SZTÁ14 BIZIG
INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT
kivonata

1. A SZABÁLYZAT CÉLJA

MVM Mátra Energia Zrt. (székhely: 3271 Visonta Erőmű út 11. továbbiakban: Társaság) területén a munkát végző szerződéses partner társaságok munkavállalói, megismerjék az információbiztonságra vonatkozó előírásokat.

2. A SZABÁLYZAT HATÁLYA

2.1. Területi hatály

A Munkavédelmi szabályzat területi hatálya az MVM Mátra Energia Zrt. (továbbiakban: társaság) minden olyan területére (telephelyek, külső létesítmények, bányászati területek) kiterjed, amelyekben szervezett munkavégzés zajlik.

2.2. Személyi hatály

A Szabályzat személyi hatálya kiterjed:

- a Társaság valamennyi szervezeti egységére és munkavállalójára, akik informatikai és/vagy telekommunikációs eszközt használnak;
- a Társaság által igénybe vett
    - ügyviteli informatikai (IT) rendszerekkel, szolgáltatásokkal, valamint
    - technológiai folyamatirányító (OT) rendszerekkel összefüggésben
- a Társasággal szerződéses jogviszonyba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (a továbbiakban: külső személy), a velük kötött szerződésben, illetve a titoktartási nyilatkozatban rögzített mértékben;
- a Társaság által igénybe vett IT rendszereket használó, a rendszerekhez és alkalmazásokhoz bármilyen hozzáféréssel rendelkező természetes vagy jogi személyre, a velük kötött szerződésben, illetve a titoktartási nyilatkozatban rögzített mértékben.
- Jelen Kivonatot, illetve annak kivonatát minden a Társasággal munkavégzésre irányuló jogviszonyban álló jogi és természetes személynek meg kell ismernie.

2.3. Tárgyi hatály

A Kivonat tárgyi hatálya általánosan kiterjed

- a Társaság által használt valamennyi informatikai rendszerre (hardver, szoftver, hálózati elem) és informatikai szolgáltatásra, amely kezeli, azaz rögzíti, tárolja, feldolgozza, eléri, továbbítja, illetve felügyeli, ellenőrzi a Társaságnál keletkező, illetve felhasznált adatokat, információkat;
- az ezen informatikai rendszerek és szolgáltatások által kezelt adatokra és információkra;

azok teljes életciklusa (tervezés, fejlesztés, beszerzés, bevezetés, üzemeltetés, kivonás) alatt.

A Kivonat tárgyi hatálya alá tartozó eszközrendszerek:

2.3.1. Ügyviteli informatikai eszközök (IT)

A Kivonat tárgyi hatóköre az alábbiakba felsorolt ügyviteli informatikai eszközökre terjed ki. Az ügyviteli az informatikai rendszereket az IT Szolgáltató üzemelteti.

A hatókörbe tartozó Ügyviteli informatikai eszközök:

- munkaállomások,
- szerverek,
- hálózati eszközök,
- multifunkciós másoló-nyomtatók-szkennerek, nyomtatók,
- egyéb IT eszközök,
- okoseszközök (okostelefonok, tabletek, PDA-k stb.),
- külső hordozható adattároló eszközök.

2.3.2. Technológiai informatikai eszközök (OT)

A Kivonat hatókörébe tartozik minden technológiai informatikai, számítástechnikai vezérlés és szabályozástechnikai eszköz (OT) amelyek a Társaság technológiai folyamatait vezérlik, szabályozzák, monitorozzák, naplózzák és amelyek az elkülönített technológiai hálózathoz csatlakoznak. (speciális a technológiai rendszer részét képező eszközök, PLC-k, adatgyűjtők, munkaállomások, szerverek, nyomtatók).

