| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Ide írja be a bejegyzett jogi személy nevét | | | | | | | |
| Dokumentumszám:<br>P24 | | | | | Dokumentum címe:<br>**Biztonságos fejlesztési szabályzat** | | | | | | | |
| Verzió:<br>1.0 | | Hatálybalépés dátuma:<br>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** |
| | | | |
| | | | |

## 1. Cél

1.1 Jelen szabályzat meghatározza a szervezeten belüli szoftver- és rendszerfejlesztési tevékenységekre vonatkozó kötelező biztonsági követelményeket, ideértve a belső projekteket, a kiszervezett fejlesztést és a harmadik féltől származó kód integrálását.

1.2 A cél annak biztosítása, hogy a biztonság a szoftverfejlesztési életciklus (SDLC) teljes egészébe beépüljön, és hogy a sérülékenységeket az éles bevezetést megelőzően azonosítsák, mérsékeljék és megelőzzék.

1.3 Jelen szabályzat támogatja az ISO/IEC 27001:2022 8. pontjának és az A melléklet 8.25–8. kontrolljainak alkalmazását a biztonságos fejlesztés irányításának, a kódfelülvizsgálati gyakorlatoknak és a harmadik fél által végzett fejlesztés felügyeletének egységesítésével.

## 2. Hatály

### 2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 Belsőleg vagy külső fél által fejlesztett szoftverekre, alkalmazásokra, szkriptekre, integrációkra és automatizálási eszközökre

2.1.2 Fejlesztőcsapatokra, terméktulajdonosokra, DevOps, QA, architekt, projektmenedzseri és vállalkozói szerepkörökre

2.1.3 Az SDLC környezeteire, beleértve a fejlesztői, tesztelési, előéles és éleshez közeli környezeteket

2.1.4 A belső alkalmazásokba integrált nyílt forráskódú és harmadik féltől származó komponensekre

2.1.5 A helyszíni, privát felhő, hibrid vagy nyilvános felhő környezetekben bevezetett szoftverekre

2.2 Jelen szabályzat hatálya alá tartozik valamennyi felhasználó és szervezeti szereplő, aki a szervezeti környezetben rendszerfejlesztésben, tesztelésben vagy bevezetésben vesz részt, beleértve a menedzselt szolgáltatókat és platformszolgáltatókat is.

## 3. Célkitűzések

3.1 A biztonsági kontrollok beépítése a szoftverfejlesztés valamennyi szakaszába, a tervezéstől a bevezetésig, annak biztosítása érdekében, hogy a kockázatcsökkentés proaktív és folyamatos legyen.

3.2 A kihasználható sérülékenységek bevezetésének megelőzése, ideértve különösen az injektálási hibákat, a nem biztonságos hitelesítést és az ismert, harmadik féltől származó gyengeségeknek való kitettséget.

3.3 Olyan biztonságos kódolási gyakorlatok kialakítása és alkalmazása, amelyek összhangban állnak az OWASP, a SANS CWE és a keretrendszer-specifikus iránymutatásokkal.

3.4 Annak biztosítása, hogy valamennyi kód éles bevezetés előtt társfelülvizsgálaton, automatizált elemzésen és biztonsági ellenőrzésen essen át.

3.5 A kiszervezett tevékenységekből, a harmadik féltől származó kód beemeléséből és a nyílt forráskódú szoftverek újrafelhasználásából eredő fejlesztési kockázatok kezelése.

3.6 A fejlesztői, teszt- és előéles környezetek védelme a jogosulatlan hozzáféréssel szemben, valamint az éles adatok használatának megakadályozása jóváhagyott adatmaszkolás vagy anonimizálás nélkül.

3.7 A fejlesztők, termékmenedzserek és minőségbiztosítási szakemberek biztonságtudatosságának erősítése szerepköralapú képzés és a kialakuló fenyegetésekről szóló folyamatos tájékoztatás útján.

## 4. Szerepkörök és felelősségi körök

### 4.1 Információbiztonsági vezető

4.1.1 Jelen szabályzat gazdája, és biztosítja, hogy a biztonságos fejlesztés követelményeit szervezeti szinten alkalmazzák.

4.1.2 Jóváhagyja a biztonságos kódolási szabványokat és a harmadik fél által végzett fejlesztésre vonatkozó megállapodásokat.

4.1.3 Felülvizsgálja a nem megszüntetett vagy elhalasztott sérülékenységekre vonatkozó kockázatkezelési döntéseket.

**4.2 Alkalmazásbiztonsági vezető / DevSecOps vezető**

4.2.1 Kidolgozza, karbantartja és közzéteszi a biztonságos kódolási iránymutatásokat.

4.2.2 Integrálja a statikus és dinamikus biztonsági tesztelést a CI/CD folyamatokba.

4.2.3 Kódbiztonsági felülvizsgálatokat végez, és meghatározza a kötelező helyesbítő intézkedéseket.

[ ... 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, vagy az alábbi esetekben ennél gyakrabban felül kell vizsgálni:**

9.1.1 a fejlesztési módszertanokban vagy a DevOps eszközkészletben végrehajtott jelentős módosítások esetén

9.1.2 alkalmazássérülékenységekből eredő jelentős biztonsági incidensek esetén

9.1.3 a biztonságos szoftverfejlesztésre vonatkozó szabályozási követelmények változása esetén (pl. GDPR, DORA)

9.1.4 új iparági szabványok vagy fenyegetettségi információk megjelenése esetén (pl. OWASP Top 10, SLSA, MITRE CWE)

9.2 A szabályzat felülvizsgálatát az alkalmazásbiztonsági vezető vezeti az információbiztonsági vezetővel, a szoftverarchitektekkel, a QA vezetőkkel és a jogi tanácsadóval együttműködésben (a harmadik féltől származó kód következményei tekintetében).

