OPTESZ OPUS Zrt.

Információbiztonsági követelmények

Szerződéses partnerek részére

Utolsó felülvizsgálat: 2026.04.16.

Tartalomjegyzék

I. Bevezetés

Jelen dokumentum rögzíti az OPTESZ OPUS Zrt. (a továbbiakban: Társaság) által a vonatkozó jogszabályi előírásoknak megfelelően a Szerződéses Partner, illetve Felhőszolgáltató (a továbbiakban együttesen: Szerződéses Partner) felé támasztott, és a Szerződéses Partner által teljesítendő információbiztonsági követelményeket.

A dokumentum célja az elektronikus információs rendszerek (a továbbiakban: EIR) és az azokban kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának védelme, összhangban, többek között az alábbi vonatkozó jogszabályokkal:

- Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.)
- A Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet (a továbbiakban: Vhr.)
- A biztonsági osztályba sorolás követelményeiről szóló 7/2024. (VI. 24.) MK rendelet (a továbbiakban: MK rendelet)

A Társaság a jelen dokumentum elfogadtatásával gondoskodik arról, hogy az elektronikus információs rendszereit érintő tevékenységgel összefüggésben a szükséges kiberbiztonsági követelmények a jogszabályokban foglaltaknak megfelelően szerződéses kötelemként teljesüljenek.

II. Általános elvek

1. Arányosság és kockázatalapú megközelítés

A Szerződéses Partner köteles gondoskodni az EIR-ek és azok fizikai környezetének biztonságáról, a kiberfenyegetések által okozható károk mértékével arányos módon.

2. Bizalmasság, sértetlenség és rendelkezésre állás (CIA)

A biztonságnak ki kell terjednie a tárolt, továbbított vagy feldolgozott adatok, információk, valamint az EIR-ek által nyújtott vagy azokon keresztül elérhető szolgáltatások bizalmasságára, sértetlenségére és rendelkezésre állására.

3. Átfogó védelem

A védelemnek ki kell terjednie az adminisztratív, logikai és fizikai intézkedésekre egyaránt, valamint az EIR-ek teljes életciklusára, a fejlesztés megkezdésétől, egészen az élesüzemből való kivonásig.

4. Ellátási lánc biztonsága

A vonatkozó jogszabályok értelmében a Társaság köteles figyelembe venni a beszállítói és szolgáltatói kapcsolatokból eredő kockázatokat. Ez alapján a Szerződéses Partner köteles:

- a Társaság számára átlátható módon bemutatni saját, vonatkozó biztonsági intézkedéseit;
- tájékoztatni a Társaságot az általa igénybe vett további közreműködőkről (alvállalkozók);
- biztosítani, hogy az általa igénybe vett közreműködők is teljesítik a vonatkozó biztonsági követelményeket;
- a Társaság előzetes írásbeli jóváhagyása nélkül közreműködőt nem bevonni.

5. Átláthatóság és együttműködés

A Szerződéses Partner köteles átlátható módon tájékoztatni a Társaságot a biztonsági intézkedésekről, incidensekről és az adatok kezelésének módjáról. A Kiberbiztonsági tv. szerinti hatósági ellenőrzés, audit vagy incidensvizsgálat során a Szerződéses Partner köteles a Társasággal és az eljáró hatósággal teljeskörűen együttműködni.

6. Vezetői felelősség

A Szerződéses Partner köteles biztosítani, hogy a saját szervezetén belül a kiberbiztonság vonatkozású kockázatkezelési intézkedések jóváhagyása és a végrehajtás felügyelete megfelelő vezetői szinten történik.

III. Adminisztratív intézkedések

1. Információbiztonsági irányítási rendszer (IBIR/ISMS)

A Szerződéses Partner köteles létrehozni, karbantartani és felügyelni egy olyan irányítási rendszert, amely lehetővé teszi a vezetőség számára az információbiztonság hatékony irányítását és ellenőrzését. Az irányítási rendszernek összhangban kell lennie az MK rendelet szerinti kockázatmenedzsment keretrendszer követelményeivel.