Az OT eszközöknek ügyviteli hálózati kapcsolata nincs, vagy erősen korlátozott. Az OT eszközök Társaság tulajdonát képezik és saját szervezeti egységek általi üzemeltetésében vannak:

- Erőmű Folyamatirányítási Osztály (EFO - Visonta Erőmű)
- Visontai Villamos Üzemeltetési és Karbantartó Osztály (VVKO - Visonta Bánya)
- Bükkábrányi Villamos Üzemeltetési és Karbantartó Osztály (BVKO - Bükkábrány Bánya)

Ezen eszközök információbiztonsági, IT biztonsági szempontú kockázatelemzése és kockázatarányos védelmének biztosítása a Társaság IT Biztonsági Szakterületének feladata és felelőssége az

- Erőmű Folyamatirányítási Osztály (EFO – Visonta Erőmű),
- Visontai Villamos Üzemeltetési és Karbantartó Osztály (VVKO – Visonta Bánya)
- Bükkábrányi Villamos Üzemeltetési és Karbantartó Osztály (BVKO - Bükkábrány Bánya)

együttműködési és támogatási kötelezettsége mellett.

A technológiai informatikai rendszerekre, ahol külön nem kerül jelölésre, ugyanazon biztonsági elvárások vonatkoznak, mint az ügyviteli eszközökre.

Technológiai informatikai eszközöknél a fentieken túli külön általános előírás, hogy:

- a rendszer csak akkor kapcsolódhat megfelelő tűzfalas védelem kialakítása mellett az Internetre, amennyiben a rendszer működésének ez közvetlen célja, vagy a működéséhez elengedhetetlenül szükséges. Ebben az esetben a csatlakozás módját és szabályait a rendszerhez kapcsolódó rendszerdokumentációban rögzíteni kell.
- nem helyezhetők el a Társaság, illetve az üzemeltetést/támogatást ellátó Társaság telephelyein kívüli, nem a rendeltetésszerű működést célzó helyszínen (pl. lakásban),
- nem menedzselhetőek nem a Társaság, vagy a szerződéses partner tulajdonában álló eszközről,
- csak vállalati, dedikált adathordozók, illetve előzetesen jóváhagyott és engedélyezett eszközök csatlakoztathatóak hozzájuk,
- sérülékenység vizsgálatot kell végrehajtani rajtuk a KIE-17 előírásainak megfelelően.

Az OT rendszerek speciális biztonsági előírásait a Társaságra vonatkozóan a ***SZTÁ 2.1 EIG Technológiai irányítástechnikai és dokumentációs rendszerek biztonsági előírása*** szabályzat tartalmazza.

2.4. Területi hatály

Az Kivonat területi hatálya kiterjed minden olyan helyszínre, telephelyre, amely a Társaság, vagy a Tásaság tag- és leányvállalatai irányítása alá tartozik.

2.5. Időbeli hatály

Jelen kivonat kiadásának napjától a hatályon kívül helyezésig hatályos és alkalmazandó. Jelen szabályzat mellékletei és formanyomtatványai a szabályzat egységes, elválaszthatatlan részét képezik.

3. A FIZIKAI BELÉPÉS SZABÁLYAI

Az informatikai eszközöket tároló helyiségekbe való belépésre csak abban az esetben adható felhatalmazás, ha az adott személynek arra:

- munkaköri kötelességének, feladatának ellátásához,
- külső személy esetén a Társasággal szembeni szerződéses kötelezettség teljesítéséhez szüksége van.

A külső felek beléptetését a Társaság területére a portaszolgálat végzi az ***SZTÁ12 BIZIG Vagyonvédelmi szabályzat*** előírásai alapján. A külső felek belépése esetén biztosítani kell, hogy a látogatók csak kísérettel tartózkodhassanak a Társaság területén. Kivétel biztonsági igazgatói engedélye alapján adható.

3.1. Nyilvános területek (T1)

A Társaság mindazon területei, helyiségei, amelyek látogatók számára nyilvánosak, ugyanakkor a Társaság szempontjából magánterületnek minősülnek. Ilyen a recepció és az ügyfélváró, továbbá a vendég mellékhelyiség.

3.2. Irodai terület kategória (T2)

Csak a társaság munkavállalói, **harmadik fél (külső partnerek) – külön engedély alapján –** belépésre jogosult munkavállalói, illetve vendégek csak kísérettel léphetnek be. Ilyen a nyílt irodai tér, a tárgyalók és projektszoba helyiségek.

3.3. Fokozottan védett kategória (T3)

Fokozottan védett helyiségnek kell tekinteni azokat a helyiségeket, ahol bizalmas adatok feldolgozására, tárolására alkalmazott kiegészítő informatikai erőforrások találhatók, valamint ide sorolandók a felsővezetői munkaszobák. Az ide tartozó helyiségeket zárható ajtóval kell ellátni. A bejutást ellenőrzött módon kell lehetővé tenni.

