					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P25					Dokumentum címe: **Alkalmazásbiztonsági követelmények szabályzat – SME**							
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**

A vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	8. fejezet	—
ISO/IEC 27002:2022	8.25–8.26 kontroll	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
GDPR	25., 32. cikk	—
NIS2 irányelv	21. cikk (2) bekezdés f) pont, 23. cikk	—
DORA-rendelet	9., 11. cikk	—
COBIT 2019	BAI03, BAI09, DSS	—

1. cél

1.1 Jelen szabályzat meghatározza a szervezet által fejlesztett, beszerzett, integrált vagy bevezetett szoftverekre vonatkozó kötelező alkalmazásbiztonsági követelményeket. Biztosítja, hogy valamennyi alkalmazás tervezése, megvalósítása és üzemeltetése a biztonságos fejlesztés elveivel, a szabályozási kötelezettségekkel és a szervezet kockázatvállalási hajlandóságával összhangban történjen.

1.2 Jelen szabályzat előírja a biztonsági követelmények érvényesítését az alkalmazások teljes életciklusa során, ideértve a felhasználók hitelesítését, az adatkezelést, az interfészek védelmét, valamint az API-kkal és szolgáltatásokkal való biztonságos együttműködést.

1.3 A szabályzat alkalmazásának célja a szoftversérülékenységek bevezetésének megelőzése, az érzékeny adatok védelme, továbbá a visszakövethetőség és az exploitokkal, illetve visszaélésekkel szembeni reziliencia biztosítása.

2. hatály

2.1 Jelen szabályzat hatálya kiterjed:

2.1.1 a belső fejlesztésű vagy külső forrásból származó alkalmazásokra, beleértve a SaaS-megoldásokat és az egyedi fejlesztésű eszközöket;

2.1.2 a kritikus üzleti működést, az ügyfélhozzáférést vagy szabályozott adatok kezelését támogató alkalmazásokra;

2.1.3 a fejlesztési, DevOps, QA, termékfejlesztési és biztonsági csapatokra;

2.1.4 a harmadik fél fejlesztőire, szoftverszállítóira és integrációs partnereire, akik hozzáférnek a szervezeti alkalmazásokhoz vagy API-khoz.

2.2 A szabályzat valamennyi környezetre alkalmazandó: fejlesztési, tesztelési, előéles, éles és katasztrófa utáni helyreállítási környezetre, függetlenül attól, hogy azok helyszíni, saját adatközponti vagy nyilvános felhőkörnyezetben működnek.

3. célkitűzések

3.1 Valamennyi alkalmazásra vonatkozóan meg kell határozni azokat az alapvető funkcionális és nem funkcionális biztonsági követelményeket, amelyek teljesítése a fejlesztési módszertantól vagy technológiai veremtől függetlenül kötelező.

3.2 Biztosítani kell az alkalmazásrétegű védelmi intézkedések integrációját, ideértve a bemeneti adatok ellenőrzését, a kimeneti kódolást, a hibakezelést és a munkamenet-védelmi intézkedéseket.

3.3 Elő kell írni a hitelesítési, jogosultságkezelési és hozzáférés-szabályozási mechanizmusok biztonságos megvalósítását a szervezet identitás- és hozzáférés-kezelési szabályzataival összhangban.

3.4 Elő kell írni az API-kkal, webes interfészekkel és harmadik fél komponenseivel való biztonságos együttműködést jóváhagyott protokollok és biztonsági kontrollok alkalmazásával.

3.5 Biztosítani kell a sérülékenységek korai felismerését és kockázatcsökkentését statikus és dinamikus elemzéssel, kódfelülvizsgálattal és fenyegetésmodellezéssel.

3.6 Az érzékeny adatokat a szabályozási követelményeknek megfelelően kell védeni a titkosítás, az osztályozás és az adatmegőrzési szabályok érvényesítésével.

