| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Ide írja be a bejegyzett jogi személy nevét | | | | | | | |
| Dokumentumszám:<br>P27 | | | | | Dokumentum címe:<br>**Felhőszolgáltatások használatára vonatkozó 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** |
| | | | |
| | | | |

A vonatkozó szabványokkal és jogszabályokkal összhangban

| Szabvány/jogszabály | Pont/cikk | Megjegyzés |
|---|---|---|
| ISO/IEC 27001:2022 | 8. pont | A felhőalapú működéstervezés és -szabályozás követelményei. |
| ISO/IEC 27002:2022 | 5.23–5.25 kontrollok | A felhőszolgáltatások használatára, irányítására és biztonságára vonatkozó előírások. |
| NIST SP 800-53 Rev.5 | AC-20, SA-9(5), SC-12 – SC-28, SR-5 | Külső rendszerek használata, szerződéses és technikai követelmények, kriptográfiai védelem, ellátási lánc védelme. |
| GDPR | 28. cikk, 32. cikk, V. fejezet | A felhőalapú adatfeldolgozókra vonatkozó követelmények, az adatkezelés biztonsága, adattovábbítások. |
| NIS2 irányelv | 21. cikk (2) bekezdés f), i) pont | Harmadik féllel kapcsolatos kockázatok és az ellátási láncra vonatkozó követelmények. |
| DORA-rendelet | 5. cikk (2) bekezdés, 28. cikk | IKT- és harmadik félhez kapcsolódó felügyeleti követelmények pénzügyi szervezetek esetén. |
| COBIT 2019 | BAI04, DSS01, DSS05 | A felhőszolgáltatások rendelkezésre állásának, üzemeltetésének és biztonsági szolgáltatásainak kezelése. |

**1. Cél**

1.1 Jelen szabályzat meghatározza a szervezet kötelező követelményeit a felhőszolgáltatások biztonságos, szabályszerű és felelős használatára az Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) és Software-as-a-Service (SaaS) szolgáltatási modellekben.

1.2 A szabályzat célja annak biztosítása, hogy a felhőszolgáltatások bevezetése és irányítása az információs vagyon bizalmasságát, sértetlenségét és rendelkezésre állását védő módon történjen, a jogszabályi, szerződéses és egyéb megfelelési kötelezettségek teljesítése mellett.

1.3 A szabályzat meghatározza a felhőkockázatok kezelésére, az adatok védelmére, a szolgáltatók megfelelőségének nyomon követésére és a jogosulatlan használat megszüntetésére szolgáló kontrollokat. Emellett támogatja az üzleti innovációt a felhőplatformok használatán keresztül azáltal, hogy összhangot teremt a biztonság, az üzemi megbízhatóság és a költséghatékonyság között.

**2. Hatály**

2.1 Jelen szabályzat valamennyi munkavállalóra, vállalkozóra, harmadik fél szolgáltatóra és külső tanácsadóra alkalmazandó, akik a szervezet nevében felhőszolgáltatásokat hoznak létre, konfigurálnak, érnek el, kezelnek vagy használnak.

**2.2 A szabályzat minden olyan környezetre kiterjed, ahol a szervezet adatai vagy munkaterhelései feldolgozásra kerülnek, ideértve különösen a következőket:**

2.2.1 Nyilvános, privát, hibrid és közösségi felhőtelepítések

2.2.2 Valamennyi felhőszolgáltatási modell (IaaS, PaaS, SaaS)

2.2.3 Többfelhős és föderált architektúrák

2.2.4 Shadow IT vagy személyes felhőfiókok üzleti célú használata

2.3 A szabályzat valamennyi osztályozási kategóriájú adatra kiterjed, és alkalmazandó mind a belső rendszerekre, mind a beszállító által üzemeltetett platformokra, ahol a szervezet tulajdonában álló vagy szabályozott adatot tárolnak vagy kezelnek.

**3. Célkitűzések**

3.1 A felhőtechnológiák biztonságos és következetes használatának biztosítása egyértelmű használati iránymutatások, előírt alapkonfigurációk és irányítási szerepkörök révén.

3.2 A felhőalapú működéshez kapcsolódó működési és megfelelési kockázatok minimalizálása, ideértve a jogosulatlan hozzáférést, az adatsértéseket, a hibás konfigurációt, a meg nem felelést és a szolgáltatáskimaradást.

3.3 A biztonsági és adatvédelmi követelmények érvényesítése valamennyi felhőszolgáltatóval szemben, valamint a megfelelés ellenőrzése szerződéses záradékok, értékelések és auditjog útján.

3.4 A skálázható és reziliens felhőbevezetés lehetővé tétele a kockázati helyzet, a jogi követelmények vagy az üzletmenet-folytonosság veszélyeztetése nélkül.