Fokozottan védett kategóriába a következő helyiségeket kell sorolni:

- az aktív hálózati elemek elhelyezésére és üzemelésére szolgáló helyiségek, szekrények;
- használaton kívüli, adathordozót tartalmazó IT eszközök tárolására szolgáló helyiségek;
- a vezérigazgató, a vezérigazgató-helyettesek, az igazgatók szobái, valamint a biztonsági terület tevékenysége során keletkező dokumentumok (adathordozók, nyomtatványok stb.) és technikai eszközök tárolására kijelölt helyiség.

3.4. Kiemelten védett kategória (T4)

Kiemelten védett helyiségnek kell tekinteni azokat a helyiségeket, ahol bizalmas adatok feldolgozására, tárolására alkalmazott központi informatikai erőforrások találhatók.

Kiemelten védett (zárt) helyiségekbe csak ellenőrzött módon és csak a feljogosított személyek juthatnak be. A bejutás idejét, célját be kell jelenteni és a bejutás tényét naplózni kell (belépési napló). A bejutás és benntartózkodás során kíséretet kell biztosítani a külső személyek részére. A belépési naplókat rendszeren felül kell vizsgálni, amelynek részletes szabályozása a ***SZTÁ12 BIZIG Vagyonvédelmi szabályzatban*** található.

Ebbe a kategóriába az alábbi helyiségek tartoznak:

- Titkos ügyirat kezelő (TÜK) tároló és betekintő helyiség;

- Vagyonvédelmi és központi kiszolgáló informatikai eszközök elhelyezésére használt helyiség (továbbiakban: szerverszoba, szerverhelyiség).

Informatikai rendszerek fejlesztésére és beszerzésére vonatkozó szabályok

Informatikai rendszerek fejlesztése tekintetében a használt alkalmazásoknak két típusát különböztetjük meg:

- **Belső fejlesztésű** rendszerek: A társaság informatikai szolgáltatója vagy belső szervezete által fejlesztett ügyviteli vagy technológiai alkalmazások.
- **Külső fejlesztésű** rendszerek: Nem a társaság informatikai szolgáltatója, hanem **harmadik fél** által fejlesztett alkalmazások, olyan ügyviteli vagy technológiai informatikai rendszerek vagy rendszerelemek, melyeket a társaság külső szolgáltatótól vesz igénybe, közvetlenül vagy az informatikai szolgáltatón keresztül. Ezen belül három alkategória különböztethető meg:
  - Dedikáltan a társaság számára fejlesztett alkalmazás, melyet más személy vagy vállalat nem használhat.
  - Általános funkciókat ellátó, bárki számára elérhető alkalmazás („dobozos” termék).
  - Felhő alapú szolgáltatás.

A **külső fejlesztésű rendszerek szerződésének** minden esetben kötelezően tartalmaznia kell a telepítési és használati feltételeket, valamint a fejlesztési lehetőségeket, verziókövetést. **Ebben az esetben a fejlesztővel/szállítóval kötött szerződésben kell kitérni az IT biztonsági követelményekre, melyet a Társaság Biztonsági Igazgatóság IT Biztonsági Szakterület ellenőriz.**

A **külső fejlesztésű rendszerek szerződéseinek** minden esetben kötelezően tartalmaznia kell a következőket:

- IT biztonsági előírások és ennek megvalósítási módja (rendszerbiztonsági terv, biztonsági minőségbiztosítás, stb.)
- telepítési és használati feltételek és előírások,
- fejlesztett kód tulajdonjoga és elhelyezése
- fejlesztési lehetőségek,
- verziókövetés.

A fejlesztővel/szállítóval kötendő szerződésnek minden esetben tartalmaznia kell részletes IT biztonsági követelményeket, melyet az IT Biztonsági Szakterület kontrollál az alábbiak szerint:

Mind külső, mind pedig belső új fejlesztési igény egyeztetési folyamatába be kell vonni a Társaság IT Biztonsági Szakterületét (IT Biztonsági Szakértők, Információbiztonsági Felelős) az új rendszerrel vagy fejlesztéssel kapcsolatos kockázatok korai azonosítása és feltárása érdekében.

