					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P27S					Dokumentum címe: **Felhőszolgáltatások használatára vonatkozó 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	
ISO/IEC 27002:2022	Kontrollok 5.23–5.25	
NIST SP 800-53 Rev. 5	AC-20, SC-12, SC-13, SR-5	
GDPR	28. cikk, 32. cikk és V. fejezet	
NIS2 irányelv	21. cikk (2) bekezdés f) és i) pont	
DORA-rendelet	5. cikk (2) bekezdés, 28. cikk	
COBIT 2019	DSS01, DSS05, BAI04	

1. Cél

1.1 Jelen szabályzat meghatározza a felhőszolgáltatások szervezeten belüli biztonságos használatának követelményeit. Biztosítja, hogy a felhőben kezelt vagy tárolt adatok megfelelő védelemben részesüljenek, a hozzáférések szabályozottak legyenek, és a kockázatkezelés felelősségteljes módon történjen.

1.2 A szabályzat támogatja a KKV-kat a jogszabályi kötelezettségek és ügyfélelvárások teljesítésében az érzékeny információk védelme, az adatszivárgás megelőzése és a felhőalapú kockázatok hatékony kezelése terén, anélkül hogy vállalati léptékű infrastruktúrát igényelne.

1.3 Jelen szabályzat támogatja az ISO/IEC 27001 szerinti tanúsítást, a GDPR-nak való megfelelést és az ellátási lánc biztonságát a harmadik fél által nyújtott felhőszolgáltatások következetes irányítása révén.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 Minden olyan felhőalapú szolgáltatásra, amelyet vállalati adatok tárolására, kezelésére vagy továbbítására használnak

2.1.2 Valamennyi munkavállalóra, vállalkozóra vagy szolgáltatóra, akik a szervezet nevében felhőalapú eszközöket használnak

2.1.3 Ingyenes és fizetős felhőmegoldásokra, beleértve az e-mail-platformokat, a dokumentummegosztást, a SaaS-eszközöket, a biztonságimentés-platformokat, a videókonferencia-megoldásokat és az ügyfélplatformokat

2.1.4 Minden olyan eszközre (asztali számítógép, mobileszköz, táblagép), amely felhőalkalmazásokon keresztül vállalati információkhoz fér hozzá

2.2 Ideértve különösen, de nem kizárólagosan:

2.2.1 Microsoft 365, Google Workspace, Dropbox Business

2.2.2 Zoom, Microsoft Teams, Google Meet

2.2.3 AWS, Azure, GCP

2.2.4 Felhőalapú biztonsági mentési és katasztrófa utáni helyreállítási eszközök

2.2.5 Számlázáshoz, projektmenedzsmenthez vagy ügyfélkommunikációhoz használt megosztott mappák vagy alkalmazások

3. Célkitűzések

3.1 A nem jóváhagyott felhőszolgáltatások jogosulatlan vagy magas kockázatú használatának megelőzése.

3.2 Annak biztosítása, hogy a felhőben tárolt bizalmas vagy szabályozott adatokat megfelelő technikai és adminisztratív kontrollok védjék.

3.3 Egyértelmű szerepkörök meghatározása a felhőszolgáltatások jóváhagyására, konfigurálására, felügyeletére és kivezetésére.

3.4 Az adatáramlások szabályozása, valamint a felhőben tárolt információkra vonatkozó megőrzési, törlési és adatvédelmi kötelezettségek érvényesítése.

3.5 A személyes fiókokra vagy nem felügyelt eszközökre való támaszkodás csökkentése azáltal, hogy minden üzleti célra használt felhőrendszer előzetes jóváhagyása kötelező.

3.6 Az ISO/IEC 27001:2022, a GDPR, a NIS2 és a DORA külső felhőfüggőségek kezelésére vonatkozó követelményeinek való megfelelés biztosítása.

4. Szerepkörök és felelősségek

4.1 Ügyvezető

4.1.1 Jóváhagyja valamennyi új felhőszolgáltatás használatát

4.1.2 Felülvizsgálja a felhőszolgáltatókkal és szolgáltatástípusokkal kapcsolatos kockázatokat

4.1.3 Biztosítja a szabályzat betartatását, és felügyeli a kivételekkel kapcsolatos döntéseket

4.2 Külső IT-szolgáltató vagy műszaki támogató

4.2.1 Értékeli és megvalósítja a felhőszolgáltatások biztonságos konfigurációját

4.2.2 Beállítja a fiókokat, a hozzáférés-szabályozást és a biztonsági mentéseket

4.2.3 Nyomon követi a jelszókövetelményeknek, az MFA-nak és a biztonsági beállításoknak való megfelelést

[... 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 ügyvezetőnek a külső IT-szolgáltatóval együttműködésben legalább évente felül kell vizsgálnia.

