INFORMÁCIÓBIZTONSÁGI ÚTMUTATÓ

Külső partnerek, beszállítók és közreműködők számára

BEVEZETÉS

Ez az útmutató az Alpiq Magyarország vállalatcsoporttal szerződéses kapcsolatban álló, annak ügyviteli vagy üzemviteli informatikai rendszereiben hozzáféréssel rendelkező, vagy az IT/OT környezet működéséhez hozzájáruló külső partnerek, beszállítók és közreműködők számára határozza meg az alapvető információbiztonsági követelményeket. A dokumentum célja, hogy biztosítsa az Alpiq adatvagyonának, üzleti folyamatainak, informatikai és kiber-fizikai rendszereinek védelmét a közös munkavégzés során.

Az Alpiq csoport elkötelezett az információbiztonság magas színvonalú, releváns kockázatokkal arányos fenntartása mellett. Követi a NIS2 előírásait és valamennyi külső partnerétől elvárja az ellátási lánc résztvevőire vonatkozó követelmények következetes betartását. Az útmutatóban foglalt szabályok betartása kötelező minden olyan – fentebb részletezett körbe tartozó - személy és szervezet számára, aki az Alpiq nevében vagy érdekében végez tevékenységet.

1. ÁLTALÁNOS BIZTONSÁGI ELVÁRÁSOK

1.1 Titoktartási kötelezettség

Minden külső partnernek titoktartási nyilatkozatot kell aláírnia a szerződéskötés előtt. Ez a kötelezettség kiterjed minden olyan információra, amellyel az Alpiq-kal való együttműködés során találkozik. A titoktartási kötelezettség a szerződés megszűnése után is fennmarad a jogszabályokban meghatározott ideig.

A bizalmas információk közé tartoznak különösen:

- Üzleti tervek, stratégiák és pénzügyi adatok;
- Műszaki dokumentációk és technológiai megoldások, beállítások paraméterei;
- Ügyfél- és partneradatok;
- Belső szervezeti információk;
- Informatikai rendszerek felépítése és biztonsági intézkedések.

1.2 Személyi biztonság

A külső partnereknek biztosítaniuk kell, hogy az általuk delegált munkatársak megfelelő háttérellenőrzésen, biztonságtudatossági és szakmai felkészítésen estek át. Minden érintett munkatársnak el kell fogadnia az Alpiq információbiztonsági útmutatójában foglaltak betartására vonatkozó nyilatkozatot.

A külső partnerek kötelesek azonnal értesíteni az Alpiq kijelölt kapcsolattartóját, ha valamelyik munkatársuk munkaviszonya megszűnik vagy megváltozik a hozzáférési jogosultsága.

2. ADATVÉDELMI KÖVETELMÉNYEK

2.1 Személyes adatok kezelése

Az Alpiq ügyfeleinek és munkavállalóinak személyes adatait csak a szerződésben meghatározott célra és mértékben szabad felhasználni. A GDPR előírásainak megfelelően kell eljárni minden adatkezelési tevékenység során.

Kötelező intézkedések:

- Személyes adatokat csak titkosított formában szabad tárolni és továbbítani;
- Az adatokhoz való hozzáférést a minimálisan szükséges személyi körre kell korlátozni;
- Minden adatkezelési műveletet dokumentálni kell;
- Adatvédelmi incidens esetén 24 órán belül értesíteni kell az Alpiq helyi adatvédelmi felelősét.

2.2 Üzleti adatok védelme

Az Alpiq üzleti adatait szigorúan bizalmasan kell kezelni. Ezeket az információkat – előzetes írásos felhatalmazás hiányában - tilos harmadik féllel megosztani, és csak a szerződésben meghatározott feladatok elvégzéséhez szabad felhasználni.

Tiltott tevékenységek:

- Üzleti adatokból másolat készítése személyes célra;
- Információk továbbítása versenytársaknak;
- Adatok felhasználása saját üzleti előnyök szerzésére;
- Megfelelő védelem nélküli, nyilvános helyen történő adatkezelés.

