 SC-32 – Információs rendszerek particionálása: elősegíti az információs rendszerek logikai elkülönítését.

11.5 GDPR (2016/679)

11.5.1 32. cikk – Az adatkezelés biztonsága: előírja olyan technikai intézkedések alkalmazását, mint a tűzfalak és a szegmentálás, a személyes adatok védelme érdekében.

11.6 NIS2 irányelv (2022/2555)

11.6.1 21. cikk (2) bekezdés d) pont: hatékony hálózati és információs rendszervédelmet, peremvédelmet, biztonságos konfigurációt és elkülönítési kontrollokat ír elő.

11.7 DORA rendelet (2022/2554)

11.7.1 9. cikk – IKT-kockázatkezelés: kötelezi a pénzügyi szervezeteket a hálózatok és összekapcsolások jogosulatlan hozzáféréssel, adatszivárgással és működési zavarokkal szembeni védelmére.

11.8 COBIT 2019

11.8.1 DSS01.03 – Infrastruktúra felügyelete: proaktív kontrollt ír elő a hálózat állapota és kapcsolódása felett.

11.8.2 DSS05.01 – Védelem kártevők ellen: a terjedés minimalizálása érdekében szegmentálási és peremvédelmi kontrollokat is magában foglal.

11.8.3 MEA03 – A megfelelés nyomon követése, értékelése és vizsgálata: megerősíti a hálózati szabályzat érvényesítését és a megfelelőségértékeléseket.