					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P25S					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**

Vonatkozó szabványokkal és jogszabályokkal összhangban

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	8. pont	Működési kontrollok, beleértve az alkalmazásbiztonságot
ISO/IEC 27002:2022	8.25–8.26. kontrollok	Biztonságos tervezés, fejlesztés, tesztelés és kódfelülvizsgálat
NIST SP 800-53 Rev.5	SA-11, SI-10	Fejlesztői és alkalmazástesztelés, kódelemzés, hibamegelőzés
EU GDPR	25. cikk	Beépített és alapértelmezett adatvédelem
EU NIS2	21. cikk (2) bekezdés a), e) pont	Technikai intézkedések az alkalmazások védelmére és a kockázatok észlelésére
EU DORA	9. cikk (2) bekezdés c) pont, 10. cikk (2) bekezdés c) pont	Alkalmazásbiztonság a digitális működési reziliencia érdekében
COBIT 2019	BAI03	Biztonságos szoftverfejlesztés és -beszerzés kezelése

1. Cél

1.1 Jelen szabályzat meghatározza azokat a minimális, kötelező alkalmazásbiztonsági kontrollokat, amelyek a szervezet által használt valamennyi szoftverre és rendszermegoldásra vonatkoznak, függetlenül attól, hogy azok belső fejlesztésűek vagy külső beszállítóktól kerülnek beszerzésre.

1.2 Biztosítja, hogy az alkalmazások tervezése, megvalósítása és fenntartása alkalmas legyen az ügyfél-, munkavállalói és üzleti adatok jogosulatlan hozzáféréssel, visszaélésszerű használattal, módosítással vagy megsemmisítéssel szembeni védelmére.

1.3 Jelen szabályzat támogatja a szervezet ISO/IEC 27001 tanúsításának megszerzésére és fenntartására irányuló törekvéseit, a GDPR- és NIS2-kötelezettségek teljesítését, valamint a nem biztonságos szoftverbevezetésekhez kapcsolódó működési kockázatok csökkentését.

1.4 A szabályzat elősegíti az alkalmazásbiztonság egységes, auditkész megközelítésének kialakítását a KKV-k számára azáltal, hogy az alkalmazandó biztonsági funkciók és gyakorlatok egységes ellenőrzőlistáját határozza meg, a korlátozott belső műszaki erőforrásokkal rendelkező környezetekhez igazítva.

2. Hatály

2.1 Jelen szabályzat hatálya kiterjed minden olyan alkalmazásra, rendszerre, eszközre és platformra, amely:

2.1.1 belső fejlesztésű, testre szabott vagy belső használatra szkriptelt,

2.1.2 kereskedelmi szoftverként, SaaS-megoldásként vagy felhőalapú rendszerként kerül beszerzésre,

2.1.3 személyazonosításra alkalmas adatokat (PII), üzleti nyilvántartásokat vagy érzékeny működési információkat kezel, tárol vagy továbbít,

2.1.4 munkavállalók, vállalkozók, ügyfelek vagy partnerek által belső hálózaton, az interneten vagy mobilplatformokon keresztül érhető el.

2.2 A szabályzat az alábbiakra terjed ki:

2.2.1 fejlesztők (belső vagy szerződött),

2.2.2 szoftverbeszállítók és felhőszolgáltatók,

2.2.3 bevezetésért és támogatásért felelős IT-támogatási személyzet vagy rendszergazdák,

2.2.4 a rendszerjóváhagyásban és felügyeletben részt vevő alkalmazástulajdonosok és üzleti felhasználók.

3. Célkitűzések

3.1 Annak biztosítása, hogy a szervezet által használt valamennyi alkalmazás beépített és ellenőrizhető biztonsági kontrollokkal rendelkezzen, amelyek csökkentik a gyakori szoftversérülékenységek kockázatát.

3.2 Az alkalmazások által kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának védelme, függetlenül azok üzemeltetési helyétől.

3.3 Az alkalmazásbiztonság formális tesztelésének, felülvizsgálatának és ellenőrzésének előírása minden új alkalmazás vagy jelentős frissítés éles használatának jóváhagyása előtt.

3.4 A felhasználói hitelesítő adatok, a munkamenetadatok és a hozzáférési jogosultságok következetes és biztonságos kezelésének biztosítása valamennyi üzletmenet-kritikus rendszerben.

3.5 Biztonságos naplózási, auditálási és felügyeleti funkciók előírása minden alkalmazásban a gyanús tevékenységek észlelésének és az ezekre adott válaszintézkedések támogatása érdekében.

