Szerepkör	Név	Pozíció	Aláírás
Folyamatszponzor:	Balogh Szabolcs, Orgovány Ferenc	ügyvezető	Balogh Szabolcs sk., Orgovány Ferenc sk.
Folyamatgazda:	Binder Tamás	IT technológiai vezető	Binder Tamás sk.
Ellenőrizte:	Dr. Bognár Csilla	senior jogtanácsos	Dr. Bognár Csilla sk.
Ellenőrizte:	Zubreczki András	junior projektmenedzsment szakértő	Zubreczki András sk.

MOB-BSz-17

AZ MVM MOBILITI KFT.
INFORMÁCIÓBIZTONSÁGI ÉS RENDKÍVÜLI HELYZETKEZELÉSI BELSŐ SZABÁLYZATA

Balogh Szabolcs
hatályba helyező és jóváhagyó sk.
ügyvezető

Orgovány Ferenc
hatályba helyező és jóváhagyó sk.
ügyvezető

Tartalom

1. Cél

Az MVM Mobiliti Kft. (a továbbiakban: Társaság) Információbiztonsági és rendkívüli helyzetkezelési belső szabályzatának (a továbbiakban: Szabályzat) célja a KIE-17 Az MVM Csoport információbiztonsági és rendkívüli helyzetkezelési központi irányelv leképezése mellett a Társaságra vonatkozó sajátosságok rögzítése, a kapcsolódó szereplők és feladataik azonosítása, meghatározása, egyedi szabályok dokumentálása, valamint specifikus információbiztonsági feladatok meghatározásával az információbiztonsági kultúra erősítése.

2. A szabályzat hatálya

2.1. Időbeli hatály

A Szabályzat a Társaság ügyvezetése által történő hatályba helyezés napjától a hatályon kívül helyezés napjáig alkalmazandó.

2.2. Személyi hatály

Jelen Szabályzat személyi hatálya kiterjed a Társaság valamennyi szervezeti egységére és munkavállalójára.

Jelen Szabályzat kötelező érvényű előírásokat fogalmaz meg azon külső felek – beleértve az MVM Csoport tagvállalatainak munkavállalóit, kiszervezett tevékenységet ellátó szerződéses partnerek, alvállalkozók irányában is, – akik a Társaság adataihoz és informatikai erőforrásaihoz hozzáférnek.

Jelen Szabályzatot ismertetni kell minden, a személyi hatálya alá tartozó féllel, a szabályzatban foglaltak megismeréséről és betartásáról az érintett feleknek írásban nyilatkoznia kell.

2.3. Tárgyi hatály

Jelen Szabályzat tárgyi hatálya a Társaság valamennyi működési folyamatának és tevékenységének információbiztonsággal, valamint rendkívüli helyzetkezeléssel kapcsolatos aspektusára vonatkozik.

A Szabályzat tárgyi hatálya kiterjed továbbá

- minden meglévő, és a jövőben használandó, a Társaság saját tulajdonában álló és bérelt – külső fél, illetve a belső informatikai szolgáltató által biztosított – informatikai erőforrásra (hardver és szoftver eszközök, valamint azok dokumentációja egyaránt),
- a Társaság által kezelt papír alapú és elektronikus adatok teljes körére, és az azok felhasználására vonatkozó utasításokra, valamint
- a Társaság folyamataihoz kapcsolódó dokumentációk összességére.

3. Hivatkozások

A jelen Szabályzathoz tartozó hivatkozások a MOB-BSz-17-M-01 mellékletben találhatóak.

4. Meghatározások

A jelen Szabályzathoz tartozó meghatározások a KIE-17-M-01 valamint a MOB-BSz-17-M-02 mellékletben találhatóak. Esetleges ellentmondás esetén a KIE-17-M-01 fogalmi meghatározása az irányadó.

5. A szabályzat tartalma

5.1. Az információbiztonsági rendszer

Jelen Szabályzat tartalma alapján egységes rendszerbe foglalja a Társaság információbiztonsági rendszer tevékenységeit, feladatait, továbbá kialakítja az ilyen irányú tevékenységeinek monitoring és koordinatív funkcióját, képessé téve így a Társaságot, az információbiztonságot és

üzletmenet folytonosságot fenyegető veszélyekkel szembeni szervezett védekezésre, amelynek megvalósításához a Csoport biztonsági és informatikai szolgáltatója nyújt műszaki támogatást.

5.1.1. Az információbiztonsági rendszer célja és kialakítása

A Társaság információbiztonsági rendszert köteles működtetni, melynek célja a használt információk és információs rendszerek azonosítása, azok információbiztonsági kockázatainak felmérése, kockázatarányos védelmi intézkedések bevezetése és folyamatok kialakítása, valamint azok hatékony menedzsmentje. A kialakítás és működtetés folyamatát a MOB-BSz-17-FU-01 folyamatutasítás tartalmazza. Az információbiztonsági rendszer kialakítása és működtetése folyamat során meghozandó döntések:

- Döntés a kockázatkezelési módszertanon alapuló kockázatkezelési feladatok végrehajtása kapcsán a nem a módszertanban meghatározott támogató IT eszköz, azaz más szoftveres támogatás igénybevételéről (D-01)
- Döntés a kockázatok kezeléséről, javasolt védelmi intézkedések bevezetéséről, alkalmazásáról (D-02)
- Döntés a védelmi intézkedések bevezetésének ütemtervéről (D-03)

Az információbiztonsági rendszer működtetése a Társaságnál az alábbiak miatt indokolt:

- adatok, információk és támogató információs rendszerek azonosítása, kritikusságuk felmérése,
- az azonosított információk és rendszerek bizalmasságát, sértetlenségét, valamint rendelkezésre állását befolyásoló tényezők, kockázatok felmérése,
- kockázatok kezelése, kockázatarányos és költséghatékony védelem kialakítása és folyamatos fenntartása,
- információbiztonsági tudatosság fokozása
- vezetőség elkötelezettségének erősítése az információbiztonság irányában,
- folyamatos visszamérés, fejlesztés, oktatás biztosítása,
- incidensek kezelésének és kivizsgálásának hatékonyabbá tétele,
- az üzletfolytonosság menedzsment és rendkívüli helyzetkezelés támogatása,
- a vonatkozó jogszabályi kötelezettségeknek való megfelelés biztosítása.

5.1.2. Az információbiztonsági rendszer szabályzati környezete

Az információbiztonsági rendszer működtetésének alapja a megfelelően kialakított szabályozási környezet. A Társaságon belül az információbiztonság egységes és egyenszilárdságú kezelése érdekében jelen Szabályzat információbiztonsági előírásai kötelezően betartandó követelményeket jelentenek.

Az információbiztonsági rendszer működtetése során az alábbi dokumentumokkal szükséges rendelkezni:

- Információbiztonsági Politika – MOB-BSz-17-M-03 melléklet
- Információbiztonsági Stratégia – MOB-BSz-17-M-04 melléklet
- Informatikai biztonsági szabályzat (IBSZ) – jelen Szabályzat
- Kapcsolódó folyamatutasítások

Dokumentumok felülvizsgálata

A Társaságnál keletkezett, az információbiztonsági rendszer működtetésével kapcsolatos dokumentumokat szükséges éves gyakorisággal felülvizsgálni a társasági információbiztonsági felelős kezdeményezésével.

5.2. Társaság besorolása információbiztonsági kategóriákba

A Társaságot információbiztonsági szempontból a KIE-17-NY-01 Társasági besoroló kérdőív segítségével információbiztonsági kategóriákba kell sorolni, melyet évente felül kell vizsgálni. Az MVM Zrt. Csoportszintű Biztonsági Igazgatósága a besoroló táblázat alapján értesíti a Társaságot a kapott besorolási szintjéről, mely alapján a Társaságnak a saját kategóriájának megfelelő információbiztonsági intézkedéseket kell megvalósítania jelen Szabályzatban rögzítettek szerint.

5.3. Az információbiztonság és rendkívüli helyzetkezelés szervezete

Az információbiztonsági és rendkívüli helyzetkezelési követelmények teljesítéséhez, az előírt kontrollok megvalósításához és karbantartásához elengedhetetlen a szereplők mind csoportszinten, mind társasági szinten történő kijelölése, feladataik és felelősségük meghatározása. Az alábbiakban mindkét szinten bemutatjuk a szereplőket.

A társasági információbiztonsági felelős éves munkatervének csoportszintű ajánlását a KIE-17-M-03 Társasági információbiztonsági felelős melléklet tartalmazza.

A Szabályzatban felsorolt valamennyi szerepkörre kijelölt felelősnek rendelkeznie kell helyettessel, aki távolléte, illetve elérhetetlensége esetén a hiányzó személy feladat és hatáskörének megfelelően köteles eljárni.

A kijelölt felelősök munkaköri leírását ki kell egészíteni a betöltött szerepkörükkel kapcsolatos feladatokkal.

5.3.1. Csoportszintű közreműködők

A csoportszintű közreműködőknek a következő speciális, információbiztonsággal és rendkívüli helyzetkezeléssel kapcsolatos szervezetek kialakítása vagy megfeleltetése szükséges a kapcsolódó felelősségek és feladatok rögzítésével.

- REVIR Központi Ügyelet
- Rendkívüli Események Figyelőszolgálata
- REVIR tanácsadó
- Csoportszintű Krízis Team
- Csoportszintű Információbiztonsági Fórum

5.3.2. Társasági szintű közreműködők

A Társaság SzMSz-ében rögzíteni kell az információbiztonsággal és rendkívüli helyzetkezeléssel kapcsolatos felelősségeket és feladatokat, továbbá az alábbi szervezeti egységek és pozíciók létrehozását, illetve megfeleltetését, valamint az ezekhez köthető felelősségeket és feladatokat a kapott információbiztonsági besorolás (védelmi igényszint) szerint:

I. Általános védelmi igényszint

Általános védelmi igényszint esetén a következő szerepkörök, szervezetek kialakítása szükséges:

- Társasági információbiztonsági felelős
- Társasági üzletfolytonossági felelős
- REVIR ügyeletes
- Társasági Krízis Team vagy Krízis Koordinátor
- Folyamatgazdák

- Adatgazdák

II. Emelt védelmi igényszint

Az Általános védelmi igényszinten kívül a következő szerepkörök, szervezetek kialakítása szükséges:

- Társasági információbiztonsági fórum

III. Magas védelmi igényszint

Az Emelt védelmi igényszinten meghatározottakon kívül a következő szerepkörök, szervezetek kialakítása szükséges:

- Önálló biztonsági szakterület

IV. Speciális védelmi igényszint

A Magas védelmi igényszinten meghatározottakon kívül a következő szerepkörök, szervezetek kialakítása szükséges:

- Önálló biztonsági szervezeti egység
- Biztonsági referens

5.3.3. Információbiztonsági felelős és üzletfolytonossági felelős kinevezésének folyamata

A társasági információbiztonsági felelős és a társasági üzletfolytonossági felelős személyének kijelölését a Társaság ügyvezetői hagyják jóvá és megküldi az MVM Zrt. részére a KIE-17 1.6. pontjának 13) bekezdésének megfelelően. (D-04)

5.4. Az információ védelme

Annak érdekében, hogy az információ védelme a Csoporton belül egységes legyen, és a szükséges és elégséges információbiztonsági követelmények, kontrollok meghatározhatók legyenek, a Társaság – a besorolásától függetlenül – a következőket hajtja végre:

- Adatvagyon felmérés
- Adatvagyon elemek és informatikai rendszerek biztonsági osztályba sorolása
- Információbiztonsági kockázatelemzés
- Üzleti hatáselemzés
- Hozzáférés és jogosultság menedzsment folyamatok működtetése

Az információbiztonsági kockázatelemzés és az üzleti hatáselemzés kapcsolata

Az információbiztonsági kockázatelemzésnek és az üzleti hatáselemzésnek egymással szinkronban, a társasági információbiztonsági felelős és a társasági üzletfolytonossági felelős szorosan összehangolt munkájának eredményeképp kell elkészülnie és felülvizsgálatra kerülnie. Az adat rendelkezésre állása örökli a folyamat rendelkezésre állását.

Az információbiztonsági kockázatelemzés részleteiről a MOB-BSz-17-M-05 melléklet tartalmaz leírást.

5.5. Hozzáférés-menedzsment, jogosultság kezelés

A Társaságnak az általa kezelt és tárolt adatok védelme érdekében minden alkalmazott informatikai rendszerükben jogosultságkezelést kell, hogy biztosítson, melyet dokumentált módon szabályozni kell. A szabályozásnak ki kell terjednie mind az ügyviteli, mind a technológiai rendszerekre.

A Társaság által kezelt és tárolt adatokhoz és rendszerekhez kizárólag az ahhoz hozzáférési jogosultsággal rendelkező személyek férhetnek hozzá az adatgazda által meghatározott ideig,

illetve módon (írás-olvasás, csak olvasás, csak írás, törlés). A hozzáférés engedélyezett idejét és módját a jogosultság igénylés-engedélyezés során dokumentáltan rögzíteni kell.

A hozzáférés menedzsment alapelve, hogy minden, hozzáférési jogosultsággal rendelkező személy csak a számára szükséges és elégséges jogosultságokkal rendelkezzen, a felesleges többlet jogosultságok megadását el kell utasítani, illetve a már meglevő, indokolatlan többlet jogosultságokat vissza kell vonni. Ennek érdekében a jogosultságok kiadásának és felülvizsgálatának folyamatába a társasági információbiztonsági felelőst, mint jóváhagyót be kell vonni a MOB-FU-17-02 folyamatutasításban foglaltak szerint. A jogosultságok információbiztonsági kezelése folyamat során meghozandó döntés az eltérő alapjogosultsági igénylésről (D-05), továbbá a jogosultság felfüggesztésének mellőzéséről (D-06) a MOB-BSz-17-M-17 melléklet szerint történik.

5.5.1. Technikai felhasználók kezelése

Amennyiben egy rendszerben személyhez nem köthető technikai felhasználók létrehozása indokolt (pl. automatikusan lefutó task-ok végrehajtására), a fejlesztőnek/üzemeltetőnek a társasági információbiztonsági felelőst tájékoztatnia kell e technikai felhasználók létrehozásáról és tevékenységeiről a létrehozáskor, valamint az érintett adatgazda jóváhagyását kell kérni, amennyiben üzleti adatok is érintettek. A technikai felhasználókról az adatgazdáknak nyilvántartást kell vezetniük. Periodikus aktiválású, időszakos technikai felhasználók létrehozása esetén minden egyes aktiválásról tájékoztatni szükséges a társasági információbiztonsági felelőst.

5.6. Szervezeti és személyi biztonság

Jelen fejezet a humán erőforrással kapcsolatos információbiztonsági előírásokat tartalmazza, valamint azonosítja a más, releváns szabályzatokkal való kapcsolódási pontokat.

5.6.1. Munkatársak beléptetésének információbiztonsági követelményei

Az új munkavállalók beléptetésének első lépése a munkaszerződés aláírása, melyre a Társaság részére humánerőforrás szolgáltatást nyújtó szakterület vonatkozó formanyomtatványát szükséges használni. A munkaszerződés aláírásával a munkavállaló egyben nyilatkozik a munkakörével összefüggésben álló szabályok (így az információbiztonsági relevanciájú szabályzatok) megismeréséről és betartásáról is.

Az újonnan belépő munkavállalók esetén, a munkaszerződésben meghatározottakon túl, az alábbi biztonsági intézkedéseket szükséges elvégezni:

- Új munkavállalók részére a jogosultság igénylést az 5.5 alfejezetben rögzítettek szerint kell végrehajtani.
- A munkakörhöz kapcsolódó, a munkáltató által a munkavállaló rendelkezésére bocsátott eszközökkel kapcsolatban a munkavállalónak – a munka törvénykönyvéről szóló 2012. évi I. törvény rendelkezéseinek megfelelően – tudomásul szükséges vennie, hogy a Társaság által rendelkezésére bocsátott eszközöket csak és kizárólagosan munkavégzés céljára használja. Tudomásul veszi továbbá azt is, hogy amennyiben magánjellegű adatot tárolna a Társaság eszközein, a munkáltató nem vállal felelősséget azok bizalmasságának, sértetlenségének, illetve rendelkezésre állásának megóvására. A leírtakon túlmenően, tudomásul veszi a továbbiakban, hogy részére a Társaság levelező rendszerében igényelt postafiókot kizárólag munkahelyi célokra használhatja. A postafiók adattartalma a Társaság tulajdonának tekintendő, arra a Társaság adatkezelési szabályzása érvényes. A Társaság által biztosított információtechnológiai vagy számítástechnikai eszközök fentiektől eltérő használata munkajogi következményeket vonhat maga után.
- Az új munkavállalónak biztonságtudatossági oktatáson kell részt vennie, melyet a Társasági információbiztonsági felelős aláírásával igazol.
- Munkatársak kiléptetése/átléptetése

- Munkavállaló kiléptetésekor, vagy a Társaságon belüli más szervezeti egységbe történő átléptetésekor a Társaság részére humán erőforrás szolgáltatást nyújtó szakterületnek tájékoztatást kell küldenie a társasági információbiztonsági felelős részére.

Felmondás/közös megegyezéssel történő munkaviszony megszüntetés, az MVM Csoporton belüli elhelyezkedés esetén szükséges:

- a kilépés, leszámolás időpontjának rögzítése,
- rögzíteni mely társaságnál és milyen pozícióban helyezkedik el,
- összeférhetetlenség, valamint az ezáltal jelentett esetleges kockázat mértékének vizsgálata,
- jogosultságok lejáratának beállítása utolsó munkában töltött napra,
- a bejövő leveleket igény esetén az új címre lehetséges átirányítani – kivételt képeznek a kritikus munkakörök, melyek esetén ez nem megengedett, csak amennyiben a munkavállaló felettese ehhez hozzájárul,
- automatikus válaszüzenetet kell beállítani sablon szerint legalább 30 napra, vagy a felhasználó felettese által megjelölt időtartamra, mely tartalmazza, hogy a címzett elérhetetlen, a levél nem kerül automatikusan továbbításra, illetve kinek a részére kell megismételni a levél újra küldését, ennek felelőse a kilépő felhasználó,
- levelek, fájlok archiválása, kritikus munkakörnél vizsgálata, szükség esetén a kilépő felettesének/helyettesének átadása (az archívumhoz a hozzáférést egyedileg igényelni kell, nem automatikus művelet).