3. INFORMATIKAI BIZTONSÁGI KÖVETELMÉNYEK

3.1 Hozzáférés-kezelés

AZ Alpiq informatikai rendszereihez való hozzáférés csak előzetesen jóváhagyott felhasználói fiókokkal lehetséges, melyhez minden felhasználónak egyedi azonosítóval és erős jelszóval kell rendelkeznie.

Jelszókövetelmények:

- Minimum 12 karakter hosszúság;
- Nagybetűk, kisbetűk, számok és speciális karakterek használata;
- 90 naponta kötelező jelszóváltoztatás;
- Korábbi jelszavak újra felhasználása nem megengedett.

A felhasználói fiókokat tilos megosztani más személyekkel. Az Alpiq minden hozzáférési eseményt naplóz, és rendszeresen, célhoz kötötten ellenőriz.

3.2 Eszközbiztonsági előírások

Az Alpiq IT vagy OT hálózatához csatlakoztatott eszközöknek meg kell felelniük az üzemeltető által támasztott biztonsági követelményeknek:

Kötelező biztonsági szoftverek:

- Naprakész vírusvédelem telepítése és működtetése;
- Operációs rendszer biztonsági frissítéseinek rendszeres telepítése;
- Személyi tűzfal aktiválása és megfelelő konfigurálása;
- Adattitkosítás alkalmazása érzékeny információk esetén.

Tiltott tevékenységek:

- Ismeretlen vagy illegális forrásból származó szoftverek telepítése;
- Adathordozót tartalmazó eszközök (pl. pendrive, mobiltelefon engedély nélküli csatlakoztatása és használata;
- Nem engedélyezett hálózatokhoz való csatlakozás.

3.3 Távoli hozzáférés biztonsága

Az Alpiq IT vagy OT rendszereihez való távoli hozzáférés csak biztonságos, megbízó részéről elfogadott VPN vagy egyéb titkosított, távoli munkavégzést lehetővé tévő kapcsolaton keresztül engedélyezett. A távoli munkavégzés során fokozott figyelmet kell fordítani a környezeti biztonságra.

Távoli munkavégzés szabályai röviden:

- Csak zárt (bridge-mód kizárva), ellenőrzött, napra készen tartott környezetben szabad kapcsolódást kezdeményezni és dolgozni;
- A képernyőt védeni kell az illetéktelen betekintéstől;
- Nyilvános Wi-Fi hálózatok használata nem engedélyezett.

4. FIZIKAI BIZTONSÁGI INTÉZKEDÉSEK

4.1 Telephelyi hozzáférés

Az Alpiq telephelyeire való belépés csak előzetesen regisztrált és jóváhagyott személyek számára engedélyezett. Minden látogatót kísérni kell, és látogatói kártyát kell viselnie.

Belépési szabályok:

- Előzetes bejelentkezés kötelező;
- A belépési engedély kiállítása előtt személyazonosság igazolása szükséges;
- Kísérő személyt a fogadó fél biztosít;
- Biztonsági vagy üzemi területekre való belépés külön engedélyhez és védőfelszereléshez kötött.

4.2 Dokumentumok kezelése

A papír alapú dokumentumokat a bizalmasság, sértetlenség és rendelkezésre állás alapvető szabályainak megfelelően kell kezelni és tárolni. Bizalmas dokumentumokat, adathordozókat nem szabad felügyelet nélkül hagyni.

Dokumentumkezelési szabályok:

- Bizalmas dokumentumok illetéktelenek elől elzártan tárolandók;
- Fizikai vagy elektronikus másolat készítése az adatgazda engedélyéhez kötött;
- A selejtezést helyreállíthatatlanságot biztosító iratmegsemmisítővel kell elvégezni;
- Bizalmas információt tartalmazó dokumentumok szállítása zárt borítékban, irathordozóban lehetséges.

5. KOMMUNIKÁCIÓBIZTONSÁGI ELŐÍRÁSOK

5.1 E-mail biztonság

Az elektronikus levelezés során fokozott figyelmet kell fordítani az üzleti információk védelmére. Bizalmas információkat csak titkosított e-mailben szabad küldeni.

E-mail biztonsági szabályok:

- Gyanúsnak ítélt mellékletek megnyitása tilos;
- Bizalmas információk titkosítása (pl. PGP titkosítással vagy jelszavazott zip fájlban) kötelező;
- Személyes e-mail címek használata üzleti együttműködés céljából nem támogatott.