Az IT Biztonsági Szakterület biztonsági előírásokat és ajánlásokat fogalmaz meg a fejlesztésre vonatkozóan. A biztonsági előírások pontos implementációja kötelező a fejlesztésben, attól eltérni nem lehet.

Külső fejlesztésű rendszerek esetén a beszerzés előírásait kell figyelembe venni, továbbá már a beszerzési kiírásba és eljárásba is be kell vonni a Társaság Biztonsági Igazgatóját, illetve az IT Biztonsági Szakterületet, amely azonosítja az a külső fejlesztéssel járó további IT biztonsági kockázatokat és előírja azok kezelésére vonatkozó kontrollokat.

Az információbiztonsági szempontú véleményezésnek, biztonsági követelmény előírásoknak és a jóváhagyásnak minden esetben dokumentált módon kell megtörténnie.

A Fejlesztési Terveknek és a kapcsolódó dokumentációknak minden esetben tartalmaznia kell a fejlesztésre vonatkozó IT biztonsági követelményeket, előírásokat, ajánlásokat (pl. rendszerbiztonsági fejezet a rendszertervekben, vagy külön rendszerbiztonsági terv, vagy ezeknek megfelelő szakmai tartalmú fejlesztési dokumentációs elem)

- mind a fejlesztett termék/alkalmazás biztonsági relevanciával bíró funkcionalitásaira,
- mind pedig a fejlesztési és az üzemeltetési környezet biztonsági előírásaira vonatkozóan.

A fejlesztőknek a biztonsági funkciókat a Fejlesztési Terv IT biztonsági előírásainak megfelelően kell megvalósítaniuk. Ezek megfelelő megvalósítását (kódolását, implementációját) az IT Biztonsági Szakterület, vagy az általa megbízott külső szakértő, IT biztonság szempontból ellenőrizheti, minőségbiztosíthatja.

A vonatkozó előírásokat részletesen a Társaság Információbiztonsági Szabályzatának (SZTÁ14 BIZIG Információbiztonsági szabályzat) 6.12.1.3. Fejlesztési folyamatok biztonsági előírásai (A14.2.5.) fejezete tartalmazza.

4. KÜLSŐ KÖZREMŰKÖDŐK, HARMADIK FÉL HOZZÁFÉRÉSE

Dokumentumok, adathordozók, felhasználói azonosítók átadása és visszavétele, valamint a Társaság informatikai hálózatához, annak részeihez, vagy meghatározott alkalmazásokhoz való hozzáférés csak az alábbiakban leírt zárt folyamatban, dokumentáltan történhet.

Az információbiztonsági szabályozás szempontjából külső közreműködőnek, harmadik félnek tekintendő minden olyan külső szervezet, szerződéses partner, akinek tevékenysége indokolttá teszi az MVM Csoport bármely Társaságának csoportszintű belső használatú vagy annál magasabb minősítésű adataihoz, vagy bármely informatikai rendszeréhez történő hozzáférést. Ilyen módon külső közreműködőnek minősülnek az MVM Csoport Társaságainak alvállalkozói, szerződéses partnerei, valamint az MVM Csoportba nem tartozó Társaságok, a hatóságok, a média, továbbá Társasági belső használatú vagy annál magasabb minősítésű adatok esetén az MVM Csoport többi Társasága is külső közreműködőnek tekintendő.

A Társaság nevében külső szervezetek, hatóságok, sajtó, vagy bármely egyéb szereplő irányába információt, adatot kiadni csak a jelen fejezetben meghatározott csatornákon keresztül, a meghatározott formában, személyes felhatalmazás és megfelelő engedélyezés alapján, az érintett információ, adat érzékenységének figyelembevétele után szabad (lásd ***4.2 Adatok átadása harmadik félnek*** fejezet).

4.1. Külső felek közreműködésével kapcsolatos általános szabályok

Csoportszintű belső használatú vagy annál magasabb minősítésű adatot külső félnek továbbítani, vagy ahhoz hozzáférést biztosítani csak jogszabályi kötelezettség, szerződéses kapcsolat vagy a Társaság szakterületi igazgatóinak meghatalmazása alapján lehet, kizárólag az adott feladattal összefüggésben, az ahhoz szükséges mértékben, formában és tartalommal, az adott jogviszonyban meghatározott időtartamra.