2. Dokumentált eljárások és szabályzatok

A Szerződéses Partner köteles dokumentált eljárásokat kialakítani és karbantartani az alábbi területeken:

- Információbiztonság
- Kockázatelemzési és kockázatkezelés
- Hozzáférés-kezelés
- Incidenskezelés tervezése
- Üzletmenet-folytonossági és katasztrófa utáni helyreállítás tervezése
- Változáskezelés
- Adatosztályozási és adatkezelés

3. Humán erőforrás biztonsága és kiberbiztonsági képzés

A Szerződéses Partner köteles:

- megfelelő intézkedéseket hozni a humánerőforrással kapcsolatos biztonsági kockázatok kezelésére;
- biztosítani, hogy a Társaság EIR-jéhez hozzáférő munkatársai rendszeres kiberbiztonsági tudatossági és szakmai képzésben részesüljenek.

4. Megfelelőség menedzsment és kiberbiztonsági audit

A Szerződéses Partner köteles:

- rendszeres belső megfelelőségi vizsgálatokat végezni;
- biztosítani, hogy minden rendszer és folyamat megfelel a vonatkozó biztonsági szabályzatoknak;
- a Kiberbiztonsági tv.-ben előírt kétévenkénti kiberbiztonsági audit során a Társasággal együttműködni;
- a kiberbiztonsági audit során feltárt hiányosságok megszüntetésére 90 napon belül intézkedési tervet készíteni.

5. Közreműködők kezelése

Amennyiben a Szerződéses Partner közreműködőt kíván igénybe venni a Társaság EIR-jét érintő szolgáltatás nyújtásához, köteles a Társaság előzetes írásbeli hozzájárulását kérni, és biztosítani, hogy a közreműködő a jelen dokumentumban foglalt követelményeket maradéktalanul teljesíti. A közreműködő nem megfelelése esetén a Szerződéses Partner teljes felelősséggel tartozik.

6. Felhőszolgáltatás-specifikus adminisztratív követelmények

a) Szabványmegfelelés

A Felhőszolgáltató köteles megfelelni a releváns felhőbiztonsági szabványoknak és erről érvényes tanúsítványt bemutatni.

b) Adatlokalizáció és joghatóság

A Felhőszolgáltató köteles tájékoztatást adni az adatok tárolási helyéről és az alkalmazandó joghatóságról. Az adatok tárolása és feldolgozása az EGT területén kell történjen, kivéve a Társaság írásbeli eltérő rendelkezése esetén.

c) Felhő-hozzáférési engedélyezés

Amennyiben a felhőszolgáltatás igénybevételéhez a Vhr. szerinti felhő-hozzáférési engedélyezési eljárás szükséges, a Felhőszolgáltató köteles az ehhez szükséges műszaki és biztonsági információkat a Társaság rendelkezésére bocsátani.

7. Mesterséges intelligencia használata

A Szerződéses Partner a mesterséges intelligencia (MI) és gépi tanulás (ML) alapú megoldások — különösen a generatív mesterséges intelligencia (GenAI) — alkalmazását belső szabályozási rendszerében dokumentáltan kezeli. A szabályozás kiterjed legalább az engedélyezett eszközök körére, a használat feltételeire, a felelősségi viszonyokra, valamint a Társaság adataival kapcsolatos felhasználási korlátozásokra.

A Partner az MI- és ML-megoldások használatából eredő kockázatokat — ideértve különösen az adatszivárgás, a kimenetek megbízhatatlansága, a szerzői jogi és az ellátási lánc-kockázatokat — kockázatkezelési rendszerében azonosítja, értékeli és kezeli, az általános kockázatkezelési elvekkel összhangban.

A Partner a Társaság bizalmas, minősített vagy üzleti titkot képező adatait nyilvánosan elérhető, illetve a Társaság által előzetesen jóvá nem hagyott MI-szolgáltatás bemenetéhez (prompt, tanítóadat, kontextus) nem használhatja fel.

IV. Logikai intézkedések

1. Rendszer-hozzáférés kezelése

A Szerződéses Partner köteles az MK rendelet 2. mellékletének vonatkozó követelménycsaládjai alapján:

- szigorú hozzáférés-kezelési politikát alkalmazni (legkisebb jogosultság elve, feladatkörök szétválasztása);
- kiemelt (privilegizált) jogosultságok szigorú ellenőrzését és naplózását biztosítani;
- magas biztonsági osztályú rendszereket érintően többtényezős hitelesítést (MFA) alkalmazni minden távoli hozzáféréshez;
- a jogosultságokat rendszeresen, de legalább évente felülvizsgálni;
- a hozzáférések létesítését, módosítását és megszüntetését dokumentáltan végrehajtani.