3.5 A felhőhasználat és a kapcsolódó irányítás összehangolása a szervezet információbiztonsági irányítási rendszerével (IBIR), jogi kötelezettségeivel (pl. GDPR, DORA), ágazatspecifikus iránymutatásokkal és az iparágban elismert legjobb gyakorlatokkal (pl. NIST, COBIT).

**4. Szerepkörök és felelősségek**

**4.1 Felső vezetés**

4.1.1 Jóváhagyja a Felhőszolgáltatások használatára vonatkozó szabályzatot és a felhőbevezetés stratégiai ütemtervét.

4.1.2 Felülvizsgálja és jóváhagyja a magas kockázatú kivételeket a standard felhőirányítási követelmények alól.

4.1.3 Biztosítja, hogy a felhőkezdeményezések megfelelő finanszírozást, felügyeletet és a vállalati kockázatkezelési keretrendszerhez való illeszkedést kapjanak.

**4.2 Információbiztonsági vezető**

4.2.1 A szabályzat és a szervezeti Felhőszolgáltatási Nyilvántartás tulajdonosa.

4.2.2 Jóváhagyja új felhőszolgáltatók bevonását a kellő gondosság elve szerinti vizsgálat és a kockázatértékelés eredményei alapján.

4.2.3 Felülvizsgálja a szolgáltatói megfelelőségi dokumentációt, és ellenőrzi a biztonsági követelményeknek 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 legalább évente felül kell vizsgálni, és szükség szerint frissíteni kell a folyamatos összhang biztosítása érdekében az alábbiakkal:**

9.1.1 a változó jogi és szabályozási követelményekkel (pl. GDPR, NIS2, DORA)

9.1.2 az ISO/IEC 27001 vagy ISO/IEC 27002 szabványok változásaival

9.1.3 a szervezet felhőarchitektúrájának, kockázati környezetének vagy szolgáltatási portfóliójának változásaival

9.1.4 incidensvizsgálatokkal, auditeredményekkel vagy a működés során levont tanulságokkal

**9.2 Az információbiztonsági vezető felelős a felülvizsgálat kezdeményezéséért és az érintett felek bevonásáért, ideértve az alábbiakat:**

9.2.1 felhőbiztonsági architekt

9.2.2 jogi és megfelelőségi csapat

9.2.3 beszerzési és beszállítókezelési vezetők

9.2.4 szolgáltatásgazdák és IT-üzemeltetés

**9.3 Minden módosításnak meg kell felelnie az alábbi követelményeknek:**

9.3.1 verziókezeléssel kell ellátni és dátummal kell rögzíteni

9.3.2 a felső vezetésnek jóvá kell hagynia

9.3.3 közölni kell az érintettekkel, ideértve a munkavállalókat, a vállalkozókat és a harmadik feleket

9.3.4 a belső dokumentációs szabályokkal összhangban archiválni kell

**9.4 Soron kívüli felülvizsgálatot különösen az alábbi események válthatnak ki:**

9.4.1 új felhőszolgáltatói együttműködések vagy jelentős migrációk

9.4.2 a felhőinfrastruktúrát érintő kialakulóban lévő kockázatok

9.4.3 szerződéses, jogi vagy ágazatspecifikus kötelezettségek lényeges változásai

## 10. Kapcsolódó szabályzatok és összefüggések

**10.1 Jelen szabályzat szorosan kapcsolódik az alábbi belső szabályzatokhoz, és azok alkalmazására épül:**

10.1.1 P1 – Információbiztonsági szabályzat: Meghatározza a rendszerek és szolgáltatások biztonságos működtetésének átfogó elveit, amelyeket jelen szabályzat a felhőkörnyezetben érvényesít.

10.1.2 P5 – Változáskezelési szabályzat: Minden felhőkonfigurációs változtatást a P5-ben meghatározott változáskezelési eljárások szerint kell végrehajtani.

10.1.3 P13 – Adatosztályozási és címkézési szabályzat: Meghatározza az adatok felhőbe történő átvitel előtti értékelésének módját, valamint azt, hogyan kell olyan kontrollokat alkalmazni, mint a titkosítás és az adattárolási helyre vonatkozó követelmények.

10.1.4 P18 – Kriptográfiai kontrollok szabályzata: Szabványokat ír elő a titkosításra, a kulcskezelésre és a kriptográfiai algoritmusok használatára, amelyek közvetlenül alkalmazandók a felhőszolgáltatások konfigurációiban.

10.1.5 P22 – Naplózási és felügyeleti szabályzat: Meghatározza a naplógyűjtésre, a megőrzésre és az elemzésre vonatkozó követelményeket, amelyeket a felhőkörnyezetekben is érvényesíteni kell.

10.1.6 P30 – Incidenskezelési szabályzat: Meghatározza a felhővel kapcsolatos biztonsági eseményekre alkalmazandó eszkalációs, elkülönítési és helyesbítő intézkedési eljárásokat.

