					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P28S					Dokumentum címe: **Kiszervezett 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	5.1, 6.1, 8. pont	Alkalmazandó IBIR- és beszállítókezelési kontrollok
ISO/IEC 27002:2022	5.19, 5.20, 8.25–8.27 kontrollok	Beszállítói kapcsolatokhoz és a biztonságos fejlesztési életciklushoz kapcsolódó kontrollok
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-11, SA-15, SR-3	Beszerzési, ellátásilánc-biztonsági, biztonságos fejlesztési és beszállítói megállapodásokra vonatkozó követelmények
GDPR	28. cikk	A harmadik fél általi adatkezelésre vonatkozó szerződéses és adatvédelmi követelmények
NIS2 irányelv	21. cikk (2) bekezdés a), h) pont	Az ellátásilánc-biztonságra és a biztonságos alkalmazásfejlesztésre vonatkozó kontrollok
DORA-rendelet	10. cikk	IKT-harmadikfélkockázat-kezelés, beleértve a kiszervezett fejlesztést
COBIT 2019	BAI03, DSS05 – Biztonsági szolgáltatások kezelése	Külső fejlesztésre és külső IT-szolgáltatókra vonatkozó követelmények

1. cél

1.1 Jelen szabályzat biztosítja, hogy valamennyi kiszervezett szoftverfejlesztés – függetlenül attól, hogy azt szabadúszó, ügynökség vagy harmadik fél szolgáltató végzi – biztonságosan, szerződésben szabályozott módon, valamint az alkalmazandó jogi, szabályozási és auditkövetelményekkel összhangban történjen.

1.2 A szabályzat a nem biztonságos kódolással, a nem egyértelmű tulajdonjoggal, az adatkitettséggel és a beszállítók nem megfelelő kezelésével kapcsolatos kockázatoktól védi a szervezetet azáltal, hogy kikényszeríthető fejlesztési követelményeket és beszállítói felügyeletet ír elő, dedikált IT-részleg hiánya esetén is.

1.3 Jelen szabályzat támogatja az ISO/IEC 27001:2022 szerinti tanúsítást azáltal, hogy egyértelműen meghatározott fejlesztési elvárásokat, elszámoltathatóságot és dokumentált kontrollokat biztosít a harmadik fél által végzett fejlesztési tevékenységek felett.

2. hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 valamennyi kiszervezett fejlesztőre, beleértve a szabadúszókat és fejlesztő ügynökségeket;

2.1.2 minden olyan fejlesztési munkára, amely belső eszközöket, nyilvánosan elérhető weboldalakat, szoftveralkalmazásokat vagy üzleti automatizálást érint;

2.1.3 azokra a munkatársakra, akik a külső fejlesztők kiválasztásáért, kezeléséért vagy felügyeletéért felelősek;

2.1.4 minden olyan, harmadik fél által végzett rendszerintegrációra, szkriptelésre vagy fejlesztésre, amely a vállalat adataival vagy rendszereivel kapcsolatba kerül.

2.2 A szabályzat hatálya kiterjed továbbá minden olyan félre vagy platformra, amely hozzáfér a vállalati hitelesítő adatokhoz, adattárakhoz, forráskód-adattárakhoz, tesztkörnyezetekhez vagy éles rendszerekhez.

3. célkitűzések

3.1 Biztosítani kell, hogy minden kiszervezett fejlesztés megfeleljen a biztonságos kódolás elveinek, és hogy a fejlesztőket szerződésben kötelezzék a dokumentált szabványok és titoktartási záradékok betartására.

3.2 Egyértelmű tulajdonosi felelősséget kell meghatározni minden leszállított eredményre – ideértve a kódot, az eszközöket, a hitelesítő adatokat és a dokumentációt –, biztosítva a jogok teljes körű átruházását a vállalatra és a projekt lezárásakor a visszakövethető átadást.

3.3 Meg kell előzni a gyakori fejlesztési kockázatokat, beleértve a saját fejlesztésű kód újrafelhasználását, a könyvtárakon keresztüli ellátásilánc-alapú támadásokat, a nem támogatott keretrendszerek használatát és a nem ellenőrzött adminisztrátori hozzáférést.

3.4 Minden kiszervezett projekthez kötelezően rendelkezésre kell állnia az együttműködés megkezdése előtti dokumentációnak, beleértve a szerződéseket, a titoktartási megállapodásokat és a minimális biztonsági elvárásokat.

