					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P19S					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. fejezet	
ISO/IEC 27002:2022	8.8. kontroll	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
EU NIS2	21. cikk (2) bekezdés d), 21. cikk (2) bekezdés e)	
EU DORA	8. cikk (1) bekezdés, 10. cikk (2) bekezdés	
COBIT 2019	DSS05.02, APO12	
EU GDPR	32. cikk (1) bekezdés b)	

1. Cél

1.1 Jelen szabályzat meghatározza, hogy a szervezet milyen módon azonosítja, értékeli és kezeli a rendszerekben, alkalmazásokban és infrastruktúrában fennálló sérülékenységeket.

1.2 Célja a kiberbiztonsági kockázatok csökkentése az időszerű javítástelepítés és a kockázatalapú helyesbítő intézkedések előírásával, a KKV-k működéséhez igazodó módon.

1.3 Jelen szabályzat támogatja az ISO/IEC 27001:2022 szerinti tanúsítási megfelelést, és hozzájárul a GDPR, a NIS2 és a DORA szerinti szabályozási kötelezettségek teljesítéséhez azáltal, hogy előírja a technikai sérülékenységek proaktív kezelését.

1.4 A szervezet elismeri, hogy a nem javított rendszerek jelentős fenyegetést jelentenek az információbiztonságra, ezért ezeket rendszerszinten és indokolatlan késedelem nélkül kezelni kell.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 A szervezet által használt valamennyi szerverre, asztali számítógépre, laptopra, mobileszközre, hálózati eszközre és felhőalapú platformra

2.1.2 Az üzleti működés során használt valamennyi operációs rendszerre, harmadik fél által biztosított szoftverre, bővítményre és alkalmazásra

2.1.3 A rendszerkarbantartásért, frissítésekért vagy felügyeletért felelős belső informatikai munkatársakra vagy külső szolgáltatókra

2.1.4 A szervezet által vagy annak megbízásából karbantartott valamennyi egyedi fejlesztésű kódra vagy beágyazott szoftverre

2.2 A szabályzat kiterjed mind a szervezet által közvetlenül kezelt infrastruktúrára, mind a szerződött beszállítók vagy tárhelyszolgáltatók által üzemeltetett rendszerekre.

3. Célkitűzések

3.1 Az ismert sérülékenységek időben történő és egységes azonosítása és értékelése valamennyi informatikai eszköz esetében

3.2 Javítások és szoftverfrissítések alkalmazása a súlyosság és a szervezeti működésre, illetve a személyes adatokra gyakorolt kockázat alapján

3.3 Az olyan technikai gyengeségek kihasználásának megelőzése, amelyek szolgáltatáskieséshez, adatsértéshez vagy jogszabályi meg nem feleléshez vezethetnek

3.4 A telepített javításokról, a fennálló problémákról és a kivételekről pontos nyilvántartások fenntartása az auditkész állapot biztosítása érdekében

3.5 A szervezet méretéhez és működési összetettségéhez igazodó eszközök és folyamatok alkalmazása a hatékonyság csökkentése nélkül

3.6 A jogi és szabályozási megfelelés támogatása, beleértve a GDPR 32. cikkét és az ISO/IEC 27001 A mellékletének 8. kontrolljait

4. Szerepkörök és felelősségi körök

4.1 Ügyvezető

4.1.1 Átfogó felelősséggel tartozik annak biztosításáért, hogy a javításkezelési és sérülékenységkezelési tevékenységek végrehajtása megtörténjen

4.1.2 Jóváhagyja a kockázati kivételeket, ha a javítások nem alkalmazhatók, és felülvizsgálja a kapcsolódó kockázatcsökkentő intézkedéseket

4.1.3 Felülvizsgálja a javításkezelési állapotjelentéseket, és biztosítja a javításkezelési kötelezettségek teljesítéséhez szükséges erőforrásokat

4.2 IT-támogatási szolgáltató / belső rendszergazda

4.2.1 Figyelemmel kíséri a rendszereket sérülékenységek és elérhető javítások szempontjából a beszállítói riasztások, fenyegetettségi tájékoztatók és operációsrendszer-szintű értesítések alapján

4.2.2 A meghatározott határidőn belül telepíti az operációs rendszer-, firmware- és alkalmazásfrissítéseket

4.2.3 Formális javítási naplót vezet, és dokumentálja a meg nem oldott vagy elhalasztott frissítéseket

4.2.4 Elvégzi a kritikus frissítések tesztelését és ütemezését az üzleti működés zavarásának minimalizálása érdekében

[... 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 vizsgálni az ügyvezető által, az IT-szolgáltató és az adatvédelmi koordinátor bevonásával

