					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P31					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	8. pont	
ISO/IEC 27002:2022	5.25–5.27. kontrollok, 8. pont	
ISO/IEC 27035:2016	1. és 3. rész	
NIST SP 800-53 Rev.5	IR-1–IR-9, AU-6, PL-2	
NIST SP 800-101 Rev.1	Mobil- és adathordozó-forenzika	Mobil- és adathordozó-forenzika
NIST SP 800-86	Forenzikus technikák integrálása	Forenzikus technikák integrálása az incidenskezelésbe
GDPR	5., 33–34. cikk	
NIS2 irányelv	23. cikk (1)–(4) bekezdés	
DORA-rendelet	17. cikk (1)–(3) bekezdés	
COBIT 2019	DSS01.07, DSS05 – Biztonsági szolgáltatások kezelése	

1. Cél

1.1 Jelen szabályzat meghatározza a tényleges vagy feltételezett biztonsági incidensek során alkalmazandó digitális bizonyítékok azonosítására, gyűjtésére, megőrzésére, elemzésére és megsemmisítésére vonatkozó strukturált és jogilag védhető keretrendszert.

1.2 A szabályzat biztosítja, hogy a forenzikus felkészültség és a bizonyítékkezelési folyamatok:

1.2.1 fenntartsák a bizonyítékok sértetlenségét és a bizonyítékláncot,

1.2.2 támogassák a belső vizsgálatokat, a jogi eljárásokat vagy a szabályozói jelentéstételt,

1.2.3 összhangban legyenek a nemzetközileg elfogadott forenzikus szabványokkal és a jogi elfogadhatóság követelményeivel.

1.3 A szabályzat támogatja a szervezet proaktív incidenskezelésre, jogszabályi megfelelésre és átlátható irányításra vonatkozó elkötelezettségét, a működési fennakadások minimalizálása mellett.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 valamennyi munkavállalóra, vállalkozóra, beszállítóra és szolgáltatóra, aki rendszergazdai, incidenskezelési vagy vizsgálati tevékenységben vesz részt,

2.1.2 valamennyi, a szervezet irányítása vagy szerződéses felelőssége alá tartozó végpontra, szerverre, alkalmazásra, hálózatra és felhőplatformra,

2.1.3 minden olyan incidensre vagy eseményre, amely bizonyítékkezelést igényel, ideértve:

2.1.3.1 a belső fenyegetéseket, adatsértéseket vagy csalásvizsgálatokat,

2.1.3.2 a rendszerek vagy hitelesítő adatok nem rendeltetésszerű használatát,

2.1.3.3 az operatív technológiai (OT) vagy ipari irányítási incidenseket,

2.1.3.4 a digitális eszközöket érintő fizikai hozzáférési szabálysértéseket.

2.2 A szabályzat kiterjed továbbá a harmadik fél forenzikus szolgáltatóival vagy a bűnüldöző szervekkel folytatott minden együttműködésre jogi eszkaláció vagy hatósági eljárás esetén.

3. Célkitűzések

3.1 Gyors, biztonságos és a szabályzattal összhangban álló bizonyítékgyűjtés biztosítása biztonsági események vagy vizsgálatok során.

3.2 Az összegyűjtött digitális bizonyítékok sértetlenségének, hitelességének és elfogadhatóságának megőrzése a hozzáférés, a naplózás és az ellenőrzési eljárások szigorú szabályozásával.

3.3 Annak biztosítása, hogy minden forenzikus tevékenység összhangban legyen a jogi és szabályozási kötelezettségekkel, beleértve az adatvédelmet, a munkajogot és a nemzetközi adattovábbítási korlátozásokat.

3.4 Az incidens utáni elemzés, a gyökérok meghatározása és a kontrollok fejlesztésének támogatása magas színvonalú forenzikus eredményekkel.

3.5 A forenzikus felkészültség integrálása az átfogó információbiztonság-irányítási rendszerbe (ISMS), támogatva az auditokat, az incidensbejelentéseket és a vezetői döntéshozatalt.

