					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P22					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**

1. Cél

1.1 Jelen szabályzat célja, hogy egyértelmű és kikényszeríthető követelményeket határozzon meg a szervezet IT-környezetében a kulcsfontosságú rendszer- és biztonsági eseményeket rögzítő naplók előállítására, védelmére, felülvizsgálatára és elemzésére.

1.2 A naplózás és a felügyelet alapvető fontosságú az anomáliák észleléséhez, a fenyegetésekre adott reagáláshoz, a forenzikus vizsgálatokhoz, az auditra való felkészültséghez és a jogszabályi megfeleléshez. Jelen szabályzat biztosítja, hogy a rendszerek által előállított események megfelelően rögzítésre, megőrzésre és időszinkronizált módon korrelálásra kerüljenek.

1.3 Jelen szabályzat elengedhetetlen az ISO/IEC 27001 8. pontjának, valamint az A melléklet 8.15 (Naplózás), 8.16 (Felügyelet) és 8.17 (Óraszinkronizálás) kontrolljainak támogatásához, továbbá közvetlenül kapcsolódik a GDPR, a NIS2, a DORA és a COBIT 2019 szerinti szabályozási kötelezettségekhez.

2. Hatály

2.1 Jelen szabályzat az információbiztonság-irányítási rendszer (IBIR) hatálya alá tartozó, adatokat tároló, feldolgozó vagy továbbító valamennyi rendszerre, szolgáltatásra és környezetre alkalmazandó, ideértve különösen az alábbiakat:

2.1.1 helyszíni infrastruktúra, felhőszolgáltatások (pl. IaaS, PaaS, SaaS) és hibrid környezetek;

2.1.2 operációs rendszerek, adatbázisok, alkalmazások és hálózati eszközök;

2.1.3 biztonsági rendszerek, például SIEM-megoldások, tűzfalak, EDR-platformok, VPN-koncentrátorok és identitásszolgáltatók.

2.2 A hatály az alábbi érintett felekre terjed ki:

2.2.1 belső felhasználók rendszer- vagy adminisztrátori jogosultságokkal;

2.2.2 infrastruktúra- és IT-üzemeltetési személyzet;

2.2.3 biztonsági műveleti központ (SOC) és fenyegetésészlelési csapatok;

2.2.4 szoftverfejlesztők és alkalmazástulajdonosok;

2.2.5 naplót előállító rendszereket kezelő külső szolgáltatók.

3. Célkitűzések

3.1 Biztosítani kell, hogy minden kritikus rendszer olyan biztonsági eseménynaplókat és rendszertevékenységi nyilvántartásokat állítson elő, amelyeket a jogszabályi, szerződéses és egyéb megfelelési követelményeknek megfelelően kell megőrizni.

3.2 Meg kell határozni azokat a minimális eseménytípusokat és naplótartalmakat, amelyek szükségesek a jogosulatlan tevékenységek észleléséhez, a felhasználói műveletek visszakövetéséhez és a forenzikus vizsgálatok támogatásához.

3.3 Olyan védelmi intézkedéseket kell alkalmazni, amelyek megakadályozzák a naplók manipulálását, jogosulatlan törlését vagy a naplóadatokhoz való nem szabályozott hozzáférést.

3.4 Központosított naplózási és riasztási rendszereket (pl. SIEM) kell kialakítani a gyanús tevékenységek közel valós idejű gyűjtésére, korrelálására és eszkalációjára.

3.5 Biztosítani kell a rendszerórák szinkronizálását annak érdekében, hogy megvalósuljon a rendszerek közötti pontos korreláció és az incidenselemzés.

3.6 A folyamatos fejlesztést és a megfelelést támogatni kell a naplófelügyelet audit-, kockázat- és incidenskezelési folyamatokba történő integrálásával.

4. Szerepkörök és felelősségi körök

4.1 Információbiztonsági vezető

4.1.1 Jelen szabályzat gazdája, és biztosítja annak összhangját a szervezet kockázati helyzetével, auditkövetelményeivel és az IBIR-kötelezettségekkel.

4.1.2 Jóváhagyja a naplózás hatókörét a szabályozott vagy magas kockázatú rendszerek esetében, és felügyeli a megfelelőségi jelentéstételt.

4.2 A biztonsági műveleti központ (SOC) vezetője

4.2.1 Üzemelteti és fenntartja a központosított naplókezelő platformokat (pl. SIEM).

4.2.2 Meghatározza a naplóaggregálási szabályokat, a riasztási küszöbértékeket és az incidensek elsődleges értékeléséhez kapcsolódó eszkalációs útvonalakat.

4.2.3 Napi jelentéseket vizsgál felül, és biztosítja, hogy az anomáliák elemzése, dokumentálása és szükség szerinti eszkalációja megtörténjen.

[... 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 évente felül kell vizsgálni, vagy ennél korábban, ha az alábbiak valamelyike bekövetkezik:

9.1.1 jelentős változások a rendszerarchitektúrában vagy a naplózási infrastruktúrában (pl. SIEM-migráció);

9.1.2 a szabályozási naplózási követelmények módosulása (pl. NIS2, DORA naplózási előírásai);

9.1.3 auditokból vagy incidenseket követő értékelésekből származó megállapítások;

9.1.4 újonnan megjelenő fenyegetések, amelyek fokozott megfigyelést igényelnek (pl. belső fenyegetések, ellátási lánc kompromittálódása).