5.2 Közösségi média használata

Az Alpiq-kal kapcsolatos üzleti vagy belső információk közösségi médiában történő megosztása szigorúan tilos. Ez vonatkozik a projektek részleteire, munkatársakra és üzleti folyamatokra egyaránt.

6. INCIDENSKEZELÉSI KÖTELEZETTSÉGEK

6.1 Biztonsági események bejelentése

Minden biztonsági incidenst vagy gyanús tevékenységet haladéktalanul be kell jelenteni az Alpiq információbiztonsági felelősének az ibf.hun@alpiq.com címen.

Bejelentendő események:

- Megbízó adatvagyonát érintő adatvesztés vagy adatszivárgás;
- Jogosulatlan hozzáférési kísérletek a megbízó vagy a megbízott adatvagyonához;
- Vírusfertőzés vagy rosszindulatú szoftver észlelése abban a munkakörnyezetben, amely közvetve vagy közvetlenül kapcsolatba kerülhet az Alpiq IT vagy OT infrastruktúrájával;
- Fizikai biztonsági események (pl. jogosulatlan belépés, természeti kár);
- Eszközök elvesztése vagy ellopása.

6.2 Együttműködési kötelezettség

Biztonsági incidens esetén a külső partnereknek teljes mértékben együtt kell működniük az Alpiq vizsgálatában. Ez magában foglalja a szükséges információk szolgáltatását és a helyreállítási munkálatok támogatását.

7. MEGFELELŐSÉG ÉS ELLENŐRZÉS

7.1 Auditálási jogok

Az Alpiq fenntartja a jogot, hogy ellenőrizze a külső partnerek információbiztonsági megfelelőségét. Ez magában foglalja az előre egyeztetett tartalmú helyszíni auditokat és a bizonyítékként benyújtott dokumentációk felülvizsgálatát.

7.2 Szerződésszegés következményei

Az információbiztonsági követelmények bizonyított megsértése súlyos szerződésszegésnek minősül, amely a szerződés azonnali felmondását és kártérítési igényt vonhat maga után.

8. KÉPZÉSI ÉS TUDATOSSÁGI KÖVETELMÉNYEK

8.1 Kötelező képzések

Minden külső partner munkatársának el kell végeznie az Alpiq információbiztonsági (e-learning) alapképzését a munkavégzés megkezdése előtt. A jelen dokumentum tartalmának elsajátítását és egy ellenőrző kérdéssor sikeres megválaszolását magába foglaló képzést évente meg kell ismételni.

9. TECHNOLÓGIAI KÖVETELMÉNYEK

9.1 Szoftverhasználat

Csak jogtiszta és biztonsági szempontból átvizsgált szoftvereket szabad használni az Alpiq projektjein. A szoftverek biztonsági frissítéseit rendszeresen telepíteni kell.

9.2 Adatmentés és helyreállítás

A kritikus adatokról rendszeres biztonsági mentést kell készíteni. A mentési eljárásokat tesztelni kell, és a helyreállítási terveket naprakészen kell tartani az adatvesztés kockázatának minimalizálása érdekében.

10. SZERZŐDÉS MEGSZŰNÉSE

10.1 Adatok visszaszolgáltatása

A szerződés megszűnésekor minden Alpiq tulajdonába tartozó adatot, információt és dokumentumot vissza kell szolgáltatni a megbízónak vagy a megbízóval közös döntés alapján helyreállíthatatlanul meg kell semmisíteni azt.

10.2 Hozzáférések megszüntetése

Minden informatikai hozzáférést haladéktalanul meg kell szüntetni a szerződés lejártakor vagy felmondásakor.

Ez az útmutató az Alpiq Magyarország vállalatcsoport információbiztonsági szabályzatának kivonata. A benne foglalt követelmények betartása minden külső partner számára kötelező. Kérdések esetén forduljon az Alpiq információbiztonsági felelőséhez az ibf.hun@alpiq.com elektronikus levelezési címen.

Hatálybalépés: a szerződés aláírásának napja.

Felülvizsgálat: évente vagy jelentős változás esetén.