Információbiztonsági követelmények

Jelen „Információbiztonsági követelmények” című dokumentum alkalmazandó az OPTESZ OPUS Zrt. / OPUS TIGÁZ Zrt. / OPUS TITÁSZ Zrt. szerződéskötési folyamatainak eredményeként megkötött szerződések kapcsán, a szerződéses klauzula alkalmazása útján.

Az OPUS TIGÁZ Zrt.-nek és az OPTESZ OPUS Zrt.–nek az igénybejelentőkkel/felhasználókkal kötendő elosztói (hálózati) csatlakozási és (elosztó)hálózat-használati szerződéses jogviszonyokban az „Információbiztonsági követelmények” című dokumentum nem alkalmazandó.

Jelen vezérigazgatói utasítás 2023. július 1. napjától visszavonásáig hatályos.

Bevezető rendelkezések

Jelen dokumentum az **OPUS Energetika** (OPUS TITÁSZ Zrt., OPTESZ OPUS Zrt., OPUS TIGÁZ Zrt. továbbiakban, mint OPUS) információbiztonsági követelményeit tartalmazza, amelyek érvényre juttatása az OPUS számára nyújtott minden olyan szolgáltatás, abban résztvevő rendszer, illetve azt működtető Szerződéses partner vonatkozásában irányadó, amelyek tekintetében a Szerződéses partner a tevékenysége során az OPUS adatait (különösen: adat, személyes adat, know-how, üzleti titok körébe tartozó információ, ismeret, kapcsolódó dokumentumok) kezeli, vagy az OPUS-nak szolgáltatott adatot létrehozza, tárolja, feldolgozza, továbbítja, megsemmisíti, illetve ezen rendszerek működését támogatja.

Szerződéses partner – az OPUS-szal kötött szerződésben – vállalta a jelen követelményjegyzékben foglaltak megismerését, és az általa ellátott tevékenység(ek) szempontjából releváns követelmények teljesítését mind saját magára (valamint közreműködőjére), mind az általa nyújtott szolgáltatásra vonatkozóan.

Amennyiben az OPUS és a Szerződéses partner közti jogviszonyban a szolgáltatás/tevékenységi kör bővül, arra vonatkozóan a Szerződéses partner a releváns követelmények figyelembevételére és betartására köteles!

1. Megbízható forrás, jogtiszta szolgáltatáselemek

Szerződéses partner biztosítja, hogy a szolgáltatás nyújtásához használt hardver és szoftver eszközök ismert és megbízható forrásból származnak, tulajdon-, illetve használati joguk rendezett, technikai támogatásuk elérhető és megbízható, valamint nyomon követhető az ellátási lánc.

2. Ellátási lánc

Amennyiben az OPUS számára nyújtott szolgáltatásban releváns, a Szerződéses partner biztosítja, hogy azonosítja és kezeli az információbiztonsági kockázatokat a szolgáltatás minden szakaszában, beleértve azt, hogy külső beszállítók bevonása esetén, a velük kötött szerződésben a – legalább jelen dokumentumban rögzített, tevékenységükre vonatkozó – követelményeket dokumentált módon rögzíti, és szavatol azok teljesüléséért, a kiszervezett kontrollok megfelelőségéért.

3. Eszköz menedzsment

Szerződéses partner biztosítja, hogy a szolgáltatással összefüggésben felhasznált eszközöket egész életciklusuk alatt védi a sérüléssel, elvesztéssel, lopással, az azokon kezelt, tárolt adatok jogosulatlan hozzáférhetővé tételével szemben. Szerződéses partner biztosítja továbbá, hogy ezeket az eszközöket szükséges jellemzőikkel, megfelelési követelményeikkel naprakészen karbantartott nyilvántartásba veszi. Szerződéses partner biztosítja, hogy minden használatban lévő eszköz tulajdonoshoz van rendelve, mely tulajdonos felelős az eszköz működtetéséért.

