					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P31S					Dokumentum címe: **Bizonyítékgyűjtési és forenzikai 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	6.1., 6.3. és 8. pont	Kockázatalapú tervezés, fejlesztési intézkedések és a bizonyítékok sértetlenségét támogató működési kontrollok
ISO/IEC 27002:2022	5.24–5.27. kontrollok	Iránymutatást ad a biztonságos kezeléshez, az incidenseket követő felülvizsgálatokhoz és a bizonyítékokon alapuló fejlesztésekhez
ISO/IEC 27035-3:2016	6.3., 6.4. és 7. pont	Előírja a digitális bizonyítékok megfelelő megtervezését, jogszerű gyűjtését és biztonságos kezelését, a bizonyítéklánc dokumentálásával együtt
NIST SP 800-53 Rev.5	IR-07, IR-08, AU-09, AU-12, PE-18	Forenzikus felkészültség, auditnaplók védelme és az incidenskezelésbe történő hatékony integráció
GDPR	33., 34. cikk	Dokumentálás és visszakövethetőség személyesadat-sértések esetén
NIS2 irányelv	23. cikk	Visszakövethető incidensjelentés és a bizonyítékok biztonságos kezelése
DORA-rendelet	17. cikk (1), 17. cikk (2)	Előírja az IKT-val kapcsolatos incidensekhez kapcsolódó bizonyítékok gyűjtését, tárolását és megőrzését, a forenzikus megbízhatóság biztosítását és a szabályozó hatósági megkeresések támogatását
COBIT 2019	DSS05.06, DSS05.07	Megbízható naplózás és strukturált bizonyítékkezelés a biztonságos, auditálható kivizsgálások érdekében

1. cél

1.1. Jelen szabályzat meghatározza, hogy a szervezet hogyan kezeli a biztonsági incidensekhez, adatvédelmi incidensekhez vagy belső vizsgálatokhoz kapcsolódó digitális bizonyítékokat. Biztosítja, hogy a bizonyítékok gyűjtése, tárolása és megőrzése jogilag megalapozott, valamint az auditra való felkészültséget támogató módon történjen, ezzel támogatva a belső döntéshozatalt és az esetleges külső eljárásokat is.

1.2. A szabályzat lehetővé teszi a kisebb szervezetek számára, hogy megőrizzék a naplók, fájlok és rendszerképek sértetlenségét, miközben igazolni tudják a kellő gondosságot az ISO/IEC 27001, a GDPR és a kapcsolódó szabványok követelményei szerint.

1.3. A szabályzat egyértelmű szerepkörök, folyamatok és megőrzési követelmények meghatározásával támogatja a forenzikus felkészültséget anélkül, hogy fejlett műszaki erőforrásokat vagy teljes munkaidős IT-csapatot igényelne.

2. hatály

2.1. Jelen szabályzat hatálya kiterjed:

2.1.1. minden olyan munkavállalóra, IT-szolgáltatóra és külső tanácsadóra, aki incidenskezelésben, kivizsgálásban vagy incidenselemzésben vesz részt,

2.1.2. a vállalat valamennyi rendszerére, ideértve a laptopokat, mobileszközöket, szervereket, e-mail-fiókokat, SaaS-platformokat és felhőalapú tárhelyeket (pl. Microsoft 365, Google Workspace),

2.1.3. minden olyan eseményre, amely belső fegyelmi intézkedéshez, jogi védelemhez, biztosítási igényhez vagy szabályozó hatósági eljáráshoz bizonyítékot igényel.

2.2. A szabályzat a tényleges és a feltételezett eseményekre egyaránt kiterjed, különösen az alábbi esetekben:

2.2.1. adatszivárgás,

2.2.2. belső fenyegetés vagy visszaélés,

2.2.3. biztonsági incidensek (pl. malware, jogosulatlan hozzáférés),

2.2.4. olyan ügyfélpanaszok, amelyek digitális ellenőrzést igényelnek,

2.2.5. szabályozó hatósági vagy bűnüldöző szervtől érkező megkeresések.

3. célkitűzések

3.1. Biztosítani kell, hogy minden bizonyíték gyűjtése és kezelése a sértetlenség, a hitelesség és a bizonyítéklánc megőrzésével történjen.

