OPUS TITÁSZ Zrt.
4024 Debrecen
Kossuth u. 41.
www.opustitasz.hu

Információbiztonsági követelmények

I. Bevezetés

Jelen dokumentum rögzíti az **OPUS TITÁSZ Zrt.** (továbbiakban: **Társaság**) által a vonatkozó jogszabályi előírásoknak megfelelően a Szerződéses partner / Felhőszolgáltató felé támasztott és a Szerződéses partner / Felhőszolgáltató által teljesítendő információbiztonsági követelményeket. A jelen dokumentumban megfogalmazott követelmények célja az elektronikus információs rendszerek és az azokban tárolt adatok védelme, összhangban a vonatkozó jogszabályi előírásokkal.

II. Általános elvek

1. Arányosság elve
   A Szerződéses partner köteles gondoskodni az elektronikus információs rendszerei és azok fizikai környezetének biztonságáról, a kiberfenyegetések által okozható károk mértékével arányos módon.

2. CIA/BSR elvek
   A biztonságnak ki kell terjednie a tárolt, továbbított vagy feldolgozott adatok, információk, valamint az elektronikus információs rendszerek által nyújtott vagy azon keresztül elérhető szolgáltatások bizalmasságára, sértetlenségére és rendelkezésre állására.

3. Kockázatalapú megközelítés
   A Szerződéses partner köteles rendszeres kockázatelemzést végezni, és a biztonsági intézkedéseket a feltárt kockázatok alapján meghatározni.

4. Átfogó védelem
   A védelemnek ki kell terjednie az adminisztratív, logikai és fizikai intézkedésekre egyaránt, valamint az elektronikus információs rendszerek teljes életciklusára.

5. Átláthatóság
   A Szerződéses partner köteles átlátható módon tájékoztatni a Társaságot a biztonsági intézkedésekről, incidensekről és az adatok kezelésének módjáról.

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 vezetősége számára az információbiztonság hatékony irányítását és ellenőrzését.

2. Dokumentált eljárások
   A Szerződéses partner köteles dokumentált eljárásokat kialakítani és karbantartani minden kritikus információbiztonsági folyamatra vonatkozóan.

3. Humán erőforrás biztonsága
   A Szerződéses partner köteles megfelelő intézkedéseket hozni a humánerőforrással kapcsolatos biztonsági kockázatok kezelésére.

4. Megfelelőség menedzsment
   A Szerződéses partner köteles rendszeres megfelelőségi vizsgálatokat végezni, és biztosítani, hogy minden rendszer és folyamat megfelel a vonatkozó biztonsági szabályzatoknak, jogi előírásoknak.

5. Közreműködők kezelése
   Amennyiben a Szerződéses partner közreműködőt vesz igénybe, köteles biztosítani, hogy a közreműködő is teljesíti a releváns biztonsági követelményeket.

6. Felhőszolgáltatás esetén
   a. Szabványmegfelelés
      A Felhőszolgáltató köteles megfelelni a releváns felhőbiztonsági szabványoknak, iparági előírásoknak.

   b. Adatlokalizáció és joghatóság
      A Felhőszolgáltató köteles tájékoztatást adni az adatok tárolási helyéről és az alkalmazandó joghatóságról, valamint biztosítani a Társaság adatlokalizációs igényeinek teljesítését.

IV. Logikai intézkedések

1. Rendszer hozzáférés
   A Szerződéses partner köteles szigorú hozzáférés-kezelési politikát alkalmazni, beleértve a legkisebb jogosultság elvét, a feladatkörök szétválasztását, és a kiemelt jogosultságok szigorú ellenőrzését.

2. Kártékony kódokkal szembeni védelem
   A Szerződéses partner köteles naprakész védelmet biztosítani a kártékony kódok ellen minden releváns rendszeren és eszközön.

3. Biztonsági események naplózása és elemzése
   A Szerződéses partner köteles biztosítani a biztonsági események megfelelő naplózását és rendszeres elemzését.

4. Sérülékenységvizsgálat és javítás
   A Szerződéses partner köteles rendszeres sérülékenységvizsgálatokat végezni, és a feltárt hibákat indokolatlan késedelem nélkül javítani.