4. Biztonságos megsemmisítés és újra felhasználás

A Szerződéses partner biztosítja, hogy az OPUS számára nyújtott szolgáltatásban érintett hardverek kivonása során az adathordozók újra felhasználása vagy eladása az adatok teljeskörű, visszaállíthatatlan törlésével történik, vagy azok biztonságosan és dokumentáltan megsemmisítésre kerülnek. A biztonságos törlés vagy megsemmisítés koncepciójába az OPUS adatvagyonát illetően az OPUS betekintést nyerhet, illetve saját vonatkozásában evidenciáit megkaphatja.

5. Rendszer menedzsment

Szerződéses partner biztosítja, hogy az általa nyújtott szolgáltatással összefüggésben, az érintett rendszerek és az általuk tárolt, kezelt vagy továbbított adatok védettek a hibás működés, kibertámadás, jogosulatlan közzététel, sérülés, lopás vagy elvesztés ellen. A biztonságos üzemeltetés érdekében rendszerekhez kapcsolódó, üzletmenet-folytonossági szempontból nélkülözhetetlen adatokról és szoftverekről biztonsági mentést készít; változás menedzsment folyamatot alkalmaz és monitorozza az elfogadott szolgáltatási szint teljesülését.

6. Hálózat és kommunikáció

A Szerződéses partner biztosítja, hogy (i) a szolgáltatásában érintett, bérelt, vagy saját tulajdonú hálózatán szűri és elemzi a hálózati forgalmat, megelőzi a jogosulatlan hozzáférést, titkosított átvitelt alkalmaz. (ii) Az érintett hálózati eszközöket (beleértve a routereket, tűzfalakat, vezeték nélküli hozzáférési pontokat) úgy konfigurálja, hogy megelőzze a nem engedélyezett, illetve nem megfelelő frissítéseket.

Szerződéses partner garantálja (iii) a szolgáltatásában érintett rendszerek hardening-jét, és hogy (iv) a számítógépek, hálózatok nevét, topológiáját külső felek elől elrejti. (v) Hálózattervezés során szegmentációt, több rétegű architektúrát és DMZ-t alkalmaz azon alkalmazások esetében, melyek elérhetők az interneten keresztül, vagy nem megbízható hálózathoz kapcsolódnak.

Amennyiben a szolgáltatás szempontjából releváns, (vi) rendszereihez, hálózataihoz minimumra korlátozza a kapcsolódási módokat, és (vii) csak megbízható üzleti alkalmazásoknak, információs rendszereknek vagy meghatározott hálózati szegmenseknek engedélyez hozzáférést.

7. Hardening

A Szerződéses partnernek minden információs és hálózati rendszernek a hardeningjéről gondoskodni kell. Ez magában foglalja a szükségtelen alkalmazások, szolgáltatások, eszközök, protokollok és interfészek letiltását; gyártó által adott alapértelmezett felhasználónevek és jelszavak törlését, vagy legalább megváltoztatását; biztonságot fokozó beállítások aktiválását; technikai információk védelmét.

8. Kártékony kódokkal szembeni védelem

A Szerződéses partner biztosítja, hogy a kártékony kódok minden formája (pl. vírusok, férgek, trójai programok, kémprogramok, rootkit-ek, botnet szoftverek, billentyűzetnaplózók, ransomware-ek) ellen védelmi megoldást telepít minden informatikai rendszerén, melyen lehetséges ennek alkalmazása, és meghatározott időközönként automatikusan aktualizálja azt. A Szerződéses partner biztosítja és rendszeresen felülvizsgálja, hogy az antivírus szoftver nem került letiltásra, az a megfelelő konfigurálás szerinti funkcionalitással működik.