9.3 Minden módosítást rögzíteni kell a dokumentumkontroll-nyilvántartásban, verziókezelés alá kell vonni, és a változásokról az érintett csapatokat kiadási megjegyzések vagy kötelező képzés útján tájékoztatni kell.

9.4 Az előző verziókat a jogi és auditcélú visszakövethetőség biztosítása érdekében az archív adattárban meg kell őrizni.

**10. Kapcsolódó szabályzatok és összefüggések**

10.1 P1 – Információbiztonsági szabályzat. Meghatározza azt a stratégiai elvárást, hogy a biztonság minden információs rendszerbe beépüljön, amelynek a biztonságos fejlesztés alapvető operatív kontrollja.

10.2 P4 – Hozzáférés-szabályozási szabályzat. Meghatározza a fejlesztői környezetekhez, adattárakhoz, build eszközökhöz és CI/CD folyamatokhoz való hozzáférés korlátozására szolgáló kontrollintézkedéseket.

10.3 P5 – Változáskezelési szabályzat. Biztosítja, hogy a kódmódosítások, kiadások és bevezetések megfelelő jóváhagyáshoz, visszaállítási tervezéshez és bevezetést követő ellenőrzéshez kötöttek legyenek.

10.4 P12 – Eszközkezelési szabályzat. Támogatja a fejlesztői környezetek, forráskód-adattárak és build rendszerek mint kezelt, osztályozott és védett eszközök nyilvántartását.

10.5 P22 – Naplózási és felügyeleti szabályzat. A fejlesztési folyamatokra is alkalmazandó annak biztosítására, hogy a build folyamatok, a kód továbbítása és a bevezetési események naplózása, felügyelete és a biztonsági rendellenességek szempontjából történő elemzése megtörténjen.

10.6 P30 – Incidenskezelési szabályzat. Keretet biztosít az éles bevezetést követően vagy az alkalmazásbiztonsági tesztelés során feltárt biztonsági hibák elemzéséhez és kezeléséhez.

## 11. Hivatkozott szabványok és keretrendszerek

### 11.1 ISO/IEC 27001

11.1.1 8. pont – Működési tervezés és szabályozás: előírja a biztonságos fejlesztési folyamatok és kontrollok működésbe történő integrálását.

### 11.2 ISO/IEC 27002:2022 – 8.25–8. kontrollok

11.2.1 A melléklet 8.25. kontroll – Biztonságos fejlesztési életciklus: előírja a biztonság formális beépítését a szoftvertervezésbe és -fejlesztésbe.

11.2.2 A melléklet 8.26. kontroll – Alkalmazásbiztonsági követelmények: előírja a biztonságos kódolási és biztonsági átvételi kritériumok meghatározását.

11.2.3 A melléklet 8.27. kontroll – Biztonságos rendszerarchitektúra és mérnöki alapelvek: megköveteli a biztonságos tervezési alapelvek alkalmazását és az ismert gyengeségek kockázatcsökkentését.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3–SA-15: strukturált alkalmazásbiztonsági fejlesztési gyakorlatokat állapít meg, beleértve a tervezésre, a kód sértetlenségére és a tesztelésre vonatkozó követelményeket.

11.3.2 SI-10 – Információs bemenetellenőrzés: a biztonságos kódolási védelmekre vonatkozik.

11.3.3 SR-3 – Ellátásilánc-védelem: előírja a harmadik féltől származó szoftverek, komponensek és fejlesztési szolgáltatók átvilágítását.

### 11.4 GDPR (2016/679)

11.4.1 25. cikk – Beépített és alapértelmezett adatvédelem: előírja a biztonság és az adatvédelem beépítését a rendszerfejlesztésbe.

11.4.2 32. cikk – Az adatkezelés biztonsága: támogatja az olyan technikai intézkedéseket, mint a bemenetellenőrzés, a hozzáférés-szabályozás és a biztonságos bevezetés.

### 11.5 NIS2 irányelv (2022/2555)

11.5.1 21. cikk (2) bekezdés e)–f): olyan szoftverfejlesztési gyakorlatokat ír elő, amelyek magukban foglalják a sérülékenységkezelést, a kódbiztonságot és az incidensjelentést.

### 11.6 DORA-rendelet (2022/2554)

11.6.1 9. cikk – IKT-kockázatkezelés: megköveteli a pénzügyi szervezetek számára a biztonságos fejlesztési gyakorlatokat, ideértve a szoftverminőségi kontrollokat és a hibák helyesbítését.

11.6.2 10. cikk – Üzletmenet-folytonosság és tesztelés: ösztönzi az IKT-rendszerek, köztük az alkalmazások szigorú tesztelését és ellenőrzését.

### 11.7 COBIT 2019

11.7.1 BAI03 – Megoldások azonosításának és megvalósításának kezelése: szabályozza a tervezést, a fejlesztést és a biztonság új megoldásokba történő integrálását.

11.7.2 BAI07 – Változások elfogadásának és átvezetésének kezelése: biztosítja a biztonságos bevezetést és a bevezetést követő értékelést.

11.7.3 DSS05 – Biztonsági szolgáltatások kezelése: alkalmazza a biztonsági ellenőrzést a szoftverekre és a szolgáltatásnyújtásra.