					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P22S					Dokumentum címe: **Naplózási és felügyeleti 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	Operatív kontrollok, beleértve a naplózást
ISO/IEC 27002:2022	8.15, 8.16, 8.17 kontrollok	Eseménynaplózás, védelem és felügyelet
NIST SP 800-53 Rev.5	AU-2–AU-12, SI-4	Auditnaplók tartalma és felülvizsgálata, megőrzés, anomáliaészlelés, riasztás
GDPR	5. cikk (1) bekezdés f) pont, 32. cikk, 33. cikk	Adatok bizalmassága és sértetlensége, technikai intézkedések és incidensbejelentés
NIS2 irányelv	21. cikk (2) bekezdés d) pont, 23. cikk	Anomáliaészlelést támogató naplózási mechanizmusok és incidensjelentés 24 órán belül
DORA-rendelet	10. cikk, 15. cikk	Operatív reziliencia, szolgáltatók felügyelete és naplózása
COBIT 2019	DSS01.03, DSS05.02	A tevékenységek visszakövethetősége, valamint a védelem naplózás és felügyelet útján

1. Cél

1.1 Jelen szabályzat kötelező naplózási és felügyeleti kontrollokat határoz meg a szervezet IT-rendszereinek biztonsága, elszámoltathatósága és működési sértetlensége érdekében.

1.2 Meghatározza a naplózandó eseménytípusokat, a naplók tárolásának és felülvizsgálatának módját, valamint a munkatársak és a szolgáltatók felelősségi köreit.

1.3 A naplózás és a felügyelet támogatja a fenyegetések észlelését, a megfelelőség biztosítását, az incidenskezelést és a forenzikus elemzést.

1.4 Jelen szabályzat lehetővé teszi, hogy a szervezet teljesítse az ISO/IEC 27001 operatív kontrollkövetelményeit, és támogassa az auditkészültséget, az ügyfélbizalmat, valamint a GDPR, a NIS2 és a DORA követelményeinek való megfelelést.

2. Hatály

2.1 Jelen szabályzat a szervezet valamennyi rendszerére és felhasználójára alkalmazandó, beleértve az alábbiakat:

2.1.1 munkaállomások, laptopok, szerverek, tűzfalak, kapcsolók, útválasztók és vezeték nélküli hozzáférési pontok

2.1.2 üzleti működéshez használt felhőszolgáltatások (pl. e-mail, fájltárolás, biztonsági mentések, együttműködési eszközök)

2.1.3 vírusvédelmi szoftverek, alkalmazások, operációs rendszerek és hálózati eszközök naplózási funkciói

2.1.4 valamennyi munkavállaló, vállalkozó és menedzselt szolgáltató (MSP), aki rendszereket használ vagy adminisztrál

2.1.5 minden olyan helyszín, ahol a vállalat IT-rendszereit használják, ideértve a távoli, hibrid vagy BYOD (saját eszköz használata) környezeteket is

2.2 A szabályzat kiterjed továbbá a harmadik fél által nyújtott szolgáltatások által előállított naplókra is, amennyiben a szervezet adminisztratív hozzáféréssel vagy auditjoggal rendelkezik.

3. Célkitűzések

3.1 A rendszertevékenységek naplózásának biztosítása, ideértve a hitelesítést, a konfigurációváltozásokat, az érzékeny adatokhoz való hozzáférést és a biztonsági riasztásokat

3.2 Biztonságos és pontos naplók fenntartása a szabályzatsértések, rendszerhibák vagy jogosulatlan műveletek észlelése érdekében

3.3 A naplók gyors felülvizsgálatának biztosítása incidensek, kivizsgálások és auditok során

3.4 Az időszinkronizálás biztosítása a naplóadatok sértetlensége és korrelálhatósága érdekében

3.5 A naplók védelme a manipulációval, elvesztéssel vagy idő előtti törléssel szemben

3.6 A rendszer-elszámoltathatóságra, visszakövethetőségre és incidenskezelésre vonatkozó jogi és szabályozási kötelezettségek teljesítése

4. Szerepkörök és felelősségi körök

4.1 Ügyvezető

4.1.1 Jóváhagyja jelen szabályzatot, és biztosítja annak végrehajtását valamennyi üzleti rendszerben.

4.1.2 Felülvizsgálja az IT vagy az adatvédelmi funkció által jelentett magas súlyosságú riasztásokat és jelentős auditmegállapításokat.

4.1.3 Jóváhagyja azokat a kivételeket, amikor a naplózás vagy a megőrzés technikailag nem kényszeríthető ki.

4.2 IT-támogatási szolgáltató / belső IT-felelős

4.2.1 Bevezeti és konfigurálja a naplózást az operációs rendszerek, hálózati eszközök, vírusvédelmi megoldások és kulcsfontosságú alkalmazások esetében.

4.2.2 Biztosítja a naplók megőrzését, biztonsági mentését és módosítás elleni védelmét.

4.2.3 Ütemezetten felülvizsgálja a naplókat, és kivizsgálja a gyanús vagy jogosulatlan tevékenységeket.

4.2.4 Fenntartja azokat a riasztási mechanizmusokat, amelyek jelzik a rendellenes működést vagy a behatolásra utaló jeleket.