3.6 A jogi és megfelelési kockázatok csökkentése annak biztosításával, hogy az alkalmazások megfeleljenek a vonatkozó szabályozói biztonsági követelményeknek.

4. Szerepkörök és felelősségi körök

4.1 Ügyvezető (GM)

4.1.1 Átfogó felelősséggel tartozik az alkalmazásbiztonságért a teljes szervezetben.

4.1.2 Jóváhagyja jelen szabályzatot, és biztosítja, hogy minden beszerzési vagy fejlesztési projekt megfeleljen annak.

4.1.3 Biztosítja, hogy a beszállítókat és szolgáltatókat szerződés kötelezze az alkalmazásbiztonsági követelmények teljesítésére.

4.1.4 Felülvizsgálja és jóváhagyja a kockázati kivételeket azokban az esetekben, amikor a teljes megfelelés üzleti korlátok miatt nem biztosítható.

4.2 Alkalmazástulajdonos (ha kijelölt)

4.2.1 Azonosítja az alkalmazásspecifikus biztonsági igényeket a rendszerkiválasztás vagy a projektindítás során.

4.2.2 Ellenőrzi, hogy a kulcsfontosságú funkciók, például a bejelentkezés-védelem, a titkosítás és a tevékenységnaplózás rendelkezésre állnak-e.

4.2.3 Részt vesz a bevezetés előtti felülvizsgálatokban, és megerősíti, hogy a biztonsági kontrollok megfelelnek az üzleti igényeknek.

4.3 Fejlesztő / IT-támogatási szolgáltató

4.3.1 A jelen szabályzattal összhangban alkalmazza a biztonságos fejlesztési és bevezetési gyakorlatokat.

4.3.2 Ellenőrzőlistákat és eszközöket használ annak igazolására, hogy a szoftver megfelel az alapvető biztonsági követelményeknek.

4.3.3 Kezeli a tesztelést, a hozzáférés-szabályozást és a biztonsági konfigurációkat a rendszer beállítása során.

4.4 Külső beszállítók és szoftverszállítók

4.4.1 Kötelesek megfelelni jelen szabályzatnak, amikor a szervezet által használt bármely szoftvert biztosítanak, fejlesztenek vagy üzemeltetnek.

4.4.2 Megerősítik, hogy a szállított alkalmazások megfelelnek a jelen szabályzatban meghatározott minimális biztonsági funkcióknak.

4.4.3 A sérülékenységekre haladéktalanul reagálnak, és a szoftver teljes életciklusa során fenntartják a biztonságos konfigurációt.

5. Irányítási követelmények

5.1 Az ügyvezetőnek (GM) felügyeletet kell fenntartania a szervezet által használt összes szoftveralkalmazás felett, biztosítva, hogy minden fejlesztési és beszerzési folyamat megfeleljen jelen szabályzatnak.

5.2 A beszerzés vagy fejlesztés megkezdése előtt az alkalmazáskövetelményeket felül kell vizsgálni annak biztosítása érdekében, hogy azok tartalmazzák az alábbiakat:

5.2.1 a felhasználói hozzáférés és a felhasználóhitelesítés biztonsága,

5.2.2 biztonságos adattárolás és adattovábbítás,

5.2.3 auditnaplózás és hibakezelés,

5.2.4 munkamenet-időtúllépés és az érvénytelen hozzáférések elleni kontrollok,

5.2.5 sérülékenységek helyesbítő intézkedési mechanizmusai.

5.3 Minden, harmadik fél beszállítóval vagy felhőszolgáltatóval kötött szerződésnek:

5.3.1 jelen szabályzattal összhangban álló, kikényszeríthető biztonsági követelményeket kell tartalmaznia,

5.3.2 meg kell határoznia a sérülékenységek közzétételére, a válaszidőre és a javítások telepítésére vonatkozó kötelezettségeket,

5.3.3 biztosítania kell a szervezet számára a jogot arra, hogy a biztonsági funkciók vagy a tesztelési eredmények igazolását kérje.

5.4 Az alkalmazásdokumentációnak és a nyilvántartásoknak legalább az alábbiakat kell tartalmazniuk:

5.4.1 az alkalmazás neve, verziója és tulajdonosa,

5.4.2 a beszállító vagy fejlesztő kapcsolattartási adatai,

5.4.3 a használatba vétel előtt megerősített biztonsági funkciók,

5.4.4 a tesztelésre, jóváhagyásra és kivételekre vonatkozó nyilvántartások.

