					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P19					Dokumentum címe: **Sérülékenység- és javításkezelési 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	A technikai sérülékenységek szisztematikus kezelése; a biztonsági kontrollok folyamatos hatékonysága.
ISO/IEC 27002:2022	8.8, 8.9, 5. kontroll	Alkalmazási útmutatás a javítások telepítésére, a sérülékenységvizsgálatokra, a szoftverintegritásra, a biztonságos konfigurációra és az eszköznyilvántartásokra vonatkozóan.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	A rendszeres vizsgálat, a hibák javítása és a konfigurációkezelés előírt alkalmazása.
EU GDPR	32. cikk, (49) preambulumbekezdés	Technikai intézkedések a gyors javítástelepítéshez, a sérülékenységek kezeléséhez és a biztonság folytonosságának biztosításához.
EU NIS2	21. cikk (2) bekezdés d) pont	A sérülékenységek észlelése, kezelése és mérséklése a magas szintű kiberhigiénia érdekében.
EU DORA	8. cikk, 10. cikk (2) bekezdés f) pont	Az IKT-sérülékenységek időben történő helyesbítése; folyamatos, fenyegetésvezérelt értékelések.
COBIT 2019	DSS05.02, DSS01.03, MEA	A technikai gyengeségek vizsgálata, nyomon követése és mérséklése; az esetleges kihasználás nyomon követése; a hatékonyság auditálása, beleértve a javítási állapotot is.

1. Cél

1.1 Jelen szabályzat meghatározza a szervezet kötelező követelményeit az információbiztonság-irányítási rendszer (IBIR) hatálya alá tartozó valamennyi információs rendszerben és eszközben előforduló technikai sérülékenységek és szoftverhibák azonosítására, osztályozására, helyesbítésére és nyomon követésére.

1.2 A szabályzat biztosítja, hogy minden ismert sérülékenység kockázatalapon és megfelelő határidőn belül értékelésre és kezelésre kerüljön javítások összehangolt telepítése, konfigurációmódosítások vagy kompenzáló kontrollok alkalmazása útján, az üzleti igényekkel és a megfelelési kötelezettségekkel összhangban.

1.3 Jelen szabályzat támogatja az ISO/IEC 27001 A melléklet 8.8. kontrolljának és az ISO/IEC 27002 iránymutatásainak való megfelelést, valamint kezeli a DORA 8. cikke, a NIS2 21. cikke, a GDPR 32. cikke és a COBIT 2019 DSS és APO területei szerinti szabályozási követelményeket.

2. Hatály

2.1 Jelen szabályzat alkalmazandó minden olyan információs rendszerre, eszközre és környezetre, amely az IBIR irányítása alá tartozó adatokat tárol, kezel vagy továbbít, ideértve az alábbiakat:

2.1.1 operációs rendszerek, alkalmazások, hálózati eszközök, firmware-ek, felhőplatformok, alkalmazásprogramozási interfészek és harmadik féltől származó szoftverek.

2.1.2 fejlesztési, tesztelési, éles, biztonsági mentési és katasztrófa-helyreállítási környezetekben működő rendszerek.

2.1.3 végpontok, szerverek, IoT-eszközök, virtualizációs infrastruktúra és konténerek.

2.2 A szabályzat kötelező érvényű az alábbiakra:

2.2.1 belső munkatársak: informatikai rendszergazdák, rendszermérnökök, alkalmazásfejlesztők, biztonsági elemzők és infrastruktúraüzemeltetési csapatok.

2.2.2 külső felek: vállalkozók, menedzselt szolgáltatók (MSP-k), szoftverszállítók és rendszerintegrátorok, akik a hatály alá tartozó eszközök felett műszaki felelősséggel rendelkeznek.

2.3 A szabályzat a sérülékenység- és javításkezelés teljes életciklusára kiterjed, beleértve az alábbiakat:

2.3.1 vizsgálat és észlelés

2.3.2 kockázati osztályozás és priorizálás

2.3.3 javítás beszerzése, tesztelése, telepítése és visszaállítás

2.3.4 kivételkezelés és kompenzáló kontrollok megtervezése

2.3.5 naplózás, jelentéstétel és auditnyom biztosítása

3. Célkitűzések

3.1 Biztosítani kell, hogy minden ismert sérülékenység azonosítása, értékelése és helyesbítése olyan módon történjen, amely minimalizálja a kockázati kitettséget és igazodik az operatív prioritásokhoz.