4.1.1. Külső közreműködő bevonásának feltételei

A külső közreműködő jogosultságáról, illetve az adatok, információk kezeléséhez szükséges feltételek rendelkezésre állásáról

- érvényes és hatályos szerződés,
- azonosított és jogosult fogadó személy,
- aláírt személyes titoktartási nyilatkozat

az adattovábbítás/átadás/betekintés lehetővé tétele előtt meg kell győződni, szükség esetén az érintett adatgazda bevonásával.

A jogszabályi előíráson alapuló rendszeres vagy eseti adatszolgáltatások esetén, mindig meg kell győződni az adatközlés jogalapjáról, kétség esetén jogi szakértő közreműködését kell kérni. Adatot átadni, továbbítani csak abban az esetben lehet, ha annak jogalapja egyértelmű, célja, és az adattovábbítás címzettjének személye pontosan meghatározott.

4.1.2. Szerződésben szabályozandó alapkövetelmények

Szerződéses partnerek esetében (a továbbiakban ide értendőek a Társasági első számú vezető általi meghatalmazással rendelkezők) a szerződésnek tartalmaznia kell:

- a szerződéses jogviszony alatt fennálló információbiztonsági követelményeket,
- titoktartási megállapodást,
- valamint indokolt esetben egyéb információbiztonsági nyilatkozatot.

A szerződésben, vagy az abban előírt formában és dokumentációban nevesíteni kell minden külső személyt, aki a Társaság adataihoz, információihoz, információs vagy informatikai rendszereihez hozzáfér. A titoktartási kötelezettséget és információbiztonsági szabályokat a külső szervezetnek rájuk is ki kell terjesztenie vagy saját munkaszerződésében, vagy egyedi nyilatkozatok aláírásával. Az információbiztonsági követelmények megismeréséről és betartásáról mind szervezeti szinten, mind magánszemélyként nyilatkozni kell.

4.1.3. Szerződésben szabályozandó információbiztonsági követelmények

A szerződés vagy megállapodás információbiztonsági követelményeinek tartalmaznia kell a következőket:

- Információk bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzési követelményei.
- Külső szereplőkre vonatkozó általános információbiztonsági előírások.
- Elektronikus levelezés, fájlok titkosításának szabályai.
- Papír alapú dokumentumok kezelésének információbiztonsági szabályai,
- Amennyiben értelmezhető, látogatókra vonatkozó fizikai biztonsági szabályokat.
- Amennyiben értelmezhető, hozzáférés módja a belső IT- és információs rendszerekhez, a hozzáférés szabályai és a felhasználók felelősségei.
- Amennyiben értelmezhető, dokumentumok és adathordozók átadásának, cseréjének és kezelésének információbiztonsági követelményei és a kapcsolódó felhasználói felelősségek.
- Társaság információbiztonsági ellenőrzésének lehetőségei és feltételei.
- Szerződésben foglalt információbiztonsági követelmények megszegéséből származó szankciók.
- Szerződés megszűnésekor vagy lejártakor az információk és átadott információhordozók visszaadásának, a szerződéses partner adathordozóján lévő információk megsemmisítésének követelményei.

4.1.4. Külső közreműködők személyi változásainak kezelése

A szerződésben ki kell térni a külső közreműködőnél történő személyi változások kezelésére, illetve haladéktalan bejelentésére. Rögzíteni kell továbbá az egyéb alvállalkozók bevonására vonatkozó információbiztonsági szabályokat, ez esetben a fővállalkozó felel az alvállalkozó tevékenységéért információbiztonsági szempontból is.

A szerződés/megállapodás titoktartási nyilatkozatával kapcsolatos előírások a következők:

- Az együttműködés, a beszerzési eljárás és a szerződés előkészítése során már az első nem nyilvános információ átadása előtt a külső partner bevont képviselőivel egyoldalú, előzetes titoktartási nyilatkozatot kell aláírattatni a szerződés megkötése előtt átadott adatokra vonatkozóan is.