3.5 A vevői adatokat, rendszereket és belső folyamatokat védeni kell szigorú fejlesztésfelügyelet, szállítást követő tesztelés és a rendszerhozzáférések biztonságos kezelése útján.

4. szerepkörök és felelősségek

4.1 Ügyvezető

4.1.1 Jóváhagy valamennyi beszállítói kapcsolatot, és aláírja a fejlesztési megállapodásokat.

4.1.2 Biztosítja, hogy minden kiszervezett fejlesztés jelen szabályzat szerint történjen.

4.1.3 A projekt lezárását követően megszünteti a hozzáférést a vállalati rendszerekhez.

4.1.4 Felülvizsgálja a szállítást követő dokumentációt és eredményeket.

4.2 Projekttulajdonos (jellemzően belső munkavállaló vagy kijelölt koordinátor)

4.2.1 Irányítja a napi szintű koordinációt a külső fejlesztővel.

4.2.2 Ellenőrzi, hogy a funkcionális követelmények teljesültek-e, és hogy a leszállított eredmények tesztelése megtörtént-e.

4.2.3 Biztosítja a kód és a hitelesítő adatok biztonságos átadását.

4.2.4 Jelenti az ügyvezetőnek a fejlesztéssel kapcsolatos problémákat vagy biztonsági incidenseket.

[... 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 az ügyvezetőnek legalább évente egyszer felül kell vizsgálnia. A felülvizsgálat célja annak biztosítása, hogy a szabályzat továbbra is megfeleljen az alábbiaknak:

9.1.1.1 az ISO/IEC 27001 tanúsítás követelményeinek;

9.1.1.2 a jogi kötelezettségek változásainak (pl. GDPR 28. cikk, DORA 10. cikk);

9.1.1.3 a KKV-szintű fejlesztési gyakorlatoknak és a harmadik félhez kapcsolódó aktuális kockázatoknak.

9.2 Soron kívüli felülvizsgálatok

9.2.1 A szabályzat felülvizsgálatát akkor is el kell végezni, ha:

9.2.1.1 új kiszervezett fejlesztési beszállító vagy platform kerül bevonásra;

9.2.1.2 a kiszervezett fejlesztést érintő jelentős incidens következik be;

9.2.1.3 lényeges változás történik a használt eszközökben, platformokban vagy környezetekben.

9.3 Felülvizsgálati folyamat

9.3.1 Az ügyvezető felelős azért, hogy:

9.3.1.1 ellenőrizze a szerződések, titoktartási megállapodások és hozzáférés-szabályozási folyamatok hatékonyságát;

9.3.1.2 megerősítse, hogy a jelenlegi beszállítók és szabadúszók működése összhangban van a szabályzattal;

9.3.1.3 módosítsa a feltételeket a korábbi projektekből vagy incidensekből származó visszajelzések alapján.

9.4 Verziókezelés és a változások kommunikálása

9.4.1 Minden változtatást:

9.4.1.1 a dátummal, az indokkal és a változás leírásával együtt rögzíteni kell;

9.4.1.2 az ügyvezetőnek jóvá kell hagynia, és azt a verzióelőzményekhez hozzá kell adni;

9.4.1.3 közölni kell minden olyan munkatárssal vagy projekttulajdonossal, aki külső fejlesztőkkel dolgozik;

9.4.1.4 szükség esetén újra meg kell küldeni valamennyi érintett beszállítónak és harmadik félnek.

10. kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat közvetlenül támogatja az alábbi, KKV-környezethez igazított szabályzatok végrehajtását, és azok alkalmazására épül:

10.1.1 P2S – Irányítási szerepkörök és felelősségek szabályzata: tisztázza, hogy kiszervezett fejlesztők alkalmazásakor ki felel a beszállítók jóváhagyásáért, a hozzáférés-szabályozásért és a kockázatelfogadásért.

10.1.2 P4S – Hozzáférés-szabályozási szabályzat: meghatározza a felhasználói fiókok és az adminisztrátori hozzáférés megfelelő létrehozását, korlátozását és megszüntetését a kiszervezett fejlesztés során.

10.1.3 P8S – Információbiztonsági tudatossági és képzési szabályzat: biztosítja, hogy a belső munkatársak megértsék, hogyan kell biztonságosan együttműködni külső fejlesztőkkel, beleértve a hitelesítő adatok és projektfájlok kezelését.