Felmondás/közös megegyezéssel történő munkaviszony megszüntetés, az MVM Csoporton kívüli elhelyezkedés esetén, illetve további elhelyezkedés hiányában a fentieken túl a következő speciális előírások érvényesek:

- a bejövő levelek új e-mail címre történő átirányítása nem engedélyezhető, kivéve a kilépő dolgozó önkéntes hozzájárulása alapján,
- az automatikus válaszok beállításán indokolt esetben a társasági információbiztonsági felelős kontrollt gyakorolhat.

A munkáltató általi azonnali felmondás esetén a felmondás MVM Csoporton kívüli elhelyezkedés esetében leírtakon túl a következő speciális előírások érvényesek:

- a munkavállaló felettesének előre jeleznie kell a Társaság részére humán erőforrás szolgáltatást nyújtó szakterület és a társasági információbiztonsági felelőse részére, majd együtt konzultálnak következőkről:
  - felmondás oka,
  - kiléptetés, leszámolás időpontja – jogosultságok azonnali visszavonásának, a Társaság által biztosított eszközök azonnali visszavételének biztosítása céljából,
  - amennyiben az elbocsátott munkavállalót illetően biztonsági incidens gyanúja merül fel, indokolt esetben a közvetlen felettes kérésére például egy forensic vizsgálat kezdeményezhető – erre az MVM BSZK Zrt. tud szolgáltatást adni –, amellyel ellenőrizhető a munkavállaló által használt eszközök adattartalma, amely során a munkavállaló (munkáltató által munkahelyi célra biztosított) postaládájában lévő levelek is megtekinthetők,
- jogosultságok azonnali visszavonása, akár az eszközök fizikai visszavételével.

A munkavállaló Társaságon belüli más szervezeti egységbe történő átléptetése esetén az átadó közvetlen felettes vezető köteles haladéktalanul intézkedni a munkavállalónak az általa addigi munkakörében kezelt üzleti vagy személyes adatokhoz történő hozzáférése megszüntetéséről.

5.6.2. Biztonságtudatossági oktatás

A biztonságtudatossági oktatás célja, hogy a munkatársak értesüljenek a rájuk vonatkozó, központi, illetve a Társaság által előírt szabályozásokról, biztonsági előírásokról, tisztában legyenek azok betartásának szükségességével, tudomást szerezzenek az őket fenyegető lehetséges veszélyekről, támadási technikákról és elhárításukról, észlelésükről.

Biztonságtudatossági oktatást legalább az alábbi esetekben kell szervezni:

- Rendszeresen, évente legalább egy alkalommal ismétlő jelleggel, a Társaság minden munkavállalója részére.
- Eseti jelleggel a következő események bekövetkezése során:
  - Jelen Szabályzat alapján az információbiztonsági szabályzat társasági szinten történő kialakítása, illetve jelentős módosulása esetén minden érintett részére.
  - Új munkavállaló belépésekor az új belépő részére.
  - Incidens bekövetkezését és kivizsgálását követően az érintettek részére, amennyiben a társasági információbiztonsági felelős indokoltnak látja a képzést.

Az oktatások megszervezése (tantermi, e-learning) és lebonyolítása a társasági információbiztonsági felelős felelőssége, igény esetén a biztonsági szolgáltató munkatársait is bevonhatja a képzések megtartásába. Az oktatások tartalmazzák jelen Szabályzat előírásait is. Az oktatásokon való részvételi jelenléti ívet a társasági információbiztonsági felelős tárolja.

A felhasználók biztonságtudatossági szintjét, illetve az oktatások és kampány elemek hatékonyságát az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkciója kérdőíves felmérés, illetve helyszíni bejárás által évente méri. A kapcsolódó Social Engeering auditok hatókörét és célját szakmai szempontok alapján, a biztonságtudatossági szint fejlesztésének érdekében a társasági információbiztonsági felelős állapítja meg az MVM Zrt. Csoportszintű Biztonsági Igazgatóság támogatásával.

A felhasználók biztonságtudatossági szintjét, illetve az oktatások és kampány elemek hatékonyságát évente csoportszinten méri az MVM Zrt. Csoportszintű Biztonsági Igazgatóság.

5.6.3. Munkavállalókra vonatkozó szankciók

A Munka Törvénykönyve, indokolt esetben a Polgári Törvénykönyv, illetve a Büntető Törvénykönyv alapján a munkavállaló a munkaviszonyból származó kötelezettségének vétkes megszegésével okozott kárt köteles megtéríteni, amennyiben nem a szabályzatokban foglaltak szerint járt el, és a káresemény a munkavállaló vétkes magatartásának következményeként azonosítható.

Az információbiztonsági követelmények megszegésének eseteit továbbá a szankcionálási szempontokat a MOB-BSz-17-M-06 melléklet tartalmazza. A mellékletben felsorolt mulasztások szankcionálása érdekében a társasági információbiztonsági felelős jogosult a szankciók alapjául szolgáló bizonyítékok gyűjtésére az 5.17. alfejezetben meghatározottak szerint, továbbá munkajogi szankciók foganatosítására.

5.7. Fizikai biztonság

A speciális fizikai biztonsági intézkedésekre vonatkozó szabályzatot a társasági információbiztonsági felelőssel együttműködve, összhangban a kapcsolódó információbiztonsági követelményekkel kell kialakítani.

A fizikai biztonsági követelményeket zónánként szükséges meghatározni, ezért a Társaság székhelyén és telephelyein ki kell jelölni az 5.7.1 pontban meghatározott biztonsági zónákat.

5.7.1. Biztonsági zónák és követelményeik

A zónába sorolás az adott területen tárolt, kezelt, vagy éppen elhangzott információk biztonsági besorolásának függvényében történik az alábbi táblázatban meghatározottak szerint:

Biztonsági zóna	Adat kategóriák
Rendszeren kívüli zóna	Nyilvános adatok
Működési terület	Csoportszintű belső használatú Társasági belső használatú
Védett terület	Bizalmas (irodai környezetben)
Üzemi terület	Bizalmas (technológiai környezetben)
Kiemelten védett terület	Szigorúan bizalmas

A TÜK iratok tárolását illetően a minősített adat védelméről szóló 2009. évi CLV. törvény, a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet, valamint a Társaság biztonsági szabályzata a nemzeti minősített adatok védelméről az irányadó.

5.7.2. Alkalmazott eszközök és információbiztonsági követelményeik

Beléptető rendszer

Az információbiztonsági rendszer alapvető feltétele, hogy a Társaság székhelyén, illetve telephelyein beléptető rendszer működjön.

Kamerás megfigyelő rendszer

A kamerás megfigyelő rendszer megfelelő működését a társasági információbiztonsági felelős a Társaság adatvédelmi tisztviselőjével együttműködve évente legalább egyszer dokumentáltan ellenőrzi.

5.8. Iratkezelés rendje

5.8.1. Dokumentumok biztonsági osztályozása

Az iratkezelés rendjére vonatkozó előírásokat a Társaság iratkezelési szabályzatának kell tartalmaznia.

Annak érdekében, hogy a dokumentumok kezelése a megfelelő módon történjen, elsőként azok biztonsági osztályozására van szükség, amelynek alapja jelen Szabályzat MOB-BSz-17-M-07 melléklete. Azon dokumentumok, amelyek egyértelműen máshova nem kerültek besorolásra, a „társasági belső használatú" kategóriába tartoznak, és annak előírásai szerint kezelendőek.

Amennyiben egy dokumentum esetleg több, különböző biztonsági kategóriába sorolt adatot is tartalmaz, úgy a dokumentum egészére ki kell terjeszteni a legérzékenyebb elemének besorolását.

A bizalmas és a szigorúan bizalmas adatbiztonsági osztályba sorolt adatokat tartalmazó dokumentumokon fel kell tüntetni az irat biztonsági kategóriáját (nyomtatva vagy pecséttel). A biztonsági kategória feltüntetése azon adatgazda feladata, akinél az irat keletkezett. A biztonsági kategória esetleges módosítására szintén az adatgazdának van jogosultsága, ilyen jellegű igény esetén a feltüntetett biztonsági osztályt át kell húzni, valamint dátummal és az adatgazda aláírásával kell ellátni. Biztonsági besorolás módosítására csak abban az esetben van lehetőség, amennyiben a kapcsolódó szabályzatok módosulása ezt indokolja, vagy az adat egy meghatározott időpontig tartozik az említett két kategória valamelyikébe. A módosítás csak lefelé történhet (szigorúan bizalmas minősíthető bizalmasnak, illetve bizalmas társasági belső használatúnak).

A társasági belső használatú, csoportszintű belső használatú, illetve nyilvános besorolású információkat tartalmazó dokumentumokon külön jelölés tétele nem szükséges.

5.8.2. Dokumentumok kezelése

A papír alapú dokumentumokat biztonsági osztályba sorolásuknak megfelelően a MOB-BSz-17-M-08 mellékletben foglaltnak megfelelően szükséges kezelni. Ezen túlmenően kezelésükre az alábbi általános előírások érvényesek:

Dokumentumok tárolására használt eszközök

A csoportszintű belső használatú, valamint az ennél magasabb biztonsági kategóriába tartozó dokumentumokat az előírásoknak megfelelően elzárt helyen kell tárolni: zárható szekrényben, illetve szigorúan bizalmas adatok esetében páncélszekrényben.

A szekrények és páncélszekrények kulcskezelésre vonatkozóan a következő szabályokat szükséges betartani:

- A zárható szekrény kulcsáért az a munkavállaló felel, akinek irodájában a szekrény található, illetve aki az adott szekrényhez kulccsal rendelkezik. Amennyiben egy szerkényhez több felhasználónak is van kulcsa, ügyelni kell arra, hogy a kulcs elzárt, közösen hozzáférhető helyen legyen tárolva (pl. számzár kódos páncélszekrény), vagy minden felhasználó saját kulccsal rendelkezzen.
- Páncélszekrény kulcsához és számkódjához csak az arra jogosult, az adatgazda által jóváhagyott személyek férhetnek hozzá.
- A szekrényeket használaton kívül minden esetben, de legkésőbb a munkanap végén be kell zárni, a kulcsot nem szabad a zárban hagyni.
- A kulcsok szabadon hozzáférhető helyen történő tárolása tilos!
- Minden zárhoz kell, hogy legyen pótkulcs is, melyért az adatgazda által jóváhagyott személy felel. A pótkulcs felvételének szabályait, feltételeit írásban szükséges rögzíteni.
- A közösen használt számzárkódos páncélszekrények kódját lezárt borítékban kell tárolni az adatgazda, vagy általa felhatalmazott munkavállaló páncélszekrényében.

Minden esetben törekedni kell a tiszta asztal politika betartására, a munkanap végén irat nem maradhat az asztalokon, illetve a munkakörnyezetben.

Dokumentumok szállításának biztonsági követelményei

A dokumentumok továbbítására vonatkozó általános előírásokat a MOB-BSz-17-M-08 melléklet tartalmazza. Ezen túlmenően csoportszintű belső használatú, vagy annál magasabb biztonsági kategóriába tartozó dokumentumok tömeges szállítása során (pl. digitalizálás céljából) a MOB-BSz-17-M-09 mellékletben meghatározott eljárásrendet kell követni.

A tömeges dokumentum szállítás információbiztonsági követelményeit szolgáltatás keretein belül igénybe vett elszállítás esetén a szolgáltatóval kötött szerződésben, vagy nyilatkozatban rögzíteni kell.

Dokumentumok archiválása, digitalizálása

Az archivált anyagokat az azokban megjelenő adatok biztonsági besorolása szerint kell kezelni archiválást követően is.

A dokumentumok digitalizálása kizárólag az informatikai szolgáltató által üzemeltetett eszközökkel történhet, még külső szolgáltató bevonása esetén is. Külső fél nem kaphat jogosultságot az informatikai szolgáltató által biztosított rendszerhez, csak a szkennert kezelheti. A dokumentumok feltöltésének automatikusan kell megtörténnie, szerkesztésük nem engedélyezett.

Az archiválás és a digitalizálás információbiztonsági követelményeit a kapcsolódó szolgáltatóval kötött szerződésben, vagy nyilatkozatban rögzíteni kell.

Dokumentumok selejtezése

A dokumentumok selejtezését a Társaság iratkezelési szabályzatában foglaltak szerint kell végrehajtani.

A leselejtezett csoportszintű belső használatú, vagy annál magasabb biztonsági kategóriába sorolt dokumentumokat iratmegsemmisítővel kell megsemmisíteni az alábbi pontban foglaltak szerint.

Dokumentumok megsemmisítése

Az adatok megfelelő védelme érdekében a csoportszintű belső használatú, vagy annál magasabb biztonsági kategóriába tartozó iratokat tilos papírkosárba, vagy a kommunális hulladék közé helyezni, mivel így azok bárki számára könnyen hozzáférhetővé válnak. Ezen papír alapú dokumentumok biztonságos megsemmisítésének eszközei az alábbiak lehetnek:

- iratmegsemmisítők, illetve
- gyűjtő konténerek.

Iratmegsemmisítő használat

A szigorúan bizalmas minősítésű iratokat a biztonságos megsemmisítés érdekében iratmegsemmisítő segítségével le kell darálni. Olyan eszköz alkalmazása engedélyezett, mely megfelel a társasági információbiztonsági felelős által jóváhagyott (például a DIN 66399) szabvány előírásainak, valamint képes a CD-k, DVD-k, bankkártyák megsemmisítésére is.

Az iratmegsemmisítőket úgy kell elhelyezni, hogy azok a felhasználók számára könnyen elérhetőek legyenek, például a folyosókon, nyomtatók mellett. Azon irodákban is, melyek felhasználói gyakran dolgoznak bizalmas, vagy annál magasabb biztonsági besorolású papír alapú dokumentumokkal. Az iratmegsemmisítők elhelyezését és alkalmazását dokumentált módon szabályozni kell.

Minden felhasználó kötelessége az iratmegsemmisítő rendeltetésszerű használata, melynek keretein belül be kell tartani a következőket:

- Kerülendő az iratmegsemmisítő indokolatlan vagy magáncélú használata!
- Tilos olyan eszközök, tárgyak ledarálása, melyeket az eszköz nem támogat, és annak károsodását idézhetik elő.
- Ügyelni kell az eszköz biztonságos használatára, elkerülendő a balesetek, sérülések bekövetkezését.
- Amennyiben bármely munkavállaló az iratmegsemmisítő nem megfelelő működését vagy működtetését tapasztalja, azonnal jelentenie kell a társasági információbiztonsági felelős felé.

Az iratmegsemmisítők rendeltetésszerű használatát a társasági információbiztonsági felelős legalább évente egyszer köteles ellenőrizni.

Megsemmisítendő iratokat gyűjtő konténerek használata

Iratmegsemmisítők alkalmazása helyett/mellett lehetséges gyűjtő konténerek kihelyezés is. Az elszállításról és megsemmisítésről jegyzőkönyvet kell készíteni.

A konténerek kiválasztásával kapcsolatban figyelembe kell venni, hogy az eszközt felnyitni, megrongálni, abba belenyúlni ne lehessen. Az iratok biztonsági konténerbe helyezése minden munkavállaló felelőssége, egyben kötelessége a gyűjtő konténerek rendeltetésszerű használata, melynek keretein belül be kell tartani a következőket:

- Tilos a gyűjtő konténerbe ételt, kommunális hulladékot, illetve bármilyen más, nem a megsemmisítendő irat kategóriába tartozó tárgyat elhelyezni!
- A gyűjtő konténerekbe benyúlni, onnan iratot kiszedni szigorúan tilos! Amennyiben ilyen jellegű tevékenység válna indokolttá, a társasági információbiztonsági felelőst kell értesíteni, aki gondoskodik a konténer megfelelő átvizsgálásáról.
- Amennyiben bármely munkavállaló a gyűjtő konténerek sérülését, kompromittálódását tapasztalja, azonnal jelentenie kell az incidenst a társasági információbiztonsági felelős felé.

5.9. Informatikai rendszerek fejlesztése, beszerzése

A Társaságnak a folyamatai megfelelő ellátásához az informatikai és telekommunikációs rendszereit – az üzleti igényekkel összhangban és a változó biztonsági igényeknek megfelelően – folyamatosan fejleszteni kell. Jelen fejezet a Társaság általános információbiztonsági követelményeit foglalja össze a Társaság projektek kezelésére vonatkozó szabályzata és a Társaság infokommunikációs szabályzata tartalmával összhangban, illetve azok információbiztonsági kiegészítéseként. Továbbiakban, ha az külön nem jelölt, fejlesztés alatt értjük az informatikai rendszer beszerzéseket is.

Az informatikai rendszerek fejlesztése kapcsán külön szükséges kezelni az ügyviteli és a technológiai rendszereket. Az ügyviteli informatikai rendszereket a dedikált belső szolgáltató üzemelteti, míg a technológiai rendszerek üzemeltetését, karbantartását a Társaság saját hatáskörben biztosítja belső üzemeltetés, vagy megbízott külső szolgáltató/karbantartó (továbbiakban, ha külön nem jelölt, egyenértékű a belső üzemeltetéssel) által, azonban jelen Szabályzat általános előírásai mindkettőre kiterjednek.

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

- **Belső fejlesztésű** rendszerek: A Társaság, vagy az MVM Csoport informatikai szolgáltatója által fejlesztett ügyviteli vagy technológiai alkalmazások.
- **Külső fejlesztésű** rendszerek: Nem az MVM Csoport 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 az MVM Csoport/a Társaság számára fejlesztett alkalmazás, melyet más személy vagy társaság nem használhat.
  - Általános funkciókat ellátó, bárki számára elérhető alkalmazás („dobozos" termék)
  - Felhő alapú szolgáltatás

  A külső fejlesztésű rendszerek szerződése tartalmazza a telepítési és használati feltételeket, valamint a fejlesztési lehetőségeket, verziókövetést. Ebben az esetben a fejlesztővel/szállítóval kötött szerződésben kell kitérni az információbiztonsági követelményekre, melyet a társasági információbiztonsági felelős az 5.9.1 pontban rögzítettek szerint ellenőrizhet.