- A titoktartási nyilatkozatokat szervezet és magánszemély szintjén egyaránt alá kell íratni.
- A szerződésben kötelezően elő kell írni, hogy a külső fél minden munkavállalóját, érintett szerződéses partnerét, alvállalkozóját titoktartásra kötelezze a legalább a szerződésben előírt hatókörben.

Az információbiztonsági követelmények Társaság oldali betartásáért a szerződésben nevesített Társasági képviselők felelnek. Az információbiztonsági követelmények betartását a Társaság keretein belül a Társasági a Biztonsági igazgatóság Információbiztonsági területe (Információbiztonsági Felelős/IT biztonsági szakértő) ellenőrzi.

4.2. Adatok átadása harmadik félnek

Adatok átadása harmadik félnek csak az ***4.1. Külső felek közreműködésével kapcsolatos általános szabályok*** fejezetben rögzített feltételek teljesítését követően, a szerződésben meghatározott módon lehetséges.

Papír alapú dokumentumok átadása esetén törekedni kell a személyes átadásra, továbbá a dokumentum továbbításakor, átadásakor meg kell felelni a ***4.1. Külső felek közreműködésével kapcsolatos általános szabályok*** fejezetben, rögzített követelményeknek.

Elektronikus dokumentumok átadásánál a *Hiba! A hivatkozási forrás nem található. Hiba! A hivatkozási forrás nem található.* fejezetben rögzített titkosítási eljárásokat kell követni az elektronikus levelezés során, illetve nagy mennyiségű adat átadása esetén preferálni kell a titkosított adathordozók használatát.

A szerződéses partnernek biztosítana kell saját munkavégzői számára:

- a biztonságtudatos munkavégzés feltételeit,
- továbbá a munkakör ellátásához szükséges, megfelelő biztonsági feltételeket és eszközöket.

Amennyiben a szerződéses partner a rögzített feltételek teljesítését nem tudja biztosítani, vagy az átadott adatok biztonsági minősítése megköveteli, a Társaság a munkavégzés idejére:

- munkaállomást,
- projektszobát,
- VPN hozzáférést,
- biztonságos állománycsere megoldást,
- stb.-t

biztosíthat.

Az adatok biztonságos módon való átadása a Társaság és a szerződött külső fél közös felelőssége. A nem megfelelő adatátadásból származó károkért az érintett természetes és jogi személyek a Társaság és a szerződött partner oldalán egyaránt felelősségre vonhatók a Társaság Információbiztonsági Szabályzatának (SZTÁ14 BIZIG Információbiztonsági szabályzat) ***6.9.4 Fegyelmi eljárás és alkalmazható szankciók (A7.2.3.)*** fejezetében foglaltak szerint.

4.3. Határozott időre szóló belépési jogosultság adása harmadik félnek

Amennyiben a szerződött külső féllel való munka indokolja (pl. projekt, tartós, vagy rendszeres munkavégzés), a külső szereplők számára igényelhető ideiglenes belépőkártya, melynek igénylése és használata során a Társaság Információbiztonsági Szabályzatának (SZTÁ14 BIZIG Információbiztonsági szabályzat) ***6.11 Fizikai biztonság (A11., A11.1.4.)*** fejezete előírásait kell figyelembe venni. Az ideiglenes belépőkártya engedélyezéséről a projekt vezetője és a Biztonsági Igazgató dönt.

4.4. Külső szereplők IT rendszerekhez való hozzáférése

Külső szereplőknek adott felhasználói azonosítókról naprakész nyilvántartást kell vezetni, valamint gondoskodni kell ezek folyamatos kontrolljáról, monitorozásáról és naplózásáról. A nyilvántartás vezetése a Társaság Információbiztonsági területének feladata.

4.4.1. Külső szereplők IT rendszerekhez való hozzáférési jogosultságai

Nem az informatikai szolgáltatók által biztosított számítógépek az MVMH hálózatra nem csatlakoztathatók, így a külső partner által hozott, az ő tulajdonát képező számítógép sem. Ezen eszközök esetében előzetes egyeztetés alapján vendég WiFi hozzáférés kérhető.

Amennyiben a külső félnek átadandó, vagy általa létrehozandó adatok biztonságos megosztása nem lehetséges, vagy azok külső eszközön történő kezelése nem engedélyezett, lehetőség van a külső fél munkatársainak hordozható adattároló, munkaállomás és a szükséges informatikai rendszerekhez jogosultság igénylésére.

