					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P18S					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	8.24. és 8.25. kontroll	
NIST SP 800-53 Rev. 5	SC-12–SC-17	
EU NIS2 irányelv	21. cikk (2) bekezdés d) és e) pont	
EU DORA-rendelet	6. cikk (2) bekezdés d) pont; 9. cikk (2) bekezdés f) pont	
COBIT 2019	DSS05.01, APO13	
EU GDPR	32. cikk (1) bekezdés a) pont; 34. cikk	

1. Cél

1.1 Ez a szabályzat meghatározza az üzleti és személyes adatok bizalmasságának, sértetlenségének és hitelességének védelmét szolgáló titkosítási és kriptográfiai kontrollok alkalmazására vonatkozó kötelező követelményeket.

1.2 Biztosítja, hogy a kriptográfiai megoldásokat a KKV-környezetben működtetett rendszerekben, eszközökön és felhőszolgáltatásokban megfelelően alkalmazzák.

1.3 Ez a szabályzat közvetlenül támogatja az ISO/IEC 27001:2022 szerinti tanúsítást, és elősegíti, hogy a szervezet teljesítse a GDPR, az EU NIS2 irányelv és a DORA-rendelet szerinti jogi kötelezettségeit.

1.4 A szabályzat hatálya alá tartozó kriptográfiai kontrollok közé tartoznak az adattitkosítás, a tanúsítványkezelés, a kulcsok biztonságos kezelése és a titkosított biztonsági mentések.

2. Hatály

2.1 Ez a szabályzat az alábbiakra alkalmazandó:

2.1.1 a vállalati adatokat kezelő valamennyi munkavállalóra, vállalkozóra és harmadik felekre

2.1.2 minden olyan üzleti rendszerre, végpontra és felhőplatformra, amelyet bizalmas információk tárolására, továbbítására vagy elérésére használnak

2.1.3 a szervezet adatosztályozási szabályzata szerint besorolt valamennyi személyes, pénzügyi, jogi vagy érzékeny nyilvántartásra

2.1.4 minden kriptográfiai kontrollra, beleértve a titkosítási módszereket, kulcsokat, jelszavakat, tanúsítványokat és biztonsági modulokat

2.2 Ez a szabályzat kiterjed a nyugalmi állapotban lévő adatokra, az átvitel alatt álló adatokra és a használatban lévő adatokra. Továbbá kiterjed a biztonsági mentésekre, az e-mailre, a külső adattovábbításokra és a nyilvánosan elérhető weboldalakra alkalmazott titkosításra.

3. Célkitűzések

3.1 Biztosítani kell, hogy az érzékeny és szabályozott adatokat mindenkor megfelelő kriptográfiai intézkedések védjék

3.2 Meg kell határozni a titkosítási eszközök kiválasztására, konfigurálására és kulcskezelésére vonatkozó felelősségi köröket

3.3 Meg kell előzni a jogosulatlan hozzáférést, a manipulációt és az adatszivárgást a biztonságos adatátviteli és tárolási kontrollok érvényesítésével

3.4 Meg kell felelni azoknak a jogi és szabályozói követelményeknek, amelyek a személyes és üzleti adatok titkosítását írják elő

3.5 Fenn kell tartani az üzemeltetési biztonságot és a rendelkezésre állást a tanúsítványok és a kriptográfiai kulcsok hatékony kezelésével

4. Szerepkörök és felelősségek

4.1 Ügyvezető

4.1.1 Jóváhagyja ezt a szabályzatot, és biztosítja a kriptográfiai követelmények érvényesítését

4.1.2 Felülvizsgálja a kivételeket, az incidensbejelentéseket és a beszállítók titkosítási kikötéseknek való megfelelőségét

4.1.3 Ellenőrzi, hogy a kiszervezett szolgáltatások és a felhőszolgáltatások megfelelnek-e a titkosítási szabványoknak

4.2 Informatikai szolgáltató / belső informatikai rendszergazda

4.2.1 Megvalósítja és fenntartja a titkosítási megoldásokat (pl. teljes lemezes titkosítás, SSL/TLS-tanúsítványok, VPN-ek)

4.2.2 Kezeli a kriptográfiai kulcsok életciklusát és a biztonságos tárolást biztosító megoldásokat

4.2.3 Beállítja és felügyeli a biztonsági mentések, weboldalak és eszközök védelmét szolgáló titkosítást

[... 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 E szabályzatot legalább évente egyszer felül kell vizsgálnia az ügyvezetőnek az informatikai szolgáltató / belső informatikai rendszergazda és az adatvédelmi vagy információbiztonsági koordinátor bevonásával.