5.9.1. Általános irányelvek informatikai rendszerek fejlesztésére, beszerzésére vonatkozóan

Az informatikai rendszerek fejlesztését a következő információbiztonsági követelmények szerint kell végrehajtani.

Igények azonosítása

Amennyiben a Társaság esetében igény merül fel új rendszer bevezetésére, vagy a meglévő rendszerek módosítására, azt ügyviteli rendszer esetében az informatikai szolgáltató, technológiai rendszer esetében a helyi üzemeltetés felé szükséges jelezni a Társaság projektek kezelésére vonatkozó szabályzata és a Társaság infokommunikációs szabályzata alapján.

Az új igény egyeztetése során be kell vonni a társasági információbiztonsági felelőst az új rendszerrel vagy fejlesztéssel kapcsolatos kockázatok korai feltárása végett. Az információbiztonsági szempontú véleményezésnek minden esetben dokumentált módon kell megtörténnie.

Fejlesztési terv készítése és jóváhagyása

A fejlesztési terv elkészítésénél minden esetben figyelembe kell venni az információbiztonsági követelmények biztosítását is, ezért a dokumentum összeállításába a társasági információbiztonsági felelőst is be kell vonni. A társasági információbiztonsági felelős bevonásának elmaradásából származó károkért a fejlesztési projekt vezetője felelős.

A fejlesztési tervnek tartalmaznia kell a fejlesztéssel/beszerzéssel kapcsolatos információbiztonsági kockázatokat, azok valószínűségét és becsült hatását, valamint a lehetséges védelmi intézkedéseket és maradvány kockázataikat. Ezen kockázatok fejlesztési tervben történő feltüntetése a társasági információbiztonsági felelős feladata és felelőssége (a kockázatok megállapításába más szakértőket is bevonhat). A kockázatok kezeléséről való döntés és a maradványkockázatok elfogadása a MOB-FU-17-01 folyamatutasítás szerint történik.

Fejlesztés csak abban az esetben kerülhet megkezdésre, amennyiben az érintett felek, köztük a társasági információbiztonsági felelős is, jóváhagyták a fejlesztési tervet, figyelembe vették és kezelték az információbiztonsági kockázatokat, valamint a maradványkockázatok elfogadásra kerültek.

Fejlesztés megvalósítása

Belső fejlesztés esetén az informatikai szolgáltatónak, vagy a fejlesztésben érintett társaságnak fejlesztési módszertannal/szabályzattal kell rendelkeznie, mely dokumentálja a fejlesztések megvalósításának menetét, szabályait, kitérve az információbiztonsági követelményekre.

A Társaságban történő belső fejlesztés esetén – amennyiben az azonosított kockázatok indokolják – a társasági információbiztonsági felelőst rendszeresen tájékoztatni kell a projekt státuszáról és az információbiztonsági kockázatok kezeléséről.

Amennyiben a fejlesztés során jelentős, nem kezelt információbiztonsági kockázat merül fel, a társasági információbiztonsági felelős magához vonhatja a projekt irányítását a kockázat kezelésének időszakára.

Külső fejlesztésű rendszerek esetén a beszerzés előírásait kell figyelembe venni, továbbá a beszerzési kiírásba és eljárásba be kell vonni a társasági információbiztonsági felelőst (illetve minden, a fejlesztésben közvetlenül érintett további társaságok információbiztonsági felelőseit), aki azonosítja az információbiztonsági kockázatokat, azok kezelését, valamint meghatározza a fejlesztő számára előzetesen kiadható információkat és azok kiadásának feltételeit.

A beszerzés során a Társaság rendszerei esetében a társasági információbiztonsági felelősnek betekintést kell nyernie a külső fejlesztő fejlesztési módszertanába, valamint a fejlesztés során a fejlesztési tervbe az abban meghatározott információbiztonsági követelmények teljesítésének, kockázatok csökkentésének vizsgálata céljából. A projekt méretétől és jellegétől, valamint a bevezetni kívánt rendszer kockázataitól függően a társasági információbiztonsági felelőst be kell vonni a fejlesztési projektbe, legalább a státuszriportok elérése céljából. Amennyiben a fejlesztés során jelentős információbiztonsági kockázat merül fel, a társasági információbiztonsági felelős magához vonhatja a projekt irányítását a kockázatok elfogadható mértékű szintre történő csökkentéséig.

Felhő alapú rendszerek igénybevételének igénye esetén a rendszer bevezetése előtt az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkciónak ellenőriznie kell a szolgáltató információbiztonsági megoldásainak megfelelőségét (interjú vagy dokumentum vizsgálat), valamint jóvá kell hagynia a rendszerben tárolt/kezelt adatok körét, figyelembe véve az adatok besorolását. Az ellenőrzés eredményét dokumentált módon rögzíteni kell, a dokumentáció tárolása a társasági információbiztonsági felelős feladata. Bizalmas adat csak maszkolva, illetve megfelelő titkosítás mellett kerülhet fel a felhő alapú alkalmazásba, szigorúan bizalmas adatok felhőben való tárolása nem engedélyezett.

A felhő alapú rendszerek információbiztonsági vizsgálatának szempontjait a MOB-BSz-17-M-10 melléklet tartalmazza, ezen információk, adatok beszerzése a társasági információbiztonsági felelős felelőssége.

Tesztelés

A fejlesztés során minden tételnek van tesztelési időszaka, csak a jóváhagyott csomagok kerülhetnek be az éles rendszerbe.

A belső fejlesztésű alkalmazásoknál el kell különíteni a fejlesztői, teszt és éles környezetet egymástól.

A fejlesztői és teszt környezetre vonatkozó általános előírások:

- A környezet nem tartalmazhat valós adatokat.
- A teszt és fejlesztői környezetben csak teszt adatokat szabad használni.
- Az éles rendszernek fizikailag is el kell különülnie a fejlesztői és teszt környezettől.

Éles környezetben csak a tesztelt, jóváhagyott változat kerülhet implementálásra. Amennyiben a társasági információbiztonsági felelős nem találja megfelelőnek (felvállalhatatlan kockázatokat tár fel), a rendszer nem vezethető be.

A fejlesztés és a tesztelés során az anonimizálástól eltérni csak az üzleti oldali funkciógazda (az adatgazda és a társasági információbiztonsági felelős) jóváhagyásával lehet. Minden eltérés esetében kockázatelemzést kell végezni, annak eredményét az adatgazda dokumentálni köteles a Társaság személyes adatkezelési és adatvédelmi szabályzatának rendelkezéseit figyelembe véve.

A tesztelés kritériumait a tesztelési tervek dokumentáltan kell, hogy tartalmazzák. A tesztelési tervben rögzíteni kell a teszteseteket, valamint azok várt eredményét.

A tesztelést követően tesztelési jegyzőkönyvet kell készíteni, mely tartalmazza a tesztelési tervre való hivatkozást, a teszt eredményét, valamint amennyiben a teszt eredménye nem egyezik meg az előzetesen várt eredménnyel, rögzíteni kell az eltérést, annak (feltételezett) okát, valamint az alkalmazott megoldást.

A tesztelési tervek és jegyzőkönyvek meglétét, a dokumentumok tartalmát a Társaság általi fejlesztés esetén a társasági információbiztonsági felelős bármikor ellenőrizheti. A kért dokumentumokat mind az informatikai szolgáltató, mind a külső fejlesztő a társasági információbiztonsági felelős rendelkezésére kell, hogy bocsássa betekintés céljából.

Kiadás, élesítés

A Társaságnak rendelkeznie kell az általa használt üzleti folyamatot támogató informatikai rendszerekhez minden olyan dokumentációval, amely a rendszerek biztonságos működtetéséhez szükséges, még a szoftver szállítójának esetleges megszűnése esetén is. Ennek érdekében

- részben, vagy teljes mértékben saját fejlesztésű alkalmazásoknál változáskezelés keretén belül a fejlesztett alkalmazás dokumentációját és forráskódját archiválni kell;
- teljes mértékben külső fejlesztésű alkalmazásoknál át kell adni az adatok szintaktikai szabályait, tárolási szerkezetét, valamint az adatbázis részletes dokumentációját;
- ha a külsős fejlesztő/szállító nem teljesíti hibajavítási vagy továbbfejlesztési kötelezettségeit, akkor a szervezetnek valamilyen módon hozzá kell tudnia jutni az alkalmazás forráskódjához és fejlesztési dokumentációjához, ennek egyik lehetséges módszere a forráskód letétbe helyezése.

A kiadást, élesítést dokumentált módon jegyzőkönyvezni kell.

A rendszer bevezetését követően az 5.10. alfejezetben foglaltak szerint kell gondoskodni az információbiztonsági szempontból megfelelő működtetésről, karbantartásról.

5.9.2. Változáskövetés

Amennyiben a Társaság informatikai rendszert fejleszt/üzemeltet rendelkeznie kell olyan informatikai rendszerrel, illetve szabályozással, amely lehetővé teszi a megfelelő változáskövetés és változáskezelés fenntartását. Változás alatt kell érteni nem csak a rendszerfejlesztéseket,

hanem a rendszerek komponenseinek, illetve biztonsági beállításainak lényeges és az elfogadott standardoktól/szabályoktól eltérő módosítását is.

Minden olyan információ feldolgozó eszközökben és rendszerekben (éles, fejlesztői és teszt környezetben egyaránt) bekövetkező változást, amely hatással van az információbiztonságra, felügyelet alatt kell tartani, illetve dokumentálni kell.

Minden tervezett változtatásról igényt kell küldeni a társasági információbiztonsági felelős részére is.

Az igény megérkezését követően a társasági információbiztonsági felelős feladata megvizsgálni az igény létjogosultságát, illetve megvalósíthatóságát információbiztonsági szempontok figyelembevételével.

Az igény elbírálásának eredménye a következő lehet:

- **Igény azonnali elutasítása**: Ebben az esetben a vizsgálatot végző személy megfelelő, részletes indoklással elutasítja az igényt.
- **Igény felfüggesztése határozott időre**: Ebben az esetben az igény részben vagy egészben megfelel a vizsgálatot végző személyek szerint a követelményeknek, de egyéb kapcsolódó információbiztonsági körülmény (pl. folyamatban levő kapcsolódó projekt, kontroll bevezetés, stb.) miatt meghatározott időre felfüggeszti.
- **Igény felfüggesztése határozatlan időre**: Ebben az esetben az igény részben vagy egészben megfelel a vizsgálatot végző személyek szerint a követelményeknek, de egyéb kapcsolódó információbiztonsági körülmény (pl. kezelendő kockázatok, stb.) miatt határozatlan időre felfüggeszti.
- **Igény visszaküldése módosításra**: Az igény teljes vagy részleges nem-megfelelőség miatt elutasításra kerül, de csak arra az időre, amíg az igénylést feladó fél nem módosítja a vizsgálatot végző személyek által meghatározott paramétereket.
- **Igény elfogadása**: Az igény a vizsgálatot végző személy által elfogadásra kerül.

A jóváhagyott igényt követően a változás végrehajtását célzó feladat felelőse és az általa bevont személyek az elkészített ütemtervnek megfelelően a megadott határidőre teljesítik az igény megvalósítását egy folyamatos és nyomon követhető dokumentáció kíséretében. A projekt végrehajtása során a társasági információbiztonsági felelősnek rendszeres tájékoztatást kell nyújtani a változás megvalósításával kapcsolatban az esetlegesen felmerülő információbiztonsági kockázatok mielőbbi azonosítása és kezelése érdekében.

Az igény megvalósítását követően az eredmény és a végrehajtás ideje alatt készült dokumentáció megfelelőségét információbiztonsági szempontból a társasági információbiztonsági felelős ellenőrzi, majd megfelelőség esetén jóváhagyja. Amennyiben az eredmény nem megfelelő, a változás nem tekintendő lezártnak, a kért módosításokat a megfelelő dokumentáció mellett el kell végezni.

5.10. Informatikai rendszerek működtetése

A Társaság ügyviteli informatikai rendszerét az MVM Csoport informatikai szolgáltatója az MVMI Informatika Zrt. látja el SLA szerződés keretében.

A Társaság nem üzemeltet saját hatáskörben technológiai rendszert.

Az informatikai rendszereket érintő, az MVM BSZK Zrt. által nyújtott szolgáltatások igénybevételét (pl. adattörlés, visszaállítás, stb.) a társasági információbiztonsági felelős kezdeményezi.

Olyan rendszereket, melyek az 5-ös osztályba tartozó adatokat tárolnak, vagy kezelnek és az adatok bizalmassága, sértetlensége és/vagy rendelkezésre állása kritikus, minősített rendszernek kell tekinteni. Ezekről a rendszerekről a társasági információbiztonsági felelős nyilvántartást vezet, amelyet legalább évente egyszer felülvizsgál.

Az informatikai rendszerek működtetésének, üzemeltetésének általános információbiztonsági követelményei a következők:

- minden rendszerben biztosítani kell a naplózást az 5.10.5 pontban foglaltak szerint
- ügyviteli rendszerek esetében a naplózáson túl biztosítani kell a kiemelt felhasználó monitoring lehetőségét az 5.10.6 pontban foglaltak szerint
- minden rendszerben az 5.10.7 pontban foglaltak szerint kell biztosítani az adatok archiválását
- minden rendszerről a jelen Szabályzatban meghatározottak szerint biztonsági mentések készítése szükséges az 5.10.9 pontban foglaltak alapján
- minden rendszerben végre kell hajtani az 5.10.4 pontban foglaltak szerinti karbantartási feladatokat
- minden rendszer esetében az 5.23.2 pontban meghatározottak szerint sérülékenységvizsgálatokat kell lefolytatni
- a rendszereket üzemeltető felhasználók esetében be kell tartani az 5.5. alfejezetben foglalt jogosultsági előírásokat.

Az ügyviteli informatikai eszközök információbiztonsági szempontból megfelelő működtetéséért az informatikai szolgáltató felel, az információbiztonsági követelmények teljesülését a társasági információbiztonsági felelős a szolgáltatóval kötött szerződésben foglaltak alapján rendszeresen ellenőrizheti, illetve külső auditok alkalmával ellenőriztetheti az informatikai szolgáltatóval együttműködve. Az informatikai szolgáltató köteles naprakész tájékoztatást adni a társasági információbiztonsági felelős számára a Társaságot érintő rendszerek információbiztonsági állapotáról betekintés, dokumentum kivonatok, illetve riportok formájában. A Társaságot érintő rendszer alatt kell érteni minden olyan eszközt és alkalmazást, melyet a Társaság az informatikai szolgáltatótól vesz igénybe, és a vele kötött szerződés a rendszerekre kiterjed.

Technológiai rendszerek esetében az üzemeltetés információbiztonsági szempontjainak kialakítása és betartatása a társasági információbiztonsági felelős felelőssége, a végrehajtás a belső üzemeltetés, vagy az érintett rendszerek üzemeltetésére szerződött szolgáltató feladata. Az információbiztonsági követelmények megvalósítását a társasági információbiztonsági felelős a jelen Szabályzatban meghatározottak szerint ellenőrzi. Külső szolgáltató esetén az ellenőrzés végrehajtásához biztosítani kell a szükséges adatok átadását, vagy a betekintés jogát a társasági információbiztonsági felelősnek, melyet szerződésben is rögzíteni kell.

5.10.1. Ügyviteli informatikai eszközök

A Társaság az alábbiakban részletezett ügyviteli informatikai eszközeit az informatikai szolgáltató üzemelteti. Az eszközök működtetésére a következő információbiztonsági előírások vonatkoznak. A technológiai informatikai eszközök, illetve azokhoz kapcsolódó kiegészítések az 5.10.2 pontban kerülnek rögzítésre.

Munkaállomások

A Társaság minden ügyviteli területen dolgozó munkavállalója számára biztosít asztali munkaállomást és/vagy laptopot.

Az MVM Csoport belső hálózatára csak az informatikai szolgáltató által üzemeltetett munkaállomások csatlakoztathatok.

A Társaság által biztosított eszközökbe csak domain-be regisztrált felhasználók rendelkezhetnek belépési jogosultsággal. Alapesetben a domain szintű jogosultságok határozzák meg, hogy az adott felhasználó milyen rendszerhez fér hozzá. Alapelv, hogy minden felhasználó csak a munkájához szükséges adatokhoz rendelkezzen hozzáférési jogosultsággal. A jogosultságigénylés menetét az 5.5. alfejezet tartalmazza.

A munkaállomáson használt felhasználói jelszavakra vonatkozó előírásokat az 5.10.3 pontban foglaltak tartalmazzák. Az előírások betartását a rendszer automatikusan kikényszeríti.

A munkaállomásokra vonatkozó kontrollokat ügyviteli területen az informatikai szolgáltató biztosítja, például a frissítések kiküldése is az ő felelőssége és feladata, a frissítések fogadása a Társaság felelőssége. A hardveres és szoftveres karbantartás, hibaelhárítás szintén az informatikai szolgáltató felelőssége és feladata.

Alapértelmezetten az ügyviteli munkaállomásokon az optikai meghajtók és az USB portok csak olvasható (read-only) módban üzemeltethetőek. Adatok kiírására csak a központilag engedélyezett, dedikált USB eszközök használhatóak – kizárólag indokolt esetben – a munkavégzés során. Amennyiben a munkavégzés során egyedi adatkiírás indokolt, (pl. DVD írás hivatalos adatszolgáltatás érdekében) akkor az adatok kiírását a társasági információbiztonsági felelős hozzájárulásával az informatikai szolgáltató munkatársa végzi el helpdesk bejelentés alapján.

A munkához használt adatok lokális tárolása nem támogatott, mivel fennáll a kockázata, hogy amennyiben az eszköz eltulajdonításra kerül, a rajta tárolt adatok kompromittálódnak, valamint az eszköz elvesztése, eltulajdonítása vagy meghibásodása esetén a rajta tárolt adatok rendelkezésre állása sérül, hiszen a munkaállomásokról, laptopokról nem készül biztonsági mentés. Ezért erre a célra a fájlszerver adott megosztásait kell alkalmazni. Amennyiben a lokális tárolás elkerülhetetlen, a jelen Szabályzatban meghatározott, biztonságos módon kell a számítógép háttértároló eszközére menteni a fájlokat.