5. Biztonságos kommunikáció
   A Szerződéses partner a szerződés teljesítése során adatok fogadására és továbbítására kizárólag egyeztetett csatornát használ.

6. Felhőszolgáltatás esetén
   a. Multitenant környezet biztonsága
      A Felhőszolgáltató köteles biztosítani a különböző ügyfelek adatainak és rendszereinek megfelelő elkülönítését a megosztott infrastruktúrán.
   b. Hozzáférés-kezelése
      A Felhőszolgáltató köteles olyan hozzáférés-kezelési rendszert biztosítani, amely lehetővé teszi a Társaság számára a saját felhasználóinak és jogosultságainak kezelését.
   c. Titkosítás a felhőben
      A Felhőszolgáltató köteles biztosítani az adatok titkosítását mind tárolás, mind továbbítás során a Társaság által jóváhagyott módon.
   d. Virtualizációs biztonság
      A Felhőszolgáltató köteles megfelelő biztonsági intézkedéseket alkalmazni a virtualizációs rétegben (hypervisor biztonság, VM izoláció).

V. Fizikai intézkedések

1. Eszköz menedzsment
   A Szerződéses partner köteles az eszközöket teljes életciklusuk alatt védeni, beleértve a leltározást, a biztonságos tárolást és a biztonságos megsemmisítést.

2. Fizikai és környezeti biztonság
   A Szerződéses partner köteles megfelelő fizikai és környezeti védelmet biztosítani az elektronikus információs rendszerek és azok fizikai környezete számára.

VI. Technikai intézkedések

1. Hálózat és kommunikáció biztonsága
   A Szerződéses partner köteles megfelelő intézkedéseket hozni a hálózati biztonság érdekében, beleértve a hálózati forgalom szűrését, a titkosított kommunikációt és a hálózati szegmentációt.

2. Rendszer megerősítés (Hardening)
   A Szerződéses partner köteles minden rendszerét megfelelően megerősíteni, beleértve a szükségtelen szolgáltatások és protokollok kikapcsolását, valamint a biztonsági beállítások optimalizálását.

3. Teszt és éles rendszerek szétválasztása
   A Szerződéses partner köteles biztosítani a teszt és éles rendszerek megfelelő elkülönítését, és megakadályozni az éles adatok használatát tesztkörnyezetben.

VII. Folyamatok

1. Információbiztonsági incidensek kezelése
   A Szerződéses partner köteles hatékony incidenskezelési folyamatot működtetni, amely magában foglalja az incidensek megelőzését, felismerését, kezelését és a hatások csökkentését.

2. IT változáskezelés
   A Szerződéses partner köteles strukturált változáskezelési folyamatot alkalmazni, amely biztosítja a változtatások biztonságos végrehajtását és a kockázatok megfelelő kezelését.

3. Üzletmenet-folytonosság és katasztrófa utáni helyreállítás
   A Szerződéses partner köteles üzletmenet-folytonossági és katasztrófa utáni helyreállítási terveket kidolgozni és rendszeresen tesztelni.

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.

5. Felhőszolgáltatás esetén
   a. Adatok hordozhatósága és törlése
      A Felhőszolgáltató köteles biztosítani a Társaság számára az adatok szabványos formátumban történő exportálását és a szerződés megszűnése után az adatok biztonságos törlését

VIII. Záró rendelkezések

1. Vonatkozó jogszabályok
   A Szerződéses partner a jelen dokumentumban meghatározott elvárásokon túlmenően köteles minden olyan elvárást is teljesíteni, amelyet vonatkozó jogszabály rá nézve meghatároz.

2. Rendszeres felülvizsgálat és fejlesztés
   A Szerződéses partner köteles rendszeresen felülvizsgálni és frissíteni az információbiztonsági intézkedéseit, figyelembe véve a technológiai fejlődést, a változó fenyegetéseket és a jogszabályi környezet változásait.

3. Megfelelés ellenőrzése
   A Társaság fenntartja a jogot, hogy előzetes értesítés után ellenőrizze a Szerződéses partner megfelelését a jelen dokumentumban foglalt követelményeknek.

4. 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.

   A Társaság részéről információbiztonsággal összefüggésben kijelölt kapcsolattartó:

   Fejes Zoltán
   információbiztonsági felelős
   fejes.zoltan@opusenergetika.hu
   +36 70 698 3593