A külső partnernek a Társaság informatikai rendszeréhez adott felhasználói azonosítók csak azokhoz az információkhoz és olyan mértékben adhatnak hozzáférést és jogosultsági szintet, amennyi az együttműködés során a munkavégzéshez feltétlen szükséges. Harmadik fél hozzáférési jogosultságáról az adatgazda, valamint a Biztonsági Igazgató/Társasági Információbiztonsági Szakterület dönthet, a Társaság Információbiztonsági Szabályzatának (SZTÁ14 BIZIG Információbiztonsági szabályzat) ***6.7 Jogosultságkezelés (hozzáférés-menedzsment) (A9***.) fejezetében foglaltak szerint. A jogosultság kiadását és a lejárat határidejét írásban kell rögzíteni.

Minden harmadik félnek a hozzáférési jogosultság kiadása előtt meg kell ismernie a Társaság információbiztonsági szabályzatát és írásban nyilatkoznia kell az abban foglaltak elfogadásáról és titoktartási kötelezettség vállalásáról. Titoktartási-, adott esetben egyéb információbiztonsági nyilatkozat meglétének hiányában a szükséges jogosultság nem adható ki.

A harmadik fél hozzáférési jogosultságait csak arra az időtartamra szabad kiadni, amelyre a harmadik fél szerződése vonatkozik, de legkésőbb tárgyév végéig. Amely rendszernél lehetséges, automatikus lejáratot kell beállítani, illetve a szerződés megszűnésével egyidejűleg vissza kell vonni a kiadott jogosultságokat. A jogosultságok határidőjének megfelelő kezelése a szerződésben érintett szervezeti egység vezetőjének felelőssége. A Társaság Információbiztonsági területe ezt saját hatáskörében, rendszeresen, legalább évi egy alkalommal ellenőrzi.

A hozzáférési jogosultság megújításáért a Társaság fogadó szervezeti egysége felel, év végi törlését a Társaság Információbiztonsági területe automatikusan kezdeményezi és az IT hajtja végre.

4.4.2. Külső szereplők IT rendszerekhez való privilegizált jogosultságai

Külső szereplők alapesetben nem szerezhetnek a Társaság számítógépes hálózatán semmilyen privilegizált (pl. adminisztrátori) jogosultságot, kivéve azokban az esetekben, amikor ezt a szerződéses együttműködés jellege (pl. informatikai rendszerüzemeltetés, sérülékenységvizsgálat) megkívánja.

Ilyen esetekben a kiemelt jogosultságokat dokumentálni kell, valamint a törekedni kell a kiemelt jogosultság időbeni és rendszerbeli maximális lehatárolására (csak az a munkavégzés szükséges időtartamára és csak a célrendszerre). Továbbá a szerződésben részletesen szabályozni kell, hogy a külső partner privilegizált jogosultságai mire jogosítanak fel, valamint szabályozandó ezek kontrollja, monitoringja és naplózása.

4.5. Külső szereplőknek való informatikai eszköz átadása

Külső szereplőknek hordozható informatikai eszköz (pl. laptop, USB adattároló) átadás-átvételi folyamatban, írásos dokumentációval adható át, az eszközre vonatkozó elszámolási kötelezettséggel.

A Társaság által biztosított eszközökön, és a Társaság területén a Társasági információbiztonsági szabályzatban rögzített biztonsági előírások betartása kötelező.

Azok az adatok vagy dokumentumok, amelyek szigorúan bizalmas minősítésűek, adathordozón vagy nyomtatott formában sem adhatók ki, még titoktartási nyilatkozat aláírása mellett sem. Ebben az esetben, amennyiben indokolt, a betekintést projektszobán, adatszobán keresztül kell biztosítani.

4.6. Projektszoba, adatszoba

Projektszoba, adatszoba kialakítására abban az esetben van szükség, amennyiben a külső félnek átadandó, vagy általa létrehozandó adatok biztonságos megosztása más módon nem lehetséges, vagy azok külső eszközön történő kezelése nem engedélyezett, vagy a projekt jellegéből, a külső munkatársak létszámából adódóan osztott irodai munkaállomások biztosítása nem elegendő.

A projektszoba lehet fizikai jellegű vagy elektronikus adatszoba.