3.2 Egységes, szervezetszintű folyamatokat kell kialakítani a sérülékenységvizsgálatokhoz, a súlyossági osztályozáshoz (pl. CVSS) és a javításkezeléshez, beleértve a sürgősségi kezelést és a visszaállítás-tervezést is.

3.3 Lehetővé kell tenni a biztonságos konfigurációkezelést a rendszerkeményítési alapkonfigurációk, a konfigurációváltozások szabályozása és a valós idejű fenyegetettségi információk figyelembevétele révén.

3.4 Mérhető megfelelést kell biztosítani a rendszerintegritással, a javítási higiéniával és a hibák időben történő helyesbítésével kapcsolatos jogszabályi és szabványalapú kontrollokkal szemben.

3.5 Meg kell határozni a teljes sérülékenységkezelési életciklusra vonatkozó felelősségi és elszámoltathatósági rendet a szerepkörök között annak biztosítása érdekében, hogy valamennyi érintett a meghatározott SLA-kon és jelentendő kontrollmutatókon belül járjon el.

3.6 Támogatni kell az auditra való felkészültséget és javítani kell a kialakulóban lévő fenyegetésekkel szembeni rezilienciát, ideértve a nulladik napi sérülékenységeket, az aktív kihasználási láncokat és a kiemelt beszállítói közleményeket.

4. Szerepkörök és felelősségi körök

4.1 Információbiztonsági vezető (CISO)

4.1.1 A szabályzat gazdája, és biztosítja annak integrációját az IBIR-be.

4.1.2 Meghatározza a szervezeti kockázati kitettséget, és biztosítja a szabályozási és kontrollkövetelményekkel való összhangot.

4.2 Sérülékenységkezelési vezető / biztonsági műveleti vezető

4.2.1 Felügyeli a teljes körű sérülékenység- és javításkezelési működést.

4.2.2 Koordinálja a vizsgálati ütemezéseket, a priorizálási modelleket és a helyesbítési határidőket.

4.2.3 Fenntartja a sérülékenység-nyilvántartást, és együttműködik a kompenzáló kontrollok értékelésében.

[... 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, valamint az alábbi esetekben felül kell vizsgálni:

9.1.1 jelentős szabályozási változások esetén (pl. DORA, NIS2 változásai)

9.1.2 a sérülékenység-priorizálási keretrendszerek változása esetén (pl. CVSS-frissítések)

9.1.3 jelentős IT-környezeti változások esetén (pl. felhőmigráció, EDR-átalakítás)

9.1.4 kiemelt adatsértések vagy külső tájékoztatások esetén, amelyek a szabályzat megerősítését teszik szükségessé

9.2 A felülvizsgálatot a CISO végzi a biztonsági műveletek, a kockázatkezelés és az infrastruktúra-üzemeltetés bevonásával.

9.3 A szabályzatfrissítéseknek:

9.3.1 dokumentáltnak kell lenniük az IBIR dokumentumkezelési nyilvántartásában

9.3.2 felső vezetői jóváhagyással kell rendelkezniük

9.3.3 közlésre kell kerülniük minden érintett féllel, beleértve a harmadik fél adatfeldolgozókat is

9.4 A korábbi verziókat audit- és elszámoltathatósági célból biztonságosan meg kell őrizni.

10. Kapcsolódó szabályzatok és összefüggések

10.1 P1 - Információbiztonsági szabályzat. Meghatározza a rendszerek és adatok védelmére vonatkozó átfogó elkötelezettséget, amely magában foglalja a sérülékenységek proaktív kezelését és a szoftverintegritás biztosítását.

10.2 P5 - Változáskezelési szabályzat. Szabályozza a javítások telepítését és a konfigurációmódosításokat, előírva a dokumentálást, a tesztelést, a jóváhagyást és a visszaállítási eljárásokat, amelyek kiegészítik a sérülékenységek helyesbítési folyamatait.