9. Rendszer hozzáférés

Azon eszközökhöz, melyek OPUS-hoz tartozó adatot létrehoznak, feldolgoznak, tárolnak vagy továbbítanak, illetve az OPUS számára nyújtott szolgáltatásban érintettek, Szerződéses partner a hozzáférést korlátozza a jogosult személyekre, meghatározott üzleti céllal. Ez minimálisan magában foglalja azt, hogy (i) a *„szükséges és elégséges jogosultság*" elvet alkalmazva, csak felhatalmazott felhasználók kaphatnak hozzáférést a releváns információkhoz, (ii) a hozzáférések a jóváhagyott rendszerfunkciókra/-elemekre korlátozottak, (iii) a feladatok, szerepkörök és felelősségek megfelelő szétválasztása biztosított, (iv) nincsenek közös használatú felhasználói fiókok. Szerződéses partner biztosítja, hogy az OPUS számára nyújtott szolgáltatásban érintett rendszerek rendszergazdai hozzáférése (v) minimális számú rendszeradminisztrátorra korlátozódik, (vi) 2 faktoros, vagy azzal egyenértékű biztonsági szintet garantáló autentikációval védett, (vii) minden esetben naplózott. (viii) Biztosítja továbbá, hogy eljárásrendet működtet és tart karban, amely leírja a rendszeradminisztrátori szerepek, felhasználói fiókok, hozzáférések és jogosultságok létrehozásának, rendszeres felülvizsgálatának, módosításának, zárolásának és törlésének folyamatát, valamint (ix) hozzáféréskezelése megfelelő riportálhatósággal támogatja a dokumentált, rendszeres vagy alkalmi hozzáférés-felülvizsgálatokat.

10. Biztonsági esemény naplózása, elemzése

Szerződéses partner biztosítja, hogy (i) releváns szolgáltatás vonatkozásában, biztonsággal összefüggésben az események naplózása mindenkor engedélyezett, minden olyan, a Szerződéses partner által működtetett rendszeren, mely az OPUS számára nyújtott szolgáltatásban érintett; (ii) a naplóállományok vonatkozásában konzisztens, megbízható dátum és időforrások biztosítják, hogy az esemény bejegyzések hiteles időbélyeget használnak (pl. NTP szerverek használatával); (iii) a biztonsági vonatkozású eseménybejegyzések védve vannak a jogosulatlan hozzáféréstől és a véletlen vagy szándékos módosítástól/felülírástól,

Továbbá (iv) biztosítja, hogy az OPUS információit létrehozó, tároló, kezelő alkalmazásokon bármilyen jellegű forensic elemzésre/tevékenységre csak az OPUS információbiztonsági felelősének bevonásával kerül sor, a négyszem-elv teljesülése érdekében.

11. Dokumentált eljárások

A Szerződéses partner a szerződés teljesítése szempontjából releváns tevékenységének működtetésére vonatkozó felelősségeket, eljárásokat kialakította, a működtetés kontrolljai és dokumentáltsága összhangban van a szerződéses, illetve a hatályos jogszabályi követelményekkel és jelen megállapodás időtartama alatt mindenkor naprakész. A működési eljárások dokumentációjába, saját magára vonatkozóan, indokolt esetben az OPUS betekintést nyerhet.

12. Információbiztonság menedzsment

(i) Szerződéses partner létrehoz, karbantart és felügyel egy olyan irányítási (keret)rendszert, illetve folytat olyan tevékenységet, amely lehetővé teszi a Szerződéses partner vezetősége részére, hogy egyértelmű irányokat mutasson, és bizonyítsa elkötelezettségét az információbiztonság vonatkozásában. (ii) Szolgáltatónál létezik

információbiztonság vonatkozású funkció vagy szerepkör, mely biztosítja az információbiztonsági jó gyakorlatok hatékony és következetes alkalmazását, illetve az információbiztonságot érintő jogi, szabályozási és szerződéses előírásoknak való megfelelést. Szerződéses partner átfogó, folyamatos biztonságtudatossági programot tart fenn annak érdekében, hogy támogassa és beépítse az elvárt biztonságtudatos magatartást mindazon személyeknél, akik OPUS számára nyújtott szolgáltatásban közreműködnek.

13. Információbiztonsági incidensek kezelése

A Szerződéses partner biztosítja, hogy információbiztonsággal összefüggésben bekövetkező incidensek kezelésére incidensfelügyeleti folyamatot működtet, melyben az incidensek (rögzítése, besorolása, kezdeti támogatása, vizsgálata, megoldása, a szolgáltatás visszaállítása) teljes életciklusa megfelelően követhető, illetve kezelve van, és mely folyamat során keletkezett dokumentumokba/nyilvántartásokba, saját magára vonatkozóan és indokolt esetben az OPUS betekintést nyerhet.