3.2. Meg kell előzni a kivizsgálásokhoz szükséges naplók, fájlok vagy rendszerképek véletlen módosítását, törlését vagy nem megfelelő kezelését.

3.3. Egységes és auditálható megközelítést kell biztosítani a bizonyítékkezeléshez, amely megfelel a jogi és szabályozási elvárásoknak (pl. GDPR szerinti incidensbejelentés, NIS2 szerinti visszakövethetőség).

3.4. Egyértelmű szerepköröket és felelősségeket kell meghatározni annak biztosítására, hogy a bizonyítékok rögzítése biztonsági incidensek során gyorsan, biztonságosan és jogszerűen történjen.

3.5. Támogatni kell a KKV-szintű forenzikus felkészültséget úgy, hogy az minimális komplexitással és a napi működés indokolatlan zavarása nélkül valósuljon meg.

4. szerepkörök és felelősségek

4.1. ügyvezető

4.1.1. Jóváhagy minden olyan formális vizsgálatot, amely bizonyítékgyűjtést igényel.

4.1.2. Felülvizsgálja és jóváhagyja azokat az incidensjelentéseket, amelyek lehetséges jogi vagy fegyelmi következményekkel járhatnak.

4.1.3. Dönt arról, hogy szükséges-e külső jogi tanácsadó vagy szabályozó hatóság értesítése.

4.1.4. Biztosítja a szabályzat rendszeres felülvizsgálatát és aktualizálását.

4.2. külső IT-szolgáltató / rendszergazda

4.2.1. A digitális bizonyítékokat biztonságos eljárások szerint gyűjti és őrzi meg.

4.2.2. Dokumentálja az időbélyegeket, a rendszeradatokat és a kezelési lépéseket.

4.2.3. Minden begyűjtött anyagot védett helyen tárol.

4.2.4. Szükség esetén támogatást nyújt a forenzikus elemzéshez.

[... 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 szabályzat-felülvizsgálat

9.1.1. Jelen szabályzatot az ügyvezetőnek legalább 12 havonta egyszer felül kell vizsgálnia annak megerősítésére, hogy:

9.1.1.1. összhangban van az ISO/IEC 27001 A mellékletében meghatározott kontrollokkal,

9.1.1.2. továbbra is releváns az aktuális digitális platformok és IT-szolgáltatások szempontjából,

9.1.1.3. a naplózási, bizonyítékmegőrzési és forenzikus felkészültségi eljárások megfelelőek.

9.2. A szabályzat felülvizsgálatát kiváltó események

9.2.1. A szabályzatot az alábbi esetekben is felül kell vizsgálni, és szükség szerint frissíteni kell:

9.2.1.1. minden olyan jelentős incidens után, amely bizonyítékgyűjtést igényelt,

9.2.1.2. sikertelen audit vagy olyan szabályozó hatósági megkeresés után, amely során a bizonyítékok sértetlensége megkérdőjeleződött,

9.2.1.3. új eszközök vagy eljárások bevezetése után incidenskezelési vagy rendszerfelügyeleti célból,

9.2.1.4. jogszabályi változások esetén (pl. frissített GDPR- vagy NIS2-iránymutatás).

9.3. Módosítások jóváhagyása és terjesztése

9.3.1. Minden módosítást az ügyvezetőnek felül kell vizsgálnia és jóvá kell hagynia.

9.3.2. A frissített változatot meg kell osztani:

9.3.2.1. a vizsgálatokban részt vevő IT-szolgáltatókkal és tanácsadókkal,

9.3.2.2. minden olyan munkatárssal, aki rendszeradminisztrációs felelősséggel rendelkezik.

9.3.3. A frissített példányt a vállalat szabályzatarchívumában meg kell őrizni, és kérésre az auditorok rendelkezésére kell bocsátani.

10. kapcsolódó szabályzatok és összefüggések

10.1. Jelen szabályzat az alábbi, KKV-kra szabott szabályzatokkal együtt értelmezendő:

10.1.1. P2S – Irányítási szerepkörök és felelősségek szabályzata: meghatározza az incidensvizsgálatokkal, a bizonyítékokkal kapcsolatos döntésekkel és a jogi eszkalációval kapcsolatos hatásköröket.