Biztonsági okokból tiltani kell, hogy a felhasználók a munkaállomásokon tudjanak mappát megosztani. Az ideiglenes fájlmegosztást és nagyméretű fájlcserét a központi fájlszerver jelen Szabályzatban megjelölt mappájának használatával, illetve egyéb belső, támogatott megoldás alkalmazásával lehet elvégezni.

A notebookok, laptopok használatára vonatkozó speciális előírásokat az 5.15. alfejezet tartalmazza.

Szerverek

Az ügyviteli szerverek üzemeltetését az informatikai szolgáltató, a technológiai szerverekét maga a Társaság belső üzemeltetése, vagy az általa megbízott külső szolgáltató végzi.

A szerverekkel kapcsolatos feladatok, melyeket jelen Szabályzat alább jelölt pontjai tartalmaznak a következők:

- Karbantartás (5.10.4 pont)
- Naplózás (5.10.5 pont)
- Archiválás (5.10.7 pont)
- Biztonsági mentések (5.10.9 pont)

Egyéb eszközök

A Társaság egyéb ügyviteli IT erőforrásai közé sorolhatók a nyomtatók, faxok, scannerek. Jelen alpont ezek speciális biztonsági követelményeit tartalmazza.

Nyomtatás

A Társaságnál elsősorban az irodákban, illetve a folyosókon kihelyezett központi nyomtatók alkalmazandóak. Belső használatú és bizalmas dokumentumok nyomtatása esetén fel kell hívni a felhasználók figyelmét arra, hogy fordítsanak figyelmet a nyomtatás felügyeletére, vagyis a kinyomtatott dokumentumok ne felejtődjenek a nyomtató tálcáján. Az informatikai szolgáltatónak a központi nyomtatók üzemeltetésénél, egy a felhasználó által elindított nyomtatási folyamat elindítása során arra figyelnie szükséges, hogy sikertelen nyomtatás esetén a nyomtatási sorból törlődjön a nyomtatási kérés, ezzel megakadályozva a felhasználói felügyelet nélküli nyomtatást, illetéktelen kézbe kerülést.

Bizalmas dokumentumok esetén, amennyiben a kártyás vagy PIN kódos nyomtatás nem biztosított, valamint szigorúan bizalmas anyagok nyomtatása esetén minden esetben a privát nyomtató (a nyomtatást végző személy irodájában állnak rendelkezésre) alkalmazásával kell végrehajtani a nyomtatást, vagy ezzel egyenértékű kompenzáló kontrollról kell gondoskodni.

A nyomtatók meghibásodása esetén az informatikai szolgáltatót kell értesíteni, és a nyomtatást egy másik eszközön végrehajtani, fénymásoló szalonok igénybe vétele, illetve saját, otthoni eszközök használata nem megengedett.

Scannelés

A folyosókon elhelyezett központi nyomtatók scannerként is funkcionálnak. A bescannelt dokumentumokat egy külön erre a célra felhasznált hálózati meghajtó megfelelő mappájába menti az eszköz, vagy választható formátumban elküldi a megadott e-mail címre. A mappák jogosultságkezelése megakadályozza, hogy illetéktelenek hozzáférjenek a dokumentumokhoz, ennek ellenére ügyelni kell arra, hogy bizalmas és annál magasabb besorolású anyagok ne maradjanak a közösen elérhető mappákban. Elektronikus levélként való küldés esetén ügyelni kell az e-mail cím pontos megadására. A scannelés végén ügyelni kell arra, hogy a bescannelt eredeti dokumentumok ne maradjanak az eszközben.

Alkalmazások telepítése

A Társaság tulajdonát képező munkaállomásokra szoftverek csak adminisztrátori jogosultsággal telepíthetőek, mellyel az átlagfelhasználók nem rendelkezhetnek. A hálózatba léptetett ügyviteli eszközökön nem engedélyezhető adminisztrátori jogosultság, üzemviteli illetve tartományon kívüli eszközökre a társasági információbiztonsági felelős jóváhagyásával engedélyezhető.

A hordozható, un. portable alkalmazások használata alapértelmezetten tiltott, az ilyen szoftverek igénylési folyamata megegyezik a nem standard szoftverekével.

Amennyiben egy felhasználónak valamilyen szoftver telepítésére van szüksége, az igényét az 5.5. alfejezetben foglaltak szerint kell leadnia. A kérelmet az érintett felhasználó felettese, az adatgazda, valamint a társasági információbiztonsági felelős bírálja el.

A Társaság munkavállalói által benyújtott, a fentiek szerint jóváhagyott nem standard telepítési igényeket az informatikai szolgáltató IT biztonságért felelős szakterülete és az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkciója megvizsgálja – szükség esetén a biztonsági szolgáltató bevonásával – és bírálja el. A nem standard telepítési igények teljesítéséhez mindkét szakterület együttes jóváhagyása szükséges.

Az igénylés engedélyezésének kizáró okai:

- Az informatikai szolgáltató biztosít alternatív megoldást vagy szolgáltatást.
- Olyan felhő alapú megoldásokat vagy szolgáltatásokat támogat, amelyek sérülékennyé teszik az IT rendszer bármely szegmensét, illetve magas (nem felvállalható) információbiztonsági kockázatot jelent.
- Alkalmazások, szkriptek vagy programok fejlesztésére ad lehetőséget (kivéve, ha a felhasználó munkaköréhez indokolt).
- Elavult verzió, vagy a gyártó által már nem támogatott szoftver.
- Olyan publikus sérülékenységgel rendelkezik, mely segítségével az érintett eszköz vagy az IT rendszer bármely része kompromittálhatóvá válhat.
- Az MVM Csoport hálózatán kívülre VPN kapcsolaton keresztül csatlakozó megoldással rendelkező szoftverek/szolgáltatások.
- Olyan fájlmegosztó szolgáltatással rendelkezik, amely felett a Társaságnak, vagy a belső szolgáltatóknak nincs kontrolja.
- Hálózatok lehallgatására alkalmas funkcióval rendelkezik.
- Az operációs rendszerbe beépülő modulokkal, bővítményekkel rendelkezik.
- A felhasználó munkavégzéséhez nem indokolt az igényelt szoftver/szolgáltatás.
- Az igénylő felületen a szoftver szükségességének indoklása nem értékelhető vagy nem került megadásra.

- Az MVMI Zrt. IT biztonsági szakterülete vagy az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkciója egyéb, az infrastruktúrát veszélyeztető kockázatot tárt fel.
- A Társaság Ügyvezetése nem felvállalható kockázatot tárt fel.

A fentiektől eltérni kizárólag csak az informatikai szolgáltató IT biztonságért felelős szakterületének és az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció közös engedélyével lehet.

Az egyszer elutasított kérelmet érdemi változtatás nélkül újra benyújtani nem lehet.

Az igénylő üzleti területnek kötelessége minden körülményt és információt átadnia az igénylés során, valamint egyeztetni kell a társasági információbiztonsági felelőssel.

A felhasználók számára kiegészítő alkalmazás telepítése, elsődlegesen az MVMI Alkalmazás katalógusából kell, hogy megtörténjen.

5.10.2. Technológiai informatikai eszközök

Technológiai informatikai eszköznek tekinthető minden olyan munkaállomás, szerver, nyomtató, egyéb speciális eszköz, amely csak a Társaság technológiai hálózatához kapcsolódik, az ügyviteli hálózathoz közvetlen kapcsolata - általában - nincsen, a Társaság tulajdonát képezi, illetve a Társaság által bérelt erőforrás/előfizetés, üzemeltetését pedig a Társaság helyi üzemeltetőkkel, vagy szerződéses keretek között harmadik féllel megoldja, de nem az informatikai szolgáltató által menedzseli.

Ezen eszközök információbiztonsági szempontú kockázatelemzése és kockázatarányos védelmének biztosítása a társasági információbiztonsági felelős feladata.

A technológiai informatikai rendszerekre, ahol külön nem jelöljük, 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, de ebben az esetben a csatlakozás módját és szabályait a jelen Szabályzatban részletesen rögzíteni kell;
- nem helyezhetők el a Társaság, illetve az üzemeltetést/támogatást ellátó társaság telephelyein kívüli, nem a rendeltetésszerű működést célzó helyszínen – kivéve távmunka esetén – amennyiben a társasági információbiztonsági felelős helyszíni felmérést követően pozitív javaslatot tesz a szakterület vezetőjének, akinek kötelessége engedélyeztetni a Társaság Ügyvezetőivel. Az Ügyvezetők indokolás nélkül is elutasíthatják a kivételkezelést;
- ne legyenek menedzselhetőek nem a Társaság, vagy a szerződéses partner tulajdonában álló eszközről;
- csak Társasági, dedikált adathordozók, illetve előzetesen jóváhagyott és engedélyezett eszközök csatlakoztathatóak hozzájuk;
- az 5.23.2. pontban meghatározottak szerint sérülékenységvizsgálatot kell végrehajtani rajtuk. Amennyiben az nem felvállalható kockázatot tár fel nem helyezhető üzembe.

5.10.3. Az authentikáció módja

A felhasználók az általuk használt informatikai rendszerekbe csak authentikációt (azonosítást) követően léphetnek be. A Társaság által alkalmazott ügyviteli rendszerek esetében, amennyiben a felhasználó a belső hálózatban dolgozik, az authentikáció módja felhasználónév-jelszó páros megadása.

Jelszókezelés

A felhasználó az első bejelentkezéshez egy véletlenszerűen generált kezdeti jelszót kap, melyet biztonságos módon kell átadni számára, annak érdekében, hogy a kezdeti jelszót más felhasználó ne ismerhesse meg.

A kezdeti jelszót az első bejelentkezés során azonnal meg kell változtatni, melyet a rendszerek automatikusan ki kell, hogy kényszerítsenek.

A jelszó megválasztásánál is törekedni kell az általános jelszóválasztási követelményekre, melyek a következők:

- minimum 8 karakter hosszúságú (rendszer kikényszeríti)
- kis- és nagybetűket, számokat és/vagy speciális karaktereket (@, &, #, stb.) tartalmaz (rendszer kikényszeríti)
- ne legyen értelmes, szótári szó
- ne legyen személyhez köthető információ (pl. név, születési dátum, kedvenc márka, stb.)
- különböző rendszerekhez (kiváltképp Társaságon kívüli alkalmazásokhoz) nem használható ugyanaz a jelszó
- korábban már alkalmazott jelszó többször nem használható (rendszer kikényszeríti)
- a jelszót nem javasolt felírni, amennyiben a felhasználó mégis rögzíti, ügyelnie kell arra, hogy elzárt, ne könnyen hozzáférhető helyen tárolja azt.
- jelszó-tároló alkalmazások közül csak a központilag jóváhagyott, a társasági információbiztonsági felelős által támogatott alkalmazások használhatóak, egyedi, privát megoldások nem.

A jelszavakat tilos más felhasználóval megosztani, még a rendszergazdának sem adhatók át.

A jelszavakat rendszeresen cserélni kell: a felhasználói fiókhoz és az elektronikus levelezéshez tartozó jelszót legfeljebb 90 naponta, egyéb rendszerek esetében pedig a társasági információbiztonsági felelős által meghatározott kritikussági szintbe sorolástól függően. A kötelező jelszócserét a rendszerek automatikusan ki kell, hogy kényszerítsék, ellenkező esetben az adott rendszer gazdájának felelőssége kompenzáló kontrollok bevezetése.

A jelszót haladéktalanul meg kell változtatni minden olyan esetben, amikor fennáll annak gyanúja, illetve lehetősége, hogy ismertté vált, kompromittálódott.

Amennyiben egy technológiai felhasználó jelszavának rögzítése és tárolása szükséges, a jelszót lepecsételt, aláírt borítékban, páncélszekrényben kell tartani és meg kell határozni a hozzáférők körét és a hozzáférés módját. A jelszó megismerését, megváltoztatását dokumentált módon rögzíteni kell a jelen Szabályzatban meghatározottak szerint.

Erős, illetve kétfaktoros authentikáció

Erős authentikáció alkalmazása szükséges minden olyan rendszer esetében, melyben fennállhat szigorúan bizalmas adatok tárolásának lehetősége, vagy nagy mennyiségben tartalmaznak bizalmas információkat (például naplózó rendszerek, monitoring eszközök, biztonsági mentések, stb.).

Technológiai rendszerek esetében, amennyiben kikényszeríthető, kétfaktoros, erős authentikáció (felhasználónév-jelszó páros és token vagy SMS-ben kapott kód megadása, egyéb ezzel egyenértékű megoldás) alkalmazása szükséges. Az érintett rendszerek körének meghatározásáért a társasági információbiztonsági felelős felel. Az erős authentikáció alkalmazását a társasági információbiztonsági felelős belső audit keretében ellenőrizheti az 5.23. alfejezetben foglaltak alapján.

A külső hálózatról elérhető ügyviteli és technológiai rendszerek esetében mindenképpen kétfaktoros authentikáció szükséges, ennek szabályozását az 5.12.4. pont tartalmazza, a mobil

eszközökkel is elérhető rendszerek esetében pedig figyelembe kell venni az 5.15. alfejezet tartalmát.

5.10.4. Karbantartás

A biztonsági kockázatok csökkentése érdekében a Társaság mind a munkaállomások, mind a szerverek rendszeres karbantartásáról rendszeresen kell, hogy gondoskodjon (ügyviteli és technológiai rendszerek esetében egyaránt). A munkaállomások (asztali számítógépek és laptopok) karbantartásáról az informatikai szolgáltató munkatársai központilag gondoskodnak, illetve helyi támogatást is adnak, valamint az ügyviteli szerverek karbantartását is az informatikai szolgáltató munkatársai végzik. A felhasználónak az eszközök karbantartásával kapcsolatban annyi feladata van, hogy ne akadályozza meg a szükséges frissítések telepítését, illetve kérés esetén működjön együtt a rendszergazdákkal.

A technológiai informatikai eszközöket a Társaság üzemeltetési területén dolgozó munkatársai, vagy a Társaság által megbízott külső szolgáltató tartják karban a szerződésben és jelen Szabályzatban rögzített feltételek szerint.

A Társaság jelen Szabályzatban, vagy üzemeltetési eljárásrendekben foglalt rendszerességgel minden érintett eszközön karbantartást kell végezzen. A karbantartás több részletben kerülhet végrehajtásra. Az adott karbantartási ciklus feladatait a karbantartási terv írja elő, mely egyben a karbantartások megtörténtének igazolására, naplózására, nyomon követésére is szolgál.

A karbantartási terv/napló a Társaság által meghatározott formátumban, illetve rendszerben kell, hogy készüljön, és tartalmazza a következő információkat:

- karbantartott eszköz/alkalmazás neve,
- karbantartás megnevezése, rövid feladatleírás,
- rendszeres/eseti karbantartás (utóbbi esetén annak indoklása),
- karbantartás tervezett időpontja,
- karbantartó neve,
- karbantartás megvalósulásának időpontja,
- karbantartás eredménye,
- további feladatok,
- következő karbantartás várható ideje.

Eseti jellegű karbantartásnak minősülnek az előre nem tervezett karbantartások, valamint az ad-hoc frissítések, javítások.

A telepített frissítésekről külön nyilvántartás nem készül, azok az érintett rendszerben kell, hogy nyomon követhetőek legyenek.

Új verziók, javítócsomagok rendelkezésre állásáról a rendszer fejlesztője küld tájékoztatást a szerződésben meghatározott feltételek szerint az üzemeltetésnek, aki a telepítést csak előzetes biztonsági ellenőrzést és tesztelést követően hajtja végre, amennyiben az információbiztonsági kockázatok (adatvesztés, adatok kompromittálódása, stb.) minimálisnak bizonyulnak, illetve a szükséges biztonsági intézkedések (pl. mentés) megtörténtek.

Amennyiben a karbantartás vagy hibajavítás során az eszköz külső szervizbe történő szállítása indokolt, gondoskodni kell arról, hogy belső, bizalmas adatok ne kerüljenek a Társaságon kívülre ennek érdekében az eszköz háttértároló eszközének eltávolítása, vagy amennyiben ez nem megvalósítható, az adatok mentése, majd a háttértároló eszköz visszaállíthatatlan törlése indokolt szervizbe szállítás előtt. Az informatikai eszközök szervizbe szállítására csak az informatikai szolgáltató, a biztonsági szolgáltató, illetve a társasági információbiztonsági felelős jogosultak. A jelen Szabályzatban rögzítettektől eltérni csak a társasági információbiztonsági felelős előzetes írásbeli hozzájárulásával lehet.

5.10.5. Naplózás

Az MVM Csoport tagvállalatai által, vagy megbízásából üzemeltetett minden informatikai rendszert, beleértve mind az ügyviteli, mind a technológiai rendszereket naplózni kell. A naplózott rendszereket, illetve a naplózás szabályait jelen Szabályzatban dokumentáltan rögzíteni kell.

A rendszerek naplózása két okból elengedhetetlen:

- Ha bármilyen informatikabiztonsági esemény vagy incidens történt, akkor a naplózás segíthet annak megállapításában, hogy ki volt érte a felelős, illetve hogyan zajlott le az esemény. A naplóállomány evidenciaként felhasználható.
- Informatikai problémák (például nem várt leállás) esetén a naplózás segíthet a hiba okának meghatározásában, hogy a jövőben már ne fordulhasson elő ugyanez az eset.

A naplózás megvalósításával a Társaság biztosítja az elszámoltathatóságot, letagadhatatlanságot, valamint a bekövetkezett incidensek utólagos kivizsgálását támogatja.