4.7. Ellenőrzések

Jelen fejezetben rögzített, harmadik félre vonatkozó információbiztonsági előírásokat a Társaság Információbiztonsági területe a jelen szabályzatban foglaltak alapján köteles ellenőrizni.

Harmadik féllel kötött szerződésben

- ki kell kötni az külső szereplőre vonatkozó ellenőrizhetőség kötelezettség vállalását, valamint
- javasolt részletesen leírni az ellenőrzés
    - lehetséges gyakoriságát,
    - a vizsgálat tárgyát, illetve
    - a vizsgálat módját.

Az szerződésben foglalt információbiztonsági követelményektől való eltérések, nem-megfelelésekre vonatkozóan ki kell kötni ezek kezelési módját és a visszaellenőrzés lehetőségét.

Az ellenőrzésekről jelentést kell készíteni, melyet a harmadik fél képviselője és az adott vállalkozóért felelős terület vezetője felé egyaránt meg kell küldeni. Súlyos, vagy folyamatosan fennálló nem-megfelelés vagy hiányosság azonosítása esetén a Társaság IT Biztonsági Szakterülete, illetve a Biztonsági igazgató tájékoztatja a Társaság felső vezetését, amennyiben ez indokolt.

5. TECHNOLÓGIAI ELŐÍRÁSOK

5.1. Hordozható adattárolók titkosítása

Technológiai rendszerek esetében, amennyiben az adatot a vállalaton belül, vállalaton kívüli helyszínre, vagy külsős félnek szükséges továbbítani, és a továbbítás módja más, ellenőrizhető és biztonságos módon nem megoldható, olyan titkosított hordozható adattároló alkalmazása szükséges, mely a Társasági információbiztonsági felelős által jóváhagyott. Amennyiben a titkosítás megoldása nem lehetséges, vagy biztonsági kockázatot jelent, megfelelő kompenzáló kontrollok bevezetése szükséges.

5.2. Fájltitkosító megoldások használatának szabályai

Ügyviteli rendszerek esetén harmadik felekkel történő fájlcsere esetén az adatok elektronikusan csak titkosított formában, vagy titkosított csatornán adhatók.

Technológiai rendszerek esetében Technológiai (OT) rendszerek esetében törekedni kell az fájlcsere megoldás titkosítására, ahol ezt a technológia rendszer lehetővé teszi.

Ügyviteli rendszerekből történő titkosított adattovábbítás esetén a központilag alkalmazott titkosító megoldás használata kötelező.

5.3. Külső fájlmegosztó alkalmazások használatának szabályai

A külső fájlmegosztó alkalmazások (pl. DropBox, Google Drive, MammutMail) használata munkavégzéssel összefüggő célra, a Társaság IT Biztonsági Szakterületének hozzájárulásával lehetséges.

5.4. Elektronikus levelezés titkosítási előírásai

A bizalmas, érzékeny adatokat, információkat tartalmazó anyagokat minden esetben csak titkosítva lehet elküldeni:

- a levelező rendszer által támogatott, beépített titkosítása protokollok alkalmazásával (S/MIME, PGP stb.), amennyiben ez elérhető, vagy
- a Társaság IT Biztonsági Szakterülete által engedélyezett eljárással és/vagy alkalmazással (7Zip) titkosítva és a levél csatolmányaként elküldve a Kriptográfiai eszközök használata fejezetben foglaltak szerint.

A vonatkozó előírásokat részletesen a Társaság Információbiztonsági Szabályzatának (SZTÁ14 BIZIG Információbiztonsági szabályzat) ***6.17.3. Alkalmazott kriptográfiai eszközök, megoldások*** fejezete tartalmazza.

6. INCIDENSKEZELÉSI ELŐÍRÁSOK

A Társaság minden munkavégzőjének saját vállalójának és külső partner munkavégzőnek kötelessége az általa észlelt információbiztonsági incidenst, vagy annak gyanúját bejelenteni az IT Biztonsági Szakterületnek az

- itb@mert.hu email címen,
- telefonon a +36 30 624-0964 telefonszámon, vagy
- személyesen a Biztonsági Igazgatóságon belül működő IT Biztonsági Szakterületnek, látogatóközpont melletti épület 2. emelet.