					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P38					Dokumentum címe: **Biztonságos kommunikációs és többtényezős hitelesítési 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	5.30, 5.31, 8.24	
ISO/IEC 27002:2022	5.15, 5.17, 5.18, 8.24, 8.28	
NIST SP 800-53 Rev.5	IA-2, IA-3, IA-5, IA-8, SC-12, SC-13, SC-31	
GDPR	32. cikk (1) bekezdés b) pont	
NIS2 irányelv	21. cikk (2) bekezdés j) pont	
DORA-rendelet	9. cikk (2) bekezdés d) pont, 11. cikk	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Cél

1.1 Meghatározza a többtényezős hitelesítési vagy folyamatos hitelesítési megoldások rendszerhozzáférés során történő alkalmazásának követelményeit, összhangban a NIS2 irányelv 21. cikk (2) bekezdés j) pontjával.

1.2 Kontrollokat határoz meg a biztonságos hang-, videó-, szöveges és vészhelyzeti kommunikációra az információk bizalmasságának és sértetlenségének védelme érdekében.

2. Hatály

2.1 Jelen szabályzat kiterjed a szervezet által használt valamennyi hitelesítési mechanizmusra és kommunikációs rendszerre, beleértve a hanghívásokat, a videókonferenciát, az üzenetküldést és a vészhelyzeti értesítési rendszereket.

2.2 A szabályzat valamennyi munkavállalóra, vállalkozóra, valamint minden olyan külső félre vonatkozik, aki a szervezet kommunikációs csatornáit használja, vagy hozzáfér a szervezet hálózati és információs rendszereihez.

3. Célkitűzések

3.1 Biztosítani, hogy a rendszerekhez kizárólag megfelelően hitelesített felhasználók férjenek hozzá, csökkentve a jogosulatlan hozzáférés kockázatát a többtényezős hitelesítés bevezetésével.

3.2 Biztosítani, hogy a belső és vészhelyzeti kommunikáció biztonságos módszerekkel, például titkosított kommunikációs csatornákon történjen, megelőzve a lehallgatást és a manipulációt.

3.3 Megfelelni a NIS2 irányelv erős hitelesítésre és biztonságos kommunikációra vonatkozó követelményeinek, erősítve az általános kiberrezilienciát.

4. Szerepkörök és felelősségek

4.1 Információbiztonsági vezető / IT-biztonság: Meghatározza és fenntartja a többtényezős hitelesítési mechanizmusokat és a biztonságos kommunikációs eszközöket; biztosítja a jelen szabályzat műszaki végrehajtását.

4.2 Informatikai rendszergazdák: Bevezetik a többtényezős hitelesítést az érintett rendszerekben, és konfigurálják a jóváhagyott biztonságos kommunikációs platformokat; nyomon követik a megfelelést.

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

9. Nyomon követés és audit

9.1 Az IT-biztonság köteles folyamatosan figyelemmel kísérni a hitelesítési naplókat az egytényezős bejelentkezési kísérletek, illetve a rendellenes többtényezős hitelesítési hibák azonosítása érdekében. A biztonságos kommunikációs rendszerek naplóit — ahol ez alkalmazható — szintén figyelemmel kell kísérni a jogosulatlan hozzáférési kísérletek vagy konfigurációváltozások észlelése érdekében.

9.2 A belső audit évente felülvizsgálja a többtényezős hitelesítés bevezetésének megfelelőségét annak ellenőrzésével, hogy minden kritikus rendszer kikényszeríti a többtényezős hitelesítést, és megerősíti, hogy érzékeny kommunikációra kizárólag jóváhagyott biztonságos csatornákat használnak. Az auditmegállapításokat ajánlásokkal együtt a vezetés részére kell jelenteni.

10. Felülvizsgálat és karbantartás

10.1 Jelen szabályzatot legalább évente, továbbá minden olyan jelentős biztonsági incidens vagy újonnan azonosított kockázat esetén felül kell vizsgálni, amely a hitelesítéssel vagy a kommunikációval kapcsolatos (pl. a többtényezős hitelesítést érintő új támadási vektorok, nem biztonságos kommunikációs gyakorlat feltárása).

10.2 A módosításokat szükség szerint végre kell hajtani a fejlődő technológiák kezelésére (pl. robusztusabb folyamatos hitelesítési megoldások bevezetése), illetve a frissített szabályozói iránymutatásoknak való megfelelés érdekében (például a biztonságos kommunikációra vonatkozó jövőbeli ENISA-ajánlások alapján).

11. Kapcsolódó szabályzatok és összefüggések

11.1 P01 – Információbiztonsági szabályzat. Előírja a szervezetszintű hitelesítési és kommunikációvédelmi intézkedéseket.

11.2 P04 – Hozzáférés-szabályozási szabályzat. Meghatározza azt a hozzáférés-kezelési keretrendszert, amelyet a P38 szerinti többtényezős hitelesítés érvényesít.

11.3 P11 – Felhasználói fiók- és jogosultságkezelési szabályzat. Összekapcsolja a többtényezős hitelesítést az emelt jogosultságú hozzáférések életciklusával.

11.4 P18 – Kriptográfiai kontrollok szabályzata. Jóváhagyott kriptográfiai és kulcskezelési előírásokat biztosít a biztonságos kommunikációhoz.

11.5 P21 – Hálózatbiztonsági szabályzat. Védi a hang-, videó- és üzenetküldési forgalomhoz használt átviteli csatornákat.

11.6 P22 – Naplózási és felügyeleti szabályzat. Figyelemmel kíséri a hitelesítési eseményeket és a biztonságos csatornák használatát.

11.7 P32 – Üzletmenet-folytonossági és katasztrófa utáni helyreállítási szabályzat. Biztosítja a vészhelyzeti kommunikáció biztonságát válsághelyzetek során.

11.8 P08 – Információbiztonsági tudatossági és képzési szabályzat. Képzi a felhasználókat a többtényezős hitelesítésre és a kommunikációs csatornák biztonságos használatára.

12. Hivatkozások

12.1 NIS2 irányelv (EU 2022/2555), 21. cikk (2) bekezdés j) pont (többtényezős hitelesítés és biztonságos kommunikáció alkalmazása)

12.2 A Bizottság (EU) 2024/2690 végrehajtási rendelete, 11. melléklet szakasz (hozzáférés-szabályozási követelmények, beleértve az emelt jogosultságú fiókokra vonatkozó többtényezős hitelesítést)

12.3 ISO/IEC 27001:2022 és ISO/IEC 27002: