| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Ide írja be a bejegyzett jogi személy nevét | | | | | | | |
| Dokumentumszám:<br>P28 | | | | | Dokumentum címe:<br>**Kiszervezett 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** |
| | | | |
| | | | |

Összhang a szabványokkal és jogszabályokkal

| Szabvány/jogszabály | Pont/cikk | Megjegyzés |
|---|---|---|
| ISO/IEC 27001:2022 | 8.1 pont | N/A |
| ISO/IEC 27002:2022 | 5.19-5.22, 8. kontrollok | N/A |
| NIST SP 800-53 Rev.5 | SA-4, SA-9, SA-10 | N/A |
| GDPR | 28., 32. cikk | N/A |
| NIS2 irányelv | 21. cikk (2) bekezdés a), h), 23. cikk | N/A |
| DORA-rendelet | 28. cikk (1), (2) bekezdés | N/A |
| COBIT 2019 | APO10, BAI03, DSS | N/A |

**1. Cél**

1.1 Jelen szabályzat meghatározza a szoftver- vagy rendszerfejlesztés külső beszállítók, vállalkozók vagy ügynökségek részére történő kiszervezésére vonatkozó kötelező kontrollokat annak biztosítása érdekében, hogy a biztonságos gyakorlatok a fejlesztési életciklus teljes egészébe beépüljenek.

1.2 A szabályzat célja a külső fejlesztési együttműködésekből eredő biztonsági sérülékenységek, adatvesztés, a szellemi tulajdon (IP) kitettsége és a megfelelési kötelezettségek megsértésének megelőzése.

1.3 A szabályzat előírja a beszállítókezelésre, a biztonságos kódolási szabványokra, a hozzáférés-szabályozásra, a nyomon követési kötelezettségekre és a szerződés lezárásához kapcsolódó kiléptetésre vonatkozó követelményeket a fejlesztett szoftver bizalmasságának, sértetlenségének és rendelkezésre állásának fenntartása érdekében.

**2. Hatály**

**2.1 Jelen szabályzat valamennyi olyan szervezeti egységre alkalmazandó, amely szoftver- vagy rendszerfejlesztés céljából külső szervezeteket vesz igénybe, beleértve az alábbiakat:**

2.1.1 webalkalmazások, mobilalkalmazások, beágyazott rendszerek, alkalmazásprogramozási interfészek, szkriptek, automatizálási munkafolyamatok vagy platformmodulok

2.1.2 egyedi fejlesztések belső platformokhoz, ügyféloldali rendszerekhez vagy kereskedelmi termékekhez

2.1.3 harmadik fél fejlesztőkkel, szabadúszókkal, ügynökségekkel vagy offshore csapatokkal kötött együttműködések

2.2 A szabályzat kiterjed minden olyan külső szervezetre is, amely a fejlesztés során forráskódhoz, tesztkörnyezetekhez vagy CI/CD folyamatokhoz fér hozzá.

2.3 A követelmények a szerződés típusától, a fejlesztési módszertantól és a kiszervezett szolgáltató földrajzi elhelyezkedésétől függetlenül kötelezően alkalmazandók.

**3. Célkitűzések**

3.1 A biztonságos fejlesztési életciklus (SDLC) gyakorlatainak kötelező alkalmazása valamennyi kiszervezett együttműködésben, a tervezéstől a bevezetést követő ellenőrzésig.

3.2 Annak biztosítása, hogy a külső fejlesztőkkel kötött valamennyi szerződés kötelező záradékokat tartalmazzon az adatvédelemre, a biztonságos kódolásra és az IP megőrzésére vonatkozóan.

3.3 A belső rendszerekkel kapcsolatba kerülő harmadik fél fejlesztőkre vonatkozó hozzáférés-szabályozási, nyomon követési és auditkövetelmények meghatározása.

3.4 A szervezet védelme a külső fejlesztésű szoftverekhez kapcsolódó ellátásilánc-fenyegetésekkel, jogsértésekkel és reputációs kárral szemben.

3.5 A biztonsági keretrendszerekkel összhangban álló folyamatos megfelelés fenntartása, ideértve az ISO/IEC 27001, NIST, GDPR, NIS2, DORA és COBIT 2019 követelményeit.

**4. Szerepkörök és felelősségek**

**4.1 Felső vezetés**

4.1.1 Jóváhagyja a magas kockázatú kiszervezett fejlesztési projekteket, és indokolt esetben jóváhagyja a szabályzati kivételeket.