10.3 P6 - Kockázatkezelési szabályzat. Támogatja a nem kezelt sérülékenységek osztályozását és kezelését strukturált kockázatértékelések, hatáselemzés és maradványkockázat-elfogadási eljárások révén.

10.4 P12 - Eszközkezelési szabályzat. Biztosítja a rendszerek pontos nyilvántartását és osztályozását, lehetővé téve a következetes sérülékenységvizsgálatot, a tulajdonosi hozzárendelést és a teljes életciklusra kiterjedő javítási lefedettséget.

10.5 P22 - Naplózási és felügyeleti szabályzat. Meghatározza az eseményészlelésre és az auditnyom előállítására vonatkozó követelményeket. A jelen szabályzat támogatja a javítási tevékenységek, a jogosulatlan módosítások és az ismert sérülékenységeket célzó kihasználási kísérletek láthatóságát.

10.6 P30 - Incidenskezelési szabályzat. Meghatározza a kihasznált sérülékenységekre, az incidensvizsgálatokra és a jelen szabályzat kontrolljaihoz igazodó helyesbítési intézkedésekre vonatkozó eszkalációs protokollokat és elszigetelési stratégiákat.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001:2022 8.1 pont - Operatív tervezés és szabályozás: Előírja a technikai sérülékenységek szisztematikus kezelését a biztonsági kontrollok folyamatos hatékonyságának biztosítása érdekében.

11.2 ISO/IEC 27002:2022 - 8.8, 8.9, 5. kontroll: Alkalmazási útmutatást ad a javítások telepítésére, a sérülékenységvizsgálatra, a szoftverintegritásra, valamint a biztonságos konfigurációval és az eszköznyilvántartásokkal való integrációra.

11.3 NIST SP 800-53 Rev.5: RA-5 - Sérülékenységek megfigyelése és vizsgálata: Előírja a rendszeres vizsgálatot és a helyesbítési intézkedések nyomon követését. SI-2 - Hibák helyesbítése: Előírja a hibák gyors értékelését és mérséklését elérhető javításokkal vagy egyéb intézkedésekkel. CM-2 / CM-6 - Konfigurációkezelési alapállapotok és kontrollok: Megteremti a javítások érvényesítéséhez kapcsolódó biztonságos rendszerkonfigurációk alapját.

11.4 EU GDPR (2016/679): 32. cikk - Az adatkezelés biztonsága: Előírja a megfelelő technikai intézkedések bevezetését, így például a gyors javítástelepítést és a sérülékenységek kezelését a bizalmasság és a rendszerreziliencia biztosítása érdekében. (49) preambulumbekezdés: Ösztönzi az ismert fenyegetések elleni megelőző kontrollok bevezetését a biztonság és a folytonosság támogatása érdekében.

11.5 EU NIS2 irányelv (2022/2555): 21. cikk (2) bekezdés d) pont: Kötelezi az alapvető és fontos szervezeteket a rendszersérülékenységek észlelésére, kezelésére és mérséklésére, valamint a magas szintű kiberhigiénia fenntartására.

11.6 EU DORA (2022/2554): 8. cikk - IKT-kockázatkezelés: Előírja a pénzügyi rendszerekben használt információs és kommunikációs technológiák sérülékenységeinek azonosítását és időben történő helyesbítését. 10. cikk (2) bekezdés f) pont: Hangsúlyozza a folyamatos, fenyegetésvezérelt sérülékenységértékeléseket és a javítások telepítését mint az operatív reziliencia részét.

11.7 COBIT 2019: DSS05.02 - Biztonsági sérülékenységek kezelése: Előírja az ismert technikai gyengeségek vizsgálatát, nyomon követését és mérséklését. DSS01.03 - Infrastruktúra megfigyelése: Biztosítja a rendszerek felügyeletét a kihasználás vagy gyengeség jeleinek észlelése érdekében. MEA03 - A megfelelés nyomon követése, értékelése és felmérése: Előírja a kontrollok hatékonyságának rendszeres auditálását, beleértve a javítási állapotot és a kivételkezelést is.