4. Szerepkörök és felelősségek

4.1 Információbiztonsági vezető

4.1.1 A szabályzat tulajdonosa, és biztosítja, hogy minden forenzikus művelet jogilag védhető, auditálható és kockázatalapú legyen.

4.1.2 Jóváhagyja a külső jogi szereplők és forenzikus szolgáltatók felé történő eszkalációt.

4.2 Forenzikus elemzők / incidenskezelők

4.2.1 Végzik a bizonyítékok gyűjtését, megőrzését és műszaki elemzését.

4.2.2 Biztosítják, hogy a bizonyítéklánc megfelelően rögzítésre kerüljön és fennmaradjon.

4.2.3 Dokumentálják a vizsgálatok során végzett valamennyi tevékenységet, megállapítást és az alkalmazott eszközbeállításokat.

[... 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 legalább évente felül kell vizsgálni, és szükség szerint frissíteni kell az alábbiak figyelembevételével:

9.1.1 a forenzikus eljárásokat vagy adatkezelést érintő jogszabályok, szabályozások vagy ítélkezési gyakorlat változásai,

9.1.2 az iparágban elismert forenzikus szabványok vagy eszközkészletek frissítései,

9.1.3 az incidenseket követő felülvizsgálatokból, jogvitákból vagy auditmegállapításokból származó tanulságok,

9.1.4 a vizsgálat alá vont platformokat, eszközöket vagy rendszereket érintő technológiai változások.

9.2 A felülvizsgálati folyamat tulajdonosa az információbiztonsági vezető, és a folyamatnak ki kell terjednie az alábbi területekkel való egyeztetésre:

9.2.1 jogi és megfelelőség,

9.2.2 adatvédelmi tisztviselő (DPO),

9.2.3 biztonsági üzemeltetés és forenzikus csapatok,

9.2.4 belső audit.

9.3 Minden módosítást:

9.3.1 verziókezelten kell nyilvántartani és a szabályzatarchívumban kell tárolni,

9.3.2 kommunikálni kell az érintett érdekelt felek felé, ideértve a forenzikus és reagáló csapatokat,

9.3.3 össze kell kapcsolni a vonatkozó működési eljárások és képzési anyagok frissítésével.

9.4 Soron kívüli felülvizsgálatot kell indítani minden olyan kritikus incidens után, amely bizonyítékok nem megfelelő kezelésével, a bizonyítéklánc hibájával vagy jogi elfogadhatósági problémával jár.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat összhangban áll az alábbi szervezeti szabályzatokkal, és azok támogatják annak alkalmazását:

10.1.1 P1 – Információbiztonsági szabályzat: meghatározza a vizsgálatok, a bizonyítékkezelés és az alkalmazandó jogszabályoknak való megfelelés alapvető követelményeit.

10.1.2 P5 – Változáskezelési szabályzat: biztosítja, hogy a vizsgálat alá vont rendszerek az aktív forenzikus folyamatok során ne módosuljanak.

10.1.3 P14 – Adatmegőrzési és megsemmisítési szabályzat: szabályozza a bizonyítékok és az ügyhöz kapcsolódó adatok biztonságos megsemmisítését és megőrzési határidejét.

10.1.4 P18 – Kriptográfiai kontrollok szabályzata: meghatározza az érzékeny vagy bizonyító erejű adatok tárolására és továbbítására vonatkozó titkosítási követelményeket.

10.1.5 P22 – Naplózási és felügyeleti szabályzat: biztosítja az eseménynaplók és telemetriai adatok rendelkezésre állását a bizonyítékgyűjtéshez és a forenzikus korrelációhoz.

10.1.6 P30 – Incidenskezelési szabályzat: meghatározza az incidensek elsődleges értékelését és azokat az eszkalációs útvonalakat, amelyek mentén a forenzikus eljárások megindulnak.

10.1.7 P33 – Audit- és megfelelésfelügyeleti szabályzat: rendszeres auditok útján ellenőrzi a forenzikus protokolloknak és a bizonyítéklánc követelményeinek való megfelelést.

