					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P26					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. pont	Működéstervezés és -szabályozás: formális kontrollokat ír elő az IBIR-re hatással lévő harmadik fél által nyújtott szolgáltatások felett
ISO/IEC 27002:2022	5.19–5.22 kontrollok	Beszállítói kapcsolatokra vonatkozó szabályzatok és eljárások; beszállítói kockázatok kezelése; beszállítói szolgáltatásnyújtás kezelése; beszállítók monitorozása és felülvizsgálata
NIST SP 800-53 Rev. 5	SA-9, SA-10, CA-3, PS-7	Külső rendszer-szolgáltatások; fejlesztői konfigurációkezelés; rendszerkapcsolatok; harmadik fél személyzetének biztonsága
GDPR	28., 32., 33. cikk	Adatfeldolgozók kötelezettségei; az adatkezelés biztonsága; személyes adatok megsértésének bejelentése
NIS2 irányelv	21. cikk (2) bekezdés e)–f) pont	Kockázatalapú beszállítókezelés és biztonsági felügyelet
DORA-rendelet	28., 30. cikk	IKT-harmadikfél-kockázat; kritikus IKT-harmadikfél-szolgáltatók felügyelete
COBIT 2019	BAI05, DSS02, MEA03	Szervezeti változások támogatásának kezelése; szolgáltatáskérések és incidensek kezelése; megfelelés monitorozása, értékelése és felmérése

1. Cél

1.1 Jelen szabályzat meghatározza a harmadik fél beszállítókkal és szolgáltatókkal kialakított, kezelt és fenntartott biztonságos kapcsolatok információbiztonsági követelményeit.

1.2 Biztosítja, hogy minden olyan beszállítóra, amely hozzáfér a szervezet adataihoz, rendszereihez vagy infrastruktúrájához, a szolgáltatási életciklus teljes időtartama alatt szigorú biztonsági kontrollok, szerződéses védelmi intézkedések és folyamatos felügyelet vonatkozzon.

1.3 A szabályzat támogatja az ISO/IEC 27001 A. mellékletének 5.19–5.22 kontrolljait azáltal, hogy a biztonsági követelményeket beépíti a beszerzési, beléptetési, átvilágítási, szerződéskezelési, szolgáltatásfelügyeleti és kiléptetési folyamatokba.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 valamennyi olyan harmadik fél beszállítóra, vállalkozóra, felhőszolgáltatóra és szolgáltató szervezetre, amely a szervezet információs vagyonát kezeli vagy ahhoz hozzáfér;

2.1.2 valamennyi belső szerepkörre, amely részt vesz a beszállítók értékelésében, bevonásában, szerződtetésében, kockázatkezelésében, felügyeletében vagy megszüntetésében;

2.1.3 minden olyan beszállítói kapcsolatra, amely érzékeny adatokhoz való hozzáférést, éles szolgáltatásokkal való integrációt vagy üzletmenet-kritikus funkciók támogatását foglalja magában.

2.2 A szabályzat – ahol alkalmazható – kiterjed a közvetlen beszállítókra és alvállalkozóikra is, valamint magában foglalja a harmadik fél által biztosított szoftvereket, infrastruktúrát, támogatási szolgáltatásokat és menedzselt szolgáltatásokat.

3. Célkitűzések

3.1 Biztosítani kell, hogy a beszállítói biztonsági kockázatokat az együttműködés teljes életciklusa során következetesen azonosítsák, értékeljék és kezeljék.

3.2 Minden beszállítói szerződésbe be kell építeni a szabványosított biztonsági követelményeket, ideértve az incidensbejelentési kötelezettségeket, az auditjog gyakorlásának feltételeit és az adatvédelmi felelősségeket.

3.3 Új beszállítók bevonása vagy magas kockázatú szolgáltatási megállapodások megújítása előtt formális átvilágítást és dokumentált kockázatértékelést kell végezni.

3.4 Mechanizmusokat kell kialakítani a beszállítói megfelelés folyamatos nyomon követésére, beleértve a teljesítmény-felülvizsgálatokat, auditokat és az incidensek eszkalációját.