10.1.2. P4S – Hozzáférés-szabályozási szabályzat: biztosítja, hogy a vizsgálatok során csak felhatalmazott személyek férhessenek hozzá az érzékeny rendszerekhez és naplókhoz.

10.1.3. P22S – Naplózási és felügyeleti szabályzat: biztosítja a forenzikus bizonyítékként felhasznált alapadatokat, valamint meghatározza a megőrzési, hozzáférés-szabályozási és naplózási követelményeket.

10.1.4. P30S – Incidenskezelési szabályzat: kiváltja a bizonyítékgyűjtés szükségességét, és meghatározza a forenzikus megőrzéshez vezető működési folyamatot.

10.1.5. P17S – Adatvédelmi és magánszféra-védelmi szabályzat: biztosítja, hogy a bizonyítékként gyűjtött személyes adatok kezelése a GDPR és a kapcsolódó szabályozások szerint jogszerű legyen.

10.2. E szabályzatok együttesen támogatják a jogi megfelelés igazolhatóságát, a vizsgálatok sértetlenségét és a teljes ISO/IEC 27001:2022 szerinti auditra való felkészültséget.

11. hivatkozott szabványok és keretrendszerek

11.1. ISO/IEC 27001

11.1.1. 6.1. pont – A kockázatalapú tervezés magában foglalja a reagálási felkészültséget és a bizonyítékkezelési eljárásokat.

11.1.2. 6.3. pont – Támogatja az incidensekből származó bizonyítékokon alapuló fejlesztési intézkedéseket.

11.1.3. 8.1. pont – Előírja a bizonyítékok sértetlenségét biztosító működési kontrollokat.

11.2. ISO/IEC 27002

11.2.1. 5.24–5.27. kontrollok – Iránymutatást adnak a biztonságos kezeléshez, az incidenseket követő felülvizsgálatokhoz és a bizonyítékokon alapuló fejlesztésekhez.

11.3. ISO/IEC 27035-3

11.3.1. A 6.3., 6.4. és 7.3. pont előírja a digitális bizonyítékok megfelelő megtervezését, jogszerű gyűjtését és biztonságos kezelését az incidenskezelés során, beleértve a megőrzést és a bizonyítéklánc dokumentálását.

11.4. NIST SP 800-53 Rev. 5

11.4.1. Az IR-07, IR-08, AU-09 és AU-12 kontrollok biztosítják a forenzikus felkészültséget, az auditnaplók védelmét és a bizonyítékgyűjtés hatékony beépítését az incidenskezelési életciklusba.

11.5. NIST SP 800-86

11.5.1. Meghatározza a digitális bizonyítékok incidenskezelés során történő beszerzésének, elemzésének és védelmének legjobb gyakorlatait.

11.6. GDPR

11.6.1. A 33–34. cikk előírja az incidensek és bizonyítékok dokumentálását és visszakövethetőségét személyesadat-sértések bejelentése során.

11.7. NIS2 irányelv (2022/2555)

11.7.1. A 23. cikk visszakövethető incidensjelentést és a bizonyítékok biztonságos kezelését írja elő az alapvető és fontos szervezetek számára.

11.8. DORA-rendelet

11.8.1. A 17. cikk (1) előírja, hogy az IKT-val kapcsolatos incidensekhez kapcsolódó bizonyítékokat a forenzikus vizsgálatokat támogató módon gyűjtsék és tárolják.

11.8.2. A 17. cikk (2) előírja, hogy a pénzügyi szervezetek őrizzék meg a biztonsági eseményekhez kapcsolódó valamennyi releváns adatot és naplót, összhangban a forenzikus megbízhatósággal és a szabályozó hatósági megkeresésekkel.

11.9. COBIT 2019

11.9.1. DSS05.06 – Incidensek megfigyelése, észlelése és jelentése: hangsúlyozza a kivizsgálást támogató megbízható naplózást.

11.9.2. DSS05.07 – Incidensek kivizsgálása és intézkedés: strukturált bizonyítékkezelést ír elő a biztonságos és auditálható kivizsgálások érdekében.