					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P26S					Dokumentum címe: **Harmadik felekre és beszállítókra vonatkozó biztonsági 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	Operatív kontrollok a harmadik felekkel és beszállítókkal fennálló kapcsolatokra
ISO/IEC 27002:2022	5.19–5.22 kontrollok	Beszállítói biztonsági kontrollok, szerződéses biztonsági követelmények, változáskezelés, nyomon követés és felülvizsgálat
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Beszerzésre, konfigurációra, összekapcsolási megállapodásokra és külső személyzetre vonatkozó kontrollok
GDPR	28., 32. cikk	Adatfeldolgozási szerződéses kikötések, az adatfeldolgozókra vonatkozó biztonsági követelmények
NIS2 irányelv	21. cikk (2) bekezdés a), b), i), 23. cikk (1) bekezdés	Ellátásilánc-kockázatkezelés, harmadik fél által nyújtott szolgáltatások felügyelete
DORA-rendelet	5. cikk (1), (2), 28. cikk (1), (2)	Harmadik fél szolgáltatókat érintő IKT-kockázatkezelés
COBIT 2019	APO10, APO12, DSS05 – Biztonsági szolgáltatások kezelése	Beszállítókezelés és kockázati integráció

1. Cél

1.1 Jelen szabályzat meghatározza a kötelező biztonsági követelményeket azon harmadik felekkel és beszállítókkal fennálló kapcsolatok létesítésére, kezelésére és megszüntetésére, amelyek hozzáférnek a szervezet adataihoz, rendszereihez vagy szolgáltatásaihoz, illetve azokra hatással vannak.

1.2 A szabályzat biztosítja, hogy a külső szolgáltatók – ideértve az informatikai támogatást nyújtó beszállítókat, a felhőszolgáltatókat, a szoftverfejlesztőket és az üzleti folyamatokat támogató vállalkozókat – a vállalati eszközöket biztonságosan, az alkalmazandó jogszabályoknak és szabványoknak megfelelően kezeljék.

1.3 A szabályzat csökkenti az olyan kockázatokat, mint az adatszivárgás, a jogosulatlan rendszermódosítások, a szabályozói bírságok vagy a nem biztonságos, illetve nem megfelelően irányított harmadik félre épülő konstrukciókból eredő üzleti fennakadások.

2. Hatály

2.1 Jelen szabályzat minden olyan harmadik félre alkalmazandó, amely:

2.1.1 szoftvert, infrastruktúrát, tárhelyszolgáltatást vagy felhőszolgáltatást nyújt;

2.1.2 belső rendszerekhez, eszközökhöz vagy alkalmazásokhoz fér hozzá, vagy azokat kezeli;

2.1.3 vállalati adatokat, dokumentumokat vagy biztonsági mentéseket kezel;

2.1.4 üzleti működést, HR-, pénzügyi vagy ügyfélszolgálati tevékenységet támogat.

2.2 A szabályzat alkalmazandó továbbá:

2.2.1 a beszállítók kiválasztásában, megbízásában vagy felügyeletében részt vevő belső munkatársakra;

2.2.2 minden olyan munkatársra, aki az új beszállítók bevonását, szerződéseit, hozzáféréseit vagy felülvizsgálatait kezeli;

2.2.3 minden olyan rendszerre vagy folyamatra, amely harmadik fél komponenseire vagy szolgáltatásaira támaszkodik.

3. Célkitűzések

3.1 Biztosítani kell, hogy valamennyi beszállító megfeleljen az egyértelműen meghatározott biztonsági elvárásoknak.

3.2 Elő kell írni, hogy a beszállítói szerződések kikényszeríthető biztonsági, adatvédelmi és incidenskezelési kötelezettségeket tartalmazzanak.

3.3 A beszállítói kockázatokat a megállapodások aláírása vagy a hozzáférés biztosítása előtt értékelni és dokumentálni kell.

3.4 A magas kockázatú vagy kritikus beszállítók esetében rendszeres felülvizsgálatot kell végezni a megfelelés megerősítése érdekében.

3.5 Formális folyamatot kell kialakítani a kivételkezelésre, az incidenskezelésre és a szerződésfrissítésekre.

3.6 Támogatni kell az ISO/IEC 27001:2022, a GDPR, a NIS2 és a DORA beszállítóirányításhoz kapcsolódó megfelelési kötelezettségeinek teljesítését.

4. Szerepkörök és felelősségek

4.1 Ügyvezető

4.1.1 Végső felelősséget visel a beszállítók kiválasztásáért és a biztonsági megfelelésért.

4.1.2 Jóváhagyja a beszállítókat érintő szerződéseket, kivételeket és eszkalációkat.

4.1.3 Felügyeli az incidenskezelést és a döntéshozatalt, ha a beszállító nem teljesíti kötelezettségeit.

4.2 Informatikai szolgáltató vagy belső biztonsági kapcsolattartó

4.2.1 Értékeli a beszállítók által igényelt technikai hozzáférést.

4.2.2 Érvényesíti a hozzáférés-szabályozási szabályokat, felülvizsgálja a naplókat és ellenőrzi a biztonságos adatkezelést.

4.2.3 Felülvizsgálja a biztonsági kontrollokra, tanúsítványokra vagy auditor megállapításokra vonatkozó bizonyítékokat, ahol ez alkalmazandó.

[... 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 felül kell vizsgálni az ügyvezető részvételével, az informatikai szolgáltató vagy a beszállítókezelő bevonásával.