10.1.4 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: meghatározza azokat a biztonsági és jogi követelményeket, amelyek a GDPR alapján kiszervezett fejlesztők által kezelt vagy elért személyes adatokra vonatkoznak.

10.1.5 P24S – Biztonságos fejlesztési szabályzat: meghatározza, hogy a belső és külső fejlesztés során hogyan kell alkalmazni a biztonságos kódolási gyakorlatokat, valamint a könyvtárak és keretrendszerek ellenőrzését.

10.1.6 P30S – Incidenskezelési szabályzat: alkalmazandó, ha a kiszervezett fejlesztés biztonsági incidenshez vagy sérülékenységhez vezet, és iránymutatást ad az összehangolt kivizsgáláshoz és helyesbítő intézkedéshez.

10.2 E szabályzatokat párhuzamosan kell végrehajtani annak biztosítására, hogy a kiszervezett fejlesztés ne eredményezzen nem kezelt kockázatot, és ne sértse a KKV-ra irányadó megfelelési kötelezettségeket.

11. hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 6.1 pont – A szervezeteknek értékelniük és kezelniük kell a beszállítókhoz kapcsolódó információbiztonsági kockázatokat.

11.1.2 8.1 pont – Előírja a működés tervezésére és szabályozására vonatkozó követelményeket, beleértve a harmadik fél által nyújtott szolgáltatásokat, így a kiszervezett fejlesztést is.

11.2 ISO/IEC 27002

11.2.1 5.19 kontroll – Javasolja annak értékelését, hogy a beszállítók képesek-e teljesíteni az információbiztonsági követelményeket.

11.2.2 5.20 kontroll – Ösztönzi a harmadik fél által nyújtott szolgáltatások rendszeres nyomon követését és időszakos felülvizsgálatát.

11.2.3 8.25–8.27 kontrollok – Meghatározzák a biztonságos fejlesztési életciklus gyakorlatait, amelyek a kiszervezett fejlesztésre is alkalmazandók.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-4 – Előírja, hogy a beszerzési stratégiáknak információbiztonsági intézkedéseket is tartalmazniuk kell.

11.3.2 SA-9 – A külső rendszerfejlesztéssel és az ellátásilánc-kockázatokkal foglalkozik.

11.3.3 SA-11 – Meghatározza a biztonságos fejlesztési gyakorlatokat, beleértve a kódfelülvizsgálatot és a hibák javítását.

11.3.4 SA-15 – Ösztönzi az automatizált eszközök alkalmazását a hibák feltárására és a szoftverbizonyosság támogatására.

11.3.5 SR-3 – Előírja, hogy a beszállítói megállapodásoknak kiberbiztonsági követelményeket kell tartalmazniuk.

11.4 Az Európai Unió általános adatvédelmi rendelete (GDPR)

11.4.1 28. cikk – Előírja, hogy a harmadik fél adatfeldolgozókkal kötött szerződéseknek megfelelő adatvédelmi garanciákat kell biztosítaniuk; ez közvetlenül alkalmazandó azokra a fejlesztőkre, akik személyes adatokhoz férnek hozzá vagy ilyen adatokat kezelnek.

11.5 Az Európai Unió NIS2 irányelve (2022/2555)

11.5.1 21. cikk (2) bekezdés a), h) pont – Előírja az ellátásilánc-biztonsági kontrollokat és a biztonságos szoftverfejlesztési gyakorlatokat az érintett digitális szolgáltatók számára, adott esetben a KKV-kat is beleértve.

11.6 Az Európai Unió digitális működési rezilienciáról szóló rendelete (DORA)

11.6.1 10. cikk – Előírja az IKT-harmadikfélkockázat-kezelést, beleértve a fejlesztési megállapodásokat, a biztonsági kötelezettségeket és a harmadik fél szolgáltatókhoz kapcsolódó kockázati kontrollokat.

11.7 COBIT 2019

11.7.1 BAI03 – Megoldások azonosításának és kialakításának kezelése – Biztosítja, hogy a külső fejlesztés megfeleljen az üzleti követelményeknek és a biztonsági elvárásoknak.

11.7.2 DSS05 – Biztonsági szolgáltatások kezelése – Előírja, hogy a külső biztonsági szolgáltatók és fejlesztési szolgáltatók meghatározott biztonsági szabályok és felügyelet mellett működjenek.