2. Kártékony kódokkal szembeni védelem

A Szerződéses Partner köteles naprakész védelmet biztosítani a kártékony kódok ellen minden releváns rendszeren és eszközön, beleértve a végpontvédelmet, a hálózati szintű detekciót és a rendszeres ellenőrzéseket.

3. Biztonsági események naplózása és elemzése

A Szerződéses Partner köteles biztosítani a biztonsági események megfelelő naplózását, a naplók sértetlenségének védelmét és megőrzését, rendszeres elemzését, valamint magas biztonsági osztály esetén valós idejű biztonsági eseményfelügyeletet.

4. Sérülékenységkezelés

A Szerződéses Partner köteles:

- rendszeres sérülékenységvizsgálatot végezni – magas biztonsági osztály esetén legalább évente, behatolásvizsgálattal kiegészítve;
- a feltárt sérülékenységeket kockázatuk alapján priorizálni és indokolatlan késedelem nélkül javítani;
- a kritikus sérülékenységek javítását a feltárástól számított 72 órán belül megkezdeni;

5. Titkosítás és kriptográfia

A Szerződéses Partner köteles a Társaság nem nyilvános adatainak titkosítását legalább továbbítás során, jóváhagyott kriptográfiai módszerekkel biztosítani, a titkosítási kulcsok biztonságos kezelését garantálni.

6. Biztonságos kommunikáció

A Szerződéses Partner a szerződés teljesítése során adatok fogadására és továbbítására kizárólag a Társasággal előzetesen egyeztetett, biztonságos csatornát használ.

7. Felhőszolgáltatás-specifikus logikai követelmények

a) Multitenant környezet biztonsága

A Felhőszolgáltató köteles biztosítani a különböző ügyfelek adatainak és rendszereinek megfelelő logikai elkülönítését a megosztott infrastruktúrán.

b) Felhő-hozzáférés kezelése

A Felhőszolgáltató köteles olyan hozzáférés-kezelési rendszert biztosítani, amely lehetővé teszi a Társaság számára saját felhasználóinak és jogosultságainak önálló kezelését.

c) Virtualizációs biztonság

A Felhőszolgáltató köteles megfelelő biztonsági intézkedéseket alkalmazni a virtualizációs rétegben, beleértve a hypervisor biztonságát, a VM-izolációt és a konténerbiztonsági intézkedéseket.

V. Fizikai intézkedések

1. Eszközmenedzsment

A Szerződéses Partner köteles az eszközöket teljes életciklusuk alatt védeni, beleértve a leltározást, a biztonságos tárolást, szállítást és megsemmisítést, az MK rendelet vonatkozó követelményeinek megfelelően.

2. Fizikai és környezeti biztonság

A Szerződéses Partner köteles megfelelő fizikai és környezeti védelmet biztosítani az EIR-ek és azok fizikai környezete számára, beleértve a belépésellenőrzést, környezeti monitoring rendszereket és szünetmentes áramellátást.

VI. Technikai intézkedések

1. Hálózat és kommunikáció biztonsága

A Szerződéses Partner köteles megfelelő intézkedéseket hozni a hálózati biztonság érdekében:

- hálózati forgalom szűrése és tűzfalazása;
- titkosított kommunikációs csatornák alkalmazása;
- hálózati szegmentáció, különösen éles, teszt és menedzsment hálózatok elkülönítése;
- behatolásdetektálási/-megelőzési rendszerek (IDS/IPS) alkalmazása magas biztonsági osztály esetén.

2. Rendszer-megerősítés (Hardening)

A Szerződéses Partner köteles minden, a Társaság EIR-jéhez kapcsolódó rendszerét megfelelően megerősíteni, beleértve a szükségtelen szolgáltatások kikapcsolását, az alapértelmezett jelszók megváltoztatását, valamint az iparági legjobb gyakorlat szerinti optimalizálást.

3. Teszt és éles rendszerek szétválasztása

Éles adatok tesztkörnyezetben történő felhasználása kizárólag a Társaság előzetes írásbeli engedélyével, anonimizált vagy pszeudonimizált (álnevesített) formában megengedett.