14. IT változáskezelés

Szerződéses partner biztosítja, hogy releváns tevékenység, illetve rendszer esetén, az új IT környezet implementálása, vagy a már meglévő környezetet érintő nagyobb módosítások megvalósítása előtt, illetve jelentős új technológiák bevezetésekor a vonatkozó információbiztonsági kockázatokat azonosítja, értékeli, kezeli, ellenőrzi és elfogadható korlátok között tartja. A jelen pontban rögzített tevékenysége során keletkezett dokumentumokba, saját magára vonatkozóan és indokolt esetben az OPUS betekintést nyerhet.

15. Teszt és éles rendszerek szétválasztása

A Szerződéses partner biztosítja, hogy amennyiben az OPUS számára nyújtott szolgáltatásban releváns (i) a szolgáltatásban érintett teszt és éles rendszerek legalább logikailag elszigeteltek, annak érdekében, hogy csökkentsék a rendszerekben a jogosulatlan hozzáférés vagy jogosulatlan módosítás kockázatát. (ii) Amennyiben a szétválasztás nem lehetséges, a Szerződéses partner biztosítja, hogy megfelelő változás menedzsment folyamatot biztosít az éles rendszerekben bekövetkező incidensek és vészhelyzetek gyors, kiemelt kezelésére. (iii) Éles adatok használata nem engedélyezett a teszt vagy fejlesztői környezetben, illetve a személyes adatokat és személyes azonosításra alkalmas adatokat anonimizálni kell.

16. Feltárt hibák javítása

A Szerződéses partner biztosítja, hogy amennyiben az OPUS részére nyújtott, releváns szolgálatásban fejlesztett rendszeren végrehajtott sérülékenységvizsgálat során, az általa fejlesztett alkalmazásban olyan biztonsági rést azonosítanak, mely egyértelműen a Szerződéses partnernek felróható, garanciálisan javítja azt. Amennyiben a javítást követően az ismételt ellenőrzés újra hibát tár fel, az ellenőrzés költségeit a Szerződéses partner vállalja.

17. Forráskód védelme

Amennyiben a szerződésben rögzített szolgáltatás során releváns, Szerződéses partner vállalja, hogy a forráskódot megfelelő intézkedésekkel védi a jogosulatlan hozzáféréstől, minden korábbi verzióját eltárolja, a változásokat dokumentálja. AZ OPUS részére fejlesztett rendszer esetében – ha azt a szerződés máshogyan nem kezeli - az aktuális forráskódot és annak dokumentációját legalább 10 évig megőrzi, vagy az OPUS részére átadja.

18. Sérülékenységvizsgálat

Szerződéses partner biztosítja, hogy az OPUS számára nyújtott szolgáltatásban érintett, külső hálózati (pl. adatgyűjtő) eszközön, illetve publikus felületen (pl. weblap) keresztül is elérhető rendszerei időszakosan tesztelve

vannak sérülékenységek, illetve konfigurációs hibák azonosítása céljából. Minden feltárt sebezhetőség, nem-megfelelőség, mely az OPUS részére nyújtott szolgáltatást is érinti, indokolatlan késedelem nélkül megosztásra kerül az OPUS-sal.

19. Rendelkezésre állás és támogatás

Amennyiben a Szerződéses partnerrel kötött szerződésben másként nem került meghatározásra, és az OPUS számára nyújtott szolgáltatásban releváns, a Szerződéses partnernek biztosítania kell a következő követelményeket rendelkezésre állás, támogatás, RPO és RTO értékeket illetően:

- 99,6% vagy magasabb rendelkezésre állás
- 24/7 támogatás
- RPO (Szükséges visszaállítási pont) < 8 óra
- RTO (Szükséges visszaállítási idő) < 24 óra