9.2 A szabályzatot ezen felül felül kell vizsgálni:

9.2.1 bármely jelentős jogi, szabályozói vagy szerződéses kötelezettségváltozást követően;

9.2.2 beszállítóval összefüggő biztonsági incidens vagy auditmegállapítás után;

9.2.3 új beszállítói kategóriák bevezetésekor (például kritikus SaaS-platformok esetén).

9.3 Minden frissítést:

9.3.1 dokumentálni kell verzióelőzményekkel és indokolással;

9.3.2 az ügyvezetőnek jóvá kell hagynia;

9.3.3 kommunikálni kell az érintett belső munkatársak és beszállítókezelők felé;

9.3.4 az előző verziókkal együtt kell megőrizni a P14S – Adatmegőrzési és megsemmisítési szabályzat szerint.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat eredményes alkalmazása az alábbi KKV információbiztonsági szabályzatokkal való összehangolástól függ:

10.1.1 P2S – Irányítási szerepkörök és felelősségek szabályzata: meghatározza a beszállítói felügyeletért és a szerződéses kötelezettségek érvényesítéséért viselt felelősséget.

10.1.2 P4S – Hozzáférés-szabályozási szabályzat: meghatározza azokat a hozzáférés-korlátozási szabályokat, amelyeket a beszállítók rendszerhozzáférésének biztosításakor alkalmazni kell.

10.1.3 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: biztosítja, hogy a személyes adatokat kezelő beszállítók megfeleljenek az adatvédelmi elveknek és jogi követelményeknek.

10.1.4 P14S – Adatmegőrzési és megsemmisítési szabályzat: alkalmazandó minden olyan adatra vagy nyilvántartásra, amelyet beszállítóval megosztanak, vagy amelyet a beszállító tárol, és szabályozza a szerződés megszűnését követő biztonságos megsemmisítést.

10.1.5 P30S – Incidenskezelési szabályzat: meghatározza az eljárást arra az esetre, ha a beszállító biztonsági incidenst okoz vagy abban érintett, beleértve az eszkalációs útvonalakat és a bizonyítékok kezelését.

10.2 E szabályzatok együttesen biztosítják, hogy a beszállítói kockázat a szerződés teljes életciklusa során szabályozott maradjon.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 8.1 pont – Előírja az operatív kontrollok bevezetését, beleértve a harmadik felekkel és beszállítókkal fennálló kapcsolatokra alkalmazott kontrollokat is.

11.2 ISO/IEC 27002

11.2.1 5.19 kontroll – Biztosítja, hogy a beszállítói biztonsági intézkedések összhangban legyenek a szervezeti követelményekkel.

11.2.2 5.20 kontroll – Előírja a biztonsági feltételeket, felelősségeket és incidensekkel kapcsolatos kötelezettségeket rögzítő formális megállapodásokat.

11.2.3 5.21 kontroll – Szabályozza a beszállítói szolgáltatások olyan változásait, amelyek hatással lehetnek a kockázati helyzetre.

11.2.4 5.22 kontroll – Előírja a beszállítói szolgáltatások és a megfelelés nyomon követését és felülvizsgálatát.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – Szabályozza a külső rendszerek és szolgáltatások beszerzését, kockázatértékelést és meghatározott elvárásokat előírva.

11.3.2 SA-10 – Szabályozza a konfigurációs és változáskezelési eljárásokat a harmadik fél által kezelt rendszerek esetében.

11.3.3 CA-3 – Előírja a külső szervezeteket érintő rendszerekre vonatkozó összekapcsolási megállapodásokat.

11.3.4 PS-7 – Meghatározza a külső személyzet átvilágítására és elszámoltathatóságára vonatkozó követelményeket.

11.4 GDPR (2016/679)

11.4.1 28. cikk – Előírja az adatfeldolgozási szerződéses kikötéseket az adatfeldolgozóként eljáró beszállítókkal.

11.4.2 32. cikk – Megköveteli a megfelelő technikai és szervezési intézkedéseket valamennyi adatfeldolgozó esetében.

11.5 NIS2 irányelv (2022/2555)

11.5.1 21. cikk (2) bekezdés a), b), i) – Előírja az IKT-ellátási lánc kockázatkezelését és a harmadik felekre vonatkozó kontrollokat.

11.5.2 23. cikk (1) bekezdés – Előírja a harmadik fél által nyújtott szolgáltatások dokumentált felügyeletét az alapvető és fontos szervezetek esetében.

11.6 DORA-rendelet (2022/2554)

11.6.1 5. cikk (1) bekezdés – Előírja az IKT-kockázatkezelési keretrendszert, amely minden kritikus harmadik fél szolgáltatóra kiterjed.

11.6.2 5. cikk (2) bekezdés – Szerződéses és operatív kontrollokat ír elő az IKT-szolgáltatási függőségek kezelésére.

11.6.3 28. cikk (1), (2) bekezdés – Meghatározza a pénzügyi ágazat IKT-hoz kapcsolódó harmadik fél kockázatának felügyeleti szabályait.

11.7 COBIT 2019

11.7.1 APO10 – „Beszállítók kezelése” meghatározza a beszerzési kontrollokat és a kapcsolatkezelési elvárásokat.

11.7.2 APO12 – „Kockázatok kezelése” integrálja a beszállítói kockázatot a szervezeti kockázatirányításba.

11.7.3 DSS05 – „Biztonsági szolgáltatások kezelése” alkalmazandó a menedzselt harmadik fél szolgáltatókra és a kiszervezett szolgáltatókra.