4.1.2 Biztosítja, hogy a kiszervezési döntések összhangban álljanak a stratégiai célkitűzésekkel és a szervezet kockázatvállalási hajlandóságával.

**4.2 Információbiztonsági vezető**

4.2.1 Biztonsági szempontból jóváhagyja az új beszállítók bevonását.

4.2.2 Meghatározza a kiszervezett együttműködésekre vonatkozó biztonsági kontrollkövetelményeket, és felülvizsgálja az incidensjelentéseket.

[ ... 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 legalább évente egyszer, vagy az alábbi körülmények bármelyikének bekövetkezése esetén gyakrabban felül kell vizsgálni:**

9.1.1 új fejlesztésikiszervezési modellek, beszállítók vagy joghatóságok bevezetése

9.1.2 a szabályozási keretrendszerek, például a GDPR, a NIS2 vagy a DORA módosulása

9.1.3 kiszervezett kóddal, hozzáféréssel vagy teljesítéssel kapcsolatos biztonsági incidens bekövetkezése után

9.1.4 belső auditmegállapítások vagy az IBIR fejlesztésének részeként

**9.2 Az információbiztonsági vezető felelős a szabályzat felülvizsgálatának kezdeményezéséért és koordinálásáért, az alábbiakkal egyeztetve:**

9.2.1.1 jogi és beszerzési terület (a szerződéses végrehajthatósággal való összhang biztosítása érdekében)

9.2.1.2 projektgazdák és terméktulajdonosok (az operatív megvalósíthatóság biztosítása érdekében)

9.2.1.3 információbiztonsági csapat (a fenyegetésekre és kontrollokra vonatkozó frissítések érdekében)

9.2.1.4 felső vezetés (a végső jóváhagyás érdekében)

**9.3 Minden szabályzatfrissítés esetén biztosítani kell, hogy az:**

9.3.1.1 verziókezelés alatt álljon, és kijelölt dokumentumtárban kerüljön tárolásra

9.3.1.2 kommunikálásra kerüljön a kiszervezett fejlesztési tevékenységekben érintett érdekelt felek felé

9.3.1.3 kapcsolódjon a kapcsolódó szabályzatok vagy eljárásrendek módosításaihoz

9.4 Minden szabályzatverzióhoz változásnaplót kell vezetni a módosítások és jóváhagyások visszakövethetősége érdekében.

**10. Kapcsolódó szabályzatok és összefüggések**

**10.1 Jelen szabályzat az alábbi kapcsolódó dokumentumokat támogatja, és azokhoz kapcsolódik:**

10.1.1 P1 - Információbiztonsági szabályzat: Meghatározza azokat a vállalati szintű biztonsági alapelveket, amelyek a belső és a harmadik fél által végzett fejlesztési környezetekben egyaránt alkalmazandók.

10.1.2 P5 - Változáskezelési szabályzat: Biztosítja, hogy a kiszervezett kódbázisokhoz kapcsolódó valamennyi telepítési változtatás a megvalósítás előtt felülvizsgálatra és jóváhagyásra kerüljön.

10.1.3 P13 - Adatosztályozási és címkézési szabályzat: Meghatározza, hogyan kell az érzékeny adatokat azonosítani, mielőtt azok fejlesztési beszállítók vagy adattárak számára hozzáférhetővé válnak.

10.1.4 P18 - Kriptográfiai kontrollok szabályzata: Iránymutatást ad arra vonatkozóan, hogyan kell a kulcsokat, titkos adatokat és érzékeny hitelesítő adatokat a fejlesztés és az átadás során kezelni.

10.1.5 P24 - Biztonságos fejlesztési szabályzat: Meghatározza a belső és külső szoftverfejlesztési gyakorlatok alapkövetelményeit.

10.1.6 P30 - Incidenskezelési szabályzat: Szabályozza, hogyan kell a kiszervezett fejlesztést érintő adatsértéseket vagy biztonsági problémákat eszkalálni, kivizsgálni és kezelni.

10.1.7 P33 - Audit- és megfelelőségfelügyeleti szabályzat: Meghatározza a kiszervezett fejlesztési tevékenységek auditok vagy megfelelőségi felülvizsgálatok során történő ellenőrzésére vonatkozó követelményeket.