3.7 Biztosítani kell az alkalmazások kockázati helyzetének folyamatos nyomon követését a bevezetést követően teszteléssel, felügyelettel és az auditra való felkészültség fenntartásával.

4. szerepkörök és felelősségek

4.1 információbiztonsági vezető

4.1.1 Jelen szabályzat tulajdonosa, és biztosítja annak összhangját a szervezet információbiztonsági stratégiájával és kockázati helyzetével.

4.1.2 Jóváhagyja az alkalmazásbiztonsági követelményeket, és érvényesíti a kötelező kontrollokat a fejlesztési és beszerzési területeken.

4.2 alkalmazásbiztonsági vezető / DevSecOps vezető

4.2.1 Meghatározza az alkalmazáskomponensekre vonatkozó alapvető biztonsági kontrollokat és tesztelési módszertanokat.

4.2.2 Felügyeli az olyan eszközök, mint a SAST, DAST, IAST és SCA biztonságos integrációját a szoftverszállítási folyamatba.

4.2.3 Karbantartja az alkalmazásbiztonsági követelmények ellenőrzőlistáját és az ellenőrzési szempontokat.

[... 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, illetve szükség esetén ennél gyakrabban felül kell vizsgálni az alábbi esetekben:

9.1.1 kritikus sérülékenységek nyilvánosságra kerülése esetén, amelyek széles körben használt keretrendszereket vagy függőségeket érintenek;

9.1.2 az alkalmazásbiztonságra vonatkozó szabályozási kötelezettségek változása esetén, például a NIS2 vagy a DORA kapcsán;

9.1.3 a szervezet szoftverfejlesztési gyakorlatában, eszközkészletében vagy felhőarchitektúrájában bekövetkező jelentős változások esetén;

9.1.4 belső auditok vagy külső behatolástesztek megállapításai esetén.

9.2 A felülvizsgálatot az alkalmazásbiztonsági vezető vezeti az információbiztonsági vezetővel, a DevOps mérnökséggel, a Jogi területtel, a Beszerzéssel és a QA-vezetőkkel együttműködésben.

9.3 Valamennyi módosítást verziókezelés alá kell vonni az ISMS dokumentumkontroll-nyilvántartásában, és el kell juttatni minden érintett fejlesztési és termékcsapat számára.

9.4 A hatályon kívül helyezett verziókat legalább három évig archiválni kell a visszakövethetőség, az auditálhatóság és az adatsértések kivizsgálásának támogatása érdekében.

10. kapcsolódó szabályzatok és összefüggések

10.1 P1 – Információbiztonsági szabályzat. Meghatározza a rendszerek és adatok védelmének alapjait, amelynek keretében alkalmazásszintű kontrollokat kell működtetni a jogosulatlan hozzáférés, az adatszivárgás és a kihasználás megelőzése érdekében.

10.2 P4 – Hozzáférés-szabályozási szabályzat. Meghatározza azokat az identitás- és munkamenet-kezelési szabványokat, amelyeket valamennyi alkalmazásnak érvényesítenie kell, beleértve az erős hitelesítést, a legkisebb jogosultság elvét és a hozzáférés-felülvizsgálati követelményeket.

10.3 P5 – Változáskezelési szabályzat. Szabályozza az alkalmazáskód és a konfigurációk éles környezetbe juttatását, biztosítva, hogy a jogosulatlan vagy nem tesztelt változtatások blokkolásra kerüljenek.

10.4 P17 – Adatvédelmi és magánszféra-védelmi szabályzat. Előírja, hogy az alkalmazások a beépített adatvédelem elvét alkalmazzák, és valamennyi környezetben biztosítsák a személyes és érzékeny adatok jogszerű kezelését, titkosítását és megőrzését.

10.5 P24 – Biztonságos fejlesztési szabályzat. Az SDLC-be beépített biztonság tágabb keretrendszerét adja meg; jelen szabályzat ezen belül az alkalmazásrétegben megvalósítandó konkrét követelményeket és technikai kontrollokat határozza meg.