3.5 Kezelni kell a beszállítói szolgáltatásokat érintő változásokat, valamint biztosítani kell a biztonságos kiléptetést és az adatok visszaszolgáltatását vagy megsemmisítését a kapcsolat megszüntetésekor.

3.6 A harmadik felekre vonatkozó biztonsági kontrollokat összhangba kell hozni az alkalmazandó jogszabályi és szerződéses kötelezettségekkel, beleértve a GDPR-t, a NIS2 irányelvet, a DORA-rendeletet és az ISO/IEC 27001 szabványt.

4. Szerepkörök és felelősségek

4.1 Információbiztonsági vezető

4.1.1 A szabályzat gazdája, és biztosítja annak összhangját az átfogó IBIR-rel, valamint a kockázatkezelési és megfelelési stratégiával.

4.1.2 Jóváhagyja a beszállítói osztályozási szinteket, a biztonsági felülvizsgálatok eredményeit és a magas kockázatú kivételeket.

4.1.3 Részt vesz a súlyos beszállítói incidensek eszkalációjában és a kritikus szolgáltatásokra vonatkozó szerződéses tárgyalásokban.

4.2 Beszerzés és beszállítókezelés

4.2.1 Biztosítja, hogy minden új és megújított beszállítói szerződés tartalmazza a jóváhagyott biztonsági és adatvédelmi záradékokat.

4.2.2 Fenntartja a központi beszállítói nyilvántartást, és a harmadikfél-kockázatok dokumentációja tekintetében együttműködik a jogi és megfelelőségi területtel.

4.2.3 Elindítja a beléptetési folyamatokat, és biztosítja azok összhangját a szerződéskötést megelőző biztonsági értékelésekkel.

[... 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, vagy ennél korábban, ha az alábbiak valamelyike bekövetkezik:

9.1.1 lényeges változások a beszerzési stratégiában vagy a beszállítói ökoszisztémában;

9.1.2 a jogi vagy szabályozási keretrendszer módosulása (pl. DORA-rendelet, GDPR);

9.1.3 jelentős harmadik félhez kapcsolódó incidensek, adatsértések vagy auditkudarcok;

9.1.4 kockázatértékelésekből vagy külső tanúsító szervezetektől származó megállapítások.

9.2 A felülvizsgálati folyamat közös felelőssége az információbiztonsági vezetőnek, a beszerzésnek, a jogi területnek és a kockázatkezelési funkciónak.

9.3 Minden szabályzatmódosítást dokumentálni kell az IBIR dokumentumkezelési nyilvántartásában, verziókezeléssel kell ellátni, és a releváns érdekelt felek részére kommunikálni kell a beszállítói irányítási csatornákon és a munkavállalói tudatosságnövelő programokon keresztül.

9.4 A hatályon kívül helyezett verziókat a visszakövethetőség és a jogszabályi megfelelés biztosítása érdekében legalább három évig archiválni kell.

10. Kapcsolódó szabályzatok és összefüggések

10.1 P1 – Információbiztonsági szabályzat. Meghatározza a szervezet átfogó elkötelezettségét valamennyi működési terület biztonságos működtetésére, beleértve a harmadik fél beszállítókra és külső IT-szolgáltatókra való támaszkodást is.

10.2 P6 – Kockázatkezelési szabályzat. Iránymutatást ad a harmadik félhez kapcsolódó kockázatok azonosítására, értékelésére és csökkentésére, beleértve a beszállítói ökoszisztémából eredő öröklött vagy rendszerszintű kockázatokat is.

10.3 P17 – Adatvédelmi és magánszféra-védelmi szabályzat. Minden olyan beszállítóra alkalmazandó, amely személyes adatokat kezel, és megfelelő szerződéses feltételeket, adattovábbítási védelmi intézkedéseket, valamint a beépített és alapértelmezett adatvédelem elveinek alkalmazását írja elő.

10.4 P4 – Hozzáférés-szabályozási szabályzat. Szabályozza, hogy a harmadik fél személyzete miként kaphat hozzáférést a szervezet rendszereihez, érvényesítve a szerepköralapú jogosultságokat, a munkamenet-védelmi intézkedéseket és a visszavonási eljárásokat.

