					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P18					Dokumentum címe: **Kriptográfiai kontrollok szabályzata**							
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	Kontrollok 8.24, 8.25, 8	-
NIST SP 800-53 Rev.5	SC-12–SC-17, SC-28, SC-28(1), SC-12(3)	-
GDPR	32. cikk, 33–34. cikk, 83. preambulumbekezdés	-
NIS2 irányelv	21. cikk (2) bekezdés d) pont	-
DORA-rendelet	6. cikk (2) bekezdés d) pont, 11. cikk (1) bekezdés c) pont	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Cél

1.1 Jelen szabályzat meghatározza a kriptográfiai kontrollok szervezeten belüli, biztonságos és a megfelelőségi követelményekkel összhangban álló alkalmazására vonatkozó kötelező előírásokat annak érdekében, hogy biztosított legyen az érzékeny és szabályozott információk bizalmassága, sértetlensége és hitelessége.

1.2 A kriptográfia alkalmazása megalapozza a bizalmat az adatbiztonsági működésben, támogatja a biztonságos kommunikációt, érvényesíti a hozzáférés-szabályozást, valamint lehetővé teszi a jogszabályi megfelelés teljesítését hatékony titkosítási és kulcskezelési gyakorlatok révén.

1.3 Jelen szabályzat összhangban áll az ISO/IEC 27001:2022 8.1 pontjával és az A. melléklet 8.24 kontrolljával, továbbá támogatja a GDPR 32. cikke, a DORA-rendelet 6. cikk (2) bekezdés d) pontja és a NIS2 irányelv 21. cikke szerinti jogi és működési kötelezettségek teljesítését. Emellett támogatja a COBIT 2019 adatvagyon-védelemre és biztonsági szolgáltatásokra vonatkozó célkitűzéseit is.

2. Hatály

2.1 Jelen szabályzat valamennyi szervezeti egységre, üzleti funkcióra, munkatársra és harmadik fél szolgáltatóra alkalmazandó, akik kriptográfiai eszközök és módszerek használatában, adminisztrációjában vagy bevezetésében részt vesznek.

2.2 Az érintett környezetek közé tartoznak az éles, fejlesztési, tesztelési, biztonsági mentési és katasztrófa utáni helyreállítási rendszerek, amelyekben érzékeny adatok továbbítása, kezelése vagy tárolása történik.

2.3 A hatály kiterjed valamennyi kriptográfiai komponensre és felhasználási esetre, beleértve többek között az alábbiakat:

2.3.1 Szimmetrikus és aszimmetrikus titkosítás

2.3.2 Digitális aláírások és tanúsítványok

2.3.3 Hash algoritmusok

2.3.4 Biztonságos kulcsgenerálás, kulcsterjesztés és kulcsmegsemmisítés

2.3.5 Transport Layer Security (TLS), teljes lemeztitkosítás (FDE) és API-szintű titkosítás

2.3.6 Biztonságos elemek, például hardverbiztonsági modulok (HSM-ek), megbízható platformmodulok (TPM-ek) és kulcskezelő rendszerek (KMS)

2.4 Jelen szabályzat a kriptográfia használatát az alábbi területeken szabályozza:

2.4.1 Bizalmas, szigorúan bizalmas vagy szabályozott besorolású adatok

2.4.2 Hitelesítés és digitális identitás ellenőrzése

2.4.3 Biztonságos kommunikáció külső felekkel

2.4.4 Kulcsőrzési felelősség és kettős kontrollmechanizmusok

3. Célkitűzések

3.1 Biztosítani kell, hogy a kriptográfiai technológiák kiválasztása, jóváhagyása, bevezetése és fenntartása az üzleti kockázatokkal, a nemzetközi szabványokkal és a szabályozói előírásokkal összhangban történjen.

3.2 Szabványosított irányítási struktúrát kell kialakítani a kriptográfiai szolgáltatások kezelésére, beleértve a bevezetésért, ellenőrzésért és kivételkezelésért fennálló egyértelmű elszámoltathatóságot.

3.3 Formális jóváhagyási és felülvizsgálati folyamat révén meg kell előzni a kriptográfiai algoritmusok és kontrollok jogosulatlan használatát, hibás konfigurációját vagy elavulását.

3.4 Biztosítani kell, hogy a kriptográfiai kontrollok már a rendszertervezési szakaszban beépüljenek, és azokat rendszeresen ellenőrizzék az adatkitettség, a kulcsok kompromittálódása vagy a protokollok gyengülésének megelőzése érdekében.