9.2 Formális felülvizsgálatot kell végezni az alábbi esetekben is:

9.2.1 Felhőszolgáltatással kapcsolatos biztonsági incidens után (pl. adatsértés, adatvesztés)

9.2.2 Új, jelentős felhőplatform bevezetésekor

9.2.3 Jogi vagy szabályozási követelmények változása esetén (pl. GDPR-, NIS2- vagy DORA-módosítások)

9.2.4 Ha a felügyeleti tevékenységek visszaélést vagy új kockázatokat tárnak fel

9.3 Az ügyvezető köteles biztosítani, hogy:

9.3.1 A felhőszolgáltatások nyilvántartása frissüljön az új vagy megszüntetett szolgáltatásokkal

9.3.2 A jogi és adatvédelmi követelmények továbbra is teljesüljenek

9.3.3 Valamennyi változtatás kommunikálása megtörténjen az érintett felhasználók és érdekelt felek felé

9.4 Az archivált verziókat biztonságosan kell tárolni, és a szabályzat korábbi verzióit a szervezet P14S – Adatmegőrzési és megsemmisítési szabályzata szerint kell kezelni.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzatot az alábbi, KKV-kra szabott információbiztonsági szabályzatokkal összehangoltan kell alkalmazni:

10.1.1 P2S – Irányítási szerepkörök és felelősségek szabályzata: Meghatározza a felhőszolgáltatások jóváhagyásával és a szolgáltatói kapcsolatok kezelésével kapcsolatos elszámoltathatóságot.

10.1.2 P4S – Hozzáférés-szabályozási szabályzat: Támogatja a felhőplatformokhoz szükséges biztonságos bejelentkezési, munkamenet-kezelési és hozzáférés-visszavonási gyakorlatokat.

10.1.3 P14S – Adatmegőrzési és megsemmisítési szabályzat: Szabályozza, hogy a felhőalapú adatok mentése, megőrzése és törlése hogyan történik a jogi kötelezettségekkel összhangban.

10.1.4 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: Biztosítja, hogy a felhőszolgáltatásokban tárolt személyes adatok kezelése a GDPR alapelveinek megfelelően történjen.

10.1.5 P30S – Incidenskezelési szabályzat: Strukturált eljárásokat biztosít a felhőbiztonsági incidensek kezelésére, beleértve a bizonyítékok gyűjtését és a külső értesítéseket.

10.2 E szabályzatok együttesen biztosítják, hogy a felhőhasználat biztonságos, megfelelő és működési szempontból reziliens legyen.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 8.1 pont – Előírja, hogy a szervezetek működési kontrollokat vezessenek be az adatkezelésre, beleértve a felhőalapú rendszerekkel kapcsolatos kontrollokat is.

11.2 ISO/IEC 27002

11.2.1 5.23 kontroll – Előírja a felhőszolgáltatások és a harmadik fél által nyújtott SaaS-eszközök használata feletti irányítást.

11.2.2 5.24 kontroll – Előírja a kockázatokkal és szabályozási követelményekkel összhangban álló, meghatározott felhőhasználati szabályzatot.

11.2.3 5.25 kontroll – Előírja, hogy a szervezetek biztosítsák, hogy a felhőkörnyezetekben alkalmazott biztonsági kontrollok megfeleljenek a szervezeti igényeknek.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-20 – Előírja a külső rendszerekre, így a felhőszolgáltatásokra vonatkozó formális használati szabályokat.

11.3.2 SC-12, SC-13 – A felhőkörnyezeteken belüli, az átvitel közbeni és a tárolt adatok titkosítására vonatkozik.

11.3.3 SR-5 – Az ellátási láncba tartozó felhő- és harmadik fél kockázati kontrolljait fedi le.

11.4 GDPR (2016/679)

11.4.1 28. cikk – Előírja, hogy az adatfeldolgozóként eljáró felhőszolgáltatókra kötelező erejű szerződéses kötelezettségek vonatkozzanak.

11.4.2 32. cikk – Előírja a felhőalapú adatkezelésre vonatkozó technikai és szervezési intézkedéseket.

11.4.3 V. fejezet – Tiltja a felhőben tárolt személyes adatok jogosulatlan nemzetközi továbbítását.

11.5 NIS2 irányelv (2022/2555)

11.5.1 21. cikk (2) bekezdés f) és i) pont – Előírja, hogy az alapvető és fontos szervezetek megfelelő szabályzatokat alkalmazzanak a felhőszolgáltatások biztonságára és az ellátási lánc kontrolljára.

11.6 DORA (2022/2554)

11.6.1 5. cikk (2) bekezdés – Előírja, hogy a pénzügyi KKV-k integrálják a felhőbiztonságot az IKT-kockázatkezelési keretrendszerükbe.

11.6.2 28. cikk – Meghatározza a kritikus harmadik fél IKT-szolgáltatók, ideértve a felhőszolgáltatókat is, felügyeletére vonatkozó szabályokat.

11.7 COBIT 2019

11.7.1 DSS01 – „Műveletek kezelése” a felhőszolgáltatások működési integritását tárgyalja.

11.7.2 DSS05 – „Biztonsági szolgáltatások kezelése” felhőspecifikus védelmi és felügyeleti követelményeket is tartalmaz.

11.7.3 BAI04 – „Rendelkezésre állás és kapacitás kezelése” biztosítja az üzletmenet-folytonosságot és a teljesítményt felhőkörnyezetekben.