5.5 Minden rendszert az ügyvezetőnek vagy a kijelölt alkalmazástulajdonosnak jóvá kell hagynia, mielőtt az éles környezetben használatba kerül.

5.6 Az alkalmazásban használt minden külső eszközt, bővítményt vagy kódkönyvtárat nyilván kell tartani, és évente felül kell vizsgálni biztonsági hatás és javításkezelési állapot szempontjából.

6. A szabályzat végrehajtására vonatkozó követelmények

6.1 Alapvető biztonsági funkciók minden alkalmazás esetében

6.1.1 Minden fejlesztett, beszerzett vagy használt alkalmazásnak az alábbi minimális kontrollokat kell tartalmaznia:

6.1.1.1 Bemeneti adatok ellenőrzése: Minden beviteli mezőt (pl. űrlapok, lekérdezések, fájlfeltöltések) tisztítani és ellenőrizni kell az injektálási vagy kódfuttatási támadások megelőzése érdekében.

6.1.1.2 Hitelesítési kontrollok: Az alkalmazásoknak erős hitelesítést kell kikényszeríteniük, beleértve a minimális jelszóerősséget, a sikertelen próbálkozásokat követő zárolást és a munkamenet-időtúllépést.

6.1.1.3 Munkamenet-kezelés: A munkamenetadatoknak 15 perc inaktivitást követően le kell járniuk, és ahol alkalmazható, időtúllépési figyelmeztetést kell megjeleníteni.

6.1.1.4 Adattitkosítás: Minden érzékeny adatot vagy személyazonosításra alkalmas adatot (PII) titkosítani kell továbbítás közben (pl. HTTPS, Transport Layer Security [TLS]) és nyugalmi állapotban is (pl. titkosított lemezek, biztonságos adatbázismezők).

6.1.1.5 Hibakezelés: A rendszerhibákat el kell rejteni a felhasználók elől, és azok kizárólag jogosult műszaki munkatársak számára lehetnek láthatók. A naplóknak a hibákat biztonságosan kell rögzíteniük.

6.1.1.6 Hozzáférés-szabályozás: A felhasználói szerepkörök tekintetében a legkisebb jogosultság elvének érvényesítésére szerepköralapú hozzáférés-szabályozást (RBAC) vagy azzal egyenértékű mechanizmust kell alkalmazni.

6.1.1.7 Auditnaplózás: Az alkalmazásoknak naplózniuk kell a hitelesítési eseményeket (bejelentkezések, kijelentkezések, sikertelen próbálkozások), az adathozzáférést és az adminisztratív változtatásokat.

6.2 Alkalmazástesztelés és ellenőrzés

6.2.1 Bevezetés előtt minden alkalmazásnak alkalmazásbiztonsági tesztelésen kell átesnie, amely igazolja a fent felsorolt alapvető funkciók meglétét.

6.2.2 A tesztelést az alábbiak valamelyikének kell elvégeznie:

6.2.2.1 az IT-támogatási szolgáltatónak vagy belső fejlesztőnek (kis projektek esetén),

6.2.2.2 független tesztelőnek vagy harmadik fél biztonsági értékelőnek (összetett rendszerek vagy felhőalapú szolgáltatások esetén).

6.2.3 A tesztelési nyilvántartásoknak tartalmazniuk kell:

6.2.3.1 a teszt dátumát és a tesztelő nevét,

6.2.3.2 a tesztelt funkciók ellenőrzőlistáját és a megállapításokat,

6.2.3.3 a feltárt problémák összefoglalását és a megtett kockázatcsökkentő intézkedéseket.

6.2.4 Az az alkalmazás, amely nem felel meg a minimális követelményeknek, a helyesbítő intézkedések végrehajtásáig nem hagyható jóvá használatra.

6.3 Beszállítói alkalmazások

6.3.1 Harmadik fél alkalmazásainak megvásárlásakor vagy előfizetésekor a beszállítóknak írásban meg kell erősíteniük, hogy az alábbi funkciók rendelkezésre állnak:

6.3.1.1 biztonságos bejelentkezés zárolással és munkamenet-időtúllépéssel,

6.3.1.2 bemeneti adatok ellenőrzése és védelem a gyakori webes sérülékenységekkel szemben,

6.3.1.3 érzékeny adatok vagy személyazonosításra alkalmas adatok (PII) titkosítása továbbítás közben és nyugalmi állapotban,

6.3.1.4 tevékenységnaplózás a felhasználói hozzáférésekre és adminisztratív változtatásokra,

6.3.1.5 az ismert sérülékenységek haladéktalan javítása.