3.5 Érvényesíteni kell valamennyi kriptográfiai kulcs életciklus-kezelését, beleértve a létrehozást, tárolást, használatot, rotációt, visszavonást és biztonságos megsemmisítést.

3.6 Meg kell felelni a titkosítást és a biztonságos adatkezelést előíró nemzetközi és regionális szabályozásoknak, beleértve a GDPR-t, a DORA-rendeletet, a NIS2 irányelvet és a COBIT 2019-et.

4. Szerepkörök és felelősségi körök

4.1 IBIR-vezető / információbiztonsági vezető

4.1.1 Felelős jelen szabályzatért, és biztosítja annak összhangját az IBIR-rel és az ISO/IEC 27001 A. melléklet 8.24 kontrolljával.

4.1.2 Jóváhagyja a kriptográfiai algoritmusok és kontrollok használatát, valamint biztosítja a megfelelést a teljes szervezetben.

4.2 Kriptográfiai üzemeltetési vezető / biztonsági architekt

4.2.1 Felel a kriptográfiai rendszerek napi működtetéséért és adminisztrációjáért.

4.2.2 Karbantartja a Jóváhagyott Kriptográfiai Módszerek Listáját (ACML) és a Kulcskezelési Nyilvántartást.

4.2.3 Elvégzi a Kriptográfiai Tervfelülvizsgálatokat (CDR), és értékeli az új kriptográfiai technológiákat.

[... 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 az IBIR-vezetőnek és a Kriptográfiai Üzemeltetési Vezetőnek évente felül kell vizsgálnia.

9.2 A felülvizsgálatot kiváltó okok többek között a következők:

9.2.1 Kriptográfiai sérülékenységek azonosítása (pl. algoritmus-visszaminősítés, kvantumalapú támadások)

9.2.2 Olyan szabályozói változások, amelyek a titkosítási szabványok frissítését teszik szükségessé

9.2.3 Olyan működési vagy auditmegállapítások, amelyek szabályozási hiányosságokra mutatnak rá

9.2.4 Kriptográfiai eszközök frissítése vagy architekturális változások

9.3 A frissítéseket verziókezeléssel kell rögzíteni az IBIR dokumentumkontroll-nyilvántartásában, és közölni kell az alábbiakkal:

9.3.1 Valamennyi rendszergazdával, aki kriptográfiai hozzáférési szerepkörrel rendelkezik

9.3.2 A fejlesztői csapatokkal és a DevSecOps vezetőkkel

9.3.3 Azokkal a harmadik fél szolgáltatókkal, amelyekre szerződéses titkosítási kötelezettségek vonatkoznak

9.4 Az IBIR-csapatnak biztosítania kell, hogy a hatályon kívül helyezett verziók archiválásra kerüljenek, és azokra működési eljárások már ne hivatkozzanak.

10. Kapcsolódó szabályzatok és összefüggések

10.1 P1 - Információbiztonsági szabályzat. Alapvető irányítást biztosít valamennyi biztonsági intézkedéshez, beleértve a kriptográfiai kontrollok alkalmazását, az eszközvédelem biztosítását és a biztonságos kommunikációt.

10.2 P4 - Hozzáférés-szabályozási szabályzat. Biztosítja, hogy a kriptográfiai anyagokhoz és titkosításkezelő rendszerekhez való logikai hozzáférés szigorúan korlátozott legyen a legkisebb jogosultság elve és a feladatkörök elkülönítése alapján.

10.3 P6 - Kockázatkezelési szabályzat. Támogatja a kriptográfiai kontrollokkal kapcsolatos kockázatok értékelését, és dokumentálja a kivételekre, az algoritmusok elavulására vagy a kulcsok kompromittálódására vonatkozó kockázatkezelési stratégiát.

10.4 P12 - Eszközkezelési szabályzat. Előírja az érzékeny adatok és hardvereszközök osztályozását, amely közvetlenül meghatározza a kriptográfiai követelményeket és a kulcsőrzési kötelezettségeket.

10.5 P13 - Adatosztályozási és jelölési szabályzat. Meghatározza azokat az osztályozási szinteket (pl. Bizalmas, szabályozott), amelyek konkrét titkosítási követelményeket váltanak ki átvitel és tárolás során.

10.6 P14 - Adatmegőrzési és selejtezési szabályzat. Meghatározza a titkosított tárolóadathordozók és a kriptográfiai kulcsanyagok életciklusuk végén történő biztonságos megsemmisítésének eljárásait.