20. Megfelelőség menedzsment

A Szerződéses partner biztosítja, hogy (i) minden rendszer, mely az OPUS számára nyújtott szolgáltatásban érintett, rendszeresen vizsgálva van megfelelőség szempontjából legalább a Szerződéses partner saját biztonsági szabályzatainak megfelelően. (ii) A Szerződéses partner biztonsági szabályzatai/eljárásai megfelelnek és összhangban vannak a jelen dokumentumban rögzített elvárásokkal. (iii) A megfelelőségi riportok/jelentések/jegyzőkönyvek igazolják, hogy a technikai megfelelőségi ellenőrzések minden olyan IT eszközön megtörténtek az IT környezetben, melyek az OPUS számára nyújtott szolgáltatásban érintettek. A megfelelőségi riportoknak tartalmazniuk kell a kapcsolódást a jelen dokumentumban rögzített kapcsolódó kontrollok és a technikai megfelelőségi ellenőrzés között. (iv) A Szerződéses partner biztonsági szabályzataiba az OPUS indokolt esetben, előzetes egyeztetést követően betekintést nyerhet.

21. Humán erőforrás biztonsága

Minden, a Szerződéses partner megbízásából eljáró, az OPUS-nál hozzáférést igénylő személyről az OPUS kérésére a Szerződéses partnernek információt kell szolgáltatnia. A Szerződéses partner biztosítja, hogy a humánerőforrás azonosítása megtörténjen és a Szerződéses partner munkatársai közül senki ne éljen vissza a jogosultságaival. A Szerződéses partner teljeskörű felelőséggel tartozik a jogosulatlan hozzáférésből származó károkért az OPUS adatait illetően. A Szerződéses partner csak olyan személyt bíz meg, aki megfelelően kvalifikált az érintett feladatra. Amennyiben a szolgáltatás az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) hatálya alá eső rendszert érint, a Szerződéses partner az Ibtv. előírásai szerint meghatározza a szervezetével kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is, illetve biztosítja az azoknak való megfelelést és dokumentálást. Ennek keretein belül Szerződéses partner előírja, hogy amennyiben a szervezetétől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az OPUS elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül értesíti az OPUS kapcsolattartóját. Jelen előírások teljesítését az OPUS indokolt esetben, előzetes egyeztetést követően, partneri audit keretein belül ellenőrizheti.

22. Helyszíni munkavégzés követelményei

Amennyiben helyszíni munkavégzés szükségessége fennáll, a Szerződéses partner minden munkavállalója, aki az OPUS valamely telephelyén munkát végez, megismeri és betartja az OPUS hatályos biztonsági

szabályzataiban, előírásaiban foglaltakat. Ezen előírások aktuális verzióját az OPUS a helyszíni munkavégzést megelőzően megosztja Szerződéses partner érintett munkavállalóival.

23. Biztonságos kommunikáció

A szerződés teljesítése során az adatok továbbítására kizárólag az OPUS-al egyeztetett csatornák, vagy az OPUS által biztosított megoldások alkalmazhatóak. Az adatok felhasználásánál, tárolásánál megfelelő biztonsági intézkedésekkel szükséges megakadályozni a jogosulatlan hozzáférést.

24. Alapvető szolgáltató, létfontosságú rendszerelem

Amennyiben a Szerződéses partner által nyújtott szolgáltatás Ibtv. alapján alapvető szolgáltatást, vagy létfontosságú rendszerelemet érint, a Szerződéses partner releváns tevékenysége, illetve a szolgáltatás kivitelezése során betartja és közreműködőivel betartatja az Ibtv. vonatkozó követelményeit.

25. Kapcsolattartás

Amennyiben a szerződésben rögzített szolgáltatás során releváns, a Felek elfogadják, hogy nevesített kontaktszemélyek kerülnek kijelölésre a jelen dokumentumban említett vállalásokkal összefüggésben. Változás esetén az érintett Fél nevesített kontaktszemélyt jelöl ki, melyről azonnal értesíti a másik felet. AZ OPUS részéről információbiztonsággal összefüggésben kijelölt kapcsolattartó:

Fejes Zoltán
IT auditor, információbiztonsági felelős
fejes.zoltan@opustigaz.hu
+36 70 698 3593