A naplózással kapcsolatos alapkövetelmények a következők:

- Minden rendszernél lehetőség szerint naplózni kell legalább a következő eseményeket:
  - belépési kísérlet (sikeres és sikertelen egyaránt),
  - kilépés,
  - jelszóváltoztatás,
  - többletjogosultság szerzésére tett kísérlet, illetve
  - jogosulatlan művelet végrehajtásának megkísérlése.
- Kritikus rendszereknél (melynél a benne tárolt, kezelt adatok bizalmasságának, sértetlenségének, illetve rendelkezésre állásának kockázata kritikus) naplózni kell továbbá az adathoz való hozzáférés, módosítás, törlés megkísérelt eseményeit, végrehajtott műveleteit is.
- A naplóállományokat a jelen Szabályzatban meghatározottak szerinti gyakorisággal, rendszeresen elemezni kell. Az elemzés során tapasztalt, előzetesen a jelen Szabályzatban rögzített küszöbértéket meghaladó eltéréseket ki kell vizsgálni és jegyzőkönyvezni kell.
- Biztonsági események, illetve incidensek kivizsgálása esetén az érintett rendszer (ügyviteli és technológiai egyaránt) üzemeltetőjének (legyen az az informatikai szolgáltató, a helyi üzemeltetés, vagy a Társaság által megbízott szolgáltató) kötelessége átadni/betekintést biztosítani a kapcsolódó naplóállományokba a vizsgálatot koordináló társasági információbiztonsági felelősnek, vagy írásbeli kérésre az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkciójának.

A naplózott eszközökről a naplózó rendszer üzemeltetőjének naprakész nyilvántartással kell rendelkeznie, melybe kérésre betekintési lehetőséget kell biztosítania a társasági információbiztonsági felelősnek.

A naplózás során keletkező állományokat korlátozott hozzáféréssel, a bennük megjelenő adattartalom minősítése szerint kell kezelni, és a megjelenő adattartalom szerinti meghatározott ideig, központilag szükséges tárolni.

5.10.6. Monitorozás

A Társaság által, vagy megbízásából üzemeltetett minden informatikai rendszert, beleértve mind az ügyviteli, mind a technológiai rendszereket folyamatosan monitorozni kell. A monitorozó eszköz kiválasztása során az MVM Zrt. Csoportszintű Biztonsági Igazgatóság bevonása kötelező.

A monitorozó eszközök ki kell, hogy terjednek legalább a következőkre:

- informatikai rendszerek
- kiemelt felhasználók tevékenységei (ügyviteli alkalmazások esetében)
- átlagfelhasználók tevékenységei

A monitorozott eszközökről és felhasználókról a monitorozó rendszer üzemeltetőjének naprakész nyilvántartással kell rendelkeznie, melybe kérésre betekintési lehetőséget kell biztosítania a társasági információbiztonsági felelősnek, illetve a Társaság Ügyvezetőinek az üzemeltető felügyelete mellett.

A monitorozás során keletkező állományokat korlátozott hozzáféréssel, a bennük megjelenő adattartalom információbiztonsági osztályozása szerint kell kezelni, és a megjelenő adattartalom szerinti meghatározott ideig szükséges tárolni, illetve a keletkezett fájlok esetében az 5.10.5 pontban foglaltak szerint kell eljárni.

5.10.7. Archiválás

A Társaság meghatározott gyakorisággal kell, hogy elvégezze az elektronikus és papír alapú dokumentumok archiválását. Az archiválás végrehajtása elengedhetetlen a kapcsolódó törvények által előírt adatmegőrzési kötelezettség teljesítése érdekében, valamint az archivált anyagok a későbbi vitás ügyek, incidensek kivizsgálásához is szükségesnek bizonyulhatnak evidenciaként. Amennyiben a törvény vagy a személyes adatok kezelésére vonatkozó szabály másképpen nem rendelkezik a Társaságnál az adatmegőrzési idő legalább egy év, hogy a Társaság teljesíteni tudja jelen Szabályzatban (és a Társaság személyes adatkezelési és adatvédelmi szabályzatában) előírt adatszolgáltatási kötelezettségét.

Ügyviteli rendszerben tárolt elektronikus adatok esetén a tömeges archiválás végrehajtását az adatgazda megbízása alapján az informatikai szolgáltató elvégezheti, technológiai rendszereknél a belső üzemeltetés, vagy a Társaság által megbízott külső fél feladataként adható ki, de az archiválás megtörténtéért (az esetleges megbízások kiadásáért, és a végrehajtás ellenőrzéséért) mindenkor az adatgazda felel. Az archivált adatokhoz csakis az érintett adatgazda férhet hozzá, amennyiben más személynek lenne szüksége valamely archív állományra, ő engedélyezhet hozzáférést az érintett személynek.

Az archivált anyagokat azok biztonsági besorolása szerint kell tárolni, kezelni.

Az elektronikus adatok archiválásának eljárásrendjét dokumentált módon rögzíteni kell. Az archiválás biztonsági követelményeit, illetve az archivált anyagok megfelelő kezelését a társasági információbiztonsági felelős a jelen Szabályzatban meghatározottak szerint, de legalább éves szinten egyszer kell, hogy ellenőrizze.

5.10.8. Adathordozók törlése

Minden, az informatikai szolgáltató, vagy a Társaság tulajdonában álló informatikai eszközön és adathordozón tárolt adatot törölni kell az alábbi esetekben és módokon:

- egyszeri törlés szükséges az alábbi esetekben:
  - ügyviteli számítógépek esetében, amennyiben az eszköz szervezeti egységen belül kerül átadásra
- visszaállíthatatlan törlés szükséges az alábbi esetekben:
  - ügyviteli számítógépek leadását követően, amennyiben az eszköz szervezeti egységen kívül kerül felhasználásra
  - leselejtezett munkaállomások, egyéb informatikai eszközök esetében
  - okostelefonok, tabletek, USB adattárolók leadása esetén
  - informatikai eszközök külső szervizbe történő juttatása esetén, amennyiben a háttértároló nem távolítható el
  - informatikai eszközök leselejtezését követő értékesítése, adományozása esetén

A fent előírtaktól eltérni, indokolt esetben az adatgazda (vagy amennyiben nem meghatározható, akkor a szervezeti egység vezetője) és a társasági információbiztonsági felelős dokumentált együttes jóváhagyásával lehetséges.

Az egyszeri törlés végrehajtása ügyviteli eszközök esetében az informatikai szolgáltató, technológiai rendszerek esetében a Társaság üzemeltetés feladata és felelőssége, visszaállíthatatlan törlés végrehajtását a biztonsági szolgáltatótól kell igénybe venni. A visszaállíthatatlan törlés igénylését kezdeményezheti az informatikai szolgáltató, a technológiai rendszerek esetében a Társaság belső üzemeltetése, illetve az adatgazda is, attól függően, hogy az eszköz kinek került leadásra.

Munkaállomások, okostelefonok, tabletek és laptopok adatainak visszaállíthatatlan törlése előtt a leadott eszközökről indokolt esetben, az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció elrendelésére image-et készíttethet a későbbi esetleges vizsgálatok végrehajtása céljából. Ez esetben az Ügyvezetőkkel, a társasági információbiztonsági felelőssel és a DPO-val is egyeztetni szükséges. A forensic image-ek készítése és tárolása a biztonsági szolgáltató feladata. Az image-ek tárolási ideje nem haladhatja meg az egy évet.

Az adathordozók fizikai megsemmisítése esetén a biztonsági szolgáltató erre vonatkozó szolgáltatását kell igénybe venni.

5.10.9. Biztonsági mentések

Biztonsági mentések készítése

A Társaságnak gondoskodnia kell az általa használt informatikai rendszerek biztonsági mentésének elkészítéséről. A biztonsági mentések készítése ügyviteli rendszerek esetében az informatikai szolgáltató, technológiai rendszerek esetében pedig a Társaság belső üzemeltetés, illetve a Társaság által megbízott külső fél feladata. A biztonsági mentésekkel kapcsolatos igényeket (mentési gyakoriság, típus, adattároló, stb.) az érintett rendszer adatgazdájának, a társasági információbiztonsági felelősnek, illetve az üzemeltetésnek közösen kell meghatároznia és szabályzatban, illetve szerződésben dokumentált módon rögzítenie.

Mivel a lokális adattárolás nem támogatott az informatikai szolgáltató, illetve belső üzemeltetés által készített központi mentések nem terjednek ki a felhasználói munkaállomásokra, illetve mobil eszközökre. Az üzemviteli IT rendszerekről, eszközökről az üzemeltetésért felelős szakterületnek kell gondoskodnia a jelen Szabályzatban foglalt biztonsági követelményeket betartva biztonsági mentést készítenie.

A központi biztonsági mentések készítését dokumentált módon, eljárásrendben vagy üzemeltetési utasításban kell rögzíteni, melyben meg kell határozni a következőket:

- mentett rendszerek, adatok köre,
- mentés módja és eszköze,
- mentés gyakorisága,
- mentés típusa (teljes/inkrementális),
- mentési média,
- mentési média szállításának és tárolásának követelményei,
- mentési rendszer általános visszaállítási követelmények, lépések és tesztek módja és gyakorisága,
- mentés és visszaállítás dokumentáltsága.

A mentések gyakorisága és típusa rendszerenként eltérő lehet.

A biztonsági mentések készítésével kapcsolatos általános információbiztonsági követelmények:

- Olyan mentési technológiát kell alkalmazni, amely lehetővé teszi, hogy a biztonsági mentésekből szükség esetén üzletmenet folytonossági szempontból kritikus rendszereken meghatározott időn belül (RPO) helyre lehessen állni.
- A biztonsági mentéseket olyan módon kell létrehozni, hogy az adatok mellett az azok használatához szükséges szoftverkomponensek is helyreállíthatók legyenek.
- A mentésre használt adathordozónak megfelelőnek kell lennie a rajta tárolt adatok iránt támasztott követelményeknek (adatmegőrzési idő, újraírhatóság, tárolási előírások).
- A mentési adathordozók kezelése a rajtuk tárolt adatok biztonsági szintjével összhangban kell, hogy történjen, és a forrásrendszerrel azonos szintű fizikai védelemmel kell, hogy rendelkezzen.
- A biztonsági mentéseket tűzbiztos helyen kell tárolni, a mentésben szereplő állományok legmagasabb biztonsági besorolása szerint kezelve. Tilos a mentett rendszer, és róla készült biztonsági mentés azonos adattárolón való tárolása. A biztonsági mentéseket az eredeti rendszerhez viszonyított tűzkörön kívül kell elhelyezni/tárolni.
- A visszaállításhoz szükséges eszközöknek mindig rendelkezésre kell állniuk.
- A biztonsági mentések megfelelőségét, visszaállíthatóságát rendszeresen, dokumentált módon tesztelni kell.

Minden biztonsági mentés készítése dokumentált módon kell, hogy történjen a mentés készítéséért felelős szervezeti egység által. A dokumentálás az informatikai szolgáltató által biztosított mentések esetén, a hatályos mentési utasításnak megfelelő formátumban, a mentési rendszer szerint rögzített naplózás keretében valósítandó meg. A Társaság által biztosított mentések esetén a Társaság szerint meghatározott formátumban, illetve rendszerben kell, hogy történjen, mely tartalmazza minimálisan a következő információkat:

- mentett rendszer, adatok köre
- mentés típusa
- mentés időpontja
- mentési média megnevezése és azonosítója
- mentést végző személy neve (amennyiben értelmezhető)
- visszaállítási teszt dátuma és eredménye (amennyiben értelmezhető)

Biztonsági mentések visszaállítása

A biztonsági mentések visszaállítása ügyviteli rendszerek esetében az informatikai szolgáltató, technológiai rendszerek esetében a Társaság informatikai üzemeltetése, vagy a Társaság által megbízott külső üzemeltető feladata. A visszaállítás kezdeményezője lehet

- az informatikai üzemeltetés, aki észlelte az incidens következtében megvalósult adatvesztést, ebben az esetben a társasági információbiztonsági felelős és adatgazda tájékoztatása, valamint utóbbi hozzájárulása szükséges;
- a társasági információbiztonsági felelős az adatgazda tájékoztatásával és egyetértésével;
- az adatgazda a társasági információbiztonsági felelős tájékoztatásával.

A biztonsági mentések visszaállítását dokumentált módon rögzíteni kell, mely történhet a Társaság által meghatározott formában, illetve alkalmazott rendszerben. A dokumentációnak tartalmaznia kell a következőket:

- visszaállított rendszerek, adatok köre,
- visszaállítás indokoltsága,
- visszaállítást igénylő és jóváhagyó neve,
- visszaállítás dátuma,

- visszaállítás sikeressége,
- adatvesztés mértéke,
- egyéb észrevételek.

5.11. Kriptográfiai eszközök használata

A Társaság annak érdekében, hogy csökkentse az általa kezelt adatok bizalmasságának és sérülésének kockázatát, kriptográfiai eszközöket kell, hogy alkalmazzon a bizalmas és annál magasabb biztonsági besorolású adatok tárolása és továbbítása során.

Kriptográfiai megoldások alkalmazása ügyviteli rendszerek esetében kötelező, technológiai rendszerek esetén megfelelő szintű kompenzáló kontrollok bevezetése mellett hagyható el (amennyiben a kriptográfiai megoldás esetlegesen veszélyeztetné az adatok sértetlenségét és/vagy rendelkezésre állását).

Kriptográfiai megoldások alkalmazása szükséges az alábbi esetekben:

- minden olyan asztali munkaállomáson, melyen lokálisan tárolásra kerülhetnek bizalmas, vagy annál magasabb biztonsági besorolású adatok, illetve megfelelő kompenzáló kontrollok nem lehetségesek
- minden olyan laptopon/notebookon, melyen lokálisan tárolásra kerülhetnek csoport szintű belső használatú, vagy annál magasabb biztonsági besorolású adatok
- elektronikus kommunikáció, adatcsere esetén, amennyiben az adat a vállalatcsoporton kívüli csatornán, illetve helyszínen kerül továbbításra (elektronikus levelezés, külső adathordozó, stb.)
- biztonsági mentések készítése során, az adat biztonsági besorolása szerint
- személyes adatok kezelése során a törvényi előírásoknak megfelelő szintű titkosítás alkalmazása szükséges mind az informatikai és a biztonsági szolgáltató, mind a kollégák tekintetében

A Társaság alkalmazott kriptográfiai eszközei, megoldásai a következőkben kerülnek bemutatásra.

5.11.1. Teljes merevlemez titkosítás

A teljes merevlemez titkosítást lehetővé tevő szoftver telepítése és karbantartása ügyviteli rendszerek esetében az informatikai szolgáltató, technológiai rendszerek esetében a Társaság feladata.

Ügyviteli rendszerek esetében a teljes merevlemez titkosítást biztosító szoftver AD-ból kell, hogy authentikáljon, így a központi AD hitelesített felhasználók tudják csak feloldani a titkosítást, valamint csak az adott számítógépen felhasználói profillal rendelkező felhasználók jogosultak a feloldásra. A teljes merevlemez titkosítás helyreállítási kulcsait az informatikai szolgáltató tárolja, és kizárólag a társasági információbiztonsági felelősnek adhatja át írásbeli kérésre. A szoftver központilag vezérelt kell, hogy legyen, így az esetleges frissítések a központi jóváhagyások után automatikusan települnek minden titkosított munkaállomásra. A központilag alkalmazott megoldás információbiztonsági szempontú értékelése és jóváhagyása az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció felelőssége.

A központilag alkalmazott rendszertől eltérő megoldás csak technológiai rendszerek esetében alkalmazható, a társasági információbiztonsági felelős hozzájárulásával.

Az egyes partíciók titkosítása ügyviteli rendszerek esetében nem elégséges védelmi intézkedés és nem engedélyezett megoldás. Technológiai rendszerek esetében a partíciók titkosításának kialakítását a társasági információbiztonsági felelős állapítja meg.

A háttértároló(k) teljes titkosítását kell alkalmazni minden IT eszközön. A titkosítás feloldásához szükséges kulcs tárolása és naprakészen tartása az informatikai szolgáltató feladata, a kulcsok kiadása kizárólag a társasági információbiztonsági felelős kérésére adható csak ki.

A titkosítás deaktiválását, illetve ismételt aktiválását csak a társasági információbiztonsági felelős kérésére, illetve írásbeli engedélye alapján teheti meg az informatikai szolgáltató munkatársa.

5.11.2. Fájl titkosító alkalmazások használata

Fájlok harmadik féllel történő cseréje esetén, illetve MVMH tartományon kívül a bizalmas, valamint annál magasabb biztonsági besorolású adatok, illetve csoportszintű belső használatú adatok tömegesen, elektronikusan csak titkosított formában adhatók át mind ügyviteli, mind technológiai rendszerek esetében.

Ügyviteli rendszerekből történő titkosított adattovábbítás esetén a központilag alkalmazott titkosító megoldás használata kötelező. Ettől eltérés csak az adatgazdával és a társasági információbiztonsági felelőssel egyeztetve, indokolt esetben lehetséges. A központi megoldás információbiztonsági szempontú vizsgálata és jóváhagyása az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció felelőssége és feladata az informatikai szolgáltató és biztonsági szolgáltató bevonásával. A központi fájl titkosító megoldás telepítése, karbantartása, valamint a felhasználók segítése és felhasználói leírások készítése az informatikai szolgáltató felelőssége és feladata.

Technológiai rendszerek esetében – amennyiben titkosítás alkalmazása indokolt – a megfelelő megoldás kiválasztása a társasági információbiztonsági felelős felelőssége, az alkalmazás telepítése és karbantartása a Társaság, vagy a Társaság által az üzemeltetéssel megbízott külső fél feladata.

A besorolás szerinti fájlok titkosításának elmulasztásából adódó károkért a felhasználó szankcionálható jelen Szabályzat szerint.

A titkosítani kívánt csatolmányok jelszavas tömörítésekor javasolt a minél „erősebb" (min. 8 karakter hosszú, vegyes nagy- és kisbetű, szám és speciális karakter alkalmazása) jelszó és legalább AES-256-os titkosítási algoritmus használata.

Törekedni kell arra, hogy a fogadó féllel (pl. a levél címzettjével) a dekódoláshoz szükséges kulcs valamely más kommunikációs csatornán (pl. telefonon, szóban, SMS-ben vagy személyesen előre megállapodva) kerüljön megosztásra. Fel kell hívni a felhasználók figyelmét arra, hogy soha ne küldjük el ugyanabban a levélben a jelszót, mint amelyben a titkosított információ is szerepel.

Bizalmas fájlok továbbítása csak titkosítással történhet, melyre minimálisan az alábbi eszközök/szoftverek használata ajánlott:

- 7Zip: fájlok tömörítése és jelszóval történő ellátása, elektronikus levélben történő átadáshoz. A jelszóválasztásnál törekedni kell a megfelelő összetettségű jelszavak használatára, azaz minimum 12 karakter hosszúságú legyen, tartalmazzon: kis-és nagybetűket, számokat és speciális karaktereket. A titkosítás AES-256 vagy annál magasabb szintű algoritmussal történjen.
- Titkosított pendrive/külső merevlemez.