## 11. Hivatkozott szabványok és keretrendszerek

11.1 Jelen szabályzat nemzetközileg elismert biztonsági keretrendszerekkel és szabályozásokkal áll összhangban a szoftverfejlesztés biztonságos kiszervezésének és a beszállítókezelési gyakorlatok biztosítása érdekében.

### 11.2 ISO/IEC 27001

11.2.1 8.1 pont - Működéstervezés és -szabályozás: Előírja a biztonságos fejlesztésre és a harmadik fél általi teljesítésre vonatkozó folyamatkontrollokat.

### 11.3 ISO/IEC 27002:2022 - 5.19-5.21, 8. kontroll

11.3.1 A melléklet 5.19 kontrollja - Beszállítói kapcsolatok információbiztonsága: Formális megállapodásokat ír elő biztonsági és megfelelési záradékokkal.

11.3.2 A melléklet 5.20 kontrollja - Információbiztonság kezelése a beszállítói megállapodásokban: Biztosítja, hogy a fejlesztésspecifikus kontrollok beépüljenek a szerződésekbe.

11.3.3 A melléklet 5.21 kontrollja - Az IKT-ellátási lánc információbiztonságának kezelése: Magában foglalja a harmadik fél fejlesztési teljesítéseinek és kockázatainak nyomon követését.

11.3.4 A melléklet 8.30 kontrollja - Kiszervezett fejlesztés: Előírja a meghatározott biztonsági követelményeket és a hozzáférés-szabályozást a külső fejlesztésű szoftverek felett.

11.3.5 Ezek a kontrollok strukturált követelményeket határoznak meg a kiszervezett fejlesztők kiválasztására, szerződtetésére és felügyeletére, ideértve a biztonságos fejlesztési gyakorlatokat, a kódkezelést és a teljesítés ellenőrzését.

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

11.4.1 SA-4 - Beszerzési folyamat: Előírja, hogy a biztonságos fejlesztési követelményeket már a beszerzés időpontjában meg kell határozni.

11.4.2 SA-9 - Külső rendszer-szolgáltatások: Szabályozza, hogy a harmadik fél fejlesztők hogyan kapcsolódhatnak biztonságosan a belső szolgáltatásokhoz.

11.4.3 SA-10 - Fejlesztői konfigurációkezelés: Összhangban áll a külső csapatokra vonatkozó verziókezelési, kódhozzáférési és változáskövetési kötelezettségekkel.

### 11.5 GDPR (2016/679)

11.5.1 28. cikk - Adatfeldolgozói kötelezettségek: Előírja, hogy a harmadik fél fejlesztőkkel kötött szerződésekben meg kell határozni a személyes adatok kezelésére vonatkozó biztonsági, kontroll- és auditkövetelményeket.

11.5.2 32. cikk - Az adatkezelés biztonsága: Előírja a megfelelő védelmi intézkedések (pl. titkosítás, hozzáférés-szabályozás) alkalmazását a személyes adatokat kezelő rendszerek fejlesztése során.

**11.6 NIS2 irányelv (2022/2555)**

11.6.1 21. cikk (2) bekezdés a), h), valamint 23. cikk: Előírják, hogy a biztonságos fejlesztési gyakorlatokat a harmadik fél együttműködésekben és a digitális ellátási láncokban egyaránt alkalmazni kell, megfelelő felügyelet és műszaki ellenőrzés mellett.

**11.7 DORA-rendelet (2022/2554)**

11.7.1 28. cikk (1), (2) bekezdés: Előírja, hogy a pénzügyi szervezetek az IKT-harmadikfél-kockázatokat szerződéses kontrollokkal és a biztonságos fejlesztés felügyeletével kezeljék, különösen a kritikus kiszervezett fejlesztések esetében.

**11.8 COBIT 2019**

11.8.1 APO10 - Beszállítók kezelése: Strukturált követelményeket határoz meg a beszállítók értékelésére, a szerződésekre és a teljesítmény nyomon követésére.

11.8.2 BAI03 - Megoldások kialakításának kezelése: Közvetlenül illeszkedik a biztonságos SDLC-folyamatokhoz, a kódfelülvizsgálatokhoz és a fejlesztési ellenőrzéshez.

11.8.3 DSS05 - Biztonsági szolgáltatások kezelése: Összhangban áll a külsőleg vagy harmadik fél által fejlesztett rendszerek megfigyelésével és védelmével.