10.7 P30 - Incidenskezelési szabályzat. Ismerteti a szervezet válaszstratégiáját a kulcsok kompromittálódása, a tanúsítványok nem megfelelő használata vagy feltételezett algoritmikus sérülékenységek esetére, beleértve a gyors visszavonást és az incidensbejelentést.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 8.1 pont - Működési tervezés és szabályozás: Előírja a technikai biztonsági kontrollok, köztük a kriptográfiai intézkedések alkalmazását a működési védelmi intézkedések részeként.

11.2 ISO/IEC 27002:2022

11.2.1 8.24, 8.25 és 8 kontrollok: Bevezetési útmutatást adnak a kriptográfiai kontrollok céljaira, az algoritmusok kiválasztására, a protokollok érvényesítésére és a tanúsítványok életciklus-kezelésére vonatkozóan.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-12 - Kriptográfiai kulcsok létrehozása: Biztosítja a titkosítási kulcsok biztonságos előállítását és cseréjét. A P18 meghatározza, hogyan kell a szimmetrikus és aszimmetrikus kulcsokat jóváhagyott algoritmusokkal és protokollokkal létrehozni és cserélni.

11.3.2 SC-13 - Kriptográfiai védelem: Előírja a kriptográfia használatát az információk bizalmasságának és sértetlenségének védelme érdekében. A P18 az adatosztályozás alapján érvényesíti a tárolás közbeni és az átvitel közbeni titkosítást, a NIST FIPS 140-3-mal összhangban álló algoritmusszabványokkal.

11.3.3 SC-17 - Nyilvános kulcsú infrastruktúra (PKI) tanúsítványok: Előírja a PKI bevezetését a hitelesítés és a digitális aláírások támogatására. A P18 meghatározza a PKI használatát a kommunikáció, a rendszeridentitások és az adminisztratív hozzáférés védelme érdekében.

11.3.4 SC-28, SC-28(1) - Információk védelme tárolás és átvitel közben: Előírja az adatok titkosítását, ha azok tárolása vagy továbbítása nem megbízható hálózatokon történik. A P18 meghatározza a TLS, a VPN-alagutak, a teljes lemeztitkosítás és az érzékeny adatok biztonságos tárolási módszereinek alkalmazását.

11.3.5 SC-12(3) - Szimmetrikus kulcsgenerálás biztonságos tároláshoz és terjesztéshez: A szimmetrikus kulcsok biztonságos előállítására és kezelésére összpontosít. A P18 előírja erős véletlenszám-generátorok, kulcsrotációs szabályok és biztonságos kulcstárak használatát a kriptográfiai műveletekhez.

11.4 GDPR (2016/679)

11.4.1 32. cikk - Az adatkezelés biztonsága: Kifejezetten ajánlja a titkosítást mint a személyes adatok kockázatcsökkentő intézkedését.

11.4.2 83. preambulumbekezdés: Hangsúlyozza a titkosítást mint a jogosulatlan adathozzáférés megelőzését szolgáló kontrollt.

11.4.3 33. és 34. cikk: A hatékony titkosítás mentesítheti a szervezetet a kötelező incidensbejelentés alól.

11.5 NIS2 irányelv (2022/2555)

11.5.1 21. cikk (2) bekezdés d) pont: Előírja a szolgáltatások rendelkezésre állásának és sértetlenségének fenntartását szolgáló technikai és szervezeti intézkedéseket, beleértve a kriptográfiai védelmet is.

11.6 DORA-rendelet (2022/2554)

11.6.1 6. cikk (2) bekezdés d) pont: A pénzügyi intézményeknek biztosítaniuk kell az adatok védelmét, többek között a kritikus információk erős titkosításával.

11.6.2 11. cikk (1) bekezdés c) pont: Előírja a biztonságos adatkezelési kontrollokat az IKT-harmadik fél szolgáltatók számára.

11.7 COBIT 2019

11.7.1 DSS05.01 - Információs vagyon védelme: Előírja a titkosítás és a kulcskezelés használatát az adatok jogosulatlan hozzáféréssel szembeni védelme érdekében.

11.7.2 DSS06.06 - Menedzselt biztonsági tesztelés: A sérülékenységvizsgálatok részeként javasolja a kriptográfiai megfelelés ellenőrzését.

11.7.3 MEA03 - Megfelelés monitorozása, értékelése és vizsgálata: Előírja a kriptográfiai kontrollok hatékonyságának folyamatos biztosítását.