10.6 P30 – Incidenskezelési szabályzat. Előírja az alkalmazásbiztonsági incidensek strukturált kezelését, beleértve a bevezetést követően vagy behatolásteszt során azonosított sérülékenységeket, és meghatározza az eszkalációs, elszigetelési és helyreállítási eljárásokat.

11. hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001:2022

11.1.1 8.1 pont – Működéstervezés és -szabályozás: Előírja, hogy az alkalmazásbiztonság beépüljön a folyamatokba és rendszerekbe a bizalmasság, sértetlenség és rendelkezésre állás biztosítása érdekében.

11.2 ISO/IEC 27002:2022

11.2.1 8.25–8.26 kontrollok: Meghatározzák az alkalmazásbiztonsággal kapcsolatos elvárásokat, beleértve a biztonságos kódolási gyakorlatot, a fenyegetésmodellezést, az architekturális kontrollokat és a harmadik fél szoftvereinek ellenőrzését.

11.2.2 A melléklet 8.25 kontroll – Biztonságos fejlesztési életciklus: Előírja a biztonság integrálását az alkalmazás teljes életciklusa során.

11.2.3 A melléklet 8.26 kontroll – Alkalmazásbiztonsági követelmények: Előírja az alkalmazások visszaélésekkel és kompromittálódással szembeni védelmét szolgáló technikai kontrollok meghatározását és érvényesítését.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Fejlesztői biztonsági tesztelés és értékelés: Előírja a statikus, dinamikus és behatolástesztelést a fejlesztés során.

11.3.2 SA-15 – Fejlesztési folyamat, szabványok és eszközök: Formális szabványokat állapít meg a biztonságos alkalmazásfejlesztésre.

11.3.3 SI-10 – Információbevitel ellenőrzése: Előírja az injektálási és feldolgozási támadások megelőzésére szolgáló kontrollmechanizmusokat.

11.4 GDPR (2016/679)

11.4.1 25. cikk – Beépített és alapértelmezett adatvédelem: Előírja az adatvédelem és a magánszféra-védelem beépítését az alkalmazási logikába és a munkafolyamatokba.

11.4.2 32. cikk – Az adatkezelés biztonsága: Előírja a megfelelő technikai intézkedéseket, például a bemeneti adatok ellenőrzését, a titkosítást és a biztonságos hozzáférés-szabályozást.

11.5 NIS2 irányelv (2022/2555)

11.5.1 21. cikk (2) bekezdés f) pont: Előírja a sérülékenységkezelést és a biztonságos alkalmazás-életciklus gyakorlatokat az alapvető és fontos szervezetek számára.

11.5.2 23. cikk – Biztonsági incidensek jelentése: Szükségessé teszi az alkalmazásrétegű naplózási és felügyeleti képességeket a jelentős incidensek észleléséhez és bejelentéséhez.

11.6 DORA-rendelet (2022/2554)

11.6.1 9. cikk – IKT-kockázatkezelés: Kötelezi a pénzügyi szervezeteket annak biztosítására, hogy alkalmazásaik biztonságosak, teszteltek és kiberfenyegetésekkel szemben ellenállóak legyenek.

11.6.2 11. cikk – IKT-eszközök tesztelése: Ösztönzi a kritikus alkalmazások és szolgáltatások időszakos behatolástesztelését és red team gyakorlatok végrehajtását.

11.7 COBIT 2019

11.7.1 BAI03 – Megoldások azonosításának és kialakításának irányítása: Meghatározza a tervezési és kontrollkövetelményeket az alkalmazásfejlesztés során.

11.7.2 BAI09 – Alkalmazások kezelése: Hangsúlyozza az éles alkalmazások biztonságos fenntartását, felügyeletét és továbbfejlesztését.

11.7.3 DSS05 – Biztonsági szolgáltatások kezelése: Az alkalmazásvédelmet összekapcsolja a szervezet szélesebb körű biztonsági üzemeltetésével és kontrolljaival.