					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P24S					Dokumentum címe: **Biztonságos fejlesztési 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	Releváns biztonsági kontrollok az üzemeltetési gyakorlatokra, beleértve a biztonságos fejlesztést
ISO/IEC 27002:2022	8.25–8.27 kontrollok	Lefedi a biztonságos fejlesztési életciklust, a tesztelést és a külső fejlesztők biztonsági felelősségeit
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Kiterjed a biztonságos szoftverfejlesztési életciklusra, a hozzáférés-szabályozásra és a sérülékenységkezelésre a fejlesztés során
EU GDPR	25. cikk	Előírja a beépített és alapértelmezett adatvédelem alkalmazását a szoftverfejlesztés során
EU NIS2	21. cikk (2) bekezdés a), e), h) pont	Előírja a biztonságos fejlesztési szabályzatokat, a nyílt forráskódú elemek használatának felügyeletét és a kockázatcsökkentés dokumentálását
EU DORA	6. cikk (7) bekezdés, 9. cikk (1) bekezdés c) pont, 10. cikk (2) bekezdés c) pont	Az üzletmenet-kritikus IKT-rendszerek fejlesztési életciklusára vonatkozó biztonsági követelmények a pénzügyi szektorban
COBIT 2019	BAI	Keretrendszer a strukturált, visszakövethető és reziliens biztonságos fejlesztés irányításához

1. Cél

1.1 Jelen szabályzat biztosítja, hogy a szervezet vagy külső partnerei által létrehozott vagy módosított valamennyi szoftver, szkript és webalapú eszköz biztonságosan kerüljön fejlesztésre, minimalizálva a sérülékenységek, a jogosulatlan adathozzáférés és a működési zavarok kockázatát.

1.2 Meghatározza azokat a kötelező biztonságos fejlesztési szabályokat és kódolási gyakorlatokat, amelyeket valamennyi belső fejlesztőnek, vállalkozónak és beszállítónak követnie kell, a projekt méretétől vagy összetettségétől függetlenül.

1.3 Jelen szabályzat célja az ügyféladatok védelme, az adatvédelmi incidensek megelőzése, valamint annak biztosítása, hogy a szervezet által vagy a szervezet számára létrehozott vagy testre szabott szoftverek megfeleljenek a biztonsági auditkövetelményeknek, teljesítsék a jogszabályi előírásokat (pl. GDPR, NIS2, DORA), és támogassák az ISO/IEC 27001 tanúsítást.

2. Hatály

2.1 Jelen szabályzat minden olyan személyre és szervezetre kiterjed, aki vagy amely a szervezet nevében az alábbiak fejlesztésében, testreszabásában, bevezetésében vagy kezelésében részt vesz:

2.1.1 Weboldalak, alkalmazások vagy automatizálási eszközök

2.1.2 Belső fejlesztésű szkriptek vagy szoftverek

2.1.3 Külső fejlesztők vagy szabadúszók által készített kód

2.1.4 Éles rendszerekbe integrált bővítmények, könyvtárak és szoftverkomponensek

2.2 Kiterjed továbbá a fejlesztési tevékenységekhez használt valamennyi környezetre, beleértve:

2.2.1 Fejlesztési és tesztkörnyezetek

2.2.2 Tesztelési és előéles környezetek

2.2.3 Egyedi fejlesztésű kód futtatására használt éles rendszerek

2.3 A szabályzat kiterjed továbbá az adatok fejlesztés és bevezetés során történő kezelésére, különös tekintettel az éles adatok nem éles rendszerekben történő felhasználására.

3. Célkitűzések

3.1 Megakadályozni a biztonsági hibák vagy sérülékenységek bekerülését az egyedi fejlesztésű vagy külső fél által fejlesztett szoftverekbe.

3.2 Biztosítani, hogy a biztonságos kódolási gyakorlatok és a sérülékenységek megelőzése a szoftverfejlesztési életciklus minden szakaszába beépüljön.