10.1.7 P33 – Audit- és megfelelőségfelügyeleti szabályzat: Támogatja az auditra való felkészültséget és a folyamatos bizonyosságot arra vonatkozóan, hogy a felhőkontrollok érvényesítése és nyomon követése megtörténik.

## 11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001: 8.1 pont – Működéstervezés és -szabályozás: Előírja, hogy a szervezetek vezessék be és tartsák szabályozás alatt az információbiztonsági követelmények teljesítéséhez szükséges folyamatokat, beleértve a felhőkörnyezeteket érintő folyamatokat is.

**11.2 ISO/IEC 27002:2022 – 5.23–5.25 kontrollok:**

11.2.1 A melléklet 5.23 kontrollja – Felhőszolgáltatások használata: Előírja a kockázatalapú értékelést, a formális jóváhagyást és a felhőszolgáltatások használatának dokumentálását.

11.2.2 A melléklet 5.24 kontrollja – Felhőhasználati szabályzat: Előírja a szervezeti igényekkel és kockázatokkal összhangban álló formális felhőhasználati szabályzat kialakítását és betartatását.

11.2.3 A melléklet 5.25 kontrollja – Biztonság a felhőszolgáltatásokban: Előírja a biztonsági integráció, a szerződéses védelmek és a felhőben üzemeltetett munkaterhelések és adatok nyomon követésének szükségességét.

**11.3 NIST SP 800-53 Rev.5:**

11.3.1 AC-20 – Külső rendszerek használata: Előírja a szervezeti erőforrásokhoz külső vagy felhőalapú rendszerekről történő hozzáférésre vonatkozó szabályok és feltételek meghatározását.

11.3.2 SA-9(5) – Külső információs rendszerszolgáltatások: Előírja a szerződéses biztonsági követelményeket, a felügyeletet és a harmadik fél felhőrendszereinek folyamatos nyomon követését.

11.3.3 SC-12–SC-28 – Kriptográfiai védelem, határvédelem és az átvitel sértetlensége: Összhangban állnak a felhőben üzemeltetett szolgáltatások és a továbbítás alatt álló adatok titkosítási, identitáskezelési és hozzáférési követelményeivel.

11.3.4 SR-5 – Ellátási lánc védelme: Támogatja a szolgáltatásnyújtásban részt vevő felhőszolgáltatók átvilágítását és szerződéses kontrollját.

**11.4 GDPR (2016/679):**

11.4.1 28. cikk – Az adatfeldolgozók kötelezettségei: Előírja a felhőszolgáltatókkal kötött formális szerződéseket a személyes adatok kezelésének biztonsága, bizalmassága és auditálhatósága érdekében.

11.4.2 32. cikk – Az adatkezelés biztonsága: Támogatja a titkosítás, a hozzáférés-szabályozás, a naplózás és más védelmi intézkedések alkalmazását felhőkörnyezetekben.

11.4.3 V. fejezet – Nemzetközi adattovábbítások: Előírja az Európai Unión vagy EGT-n kívüli adattovábbítás jogszerűségét olyan biztosítékok alkalmazásával, mint az SCC-k vagy a megfelelőségi határozatok.

**11.5 NIS2 irányelv (2022/2555):**

11.5.1 21. cikk (2) bekezdés f), i) pont: Előírja, hogy a szervezetek kezeljék a harmadik fél felhőszolgáltatók kockázatait, és szerződéses, valamint technikai intézkedésekkel biztosítsák a digitális ellátási lánc sértetlenségét.

**11.6 DORA-rendelet (2022/2554):**

11.6.1 5. cikk (2) bekezdés – IKT-kockázatok irányítása: Előírja az IKT-hoz kapcsolódó harmadik fél kockázatok – ideértve a felhőszolgáltatásokat is – integrálását az általános kockázatirányításba.

11.6.2 28. cikk – Kritikus IKT-harmadik fél szolgáltatók felügyelete: Előírja, hogy a pénzügyi szervezetek nyomon kövessék, szabályozzák és dokumentálják a felhőszolgáltatói függőségeket, a kockázati helyzetet és a rezilienciát.

**11.7 COBIT 2019:**

11.7.1 BAI04 – A rendelkezésre állás és kapacitás kezelése: Biztosítja, hogy a felhőszolgáltatások reziliensek, felügyeltek legyenek, és megfeleljenek a meghatározott teljesítménykritériumoknak.

11.7.2 DSS01 – Üzemeltetés kezelése: Támogatja az üzemeltetési integrációt, az incidenskezelést és az előírt alapkonfigurációkat a felhőben üzemeltetett platformokon.

11.7.3 DSS05 – Biztonsági szolgáltatások kezelése: Irányt ad a felhőspecifikus biztonsági kontrollok bevezetésére, nyomon követésére és az incidensek megelőzésére a digitális szolgáltatásokban.