10.5 P22 – Naplózási és felügyeleti szabályzat. Előírja, hogy a beszállítói rendszerhozzáféréseket felügyelni, naplózni és felülvizsgálni kell, különösen olyan környezetekben, ahol emelt jogosultságú vagy adatközpontú tevékenységek zajlanak.

10.6 P30 – Incidenskezelési szabályzat. Meghatározza a beszállítói eredetű biztonsági eseményekre vagy a harmadik fél rendszereit érintő közös vizsgálatokra vonatkozó eszkalációs eljárásokat és incidensbejelentési követelményeket.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001:2022 8.1 pont – Működéstervezés és -szabályozás: formális kontrollokat ír elő az IBIR-re hatással lévő harmadik fél által nyújtott szolgáltatások felett.

11.2 ISO/IEC 27002:2022 – 5.19–5.22 kontrollok:

11.2.1 A melléklet 5.19 kontroll – Beszállítói kapcsolatokra vonatkozó szabályzatok és eljárások: kontrollokat ír elő a beszállítókkal való kapcsolatok kezelésére.

11.2.2 A melléklet 5.20 kontroll – Beszállítói kockázatok kezelése: a beszállítói kockázati helyzet azonosítására, értékelésére és folyamatos felügyeletére összpontosít.

11.2.3 A melléklet 5.21 kontroll – Beszállítói szolgáltatásnyújtás kezelése: megköveteli, hogy a teljesítmény és a biztonság összhangban legyen a szerződéses elvárásokkal.

11.2.4 A melléklet 5.22 kontroll – Beszállítók monitorozása és felülvizsgálata: megerősíti a harmadik felek megfelelésének folyamatos ellenőrzése és újraértékelése iránti igényt.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 SA-9 – Külső rendszer-szolgáltatások: meghatározza a külső szervezetek által üzemeltetett rendszerek biztonsági és kockázati követelményeit.

11.3.2 SA-10 – Fejlesztői konfigurációkezelés: akkor alkalmazandó, amikor harmadik felek szoftvert vagy környezeteket szállítanak.

11.3.3 CA-3 – Rendszerkapcsolatok: előírja a szervezetek közötti rendszeres adatáramlások felügyeletét és szabályozását.

11.3.4 PS-7 – Harmadik fél személyzetének biztonsága: biztosítja, hogy a vállalkozók és a beszállítói munkatársak megfelelő átvilágításon és felügyeleten essenek át.

11.4 GDPR (2016/679):

11.4.1 28. cikk – Adatfeldolgozók kötelezettségei: írásbeli megállapodásokat ír elő az adatfeldolgozókkal, beleértve a technikai és szervezési intézkedéseket (TOM) is.

11.4.2 32. cikk – Az adatkezelés biztonsága: megfelelő védelmi intézkedéseket ír elő mind az adatkezelők, mind az adatfeldolgozók számára.

11.4.3 33. cikk – Személyes adatok megsértésének bejelentése: incidens esetén haladéktalan értesítést követel meg a beszállítóktól.

11.5 NIS2 irányelv (2022/2555):

11.5.1 21. cikk (2) bekezdés e)–f) pont: kockázatalapú beszállítókezelést és biztonsági felügyeletet ír elő, különösen az alapvető és fontos szervezetek digitális ellátási láncaiban.

11.6 DORA-rendelet (2022/2554):

11.6.1 28. cikk – IKT-harmadikfél-kockázat: kockázatértékelési, szerződéses biztonsági és kilépési stratégiára vonatkozó kötelezettségeket ír elő a pénzügyi szolgáltatók számára.

11.6.2 30. cikk – Kritikus IKT-harmadikfél-szolgáltatók felügyelete: megerősített monitorozási és felügyeleti elvárásokat állapít meg a kulcsfontosságú beszállítókra.

11.7 COBIT 2019:

11.7.1 BAI05 – Szervezeti változások támogatásának kezelése: biztosítja, hogy a beszállítói átállások biztonságosan, szabályozott módon történjenek.

11.7.2 DSS02 – Szolgáltatáskérések és incidensek kezelése: alkalmazandó a beszállítók által jelentett problémákra és az incidenskezelés integrációjára.

11.7.3 MEA03 – Megfelelés monitorozása, értékelése és felmérése: megerősíti a beszállítói teljesítménymérés és a megfelelés nyomon követésének szükségességét.