[... 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 Jelen szabályzatot legalább évente egyszer felül kell vizsgálnia az ügyvezetőnek az IT-támogatási szolgáltató és az adatvédelmi koordinátor támogatásával.

9.2 Felülvizsgálati kiváltó okok

9.2.1 Soron kívüli felülvizsgálatot kell végezni az alábbi esetekben:

9.2.1.1 belső vagy külső auditok naplózással kapcsolatos megállapításai esetén

9.2.1.2 olyan biztonsági incidensek esetén, ahol a naplók hiányoztak, sérültek vagy nem voltak elegendők

9.2.1.3 az IT-infrastruktúra lényeges változásai esetén (pl. átállás felhőalapú naplózási platformokra)

9.2.1.4 jogi vagy szabályozási kötelezettségek változása esetén (pl. GDPR, NIS2, DORA)

9.3 Verziókezelés

9.3.1 Jelen szabályzat minden módosítását verziószámmal, dátummal és a módosítások összefoglalásával kell rögzíteni.

9.3.2 A korábbi verziókat archiválni kell, és legalább 3 évig meg kell őrizni.

9.3.3 A frissített szabályzatokat közölni kell az érintett érdekelt felekkel, különösen a rendszerszintű hozzáféréssel rendelkezőkkel.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat közvetlenül támogatja az alábbi KKV információbiztonsági szabályzatokat, és azok is támogatják e szabályzat végrehajtását:

10.1.1 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: Biztosítja, hogy a személyes adatokat tartalmazó naplóadatok kezelése a GDPR követelményeivel összhangban, megfelelő sértetlenségi, megőrzési és hozzáférés-védelmi intézkedések mellett történjen.

10.1.2 P21S – Hálózatbiztonsági szabályzat: Alapot biztosít a tűzfalakkal, vezeték nélküli hozzáféréssel, VPN-ekkel és a szegmentálás felügyeletével kapcsolatos naplók rögzítéséhez.

10.1.3 P24S – Biztonságos fejlesztési szabályzat: Biztosítja, hogy az alkalmazásnaplók (pl. bejelentkezési kísérletek, hibák és kivételek) beépüljenek a szoftvertervezésbe és az üzemeltetésbe.

10.1.4 P30S – Incidenskezelési szabályzat: A pontos és teljes naplóadatokra támaszkodik az információbiztonsági események észleléséhez, elemzéséhez és kezeléséhez.

10.1.5 P23S – Időszinkronizálási szabályzat: Biztosítja a következetes és visszakövethető időbélyegeket valamennyi rendszerben, lehetővé téve a naplók korrelációját a kivizsgálások során.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 8.1 pont – Előírja az információbiztonsági kockázatok csökkentését szolgáló operatív kontrollok bevezetését, beleértve a naplózást is.

11.2 ISO/IEC 27002

11.2.1 8.15 kontroll – Előírja az eseménynaplózást az anomáliák észlelésének és az elszámoltathatóságnak a támogatására.

11.2.2 8.16 kontroll – Előírja a naplók védelmét a manipulációval és a jogosulatlan hozzáféréssel szemben.

11.2.3 8.17 kontroll – Előírja a rendszerek felügyeletét a szokatlan tevékenységek észlelésére, valamint a felügyeleti kontrollok hatékonyságának megerősítésére.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2–AU-12 – Lefedi az auditnaplók tartalmát, felülvizsgálatát, megőrzését és az automatizált riasztást.

11.3.2 SI-4 – Előírja a rendszeranomáliák észlelését és a gyanús események jelentését.

11.4 GDPR

11.4.1 5. cikk (1) bekezdés f) pont – Előírja a személyes adatok sértetlenségét és bizalmasságát, amely magában foglalja a hozzáférések naplózását is.

11.4.2 32. cikk – Előírja a biztonságot biztosító technikai és szervezési intézkedéseket, beleértve a naplózást és a felügyeletet.

11.4.3 33. cikk – Előírja az időben megtett incidensbejelentést, amelyet a kiváltó ok elemzését lehetővé tevő naplók támogatnak.

11.5 NIS2 irányelv

11.5.1 21. cikk (2) bekezdés d) pont – Előírja az anomáliákat észlelő, valamint az incidenskivizsgálást támogató naplózási mechanizmusokat.

11.5.2 23. cikk – Előírja az incidensek 24 órán belüli jelentését, amely pontos és időszerű naplóadatoktól függ.

11.6 DORA-rendelet

11.6.1 10. cikk – Előírja a digitális operatív rezilienciát, beleértve az IKT-hez kapcsolódó incidensek naplózással biztosított visszakövethetőségét.

11.6.2 15. cikk – Előírja a szolgáltatók felügyeletét, beleértve a naplóhozzáférési és felülvizsgálati jogokat.

11.7 COBIT 2019

11.7.1 DSS01.03 – Előírja a rendszertevékenységek visszakövethetőségét naplózás és felügyelet útján.

11.7.2 DSS05.02 – A naplózást a kártevőkkel és más jogosulatlan tevékenységekkel szembeni védelem kulcsfontosságú kontrolljaként kezeli.