A bizalmas fájlok megosztására az informatikai szolgáltató által szolgáltatott SharePoint felületek használata ajánlott.

5.11.3. Elektronikus levelezés titkosítása

A teljes elektronikus levelezés titkosítása az MVM Csoportban jelenleg nem előírás, a fájlok titkosított csatolmányként való küldése megfelelő kontroll.

Amennyiben olyan ok merül fel, mely szerint a teljes elektronikus levelezés titkosítása indokolt (pl. harmadik féllel való titkosított levelezés szerződéses követelmény), a bevezetendő megoldásról az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció, a központi Infokommunikációs Igazgatóság, az informatikai szolgáltató, valamint a biztonsági szolgáltató információbiztonsági felelőse közösen hozzák meg a döntést.

5.11.4. Hordozható adattárolók titkosítása

A Társaság, mint az MVMH domain felhasználója, köteles az ügyviteli rendszerek esetében dedikált USB adathordozó használatára, mely egyúttal a megfelelő titkosítást is biztosítja.

Technológiai rendszerek esetében, amennyiben az adatot a Társaságon belül, Társaságon 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.

A titkosítatlan adathordozókon tárolt Társasági adatok kompromittálódásáért az eszközt használó munkavállaló felel, és az 5.6.3. pontban foglaltak szerint szankcionálható.

Nem titkosított, hordozható adattároló a Társaság telephelyről történő kivitele tiltott.

A belső adatok szállítása, tárolása külső adathordozó esetén csak titkosított formában történhet. Ilyen célból az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció csak az általa előzetesen jóváhagyott titkosított pendrive-okat és merevlemezeket engedélyezi. A titkosított adathordozók beszerzése minden szakterület önálló feladata.

Az optikai lemezmeghajtók használata tiltott és technológiailag ki kell kényszeríteni. Indokolt esetben kivételkezelés a társasági információbiztonsági felelős engedélyével történhet.

A jóváhagyott USB eszközöktől eltérő eszköz használatához a társasági információbiztonsági felelősének hozzájárulása szükséges. Az MVMI webshopban „VK9 Szoftver / egyedi hardver" űrlapon az USB eszköz engedélyezése menüpont kiválasztása után lehetséges az igénylés benyújtása.

5.12. Hálózatbiztonság

Jelen Szabályzat magas szinten kívánja rögzíteni az ügyviteli, illetve technológiai hálózatok alapvető biztonsági követelményeit. Hálózatbiztonsági szempontból megkülönböztetésre kerülnek a belső ügyviteli és technológiai hálózatra, illetve a külső hálózatra vonatkozó biztonsági előírások, melyeket jelen fejezet tartalmaz.

A belső ügyviteli hálózatra csatlakoztatható, MVMH domain tartományba léptetett munkaállomásokról külső hálózat felé VPN kapcsolatot létesíteni tilos. Ettől való eltérés csak az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció és az informatikai szolgáltató IT biztonsági szakterületének együttes hozzájárulásával lehetséges minden esetben egyedi elbírálás alapján. Amennyiben a szakterületek bármelyike olyan kockázatot tár fel, amely nem felvállalható, akkor tilos ilyen kapcsolat létesítése.

5.12.1. Külső hálózat

Az MVM Csoport csoportszintű belső használatú, vagy annál magasabb biztonsági osztályba sorolt adatai csak és kizárólag belső hálózaton keresztül jelenhetnek meg titkosítatlan formában. A külső hálózaton keresztül elérhető belső alkalmazások az 5.12.4 pontban foglaltak szerint csak VPN-en keresztül, vagy erős authentikációt követően szabad, hogy elérhetőek legyenek.

Technológiai rendszerek alap esetben nem kapcsolódhatnak külső hálózathoz, kivéve amennyiben ez rendeltetésszerű működésük célja, ebben az esetben külön hálózati szegmens, illetve a hálózati elérés korlátozása szükséges a jelen fejezetben foglalt biztonsági előírások betartása mellett.

Külső hálózathoz való csatlakozás csak tűzfalon (központi és lokális) keresztül lehetséges, illetve amennyiben indokolt, DMZ kialakítása szükséges. A tűzfalszabályok meghatározása és dokumentálása, illetve a hálózati szolgáltatók biztonságos üzemeltetése ügyviteli rendszerek esetében az informatikai szolgáltató feladata, technológia rendszerek esetében a Társaság feladata és a társasági információbiztonsági felelős kell, hogy ellen jegyezze. A központilag alkalmazott biztonsági megoldásokat, illetve tűzfal szabályokat az MVM Zrt. Csoportszintű

Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció az 5.23. alfejezetben foglaltak szerint auditálhatja, illetve kockázat azonosítása esetén kezdeményezheti azok módosítását. Az informatikai szolgáltatónak, illetve a Társaságnak az audit végrehajtásához szükséges dokumentumokba betekintést kell nyújtania az auditot végrehajtó félnek.

A külső hálózat felől érkező támadásokkal szembeni védekezés hatékonyságát mind ügyviteli, mind technológiai rendszerek esetében sérülékenységvizsgálatok keretein belül vizsgálni kell az 5.23.2 pontban meghatározottak szerint.

5.12.2. Belső hálózat

A belső ügyviteli hálózat biztonságos működtetése az informatikai szolgáltató felelőssége, a technológiai hálózatok biztonságos üzemeltetése a Társaság feladata a társasági információbiztonsági felelős bevonásával.

A belső hálózatok működésére a következő információbiztonsági irányelvek vonatkoznak, legyen az ügyviteli vagy üzemviteli rendszer:

- A hálózati eszközöket védett helyiségben (pl. szerverszoba, technikai helység, stb.), illetve zárt rack szekrényekben kell elhelyezni, ahol illetéktelenek nem férhetnek hozzá, hozzáférési jogosultsággal ügyviteli eszközök esetén csak az informatikai szolgáltató, technológiai hálózat esetén a Társaság rendelkeznek.
- A hálózati eszközöket biztonságos módon kell konfigurálni és rendszeresen frissíteni, ezek megtörténte ügyviteli eszközök esetében az informatikai szolgáltató, technológiai eszközök esetében pedig a Társaság feladata és felelőssége, melyet mindkét esetben a társasági információbiztonsági felelős saját hatáskörben ellenőrizhet.
- Az ügyviteli informatikai belső hálózatra kizárólag az MVMI Informatika Zrt. tulajdonában álló eszközök csatlakoztathatók, illetve csak AD-ban regisztrált és engedélyezett felhasználók érhetik azt el.
- Az Üzemviteli rendszerek esetén első sorban a Társaság tulajdonában lévő eszközök csatlakoztathatóak, ettől eltérni indokolt esetben, a társasági információbiztonsági felelőssel együttműködve lehet. Ez dokumentáltan kell, hogy megtörténjen.
- Technológiai és ügyviteli hálózaton is port security szűrés vagy azt meghaladó/modernebb megoldás alkalmazása szükséges.
- Csak a szükséges hálózati végpontok kipatchelése engedélyezett (pl. külső felek által is elérhető helyeken).
- A belső hálózat szegmentálása szükséges információbiztonsági szempontból is, az egyes szegmensekben kockázatarányos védelmi intézkedések bevezetése (pl. IDS/IPS rendszer alkalmazása) szükséges.

Az ügyviteli belső hálózatra vonatkozó információbiztonsági követelményeket az informatikai szolgáltatónak rögzíti, illetve a szükséges mértékben tájékoztatja a társasági információbiztonsági felelőst az alkalmazott megoldásokról.

Az alkalmazott biztonsági megoldások auditja során az informatikai szolgáltatónak, illetve a Társaságnak betekintést kell nyújtania az audit végrehajtásához szükséges dokumentumokba az auditot végrehajtó fél számára.

A belső hálózat információbiztonsági megfelelőségét mind ügyviteli, mind technológiai rendszerek esetében sérülékenységvizsgálatok keretein belül vizsgálni kell az 5.23.2. pontban meghatározottak szerint.

5.12.3. Vezeték nélküli hálózat

Jelen alfejezetben általános szabályokat fogalmazunk meg mind a belső (informatikai szolgáltató által biztosított), mind a külső (otthoni vagy szabadon hozzáférhető) vezeték nélküli hálózatok esetén.

Belső, vezeték nélküli hálózatok

A Társaság vezeték nélküli (WiFi) hálózatot biztosíthat a belső informatikai szolgáltató által mind a munkavállalói, mind a telephelyein ideiglenesen dolgozó külső munkavállalók, partnerek számára.

Belső, vezeték nélküli hálózatok kialakítása csak az informatikai szolgáltató által létesítve lehetséges. A Társaság telephelyein munkavégzés céljából mobil WiFi hotspotokat, illetve egyéb külsőnek minősülő vezeték nélküli hálózatot kialakítani tilos! Kivételt képez ez alól a kizárólag a technológiai rendszerek működéséhez szükséges vezeték nélküli hálózatok létesítése, melyeket a belső vezeték nélküli hálózattal megegyező védelmi igényszintű hálózatként kell kezelni, és annak megfelelő védelmi intézkedéseket kell megvalósítani ezen hálózatok üzemeltetése során is.

A belső, vezeték nélküli hálózathoz az informatikai szolgáltató által biztosított Társasági laptopokkal, illetve Társasági mobileszköz-menedzsment rendszerbe léptetett okostelefonokkal és tabletekkel szabad csatlakozni.

A Társaság informatikai szolgáltatótól igénybe vett belső, vezeték nélküli hálózatának használatához kötött jogosultságokat a MOB-BSz17-M-11 melléklet tartalmazza.

A belső, vezeték nélküli hálózati elérést biztosító szolgáltatás működtetése, üzemeltetése, a rendszer felügyelete, illetve a felhasználók adminisztrálása, incidensek kezelése az informatikai szolgáltató feladata. A belső, vezeték nélküli hálózattal kapcsolatos információbiztonsági események monitorozása, minősítése és kezelése, valamint az ezekkel kapcsolatos elhárítási feladatokra való javaslattételek megtétele, esetleg az elhárítási feladatok elvégzése a társasági információbiztonsági felelős és a biztonsági szolgáltató feladata. Az informatikai szolgáltatónak belső eljárásrendben részletesen dokumentálnia és szabályoznia szükséges az általa üzemeltetett belső vezeték nélküli hálózatok működtetését, karbantartását, információbiztonsági kontrolljait, melybe a társasági információbiztonsági felelős felülvizsgálat során betekintést nyerhet.

A vezeték nélküli hálózatok rendszeres sérülékenységvizsgálata szükséges az 5.23. alfejezetben foglaltak szerint.

Külső, vezeték nélküli hálózatok

Külső helyszínen történő munkavégzés céljából indokolt lehet külső, nem az MVM Csoport informatikai szolgáltatója által üzemeltetett vezeték nélküli hálózatok elérése is. Tekintve azonban, hogy a külső vezeték nélküli hálózatok az informatikai szolgáltató által nem kontrollálhatók, szigorúbb előírások vonatkoznak használatukra felhasználói oldalon.

Külső, vezeték nélküli hálózatnak tekintendők az alábbiak:

- mobil Internet (SIM, USB stick, mobil WiFi modem, stb., még abban az esetben is, ha a Társaság bocsátja rendelkezésre)
- privát vezeték nélküli hálózat (otthoni vagy megbízható partner társaság WiFi hálózata)
- publikus vezeték nélküli hálózat (szálloda, kávézó, stb. által biztosított ingyenes vagy fizetős WiFi hálózat)

Munkavégzés céljából a publikus vezeték nélküli hálózatok (pl. szálloda, konferencia által biztosított) használata laptopok esetében tiltott (különösen kávézók, gyorséttermek, egyéb nagyobb forgalmú helyek), okostelefonok és tabletek esetében pedig tiltott. Utóbbi eszközök esetében a felhasználó munkakörének függvényében mobil internet előfizetés kerül aktiválásra, mely nem indokolja ismeretlen, idegen eredetű hálózatokhoz való csatlakozás szükségességét. Ismert mobil internet megosztásokhoz, illetve vezeték nélküli hálózathoz laptoppal a felhasználó csatlakozhat, publikus vezeték nélküli hálózatok használata helyett pedig igényelhet a távoli munkavégzés idejére mobil internet stick-et vagy modemet.

Távmunka esetén az otthoni routerre, wifi-re csak VPN-en (MVMI DirectAcces) kapcsolattal lehet.

A távmunka helyszínén kialakított internet elérésnek minimum az alábbi követelményeknek meg kell felelni:

- A router hozzáféréseihez tartozó jelszavak nem maradhatnak alapértelmezetten – azaz minden estetben, mind az SSID-hez tartozó jelszavát, mind az adminisztrátorhoz tartozó jelszavakat meg kell változtatni – a jelen Szabályzatban leírtaknak megfelelően
- Ezeket a jelszavakat nem adhatjuk meg másnak
- Legalább a WPA2-es titkosítást kell alkalmazni
- A router firmwerét rendszeresen frissíteni kell.

A biztonsági intézkedések elmulasztásáért, valamint nem megfelelő vezeték nélküli hálózatok használatából fakadó károkért a felhasználó az 5.6.3. pontban foglaltak szerint szankcionálható.

5.12.4. Távoli elérés

Annak érdekében, hogy a Társaság folyamatosan vagy ideiglenesen külső helyszínen is dolgozó munkavállalói is el tudják érni a Társaság által biztosított, munkavégzésükhöz szükséges belső hálózati erőforrásokat, távoli elérés engedélyezése szükséges számukra.

Távoli elérés engedélyezhető az alábbi feltételek teljesülése esetén:

- állandó munkaviszonnyal rendelkező munkavállaló esetében
- határozott idejű munkaviszonnyal rendelkező munkavállaló esetében a munkavégzés időtartamára
- junior szinten megfelelő, írásbeli indoklás mellékelésével
- olyan felhasználó számára, aki nem volt közvetlenül információbiztonsági incidens okozója

A távoli elérés engedélyezéséhez a közvetlen felettes, valamint a társasági információbiztonsági felelős hozzájárulása is szükséges.

A Társaság belső ügyviteli hálózatához kívülről kizárólag VPN kapcsolattal lehetséges a csatlakozás, Direct Access alkalmazásával az informatikai szolgáltató által biztosított laptopokon/notebookokon. Társasági VPN hozzáférés beállítása ettől eltérő (pl. saját) eszközön tilos.

A VPN csatlakozáson túl lehetőség van bizonyos rendszerek külső elérésére is. A külső hálózatról elérhető rendszerek (pl. OWA, Sharepoint site-ok) esetében kétfaktoros, erős authentikáció alkalmazása szükséges az 5.10.3 pontban meghatározottak szerint. Ezen rendszerek elérése szintén csak azon felhasználók számára engedélyezett, akik az előző pontban foglalt feltételeket teljesítik, illetve a közvetlen felettesük és a társasági információbiztonsági felelős jóváhagyta az igényt.

5.13. Vírusvédelem, rosszindulatú kódok elleni védelem

5.13.1. Ügyviteli rendszerek vírusvédelme

Ügyviteli rendszerek esetében vírusvédelmi és spam-szűrő szoftverként a Társaság az informatikai szolgáltató által központilag biztosított, az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció által jóváhagyott vírusvédelmi rendszert kell, hogy alkalmazza. Az informatikai szolgáltató által telepített vírusvédelem nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem használható.

A vírusvédelmi rendszerrel szemben támasztott főbb követelmények:

- központi menedzselhetőség biztosított legyen,
- a felhasználónak ne legyen lehetősége a beállítások módosítására, illetve a vírusvédelmi rendszer kikapcsolására,
- a munkaállomások vírusdefiníciós adatbázisa folyamatosan, automatikusan frissüljön (ne legyen 24 óránál régebbi),

- a munkaállomásokon az egyes fájlműveletek során folyamatos ellenőrzés történjen a vírusvédelmi rendszer által,
- a program minden héten legalább egyszer teljes körű vírusellenőrzést hajtson végre a belső háttértárolókon,
- laptopokon és notebookokon a frissítés és a tűzfal megfelelő beállításait a számítógép tartózkodási helye (hálózati állapota) alapján automatikusan koordinálja,
- a számítógépekre csatlakoztatott külső adathordozók (pendrive, külső merevlemez stb.) vizsgálatát a rendszernek kell automatikusan indítania és végrehajtania.
- viselkedésalapú elemzés és IPS/IDS funkciók biztosítására képes legyen.

A vírusvédelmi rendszer beállításait az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció információbiztonsági auditok keretein belül ellenőrizheti, az ehhez kapcsolódó adatszolgáltatást, illetve betekintési jogosultságot az informatikai szolgáltatónak biztosítania kell a kijelölt munkatársak számára.

Egyéb vírusvédelmi intézkedések az informatikai szolgáltató által:

- központilag tiltani kell a gyanús tartalmú, kártékony kódok terjesztésére alkalmas weboldalakat,
- központilag tiltani kell a futtatható állományok elektronikus levélben történő küldését és fogadását, utóbbi esetben a felhasználó csak értesítést kaphat az ilyen tartalmú levél érkezéséről,
- központilag tiltani kell a külső forrásból érkező makrós állományokat, az ilyen tartalmú melléklet érkezéséről a felhasználó csak tájékoztatást kaphat.

5.13.2. Technológiai rendszerek vírusvédelme

A technológiai rendszerek esetében, bár általában közvetlenül nem kerülnek a külső hálózatra, szintén szükséges, hogy megfelelő vírusvédelmi rendszerrel rendelkezzenek. Az alkalmazott vírusvédelmi rendszert a társasági információbiztonsági felelős szakmai szempontok szerint választja ki, a rendszer működtetése a Társaság felelőssége.

