					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P39					Dokumentum címe: **Koordinált sérülékenység-feltárási 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	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev.5	RA-5, SI-2, PM-15, CA-8, SR-6	
GDPR	32. cikk (1) bekezdés d) pont	
NIS2 irányelv	21. cikk (2) bekezdés e) pont	
DORA-rendelet	11. cikk (1) bekezdés d) pont	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Cél

1.1 Formális folyamat kialakítása a szervezet rendszereit vagy szolgáltatásait érintő sérülékenységekkel kapcsolatos információk fogadására, kezelésére és közzétételére, összhangban a NIS2 irányelv 21. cikk (2) bekezdés e) pontjában meghatározott, a sérülékenységek kezelésére és nyilvánosságra hozatalára vonatkozó követelményekkel.

1.2 A külső biztonsági kutatók, partnerek és felhasználók ösztönzése a sérülékenységek felelős bejelentésére (Coordinated Vulnerability Disclosure – CVD), valamint annak meghatározása, hogy a szervezet miként kommunikálja a sérülékenységekkel kapcsolatos információkat az érintett felek felé.

2. Hatály

2.1 Jelen szabályzat kiterjed a szervezet tulajdonában álló vagy általa üzemeltetett valamennyi hálózati és információs rendszerre, valamint az ezekben azonosított sérülékenységekre.

2.2 A szabályzat kiterjed a belső csapatokra (információbiztonság, IT, fejlesztés), továbbá minden külső félre, aki sérülékenységet jelent be (pl. kutatók, ügyfelek, beszállítók). Szabályozza továbbá a termékbeszállítókkal vagy szolgáltatókkal folytatott kommunikációt is, ha azok komponensei érintettek a sérülékenységben.

3. Célkitűzések

3.1 A biztonsági sérülékenységek időben történő észlelése és megszüntetése a belső értékelések és a külső bejelentések együttes felhasználásával.

3.2 Egyértelmű útmutatás biztosítása a külső bejelentők számára a sérülékenységekkel kapcsolatos információk biztonságos és jogszerű benyújtásához, valamint a szervezet számára a hatékony reagáláshoz és a helyesbítő intézkedések megtételéhez.

3.3 A NIS2 követelményeivel, valamint a koordinált sérülékenység-feltárásra vonatkozó iparági legjobb gyakorlatokkal (ISO/IEC 29147 és ISO/IEC 30111) való összhang biztosítása az ökoszisztéma általános biztonságának erősítése érdekében.

4. Szerepkörök és felelősségek

4.1 Sérülékenységkezelési reagáló csoport (VRT): kijelölt csapat, amelyet az információbiztonsági vezető vagy a sérülékenységkezelési vezető irányít, és amely fogadja, előzetesen értékeli a sérülékenység-bejelentéseket, felméri a kockázatot és a hatást, továbbá koordinálja a helyesbítő intézkedéseket és a nyilvános közzétételt.

4.2 IT- és fejlesztőcsapatok: együttműködnek a VRT-vel a bejelentett sérülékenységek ellenőrzésében, a javítások vagy kockázatcsökkentő intézkedések kidolgozásában és tesztelésében, valamint a javítások bevezetésében. Szükség esetén technikai részleteket biztosítanak a tájékoztatókhoz.

[... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ...]

9. Nyomon követés és audit

9.1 A VRT köteles sérülékenység-feltárási naplót vezetni, amely minden bejelentést a beérkezéstől a lezárásig nyomon követ. E napló felülvizsgálatát havonta el kell végezni annak biztosítására, hogy a nyitott tételek kezelése megfelelő ütemben haladjon. A határidőn túli tételeket eszkalálni kell.

9.2 A belső audit vagy egy független biztonsági értékelő évente felülvizsgálja a sérülékenységkezelési folyamat eredményességét – például annak ellenőrzésével, hogy a sérülékenységi esetek mintái a szabályzatnak megfelelően kerültek-e kezelésre (visszaigazolás, javítás, időben történő közzététel). Ellenőrizni kell továbbá, hogy a nyilvánosan elérhető bejelentési csatorna működőképes-e (például a teszt e-mailek megérkeznek-e, és történik-e rájuk intézkedés).

9.3 A sérülékenységekre vonatkozó mutatókat (darabszám súlyosság szerint, helyesbítő intézkedések átfutási ideje stb.) negyedévente össze kell állítani, és be kell mutatni a kiberbiztonsági irányító bizottság részére a kockázatértékelés frissítésének támogatására.

10. Felülvizsgálat és karbantartás

10.1 Jelen szabályzatot legalább évente felül kell vizsgálni. Ezen felül minden jelentős változás az IT-környezetben (pl. új, internet felől elérhető szolgáltatás indítása) vagy a vonatkozó szabályozási környezetben bekövetkező változás (pl. új uniós jogszabály a terméksérülékenységek közzétételéről) soron kívüli felülvizsgálatot vált ki.

10.2 A szabályzat frissítéseinek be kell építeniük a külső bejelentők visszajelzéseit és a belső incidensek utáni elemzések tanulságait. A jelentős módosításokat az információbiztonsági vezető hagyja jóvá, és azokat valamennyi munkavállalóval közölni kell, továbbá az átláthatóság érdekében közzé kell tenni az online biztonsági szabályzatarchívumban.

11. Kapcsolódó szabályzatok és összefüggések

11.1 P01 – Információbiztonsági szabályzat. Vezetői felhatalmazást ad a sérülékenységek kezelésére és közzétételére.

11.2 P19 – Sérülékenység- és javításkezelési szabályzat. A CVD-bejelentésekhez kapcsolódó belső helyesbítési folyamatot szabályozza.

11.3 P24 – Biztonságos fejlesztési szabályzat. A bejelentett problémák alapján támogatja a javítások beépítését és az SDLC megerősítését.

11.4 P25 – Alkalmazásbiztonsági követelmények szabályzata. Biztosítja, hogy a termékek biztonsági követelményei alkalmasak legyenek a sérülékenységek közzétételének támogatására.

11.5 P30 – Incidenskezelési szabályzat. Kezeli a nyilvánosságra került sérülékenységek aktív kihasználását.

11.6 P31 – Bizonyítékgyűjtési és forenzikai szabályzat. Megőrzi a bejelentett vagy kihasznált hibákhoz kapcsolódó artefaktumokat.

11.7 P26 – Harmadik felek és beszállítók biztonsági szabályzata. Koordinálja a beszállítói komponenseket érintő közzétételeket.

11.8 P37 – Jogi és jogszabályi megfelelési szabályzat. Szabályozza az értesítéseket, a jogi védelemre vonatkozó megfogalmazásokat és a közzétételt.

12. Hivatkozások

12.1 NIS2 irányelv (EU 2022/2555), 21. cikk (2) bekezdés e) pont (a fejlesztés biztonsága, valamint a sérülékenységek kezelése és közzététele)

12.2 A Bizottság (EU) 2024/2690 végrehajtási rendelete, melléklet 6.10. szakasz (a sérülékenységek kezelésére és közzétételére vonatkozó technikai követelmények)

12.3 ENISA technikai útmutató a kiberbiztonsági kockázatkezelési intézkedésekről – a sérülékenységek kezelésére és közzétételére vonatkozó szakasz

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (A.5.7 kontroll: fenyegetettségi információk és sérülékenységek közzététele; A.8.28 kontroll: biztonságos fejlesztés)

12.5 ISO/IEC 29147:2018 (iránymutatások a sérülékenységek közzétételéhez) és ISO/IEC 30111:2019 (iránymutatások a sérülékenységkezelési folyamatokhoz)