VII. Kiberbiztonsági folyamatok

1. Kiberbiztonsági incidenskezelés

A Szerződéses Partner köteles hatékony incidenskezelési folyamatot működtetni.

a) Incidensjelentési kötelezettség a Társaság felé

A Szerződéses Partner köteles a Társaság EIR-jét érintő kiberbiztonsági incidenst az alábbi határidők betartásával jelenteni a szerződés szakmai kapcsolattartója, vagy a Társaság információbiztonsági felelőse felé:

Jelentés típusa	Határidő	Tartalom
Előzetes értesítés	Haladéktalanul, de legkésőbb 24 órán belül	Az incidens ténye, érintett rendszerek, kezdeti hatásértékelés
Incidensbejelentés	Az észleléstől számított 72 órán belül	Részletes leírás, hatás, érintett adatok köre, megtett intézkedések
Zárójelentés	Felszámolást követően, legkésőbb 30 napon belül	Kiváltó ok, teljes hatáselemzés, korrekciós intézkedések

Megjegyzés: A Társaság köteles a jelentős incidenseket az SZTFH és a nemzeti kiberbiztonsági incidenskezelő központ (NKI/Központ) felé is jelenteni. A Szerződéses Partner ehhez teljes körűen együttműködik.

b) Incidenskezelési terv

A Szerződéses Partner köteles incidenskezelési tervet készíteni, amely tartalmazza a megelőzés, észlelés, elemzés, elszigetelés, reagálás és helyreállítás lépéseit, a felelős személyeket és határidőket.

2. IT változáskezelés

A Szerződéses Partner köteles strukturált változáskezelési folyamatot alkalmazni. A Társaság EIR-jét érintő változásokhoz a Társaság előzetes jóváhagyása szükséges.

3. Üzletmenet-folytonosság és katasztrófa-helyreállítás (BCP/DRP)

A Szerződéses Partner köteles BCP/DRP terveket kidolgozni, rendszeresen tesztelni, a tesztek eredményeit kérésre a Társaság felé bemutatni.

4. Biztonságos szoftver- és hardverbeszerzés, -fejlesztés és -üzemeltetés

A Szerződéses Partner köteles biztonsági követelményeket alkalmazni a szoftver és hardver termékek beszerzése, fejlesztése és üzemeltetése során. A fejlesztési szerződésekben meg kell határozni a sérülékenységek javítására vonatkozó kötelezettséget, alkalmazni kell biztonságos szoftverfejlesztési életciklus elveit.

5. Felhőszolgáltatás-specifikus folyamatok

a) Adatok hordozhatósága és törlése

A Felhőszolgáltató köteles biztosítani a Társaság adatainak szabványos, egyeztetett formátumban és struktúrában történő exportálását, a szerződés megszűnése után az adatok visszaszolgáltatását és biztonságos, visszaállíthatatlan törlését, valamint a kilépési terv szerinti átállás támogatását.

b) Kiberbiztonsági gyakorlatok

A Társaság jogosult a kiberbiztonsági gyakorlatai során bevonni a Szerződéses Partnert. A Szerződéses Partner köteles az ilyen gyakorlatokban aktívan részt venni.

VIII. Záró rendelkezések

1. Rendszeres felülvizsgálat

A Szerződéses Partner köteles legalább évente felülvizsgálni és frissíteni az információbiztonsági intézkedéseit, figyelembe véve a technológiai fejlődést, a változó fenyegetéseket és a jogszabályi környezet változásait.

2. Megfelelés ellenőrzése

A Társaság fenntartja a jogot, hogy előzetes értesítés után (legalább 5 munkanap) ellenőrizze a Szerződéses Partner megfelelését, a kiberbiztonsági audit keretében az auditor a Szerződéses Partner rendszereibe is betekintést nyerjen, továbbá az SZTFH, illetve a nemzeti kiberbiztonsági incidenskezelő központ vizsgálata során a Szerződéses Partnerrel kapcsolatos információkat az eljáró hatóság rendelkezésére bocsássa.

3. Kapcsolattartás

A Felek elfogadják, hogy nevesített kontaktszemélyek kerülnek kijelölésre. Változás esetén az érintett Fél azonnal értesíti a másik felet.

A Társaság részéről információbiztonsággal összefüggésben kijelölt kapcsolattartó:

Fejes Zoltán

információbiztonsági felelős (IBF)

fejes.zoltan@opusenergetika.hu

+36 70 698 3593