6.3.2 Az ügyvezetőnek, ahol alkalmazható, dokumentációt vagy tanúsítványokat (pl. SOC 2, ISO 27001, biztonsági tesztjelentések) kell kérnie a beszállítói megfelelés igazolására.

6.3.3 Ha a beszállító bármely követelményt nem tud teljesíteni, az ügyvezető által felülvizsgált és jóváhagyott formális kivétel szükséges, kompenzáló kontrollok alkalmazása mellett.

6.4 Nyílt forráskódú vagy külső komponensek használata

6.4.1 A nyílt forráskódú könyvtáraknak, bővítményeknek vagy moduloknak:

6.4.1.1 kizárólag megbízható adattárakból vagy hivatalos forrásokból kell származniuk,

6.4.1.2 használat előtt ismert sérülékenységek szempontjából vizsgálaton kell átesniük,

6.4.1.3 rendszeresen frissítésre kell kerülniük, amikor javítások vagy új verziók jelennek meg.

6.4.2 A fejlesztőnek vagy IT-szolgáltatónak nyilvántartást kell vezetnie minden használt külső komponensről, amely legalább az alábbiakat tartalmazza:

6.4.2.1 a komponens neve és verziója,

6.4.2.2 a forrásadattár vagy beszállító,

6.4.2.3 az ismert sérülékenységek és a helyesbítő intézkedések állapota.

6.4.3 Ha kritikus sérülékenység kerül azonosításra, és javítás nem áll rendelkezésre, a komponenst el kell távolítani vagy le kell cserélni.

6.5 Adatkezelés és adatvédelmi támogatás

6.5.1 Azoknak az alkalmazásoknak, amelyek személyes, pénzügyi vagy üzletileg érzékeny adatokat kezelnek vagy tárolnak, az alábbi követelményeknek kell megfelelniük:

6.5.1.1 Az adatokat iparági szabvány szerinti módszerekkel kell titkosítani (pl. AES-256, Transport Layer Security [TLS] 1.2+).

6.5.1.2 A jogosulatlan hozzáférést hozzáférés-szabályozással és a feladatkörök elkülönítésével kell megelőzni.

6.5.1.3 Lehetővé kell tenni a személyes adatok biztonságos exportját és törlését, ha azt jogszabály előírja (pl. GDPR 17. cikk – törléshez való jog).

6.5.1.4 Biztosítani kell, hogy jelszavak és titkos információk soha ne kerüljenek tárolásra olvasható szövegként, és ne legyenek beágyazva az alkalmazáskódba.

6.6 Az alkalmazás által létrehozott naplókra és biztonsági mentési adatokra a szervezet P14S – Adatmegőrzési és megsemmisítési szabályzatában meghatározott megőrzési, megsemmisítési és osztályozási követelmények vonatkoznak.

7. Kockázatkezelés és kivételek

7.1 A jelen szabályzat bármely alkalmazásbiztonsági követelménye alól kizárólag az ügyvezető által kezdeményezett formális kivételkezelési folyamat keretében adható felmentés.

7.2 A kivételkezelési folyamatnak az alábbiakat kell tartalmaznia:

7.2.1 a hiányzó funkció vagy a meg nem felelés leírását,

7.2.2 a kivétel indokolását (pl. üzleti szükséglet, műszaki korlát),

7.2.3 a kivétel által bevezetett biztonsági kockázatok értékelését,

7.2.4 az átmeneti vagy kompenzáló kontrollok leírását,

7.2.5 a probléma megoldásának vagy az újraértékelésnek az ütemezését.

7.3 A jóváhagyott kivételeket dokumentálni kell, és felül kell vizsgálni:

7.3.1 legalább 6 havonta, vagy

7.3.2 azonnal, ha kapcsolódó incidens vagy sérülékenység kerül feltárásra.

7.4 Az ügyvezető nem engedélyezhet kivételt, ha az szabályozói, szerződéses vagy jogi kötelezettségek megsértését eredményezné (pl. GDPR, DORA, NIS2).

7.5 Ha bármely alkalmazás ismétlődő biztonsági problémák ismert forrásává válik, vagy a helyesbítő intézkedés nem hajtható végre, az ügyvezetőnek mérlegelnie kell az alkalmazás kivonását vagy cseréjét.