A technológiai területen alkalmazott vírusvédelmi rendszereknek meg kell felelniük az alábbi követelményeknek:

- tekintve, hogy a technológiai rendszerek elkülönülnek az ügyviteli rendszerektől és a külső hálózattól, ezért az alkalmazott vírusvédelmi rendszernek offline állapotban is frissíthetőnek kell lennie,
- az offline frissítést külön erre a célra biztosított, vírusmentes adathordozón kell biztosítani (pendrive, CD, DVD, stb.),
- a technológiai rendszereket futtató eszközök vírusdefiníciós adatbázisa a kapcsolódó kockázatelemzés eredménye alapján meghatározott gyakorisággal frissüljön,
- kerüljön dokumentálásra, hogy a vírusvédelmi rendszernek milyen gyakorisággal, milyen típusú ellenőrzéseket kell végrehajtania (különösen abban az esetben, ha valamilyen oknál fogva automatikus ellenőrzés nem lehetséges),
- a program minden héten legalább egyszer teljes körű vírusellenőrzést hajtson végre a belső háttértárolókon,
- a felhasználónak ne legyen lehetősége a beállítások módosítására, illetve a vírusvédelmi rendszer kikapcsolására.

Amennyiben a technológiai rendszerrel kapcsolatban külső közreműködők is érintettek, a velük kötött szerződésben külön ki kell térni a vírusvédelmi megoldásokra, illetve szabályokra.

A vírusvédelmi rendszer beállításainak auditálása során az adatszolgáltatást, illetve a betekintési jogosultságot biztosítani kell a kijelölt munkatársak számára.

5.13.3. Mobil eszközök vírusvédelme

Minden, a Társaság mobileszköz menedzsment rendszerébe léptetett eszközt központilag vírusvédelmi rendszerrel kell ellátni, amennyiben a készülék operációs rendszere azt lehetővé teszi. Az okos eszközökön alkalmazott vírusvédelmi megoldást az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció közreműködésével kell kiválasztani, mely terület a rendszerrel szemben támasztott biztonsági követelményeket meghatározza.

A mobil eszközökön alkalmazott vírusvédelmi rendszerrel szemben támasztott főbb követelmények:

- központi menedzselhetőség biztosított legyen,
- a felhasználónak ne legyen lehetősége a beállítások módosítására, illetve a vírusvédelmi rendszer kikapcsolására,
- az eszközökön a vírusdefiníciós adatbázis rendszeresen, automatikusan frissüljön.

A mobil eszközökön észlelt vírusgyanús eseményeket szintén az 5.17.2 pontban foglaltak szerint kell jelezni az illetékes területek felé.

5.13.4. Kártékony kódok kezelése

A kártékony kód rendszerbe jutását jelezheti a vírusvédelmi rendszer, de észlelheti a felhasználó is.

Amennyiben a felhasználó a vírusvédelmi rendszer riasztását, vagy a felsorolt gyanús eseteket tapasztalja, az 5.17. alfejezetben foglaltak szerint haladéktalanul jelentenie kell a tapasztaltakat.

Az informatikai szolgáltató, illetve a helyi üzemeltetés a MOB-BSz-17-FU-03 folyamatutasításban foglaltak szerint kell, hogy megkezdje az esemény vizsgálatát, illetve kezelését az alábbiak figyelembe vételével:

- Az üzemeltető jogosult a vírusveszély elhárításáig a vírusos számítógépet a hálózatról leválasztani, azon a munkavégzést megtiltani.
- Ha a vírusfertőzés pontos helye nem lokalizálható, az üzemeltetők jogosultak átmenetileg a hálózat egyes részeit, vagy a teljes hálózati elérhetőséget átmenetileg a vírusveszély elhárításáig izolálni, leválasztani.
- Az üzemeltetés az 5.17.3 pontban foglaltak szerint köteles bevonni a biztonsági szolgáltatót az esemény kivizsgálásába, de a kártékony kód vizsgálatába opcionálisan bármikor bevonhatja a biztonsági szolgáltatót.

A fertőzés elhárítását követően az informatikai szolgáltatónak vagy a Társaság informatikai üzemeltetésnek és a társasági információbiztonsági felelősnek haladéktalanul meg kell tenniük a későbbi ismételt fertőzés megelőzésére szolgáló védelmi intézkedéseket, valamint a szükséges és elégséges mértékben tájékoztatniuk kell a felhasználókat az 5.17.4 pontban foglaltak szerint.

A Társaságnál észlelt, információbiztonsággal kapcsolatos, gyanús eseteket legalább az informaciobiztonsag@mvm.hu címen kell bejelenteni.

5.14. Elektronikus kommunikáció

Jelen Szabályzat az elektronikus kommunikáció alábbi, a Társaságon belül elérhető eszközeire vonatkozóan tartalmaz előírásokat:

- Elektronikus levelezés
- Internet
- Azonnali üzenetküldő alkalmazások
- Videokonferencia

- Fájlmegosztó alkalmazások

Ezen alkalmazások használata kizárólag a jogi követelményeknek megfelelően, a Társaság előírásait és korlátozásait betartva, biztonsági, illetve hálózat menedzsment célú monitoring megvalósulása mellett megengedett az alábbiakban foglaltak szerint.

A jelen Szabályzatban ismertetett szolgáltatások csak belső, csoportszintű szolgáltatótól vehetők igénybe. Amennyiben a Társaságnak a felsoroltakon kívüli, más jellegű elektronikus kommunikációs szolgáltatásra van igénye, az informatikai szolgáltató felé kell jeleznie azt, aki az 5.9. alfejezetben meghatározottak szerint jár el.

Külső, szabadon hozzáférhető kommunikációs megoldások (pl. alternatív üzenetküldő szolgáltatások) munkavégzés céljából való használata szigorúan tilos!

5.14.1. Elektronikus levelezés

A Társaság az elektronikus levelezési szolgáltatást csak és kizárólag munkavégzés céljából, a munkaköri leírásban, illetve szerződésben rögzített feladatok hatékonyabb ellátásának érdekében biztosítja a munkavállalók, illetve szerződéses külső felek számára. Az elektronikus postafiók igénylésére az 5.5. alfejezetben foglaltak szerint van lehetőség. Az elektronikus levelezés használatára a következő információbiztonsági szabályozások vonatkoznak.

Általános alapelvek:

- A Társaság által a felhasználó rendelkezésére bocsátott e-mail cím a Társaság tulajdona, ebből kifolyólag a levelező rendszert magán célra és egyéb, a munkavégzéssel nem összefüggő célokra használni tilos.
- Az elektronikus levelezés használati engedélye személyre szóló, azt kizárólag a felhasználó saját maga veheti igénybe.
- A felhasználó saját azonosítójának és jelszavának átadása más felhasználó részére tilos.
- A munkahelyi e-mail címmel magánjellegű regisztrációt tenni különböző szabadon hozzáférhető, nem a munkavégzés céljával összeegyeztethető weboldalakon tilos.
- A külső levelezőrendszerek (pl. freemail.hu, gmail.com) használata munkavégzéssel összefüggő célból szigorúan tilos.
- Az elektronikus levelezőkliensekbe privát, külső szolgáltatók (pl. freemail.hu, gmail.com) fiókjának felcsatolása tilos.
- Privát tulajdonú IT és ICT eszközökre a Társaság levelezést beállítani szigorúan tilos.
- A felhasználó elektronikus levelezésébe az incidensek kezelésének folyamatában a társasági információbiztonsági felelős, valamint az MVM Zrt. Csoportszintű Biztonsági Igazgatósága által kijelölt személy betekintést nyerhet az informatikai szolgáltatóval együttműködve.

Az e-mailek küldésére vonatkozó előírások:

- A feladó felelős az általa küldött e-mail tartalmáért információbiztonsági szempontból is.
- Más felhasználó nevében e-mailt küldeni tilos, kivéve a rendszerbeli meghatalmazási eljárás alkalmazásán keresztül (pl. asszisztens).
- Az egyes levelek mérete belső, illetve külső levél küldése esetén csatolt melléklettel együtt is korlátozott méretű lehet.
- A rendszer a törölt elemeket meghatározott napig tárolja, utána véglegesen törlődnek a levelező rendszerből.
- A leveleket mindig célzottan kell kiküldeni, a címzettek számosságára és megjelenítésére vonatkozó korlátozások figyelembe vételével (egy levélben a címzettek száma nem

haladhatja meg a maximálisan megengedett darabot – erről az informatikai szolgáltató ad tájékoztatást).

- Automatikus válaszüzenetek tartalmát minden esetben úgy kell meghatározni, hogy a benne megadott információkkal rosszindulatú fél ne tudjon visszaélni.
- A Társaság levelezőrendszerében tiltott a lánclevelezés, a kéretlen levelek (spam), valamint az indokolatlan mértékű magáncélú tartalmak küldése.
- A Társaság levelezőrendszerében csatolt állományként nem küldhetők és fogadhatóak a végrehajtható/futtatható állományok (pl. *.exe;*.bin; *bat; *.com; *.app; *.vb; *.vbs; *.js; *jar; *.ill; *.dll; *.dat fájltípusok), illetve makrós állományok. A rendszer a fentiekben felsorolt csatolmánnyal rendelkező leveleket csatolmány nélkül kell, hogy küldje el a címzett(ek)nek.
- Nagyméretű fájlok küldése esetén az informatikai szolgáltató által biztosított fájlküldő megoldás használata szükséges. Külső forrásból elérhető, hasonló jellegű oldalakra (pl. mammutmail, wetransfer, stb.), illetve fájlmegosztó portálokra (pl. Dropbox, GoogleDrive, stb.) társasági szintű adatok, fájlok feltöltése szigorúan tilos. Ezen felületeken csak állományok fogadása lehetséges indokolt esetben!
- A bizalmas, érzékeny adatokat, információkat a tömörítés során jelszóval kell ellátni a Társaság által kijelölt alkalmazás segítségével és levél csatolmányaként elküldeni az 5.11. alfejezetben foglaltak szerint.

Az e-mailek fogadására vonatkozó irányelvek

- Bizalmas információk továbbítását kérő elektronikus levelek esetében mindig meg kell győződni az információkérés hitelességéről.
- Ismeretlen, gyanús feladótól érkezett csatolmányok, linkek megnyitása tilos! Kérdéses tartalmak megnyitása esetén a felhasználónak a társasági információbiztonsági felelőshöz vagy az informatikai szolgáltató Helpdesk-jéhez kell fordulnia.
- Téves címzés miatt kapott e-mailt, annak felismerése után a felhasználónak haladéktalanul jeleznie kell a feladó felé, és a levél tartalmának (további) olvasása nélkül törölni kell. Az abban lévő tartalmak, információk, adatok jogtalan megismerése és kezelése tilos.
- Külső vagy belső e-mail címről érkező, félrevezető tartalmú, feltehetően ártó szándékú e-mailek esetén azonnal jelenteni kell az eseményt az 5.17.2 pontban foglaltak szerint.

Távoli elérés szabályai

- A felhasználóknak lehetőségük van a levelezési szolgáltatás távoli, Társaságon kívüli elérésére is az Outlook Web Access (továbbiakban: OWA) szolgáltatáson keresztül. A távoli elérés részletes szabályait az 5.12.4 pont tartalmazza.
- Az OWA felületén keresztüli levelezés esetében is a fenti szabályok érvényesek. Kiemelten fontos azonban az 5.12.4 pontban rögzített, külső helyszínen való munkavégzés szabályainak betartása.
- A társasági levelezés a Társaság által a munkavállaló rendelkezésére bocsátott mobilkészülékről is elérhető, az 5.15.3 pontban leírtak szerint.

5.14.2. Internet használat

A Társaság az Internet használatot elsősorban munkavégzés céljából, a munkaköri feladatok hatékonyabb ellátásának érdekében biztosítja. A szolgáltatás magán célra és egyéb, a munkavégzéssel nem összefüggő célokra történő felhasználása nem engedélyezett.

Internet hozzáférés igénylésére az 5.5. alfejezetben foglaltak szerint van lehetőség. A hozzáférést a közvetlen felettesnek kell engedélyeznie.

Az Internet elérés minden felhasználó esetében korlátozva van, az informatikai szolgáltató által tiltott oldalak nem elérhetők. A tiltott oldalak listáját a MOB-BSz-17-M-12 melléklet tartalmazza.

Amennyiben a felhasználónak a munkájához szüksége van egy, az informatikai szolgáltató által korlátozott oldal használatára, felettese, illetve a társasági információbiztonsági felelős hozzájárulását követően az informatikai szolgáltató HelpDesk-jéhez fordulhat a korlátozás feloldásáért.

A tiltott internetes oldalak listája évente felülvizsgálatra kerül az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció által a társasági információbiztonsági felelős javaslatai alapján.

Az Internet használat során betartandó információbiztonsági előírások

- Az Internet használati engedély személyre szóló, azt kizárólag a felhasználó saját maga veheti igénybe.
- A kliens számítógépen proxy, VPN, és egyéb anonimizálásra szolgáló alkalmazások (Pl. Tor Browser) futtatása tilos.
- A felhasználó internet-hozzáférésének más felhasználók részére nem központi módon történő megosztása vagy tovább szolgáltatása tilos.
- A hálózati sávszélesség és erőforrások szükségesnél nagyobb, túlzott foglalása (pl. nagyméretű állományok indokolatlan letöltése) tilos. Az előírás megszegése esetén a felhasználó felettesét és a társasági információbiztonsági felelőst értesíti a szolgáltató, további intézkedés céljából.
- Tilos a Társasághoz, vagy harmadik félhez kötődő kereskedelmi szoftverek, valamint jogvédett tartalmak feltöltése, letöltése, illetve továbbítása Internetes oldalakon.
- A munkatársaknak tilos az Internetről szoftverek letöltése, futtatása. Amennyiben a felhasználónak valamilyen programra igénye merül fel, az informatikai szolgáltató felé kell jeleznie azt.
- Tilos a gyanús tartalmakra kattintás, ismeretlen felugró ablakok engedélyezése. Amennyiben a felhasználó valamiben nem lenne biztos, az informatikai szolgáltató HelpDesk-jéhez, vagy a társasági információbiztonsági felelőshöz kell segítségért fordulnia.
- Az Internet használat szabályainak egyértelmű megsértéséből származó károkért a felhasználó az 5.6.3 pontban meghatározottak szerint szankcionálható.

5.14.3. Azonnali üzenetküldő alkalmazások

A Társaságon, illetve a vállalatcsoporton belüli azonnali üzenetküldés céljából az informatikai szolgáltató által központilag biztosított alkalmazás használható, más külső forrásból elérhető szolgáltatás (pl. Viber, Facebook messenger, stb.) igénybevétele munkavégzéshez nem engedélyezett.

Az informatikai szolgáltató által biztosított csevegő alkalmazás elsősorban az MVM Csoporton belüli kommunikációra szolgál, de a partnerlistára külső felek felvétele is lehetséges előzetes engedélyezést követően. Előzetes engedélyt az igénylő közvetlen felettese adja meg és továbbítja végső engedélyezésre a társasági információbiztonsági felelősnek. (D-07).

Az alkalmazás esetében az adattovábbítási szabályok, használatára vonatkozó követelmények és biztonsági előírások megegyeznek az elektronikus levelezésre vonatkozó előírásokkal.

5.14.4. Videokonferencia

A Társaság lehetőséget biztosít videokonferencia eszköz igénybe vételére az erre a célra kijelölt tárgyalókban. A videokonferencia eszközökön elérhető kommunikációs lehetőségekről, így az informatikai szolgáltató által biztosított csevegő-, illetve bármely egyéb, azonnali üzenetküldő alkalmazás használhatóságáról a videokonferencia szolgáltatáshoz kapcsolódó felhasználói

tájékoztató ad részletes felvilágosítást. A Társaság az informatikai szolgáltató által biztosított vonalat használhatja. Videokonferencia hívások lebonyolítására kizárólag az informatikai szolgáltató által biztosított eszközök használhatóak a támogatott azonnali üzenetküldő alkalmazások lehetőségei mellett. Tilos a külső szolgáltatók által nyújtott eszközök (pl. nem az MVMI által üzemeltetett) használata munkavégzés céljából.

A videokonferencia szolgáltatás igénybevételének esetén az adattovábbítási szabályok használatára vonatkozó követelmények és biztonsági előírások megegyeznek az elektronikus levelezésre vonatkozó előírásokkal.

5.14.5. Fájlmegosztó alkalmazások

A külső fájlmegosztó alkalmazások esetében csak fájlok fogadása engedélyezett, a feltöltés viszont szigorúan tilos és technológiailag is tiltott kell, hogy legyen (amennyiben a rendszer lehetővé teszi).

A belső fájlmegosztó szolgáltatás esetében a szolgáltatást az informatikai szolgáltatónak kell biztosítania a következő információbiztonsági követelmények figyelembe vételével:

- titkosított adatátvitel,
- csak a címzett tudja letölteni a küldött fájt (pl. SMS kód küldés automatikusan),
- letöltések száma korlátozható legyen a küldő által, de az alapértelmezett érték 1,
- letöltés határideje korlátozható legyen a küldő által,
- naplózás (küldő, címzett, küldés és letöltés időpontja, adattartalom, letöltési IP cím).

5.15. Mobil eszközök használata

A Társaságnak a felhasználók munkavégzésének könnyítése és rugalmasabbá tétele végett, valamint hatékonyabbá tétele érdekében lehetősége van a munkavállalók számára mobil eszközök biztosítására. A munkavégzés céljára csak a Társaság tulajdonában álló eszköz biztosítható, melyen elsősorban a munkavégzéshez szükséges, vagy szervesen ahhoz tartozó adatok tárolhatók. Amennyiben a munkavállaló magánjellegű adatokat tárolna a mobil eszközön, azok kompromittálódása, elvesztése esetén semmilyen kártérítési igénnyel nem élhet, a Társaság eszközén tárolt privát jellegű adatokért a Társaság és az informatikai szolgáltató semmilyen felelősséget nem vállal.

Jelen szabályozás érvényes a Társaság által a felhasználók számára, munkavégzéshez biztosított minden hordozható számítógépre, illetve telekommunikációs eszközre, amelyek a hordozható számítógépekkel azonos adattárolási, adatkezelési és adatmegjelenítési funkciókkal bírnak (laptop, notebook, tablet, okostelefon, stb.), valamint a hordozható adattárolókra (külső merevlemez, pendrive, stb.).