9.2 A felülvizsgálati folyamatot a biztonsági műveleti központ (SOC) vezetője vezeti az információbiztonsági vezetővel, valamint a kockázatkezelési, megfelelőségi és IT-infrastruktúra-csapatokkal együttműködésben.

9.3 A jóváhagyott változásokat verziókövetéssel kell rögzíteni az IBIR dokumentumkontroll-nyilvántartásában, és közölni kell:

9.3.1 minden olyan érintett féllel, aki felelős a naplózási rendszerek fenntartásáért;

9.3.2 az alkalmazás- és rendszertulajdonosokkal;

9.3.3 azokkal a külső szolgáltatókkal, amelyek telemetriai vagy SIEM-integrációs feladatot látnak el.

9.4 Minden hatályon kívül helyezett verziót biztonságosan archiválni kell, és azokhoz kizárólag az erre jogosult IBIR-felelősök férhetnek hozzá audit- és jogi célból.

10. Kapcsolódó szabályzatok és összefüggések

10.1 P1 – Információbiztonsági szabályzat. Meghatározza a rendszerek és adatok védelmére vonatkozó alapvető elkötelezettséget, amelynek keretében a naplózás és a felügyelet kulcsfontosságú észlelési és reagálási képességet biztosít.

10.2 P4 – Hozzáférés-szabályozási szabályzat. Biztosítja, hogy az emelt jogosultságú hozzáférés, a felhasználói bejelentkezések és a jogosultsági események rögzítésre kerüljenek a naplókban, valamint felügyelet alatt álljanak a visszaélés vagy rendellenes viselkedés észlelése érdekében.

10.3 P5 – Változáskezelési szabályzat. Előírja azon rendszerváltozások, javítástelepítések és konfigurációfrissítések naplózását, amelyek kockázatot vagy jogosulatlan módosítást eredményezhetnek.

10.4 P21 – Hálózatbiztonsági szabályzat. Előírja a hálózati szintű naplózást (pl. tűzfalnaplók, IDS/IPS-riasztások, VPN-tevékenység) és a SIEM-integrációt a forgalmi anomáliák és a határvédelmi láthatóság biztosítása érdekében.

10.5 P23 – Időszinkronizálási szabályzat. Előírja a rendszerórák egységességét a rendszerek között, ami alapvető a megbízható naplózáshoz és a biztonsági események több környezeten átívelő korrelációjához.

10.6 P30 – Incidenskezelési szabályzat. A biztonsági incidensek azonosításához, kivizsgálásához és kezeléséhez naplóadatokra és riasztási mechanizmusokra támaszkodik, miközben megőrzi a forenzikus bizonyítékokat az incidenseket követő felülvizsgálathoz.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 8. pont – Működés: előírja az üzemeltetés felügyeletét szolgáló kontrollokat, valamint a jogosulatlan hozzáférés és a rendszerrel való visszaélés elleni védelmet.

11.2 ISO/IEC 27002:2022 – 8.15, 8.16, 8.17 kontrollok

11.2.1 Részletes naplózási követelményeket határoz meg, beleértve a rögzítendő eseményeket, a naplók védelmének és elemzésének módját, valamint az időbélyegek rendszerek közötti megbízhatóságának biztosítását.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2–AU-12: kiterjed az események kiválasztására, a naplózásra, a védelemre, az auditfelülvizsgálatra, az auditálási hibák kezelésére és az auditnapló-bejegyzések megőrzésére.

11.3.2 SI-4 – Rendszerfelügyelet: előírja az aktív rendszermegfigyelést anomális tevékenységen alapuló riasztásokkal.

11.3.3 SC-45 – Rendszeridő szinkronizálása: megerősíti az időpontok pontosságának követelményét az események visszakövethetősége és az incidenskorreláció érdekében.

11.4 GDPR (2016/679)

11.4.1 32. cikk – Az adatkezelés biztonsága: olyan technikai kontrollokat ír elő, mint a naplózás és a megfigyelés, a biztonság és az elszámoltathatóság biztosítása érdekében, különösen a személyes adatokhoz való hozzáférés tekintetében.

11.5 NIS2 irányelv (2022/2555)

11.5.1 21. cikk (2) bekezdés e) pont: eseménynaplózási és megfigyelési rendszerek alkalmazását írja elő a biztonsági incidensek gyors észlelése és kezelése érdekében.

11.6 DORA-rendelet (2022/2554)

11.6.1 9. cikk – IKT-kockázatkezelés: előírja az anomális tevékenységek észlelésére, az incidensek naplózására és a forenzikus adatok megőrzésére szolgáló mechanizmusokat.

11.6.2 11. cikk – Az üzletmenet-folytonossági tervek IKT-tesztelése: hangsúlyozza a megfigyelés folytonosságát és a naplók rendelkezésre állásának ellenőrzését működési zavarok idején.

11.7 COBIT 2019

11.7.1 DSS01.05 – Biztonsági naplók kezelése: előírja a naplózási képességek megvalósítását valamennyi kritikus infrastruktúra esetében.

11.7.2 DSS05.04 – Biztonsági események monitorozása: előírja a naplók valós idejű felügyeletét és elemzését az események észlelése és kezelése érdekében.

11.7.3 MEA03 – A megfelelés nyomon követése, értékelése és felmérése: előírja a naplózási gyakorlatok rendszeres felülvizsgálatát és a kontrollcélokkal való összhang biztosítását.