9.2 A soron kívüli felülvizsgálat kiváltó okai

9.2.1 Felülvizsgálatot kell végezni akkor is, ha:

9.2.1.1 a kriptográfiai szabványok vagy protokollok megváltoznak (pl. egy algoritmus elavulása miatt)

9.2.1.2 új rendszereket vagy felhőszolgáltatásokat vezetnek be

9.2.1.3 egy biztonsági incidens vagy adatvédelmi incidens kriptográfiai kulcs vagy tanúsítvány kompromittálódásával jár

9.2.1.4 jogi vagy szabályozói változások érintik a titkosítási követelményeket

9.3 Verziókezelés és kommunikáció

9.3.1 Minden szabályzatmódosítást dokumentálni kell a verzionaplóban

9.3.2 A munkatársakat értesíteni kell a frissítésekről, a korábbi verziókat pedig archiválni kell

9.3.3 A legutóbb jóváhagyott verziót a központi szabályzattárban kell tárolni

10. Kapcsolódó szabályzatok és összefüggések

10.1 E szabályzatot az alábbi KKV-szabályzatokkal együtt kell alkalmazni:

10.1.1 P12S – Eszközkezelési szabályzat: biztosítja, hogy az osztályozott vagyonelemek esetében a tárolás, továbbítás és megsemmisítés során titkosítást alkalmazzanak.

10.1.2 P14S – Adatmegőrzési és megsemmisítési szabályzat: meghatározza a megőrzési időket, és előírja az adatok titkosított tárolását a biztonságos törlésükig.

10.1.3 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: összhangba hozza a titkosítást az adatvédelmi elvekkel és a GDPR 32. cikke szerinti szabályozói elvárásokkal.

10.1.4 P22S – Naplózási és felügyeleti szabályzat: előírja a kulcshasználat, a titkosítási hibák és a tanúsítványok lejáratának auditcélú naplózását.

10.1.5 P30S – Incidenskezelési szabályzat: részletezi a titkosítási hiba vagy a kulcsok kompromittálódása esetén követendő eszkalációs, elszigetelési és értesítési eljárásokat.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 8.1. pont – előírja a biztonsági kockázatok kezeléséhez szükséges operatív kontrollokat, ideértve a titkosítás bevezetését is.

11.2 ISO/IEC 27002

11.2.1 8.24. kontroll – meghatározza a titkosítás alkalmazásának követelményeit a bizalmasság és a sértetlenség biztosítása érdekében.

11.2.2 8.25. kontroll – meghatározza a kriptográfiai kulcsok és tanúsítványok biztonságos kezelésére vonatkozó követelményeket.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – meghatározza a kriptográfiai kulcsok létrehozására és ellenőrzésére vonatkozó követelményeket.

11.3.2 SC-13 – meghatározza a kriptográfiai kulcsgenerálás követelményeit.

11.3.3 SC-17 – meghatározza a nyilvános kulcsú infrastruktúra (PKI) és a tanúsítványok életciklus-kezelésének követelményeit.

11.3.4 SC-28 – előírja a tárolt adatok titkosítását.

11.3.5 SC-12–SC-17 kontrollcsalád – biztosítja a rendszerekben alkalmazott kriptográfiai védelem megfelelő megvalósítását.

11.4 EU GDPR

11.4.1 32. cikk (1) bekezdés a) pont – előírja, hogy a szervezeteknek technikai intézkedéseket, így titkosítást kell alkalmazniuk az adatok bizalmasságának biztosítására.

11.4.2 34. cikk – rögzíti, hogy a titkosítás mentesítheti a szervezetet az incidensbejelentési kötelezettség alól, ha az adatok jogosulatlan személyek számára nem voltak értelmezhetők.

11.5 EU NIS2 irányelv

11.5.1 21. cikk (2) bekezdés d) pont – előírja a rendszerek és a kommunikáció védelmét szolgáló hatékony titkosítást.

11.5.2 21. cikk (2) bekezdés e) pont – hangsúlyozza az adatok védelmét és a kiberfenyegetések titkosítással történő mérséklését.

11.6 EU DORA-rendelet

11.6.1 6. cikk (2) bekezdés d) pont – előírja, hogy az IKT-rendszerek biztonságos kommunikációs csatornákat és titkosítást alkalmazzanak.

11.6.2 9. cikk (2) bekezdés f) pont – kötelezi a pénzügyi szervezeteket erős titkosítás alkalmazására a digitális kommunikáció és az adatcsere védelme érdekében.

11.7 COBIT 2019

11.7.1 DSS05.01 – előírja az érzékeny információk védelmét titkosítás és kriptográfiai protokollok alkalmazásával.

11.7.2 APO13.02 – előírja a hatékony biztonsági kontrollok – ideértve a kriptográfiai védelmi intézkedéseket is – megvalósítását az információbiztonsági tervezés részeként.