8. Végrehajtás és megfelelés

8.1 Kötelező megfelelés

8.1.1 Minden munkavállaló, fejlesztő, vállalkozó, IT-szolgáltató és szoftverbeszállító köteles megfelelni jelen szabályzatnak, amikor a szervezet nevében alkalmazásokat fejleszt, kezel vagy vezet be.

8.1.2 Az ügyvezető (GM) felelős annak biztosításáért, hogy az alkalmazásbiztonsági követelmények a szervezet egészében érvényesüljenek, és hogy a beszállítók szerződés alapján elszámoltathatók legyenek a biztonsági funkciókért és kötelezettségeik teljesítéséért.

8.1.3 Jelen szabályzat alkalmazásának elmulasztása megfelelőségi szabálysértésnek minősül, függetlenül attól, hogy az alkalmazás belső fejlesztésű vagy külső forrásból származik.

8.2 Szabálysértési példák és helyesbítő intézkedések

8.2.1 A szabálysértések például az alábbiak lehetnek:

8.2.1.1 szoftver bevezetése hitelesítési kontrollok nélkül,

8.2.1.2 olyan alkalmazások használata, amelyek érzékeny információkat olvasható szövegként naplóznak,

8.2.1.3 nem ellenőrzött bemenet engedélyezése éles alkalmazásokban,

8.2.1.4 ismert sérülékenységek javításának elmulasztása külső kódban,

8.2.1.5 a kötelező tesztelés figyelmen kívül hagyása az éles indulás előtt.

8.3 A szabálysértések következményei lehetnek:

8.3.1 az alkalmazás vagy szolgáltatás azonnali felfüggesztése,

8.3.2 a beszállítói vagy vállalkozói hozzáférés visszavonása,

8.3.3 írásbeli figyelmeztetés vagy ismételt képzés a belső munkatársak részére,

8.3.4 szerződések megszüntetése vagy fegyelmi eljárás ismétlődő meg nem felelés esetén,

8.3.5 jogi és szabályozói eszkaláció incidens vagy súlyos gondatlanság esetén,

8.3.6 minden azonosított szabálysértést haladéktalanul jelenteni kell az ügyvezetőnek. Az incidensnyilvántartásokat és a helyesbítő intézkedéseket dokumentálni és auditcélból megőrizni kell.

8.4 Auditkészség és dokumentáció

8.4.1 A szervezetnek olyan dokumentációt kell fenntartania, amely igazolja, hogyan teljesülnek az alkalmazásbiztonsági követelmények. Ennek részei:

8.4.1.1 beszállítói megerősítések,

8.4.1.2 tesztelési jelentések,

8.4.1.3 biztonsági ellenőrzőlisták,

8.4.1.4 kivételnyilvántartások,

8.4.1.5 felülvizsgálati jóváhagyások.

8.4.2 Az ügyvezetőnek biztosítania kell, hogy ezek a nyilvántartások hozzáférhetők legyenek belső felülvizsgálatok, valamint az ISO/IEC 27001 tanúsításhoz, szabályozói ellenőrzésekhez vagy szerződéses biztonsági kötelezettségekhez kapcsolódó külső auditok során.

8.4.3 A beszállítók és IT-szolgáltatók kötelesek együttműködni további megfelelőségi bizonyítékok rendelkezésre bocsátásában, ha azt az ügyvezető, ügyfelek, auditorok vagy szabályozó hatóságok kérik.

9. Felülvizsgálati és frissítési követelmények

9.1 Jelen szabályzatot az ügyvezetőnek naptári évente legalább egyszer felül kell vizsgálnia az alábbiak érdekében:

9.1.1 a szabályozói követelmények változásainak nyomon követése (pl. GDPR, NIS2, DORA),

9.1.2 az új vagy kialakulóban lévő fenyegetések és támadási technikák beépítése,

9.1.3 a megfogalmazás és a követelmények aktualizálása a platformok, beszállítók vagy fejlesztési módszerek változásainak megfelelően.

9.2 Soron kívüli felülvizsgálatot kell végezni akkor is, ha:

9.2.1 új alkalmazások kerülnek bevezetésre,

9.2.2 meglévő alkalmazások jelentős frissítésen vagy integráción mennek keresztül,

9.2.3 alkalmazással kapcsolatos incidens vagy adatsértés történik,

9.2.4 külső tájékoztatók vagy iparági riasztások alapján új kockázatokat azonosítanak.