3.3 Csökkenteni a nyílt forráskódú vagy külső komponensek használatából eredő kockázatokat megfelelő átvilágítás és nyomon követés kötelező előírásával.

3.4 Előírni a formális kódfelülvizsgálatot és az alkalmazásbiztonsági tesztelést a kiadás előtt.

3.5 Szabályozni a fejlesztési környezetekhez való hozzáférést, és biztosítani azok elkülönítését az éles rendszerektől.

3.6 Teljesíteni a nemzetközi szabványok és jogszabályok szerinti kötelező követelményeket (pl. ISO/IEC 27001, GDPR, DORA, NIS2).

4. Szerepkörök és felelősségi körök

4.1 Ügyvezető igazgató

4.1.1 Jóváhagyja a szabályzatot, és felelős annak karbantartásáért.

4.1.2 Biztosítja, hogy valamennyi szoftverfejlesztés – belső vagy kiszervezett – megfeleljen jelen szabályzatnak.

4.1.3 Felülvizsgálja és aláírja a biztonságos fejlesztésre vonatkozó záradékokat tartalmazó fejlesztési vagy szolgáltatási szerződéseket.

4.1.4 Rendszeres egyeztetések vagy biztonsági bizonyítékok bekérése útján ellenőrzi a beszállítói megfelelést.

4.2 Belső fejlesztő vagy alkalmazástulajdonos

4.2.1 Betartja a biztonságos kódolási és bevezetési gyakorlatokat.

4.2.2 Minden projektre alkalmazza a biztonságos fejlesztési ellenőrzőlistát.

4.2.3 Ellenőrzi a felhasznált nyílt forráskódú vagy külső komponensek biztonságát.

4.2.4 Haladéktalanul jelenti az ügyvezető igazgatónak az észlelt sérülékenységeket.

[... 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 az ügyvezető igazgatónak legalább évente egyszer felül kell vizsgálnia annak érdekében, hogy:

9.1.1 Ellenőrizze az ISO/IEC 27001, a GDPR, a NIS2 és a DORA követelményeinek való folyamatos megfelelést

9.1.2 Tükrözze a frissített fenyegetéseket vagy a biztonságos fejlesztési bevált gyakorlatok változásait

9.1.3 Biztosítsa az új eszközökkel, platformokkal vagy beszállítói kapcsolatokkal való összeegyeztethetőséget

9.2 Soron kívüli felülvizsgálatot kell kezdeményezni az alábbi esetekben:

9.2.1 Bármely bejelentett szoftverbiztonsági incidens

9.2.2 Új fejlesztési keretrendszer vagy tárhelyplatform bevezetése

9.2.3 Külső fejlesztési partnerek változása

9.2.4 A szoftverre vagy a biztonsági kötelezettségekre hatással lévő szabályozási változások

9.3 A szabályzat valamennyi módosítását:

9.3.1 Dokumentálni kell dátummal, a változás összefoglalásával és az ügyvezető igazgató jóváhagyásával

9.3.2 Egyértelműen kommunikálni kell minden belső és külső fejlesztésben részt vevő személy felé

9.3.3 A szervezet szabályzati verziókezelésének és változáselőzményeinek részeként meg kell őrizni

9.4 A frissített verziókat könnyen hozzáférhetővé kell tenni belső platformokon, nyomtatott dokumentációban vagy a beszállítók számára elérhető felhőszolgáltatásokon keresztül.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat több más KKV-szabályzat eredményes végrehajtását támogatja, és azokhoz kapcsolódik:

10.1.1 P2S – Irányítási szerepkörök és felelősségek szabályzata: Meghatározza a fejlesztéshez kapcsolódó biztonsági kontrollok projektek és beszállítók közötti kijelölésének, valamint ellenőrzésének elszámoltathatóságát.