9.2 Felülvizsgálatot kiváltó események

9.2.1 Soron kívüli felülvizsgálatot kell tartani, ha:

9.2.1.1 Egy jelentős sérülékenység vagy exploit a hatály alá tartozó rendszereket érinti

9.2.1.2 Jelentős rendszer- vagy szoftverváltozás történik

9.2.1.3 Egy audit hiányosságokat azonosít a javításkezelési folyamatokban

9.2.1.4 Javításkezeléssel összefüggő incidens vagy adatsértés kerül rögzítésre

9.3 Szabályzati verziókezelés

9.3.1 Minden módosítást verzionaplóban kell rögzíteni a változások összefoglalásával

9.3.2 A változásokat közölni kell az érintett munkatársakkal

9.3.3 Az elavult verziókat korlátozott hozzáféréssel archiválni kell

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat több más KKV-szabályzatot támogat, és azokhoz kapcsolódik:

10.1.1 P12S – Eszközkezelési szabályzat: Meghatározza a rendszertulajdonosi felelősséget és az osztályozást, biztosítva, hogy minden javítást igénylő eszköz azonosított legyen és szerepeljen az eszköznyilvántartásban

10.1.2 P14S – Adatmegőrzési és selejtezési szabályzat: Biztosítja, hogy a kivonásra tervezett rendszerek biztonságosan frissítve vagy törölve legyenek, csökkentve a sérülékenységi kitettséget

10.1.3 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: Az adatvédelmi jogszabályoknak való megfelelés érdekében elsőbbséget ad a személyes adatokat kezelő rendszerek sérülékenységeihez kapcsolódó helyesbítő intézkedéseknek

10.1.4 P22S – Naplózási és felügyeleti szabályzat: Támogatja a nem javított rendszerek vagy a sérülékenység-kihasználásra utaló gyanús tevékenységek észlelését

10.1.5 P30S – Incidenskezelési szabályzat: Meghatározza a biztonsági incidenseket eredményező sérülékenységekre adott válaszlépéseket, beleértve az eszkalációs és jelentéstételi lépéseket

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 8. fejezet – Előírja az operatív kockázatok kezelését szolgáló kontrollok bevezetését, beleértve a sérülékenységkezelést is

11.2 ISO/IEC 27002

11.2.1 8.8. kontroll – Meghatározza a rendszerekben található ismert gyengeségek vizsgálatára és javítására vonatkozó folyamatokat

11.2.2 8.9. kontroll – Hangsúlyozza a biztonságos konfiguráció, a javítások ellenőrzése és a változáskezelés fontosságát annak érdekében, hogy a frissítések során ne keletkezzen új kitettség

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – Előírja a sérülékenységek azonosítását és a helyesbítő intézkedések végrehajtását meghatározott határidőn belül

11.3.2 SI-2 – Előírja a javítások és frissítések haladéktalan alkalmazását a súlyosság alapján

11.3.3 CM-2 – Szabályozza a rendszer előírt alapkonfigurációit és a frissítések dokumentálását az egységes védelmi szint biztosítása érdekében

11.4 EU GDPR

11.4.1 32. cikk (1) bekezdés b) – Előírja, hogy a szervezetek megfelelő technikai intézkedéseket vezessenek be, beleértve a javításkezelést is, az adatkezelés biztonságának fenntartása érdekében

11.5 EU NIS2 irányelv

11.5.1 21. cikk (2) bekezdés d) – Előírja a sérülékenységek kezelését rendszeres vizsgálat és helyesbítő intézkedések útján

11.5.2 21. cikk (2) bekezdés e) – Kötelezővé teszi a biztonságos konfigurációt és a javításkezelést az IKT-reziliencia biztosítása érdekében

11.6 EU DORA

11.6.1 8. cikk (1) bekezdés – Előírja az IKT-kockázatok, köztük a technikai sérülékenységek azonosítását és csökkentését

11.6.2 10. cikk (2) bekezdés – Előírja a pénzügyi szervezetek számára az IKT-rendszereket és -működést érintő gyengeségek helyesbítését

11.7 COBIT 2019

11.7.1 DSS05.02 – Előírja az ismert technikai sérülékenységek kezelését a biztonságos működés fenntartása érdekében

11.7.2 APO12.01 – Összhangba hozza a kockázatkezelést a rendszergyengeségek proaktív nyomon követésével és korrekciójával