9.3 Jelen szabályzat minden frissítésének:

9.3.1 az ügyvezető jóváhagyásával kell rendelkeznie,

9.3.2 dokumentáltnak kell lennie verzióelőzményekkel és a változtatás indokával,

9.3.3 kommunikálásra kell kerülnie az alkalmazáskezelésben érintett valamennyi munkavállaló, fejlesztő és beszállító felé,

9.3.4 biztonságosan tárolva kell lennie audit- és megfelelési hivatkozási célokra.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzatot közvetlenül támogatják, és végrehajtását erősítik az alábbi, KKV-igényekhez igazított biztonsági szabályzatok:

10.1.1 P2S – Irányítási szerepkörök és felelősségek szabályzata: Meghatározza az alkalmazások jóváhagyásáért, a szabályzat végrehajtásáért és a beszállítók kezeléséért fennálló felelősségi köröket.

10.1.2 P4S – Hozzáférés-szabályozási szabályzat: Biztosítja, hogy az alkalmazáshoz való hozzáférés összhangban legyen a minimális jogosultság és a munkamenet-kezelés elveivel.

10.1.3 P8S – Információbiztonsági tudatossági és képzési szabályzat: Biztosítja, hogy a felhasználók és fejlesztők képzést kapjanak az alkalmazásokhoz kapcsolódó fenyegetések felismeréséről és jelentéséről.

10.1.4 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: Meghatározza azokat az adatvédelmi biztosítékokat, amelyeket minden személyes információt kezelő alkalmazásnak érvényesítenie kell.

10.1.5 P14S – Adatmegőrzési és megsemmisítési szabályzat: Szabályozza, hogy az alkalmazások által létrehozott naplókat, biztonsági mentéseket és érzékeny adatokat hogyan kell megőrizni, archiválni és biztonságosan megsemmisíteni.

10.1.6 P30S – Incidenskezelési szabályzat: Meghatározza az alkalmazásokhoz kapcsolódó biztonsági események azonosításának, jelentésének és elszigetelésének lépéseit.

10.2 Ezek a szabályzatok együttesen biztosítják, hogy az alkalmazásbiztonság teljes mértékben beépüljön a szervezet információbiztonsági irányítási rendszerébe (ISMS), és támogassa az auditkészséget.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 8.1. pont – Előírja, hogy a szervezetek működési kontrollokat alakítsanak ki az információbiztonsági kockázatok kezelésére, beleértve az alkalmazásokhoz és szoftverrendszerekhez kapcsolódó kockázatokat is.

11.2 ISO/IEC 27002

11.2.1 8.25. kontroll – Javasolja a biztonságos tervezési, fejlesztési és kódfelülvizsgálati gyakorlatok bevezetését valamennyi alkalmazás esetében, beleértve a beszállítók által biztosított alkalmazásokat is.

11.2.2 8.26. kontroll – Javasolja az alkalmazásbiztonsági kontrollok formális tesztelését, különösen a hozzáférés-szabályozás, a bemeneti adatok ellenőrzése és a munkamenet-kezelés területén.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Meghatározza a fejlesztői tesztelésre, a kódelemzésre és a dinamikus alkalmazásvizsgálatra vonatkozó követelményeket a bevezetés előtt.

11.3.2 SI-10 – A gyakori szoftverhibák észlelésével és megelőzésével foglalkozik, hangsúlyozva a fejlesztői tudatosságot és a technikai védelmi intézkedéseket.

11.4 EU GDPR (2016/679)

11.4.1 25. cikk – A „Beépített és alapértelmezett adatvédelem” előírja az adatvédelem és a biztonság beépítését a személyes adatokat kezelő alkalmazások alapvető tervezésébe.

11.5 EU NIS2 irányelv (2022/2555)

11.5.1 21. cikk (2) bekezdés a) és e) pont – Előírja, hogy az alapvető és fontos szervezetek technikai intézkedéseket vezessenek be az alkalmazások védelmére és a szoftverekhez kapcsolódó kockázatok észlelésére.

11.6 EU DORA (2022/2554)

11.6.1 9. cikk (2) bekezdés c) pont, 10. cikk (2) bekezdés c) pont – Előírja, hogy a pénzügyi szektorban működő KKV-k alkalmazásszintű biztonsági kontrollokat építsenek be, és rendszeres értékeléseket végezzenek a digitális működési reziliencia fenntartása érdekében.

11.7 COBIT 2019

11.7.1 BAI03 – A „Megoldások azonosításának és kialakításának kezelése” útmutatást ad a biztonságos szoftverek fejlesztéséhez vagy beszerzéséhez a kockázatokkal, a megfeleléssel és az üzleti követelményekkel összhangban, még erőforrás-korlátozott KKV-környezetben is.