10.1.2 P4S – Hozzáférés-szabályozási szabályzat: Meghatározza a fejlesztési környezetekhez és kódtárakhoz való hozzáférés korlátozásának alapvető szabályait, beleértve a feladatkörök szétválasztását.

10.1.3 P8S – Információbiztonsági tudatossági és képzési szabályzat: Biztosítja, hogy a belső fejlesztők és vállalkozók ismerjék a biztonságos kódolási gyakorlatokat és a kapcsolódó biztonsági felelősségeket.

10.1.4 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: Meghatározza, hogy a személyes adatokat miként kell kezelni a fejlesztési, tesztelési és naplózási folyamatok során a GDPR-nak való megfelelés érdekében.

10.1.5 P30S – Incidenskezelési szabályzat: Meghatározza, hogy a fejlesztéssel kapcsolatos biztonsági incidenseket – beleértve a kódhoz kapcsolódó kitettségeket – hogyan kell jelenteni, értékelni és helyesbítő intézkedésekkel kezelni.

10.2 E szabályzatok együttesen biztosítják, hogy a biztonságos fejlesztés még kis méretű vagy alacsony technikai érettségű szervezetekben is megvalósítható és igazolható legyen.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 8.1 kontroll – Előírja az olyan üzemeltetési kontrollok bevezetését, ideértve a biztonságos fejlesztést is, amelyek összhangban állnak az üzleti célkitűzésekkel és a kockázati helyzettel.

11.2 ISO/IEC 27002

11.2.1 8.25 kontroll – Javasolja a biztonság integrálását a teljes szoftver-életciklusba, beleértve a forráskódkezelést, a verziókezelést és a fejlesztői hozzáférést.

11.2.2 8.26 kontroll – Meghatározza az alkalmazástesztelés módszereit és a biztonsági funkcionalitások ellenőrzését az élesítés előtt.

11.2.3 8.27 kontroll – Előírja, hogy a külső fejlesztők ugyanazon fejlesztési szabványokat kövessék, és biztonsági felelősségeik egyértelműen meghatározásra kerüljenek.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3–SA-15 – Meghatározza a biztonságos fejlesztési folyamatokat, beleértve a fejlesztői hozzáférés-szabályozást, a tesztelést, a fenyegetésmodellezést és a dokumentálást.

11.3.2 SI-10 – Előírja, hogy a fejlesztők azonosítsák és csökkentsék a gyakori szoftveres gyengeségeket, és ahol alkalmazható, automatizált eszközöket használjanak.

11.4 GDPR (2016/679)

11.4.1 25. cikk – A „beépített és alapértelmezett adatvédelem” előírja a biztonsági és adatvédelmi garanciák integrálását a szoftvertervezés és -fejlesztés során, különösen személyes adatok kezelése esetén.

11.5 Az EU NIS2 irányelve (2022/2555)

11.5.1 21. cikk (2) bekezdés a), e) és h) pont – Előírja a biztonságos fejlesztési szabályzatokat, a nyílt forráskódú elemek használatának felügyeletét és az alkalmazásokhoz kapcsolódó kockázatok dokumentált kockázatcsökkentését az alapvető és fontos szervezetek esetében.

11.6 Az EU DORA-rendelete (2022/2554)

11.6.1 6. cikk (7) bekezdés, 9. cikk (1) bekezdés c) pont és 10. cikk (2) bekezdés c) pont – Előírja a fejlesztési életciklus biztonsági kötelezettségeit a pénzügyi szektor szervezetei, így a KKV-k számára is, különösen az üzletmenet-kritikus IKT-rendszerek tekintetében.

11.7 COBIT 2019

11.7.1 BAI03 – A „Megoldások azonosításának és kialakításának kezelése” támogatja a strukturált fejlesztési kontrollok bevezetését, amelyek a biztonságot, a visszakövethetőséget és a rezilienciát hangsúlyozzák, a KKV-k korlátaihoz igazítva.