11. Hivatkozott szabványok és keretrendszerek

11.1 Jelen szabályzat összhangban áll a nemzetközi forenzikus és incidenskezelési szabványokkal, biztosítva a bizonyítékok sértetlenségét, a jogi védhetőséget és a több joghatóságra kiterjedő megfelelést.

11.2 ISO/IEC 27001

11.2.1 8.1. pont – Támogatja a forenzikus felkészültség és a bizonyítékkezelési eljárások működéstervezését és -szabályozását.

11.3 ISO/IEC 27002

11.3.1 Az A melléklet 5.25. kontrollja – Felelősségek az incidenskezelésben: előírja az információbiztonsági incidensek és vizsgálatok kezeléséhez szükséges szerepkörök meghatározását.

11.3.2 Az A melléklet 5.26. kontrollja – Információbiztonsági események jelentése: támogatja az eseményhez kapcsolódó artefaktumok bizonyítékként történő összegyűjtését.

11.3.3 Az A melléklet 5.27. kontrollja – Reagálás információbiztonsági incidensekre: előírja a strukturált, bizonyítékalapú helyesbítő intézkedést és vizsgálatot.

11.3.4 Az A melléklet 8.27. kontrollja – Biztonságos fejlesztés és forenzika (ahol alkalmazandó): foglalkozik a rendszerek és eszközök védelmével a vizsgálatok során.

11.4 ISO/IEC 27035:2016 (1. és 3. rész)

11.4.1 Ismerteti az incidensek észlelésének, a reagálásnak és a forenzikus felkészültségnek az alapelveit, beleértve a tervezést, a bizonyítékláncot és az incidensekhez kapcsolódó bizonyítékok kezelését.

11.5 NIST SP 800-53 Rev.5

11.5.1 IR-1–IR-9, AU-6, PL-2: strukturált követelményeket határoz meg a biztonsági incidensek tervezésére, észlelésére, elemzésére, elkülönítésére és kezelésére. Támogatja a bizonyítékok

gyűjtését és auditálhatóságát (AU-6), valamint biztosítja az összhangot a rendszerbiztonsági és adatvédelmi tervekkel (PL-2) a forenzikus vizsgálatok során.

11.6 NIST SP 800-86

11.6.1 Útmutatást ad a forenzikus folyamatoknak a szélesebb incidenskezelési életciklusba történő integrálására és a forenzikus felkészültség biztosítására.

11.7 NIST SP 800-101 Rev.1

11.7.1 A digitális adathordozók és mobileszközök bizonyítékainak jogilag védhető módon történő gyűjtésére, megőrzésére és elemzésére vonatkozó legjobb gyakorlatokra összpontosít.

11.8 GDPR (2016/679)

11.8.1 5. cikk – A személyes adatok kezelésére vonatkozó alapelvek: alkalmazandó az olyan bizonyítékokra, amelyek személyes vagy érzékeny adatokat tartalmaznak, biztosítva az adattakarékosságot és a célhoz kötöttséget.

11.8.2 33–34. cikk – Adatsértés bejelentése: a forenzikus adatok támogatják az incidensbejelentési kötelezettségeknek és a jogi közzétételi folyamatoknak való megfelelést.

11.9 NIS2 irányelv (2022/2555)

11.9.1 23. cikk – Jelentéstételi kötelezettségek: a forenzikus dokumentáció és megállapítások támogatják az illetékes hatóságok felé történő időszerű és pontos incidensjelentést.

11.10 DORA-rendelet (2022/2554)

11.10.1 17. cikk – IKT-incidensjelentés: előírja a jelentős IKT-hoz kapcsolódó incidensek részletes gyökérokelemzését és a bizonyító erejű nyilvántartások vezetését, különösen a pénzügyi szektorban.

11.11 COBIT 2019

11.11.1 DSS01.07 – Biztonsági incidensek kezelése: előírja az incidensek dokumentálását és a vizsgálatok kellő alaposságát.

11.11.2 DSS05.04 – Biztonsági vizsgálatok kezelése: hangsúlyozza a digitális bizonyítékok megőrzését, valamint a fegyelmi és jogi intézkedések támogatását.