Az informatikai szolgáltatónak a mobil eszközök biztonságos használatának megteremtése érdekében központi irányítási és kontroll funkciókat biztosító mobil eszköz menedzsment megoldást kell alkalmaznia, mely lehetővé teszi

- a mobilitási szolgáltatások központi monitoringját és kontrollját,
- az IT biztonsági protokollok kikényszerítésének biztosítását,
- az IT mobil eszköz menedzsment megalapozását, eszközök távoli elérését, törlését és esetleges nyomon követhetőségét,
- a készülék szintű információbiztonság érvényesítését,
- a tömeges készülék konfiguráció támogatását.

A mobil eszköz menedzsment rendszer alkalmazása kizárólag a Társaság által biztosított, illetve a társasági információbiztonsági felelős által jóváhagyott eszközökre terjed ki, munkavégzés csak ezen eszközökön engedélyezett, ezeken az eszközökön a felhasználók ügyviteli informatikai szolgáltatásokat vehetnek igénybe. A privát, saját tulajdonú eszközök munka céljából való

használata sem ügyviteli, sem technológiai rendszerek esetében sem engedélyezett, és mind adminisztratív módon, mind technikailag is tiltott kell, hogy legyen.

Az alábbiakban az egyes mobil eszközök használatára vonatkozó előírások kerülnek rögzítésre eszközönkénti bontásban.

5.15.1. Laptop/notebook használatával kapcsolatos információbiztonsági követelmények

Kiadás

- Az eszközök belépéskori átvételéről, illetve kilépéskori leadásáról a felhasználónak átadás-átvételi nyilatkozaton, illetve a „sétáló papíron" kell írásban nyilatkoznia.
- A felhasználóknak kiadott laptopok/notebookok teljes merevlemez titkosítását biztosítani kell ügyviteli eszközök esetében az informatikai szolgáltató által.
- A felhasználók a Társaság hálózatához távolról csakis VPN megoldás alkalmazásával csatlakozhatnak az 5.12.4 pontban meghatározottak szerint, ennek hiányában a hálózati alkalmazások nem érhetőek el (kivéve a kétfaktoros authentikációval, bármilyen eszközről elérhető alkalmazások).

Használat

- A laptopok/notebookok használatának felhasználókra vonatkozó szabályai a jelen pontban foglalt kiegészítésekkel megegyeznek a munkaállomások általános használati szabályaival.
- Az informatikai szolgáltató, illetve a Társaság tulajdonát képező laptopokat/notebookokat a munkavállaló hazaviheti, vagy a munkaidő lejártával bent hagyhatja az irodában a következő feltételekkel:
  - Munkaidőn kívül a laptopokat/notebookokat zárt szekrényben vagy bezárt irodában kell elhelyezni.
  - A laptopok/notebookok őrizetlenül hagyása még zárt autóban is kerülendő. Amennyiben ez nem megoldható, az eszközt nem látható helyre kell helyezni. Az autóban őrizetlenül hagyott eszköz ellopása esetén a felelősség és a kár megtérítése a munkavállalót terheli az 5.6.3. pontban meghatározott szankciók szerint. A laptopokat/notebookokat bekapcsolt állapotban szállítani tilos.
  - A laptopot/notebookot a munkavállaló őrizetlenül csak a saját lakhelyén belül hagyhatja, de ott is csak kikapcsolt vagy zárolt állapotban.
- Külföldi kiküldetés esetén a munkavállaló által kivinni kívánt eszközöket, illetve adatokat a társasági információbiztonsági felelőssel egyeztetni szükséges, indokolt esetben az általa meghatározott külön informatikai eszközök biztosítása szükséges a kiküldetés időtartamára.
- Az eszköz eltulajdonítása, rongálódása esetén – amennyiben a káresemény bizonyíthatóan a felhasználó nem megfelelő kezeléséből adódóan keletkezett – a munkavállaló az 5.6.3. pontban foglaltak szerint szankcionálható.

Karbantartás

- Az informatikai szolgáltató által biztosított laptopok/notebookok esetében a felhasználónak karbantartási feladata nincsen, a szükséges hardveres és szoftveres karbantartást az informatikai szolgáltató végzi. Technológiai rendszerekhez kapcsolódó eszközök esetén a helyi szabályzatban kell meghatározni az üzemeltetési feladatokat.
- Indokolt esetben szükség lehet a titkosított merevlemez visszafejtésére (pl. meghibásodás következtében). A visszafejtési folyamat csak társasági információbiztonsági felelős jóváhagyásával történhet, elvégzésére csak az informatikai szolgáltató, a biztonsági szolgáltató és az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció jogosult.

- Az eszköz felhasználója az eszköz meghibásodását minden esetben jelenteni köteles az informatikai szolgáltató felé az 5.17. alfejezetben meghatározottak szerint. Az informatikai szolgáltató átveszi az eszközt javításra, szükség esetén csereeszközt biztosít. Az átadásról átadás-átvételi nyilatkozat kell, hogy aláírásra kerüljön. Amennyiben a meghibásodás az eszköz nem rendeltetésszerű használatából fakad, a felhasználó az 5.6.3. pontban foglaltak szerint szankcionálható.

Leadás, rendszerből való kivonás

- A munkavállaló kilépési szándékáról a Társaság informatikai szakterülete és a társasági információbiztonsági felelős értesítést kapnak a Társaság részére humán erőforrás szolgáltatást nyújtó szakterület felől. Az értesítést követően az informatikai terület munkatársa ellenőrzi, hogy a kilépő munkavállalónak milyen eszközöket szükséges visszaszolgáltatnia és erről értesíti a munkavállalót, a társasági információbiztonsági felelős pedig indokolt esetben ellenőrzi, hogy a kilépő felhasználó esetében szükség van-e információbiztonsági ellenőrzésre, felmerült-e valamilyen információbiztonsági incidens gyanúja.
- Amennyiben információbiztonsági incidens gyanúja merül fel, az eszköz a helyreállíthatatlan törlés előtt lefoglalható a társasági információbiztonsági felelős által, aki kivizsgálja az eseményt, szükség esetén a biztonsági szolgáltató bevonásával.
- Az eszköz leadásáról átadás-átvételi nyilatkozat készül, illetve az a „sétáló papíron" is rögzítésre kerül.
- A leadott eszközön – amennyiben biztonsági incidens gyanúja nem áll fenn – az informatikai szolgáltató munkatársa leellenőrzi, elvégzi a szükséges frissítéseket és a karbantartási munkákat annak érdekében, hogy a készülék készen álljon egy újabb munkavállalónak történő átadásra.
- Leselejtezett eszközök esetében munkavállalói értékesítés előtt mindenképpen szükséges az eszközön levő adatok visszaállíthatatlan törlésének megvalósítása a biztonsági szolgáltató által.

5.15.2. Hordozható adattárolók kezelésének információbiztonsági szabályai

A Társaságnak lehetősége van hordozható adattárolók, USB, vagy egyéb, szabályzatban engedélyezett interfészen keresztül csatlakoztatott adathordozók (pl. pendrive, külső merevlemez, stb.) használatára, amennyiben adatot a Társaságon belül, Társaságon kívüli helyszínre, vagy külső félnek szükséges továbbítani és a továbbítás módja más biztonságos módon nem megoldható, valamint az adat biztonsági osztályba sorolása megköveteli a titkosított módon történő szállítást.

Munkavégzés céljából csak a Társaság által biztosított, a következő információbiztonsági feltételeket teljesítő titkosított adathordozók használhatóak:

- az eszköz az alkalmazott végpont védelmi rendszerrel, illetve egyéb vírusvédelmi megoldásokkal tudjon együttműködni, egyedileg beazonosítható legyen az adathordozó
- az eszköz hardveres titkosítást biztosítson
- a titkosítás legalább AES 256 bit-es legyen
- kikényszeríthető legyen a jelszó előírásoknak megfelelő jelszó vagy számkódos eszköz esetén legalább 6 karakteres kódot kérjen az eszköz
- 10 hibás jelszóbeütést követően automatikusan törölje az adathordozó tartalmát
- az eszköz az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció által jóváhagyásra kerüljön

A Társaságnak törekednie kell az ügyviteli rendszerek esetében dedikált USB adathordozó használatára. A dedikált USB eszköz a Társaság tulajdonát képezi. Az eszközzel kapcsolatos

információbiztonsági esemény és incidenskezelés esetén a biztonsági szolgáltató is bevonásra kerülhet az esemény vagy incidens típusától függően.

Dedikált USB bevezetése esetén, a munkaállomásokon az USB porton keresztül csatlakoztatott nem dedikált USB eszközöket a rendszer csak olvasható (read-only) módban ismerhet fel a töltési funkció ellátása mellett.

Technológiai rendszerek esetében az ügyviteli hálózaton alkalmazott dedikált USB eszközök használata opcionális, ezen rendszerek esetében elsősorban adminisztratív úton kell kikényszeríteni, hogy a technológiai rendszerekhez csatlakoztatott adathordozók más, nem közvetlenül a munkához kapcsolódó eszközhöz ne kerüljenek csatlakoztatásra.

Mind a titkosított, mind a dedikált eszközök kezelésének előírásait az alábbiak tartalmazzák.

Kiadás

- Technológiai rendszerek esetében a helyi üzemeltetés saját hatáskörben szerezheti be az eszközöket.
- Ügyviteli rendszerek esetében adattároló eszközt igényelni állandó használatra a szervezeti egység vezetője tud magának és munkatársai részére is a beszerzésért felelős
- Dedikált USB adattároló eszközt próbaidős munkavállaló csak a közvetlen felettese és a társasági információbiztonsági felelős hozzájárulásával kaphat.

Használat

- Amennyiben az eszköz kóddal vagy jelszóval rendelkezik, be kell tartani az 5.10.3 pontban foglalt jelszóképzési szabályokat.
- A használaton kívüli eszközt minden esetben elzárt helyen, zárható szekrényben kell tárolni, amelyhez a hozzáférési jogosultság korlátozott.
- Saját tulajdonban álló adattároló eszközön üzleti, technológiai adatok tárolása szigorúan tilos.
- Az informatikai szolgáltató, illetve a Társaság által biztosított hordozható eszközökön semmilyen illegális szoftver vagy fájl (pl. zene, kép, film, stb.) nem tárolható, továbbá a magáncélú használata nem engedélyezett.
- Az informatikai szolgáltató, illetve a Társaság által biztosított hordozható eszközök eltulajdonítása, rongálódása esetén a munkavállaló az 5.6.3 pontban foglaltak szerint szankcionálható, amennyiben a káresemény egyértelműen a felhasználónak felróható módon következett be.

Karbantartás

- A felhasználó számára kiadott eszközök felhasználói szintű karbantartása (pl. munkához szükséges törlés) az eszközt használó munkatárs feladata.

Leadás, rendszerből való kivonás

- A javíthatatlanul meghibásodott hordozható eszközöket át kell adni a biztonsági szolgáltatónak, aki gondoskodik a megsemmisítésről. Az eszköz átvételéről átadás-átvételi nyilatkozat készül.
- A leselejtezendő, használaton kívüli vagy javítható módon meghibásodott adathordozó eszközökről az adatokat az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció által jóváhagyott, nem visszaállítható módon kell törölni. A speciális törlést a biztonsági szolgáltató végzi, a társasági információbiztonsági felelős bármikor jogosult szúrópróba szerűen ellenőrizni. Az előírásoknak megfelelő adatmegsemmisítésről jegyzőkönyv készül, melyet a biztonsági szolgáltató dokumentál és tárol.

- Állandó használatú eszköz a munkavállaló kilépésekor történő leadásáról átadás-átvételi nyilatkozat készül, illetve a „sétáló papíron" is rögzítésre kerül. Az eszközzel az előző pontban foglaltak szerint kell eljárni
- Amennyiben incidens gyanúja merül fel, az eszköz a felhasználó általi törlés előtt lefoglalható a társasági információbiztonsági felelős által.

5.15.3. Mobiltelefon, okostelefon, tablet használatának információbiztonsági szabályai

A Társaság munkavállalói részére biztosíthat mobil-, illetve okostelefonokat, valamint tableteket, amennyiben munkavégzésükhöz ilyen jellegű eszközök szükségesek.

Az okostelefonok és tabletek esetén biztosítani kell a központi menedzselhetőséget a Társaság mobileszköz-menedzsment rendszerének bevezetésével, ügyviteli informatikai szolgáltatások igénybevételének előfeltétele ezen eszközökön a Társaság mobileszköz-menedzsment megoldásának telepítése a készülékekre.

A Társaság mobileszköz-menedzsment rendszerének biztosítania kell a következőket:

- ki kell kényszerítenie az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció által meghatározott beállítások (pl. jelszó, titkosítás, automatikus képernyőzár, korlátozások) automatikus végrehajtását,
- ki kell kényszerítenie az erre alkalmas operációs rendszerrel rendelkező eszközök esetén vírusvédelmi szoftver alkalmazását és naprakészen tartását,
- automatikusan kell, hogy érzékelje a regisztrált mobil eszköz kompromittációját és letiltsa az eszköz csatlakozását a belső hálózathoz (pl.: jailbreakelt, rootolt eszköz),
- az eszközön tárolt adatok távoli törlését.

A mobileszköz-menedzsment rendszer bevezetéséig a Társaságnak adminisztratív módon kell kikényszerítenie a mobil eszközök biztonságos használatát.

A Társaság elektronikus levelezését, illetve a Társaság alkalmazásait és a belső hálózat elérését biztosító WiFi hálózat csak a Társaság által biztosított, központilag menedzselt eszközön állítható be, illetve a Társaság mobileszköz-menedzsment rendszere esetén technológiailag is korlátozott kell, hogy legyen. A jelen fejezetbe sorolt mobil eszközök és a szerverek közötti adatkommunikáció kizárólag biztonságos, titkosított csatornán történhet. A Társaság belső hálózatára történő csatlakozás során szükséges a kapcsolódási lehetőséget engedélyezett eszközökre korlátozni és a megfelelő alhálózathoz rendelni, illetve a nem megfelelő eszközökről a belső hálózatban lévő szerverekhez, valamint a mobil eszköz menedzsment rendszerhez történő hozzáférést korlátozni.

Kiadás

- Okostelefonok és tabletek esetében kötelező az eszköz gyárilag támogatott titkosítása. Jelen Szabályzat előírása szerint speciális titkosítási eljárás nem indokolt, a készülék által biztosított megoldás alkalmazandó.
- Okostelefonok és tabletek esetében – a központi mobil eszköz menedzsment rendszer bevezetését követően – a Társaság adatai kizárólag azon keresztül érhetők el. Ezeken az eszközökön kötelező a Társaság mobileszköz-menedzsment rendszer használatának beállítása.
- Az eszközön tárolt adatokhoz történő jogosulatlan hozzáférés megakadályozása céljából a Társaság adatainak elérését biztosító domain autentikáción túl a mobil eszközök további hozzáférési védelemmel – legalább egy 4 számjegyű kód megadásának kikényszerítésével – kell, hogy kerüljenek ellátásra.
- Az e-mail kliens beállítása csak a Társaság által biztosított készüléken engedélyezett. Az elektronikus levelezés mobil eszközön való elérését az informatikai szolgáltató indokolt

esetben letilthatja. Ezt követően a levelek fogadására és küldésére okostelefonon és tableten keresztül csak szabályozott keretek között van lehetőség.

- Saját eszközön a társasági levelezést beállítani és használni szigorúan tilos, valamint az MVM mobileszköz-menedzsment rendszerének bevezetésével technológiailag is tiltott kell, hogy legyen.
- A felhasználó számára kiadott eszközökről naprakész nyilvántartást kell vezetni. Az átadás-átvételről jegyzőkönyv készül, mely tartalmazza a mobil eszközök használatára vonatkozó előírások tudomásul vételéről és betartásáról szóló nyilatkozatot is.

Használat

- A Társaság mobileszköz-menedzsment rendszerének bevezetéséig a felhasználó felelőssége, hogy az eszközön megfelelően megválasztott számzár-kódot, illetve lehetőség szerint ujjlenyomat vagy egyéb biometrikus azonosítást állítson be. (A rendszer bevezetését követően – a korábban rögzítettek szerint – a rendszernek automatikusan ki kell kényszerítenie a központilag meghatározott feloldási formát.) Az alkalmazott kódra vonatkozó információbiztonsági követelmények a következők:
  - nem lehet egyszerű, egymás után következő, illetve ismétlődő számsorozat (pl. 0000, 1234)
  - nem lehet szorosan a felhasználó személyéhez kapcsolódó szám (pl. születési dátum, társasági törzsszám)
  - amennyiben lehetséges, válasszunk minél hosszabb számzárkódot
  - kerüljük a számzárkód felírását, különösképpen könnyen hozzáférhető helyen való tárolását
- A Társaság mobileszköz-menedzsment rendszerének bevezetéséig a felhasználónak kötelessége gondoskodnia arról, hogy a rendelkezésére bocsátott készülék biztonsági frissítései alkalmazás és operációs rendszer szinten is megtörténjenek (azaz nem tilthatja az automatikus frissítések megtörténtét). (A rendszer bevezetését követően – a korábban leírtak szerint – a rendszer automatikusan kikényszeríti a frissítések telepítését, a felhasználónak ezt megakadályoznia tilos.)
- Az okostelefonokon és tableteken is érvényesek az alkalmazások telepítésére, illetve az elektronikus levelezés szabályaira vonatkozó előírások.
- A Társaság által biztosított eszközökön – a Társaság mobileszköz-menedzsment rendszerének bevezetésének hiányában – kerülendő a magánjellegű alkalmazások használata, nem a munkamenethez szükséges, indokolatlan vagy kifogásolható fájlok tárolása, az azokból származó esetleges károk szankcionálhatók az 5.6.3. pontban rögzítettek szerint.
- A mobileszközre telepíthető alkalmazások listája korlátozásra kerülhet (a felhasználó előzetes tájékoztatása, de nem azonnali értesítése mellett), valamint a felhasználói alkalmazás jogosultságokat üzem közben is ellenőrizésre kerülhetnek.
- Amennyiben az eszközről eseti biztonsági mentés készítése szükséges (pl. szervizbe szállítás miatt), a biztonsági szolgáltató tudja elkészíteni a mentést, illetve a visszatöltést.
- Amennyiben az eszközön adatvisszaállítás szükséges, szintén a biztonsági szolgáltató tudja megcsinálni az ehhez szükséges mentést.
- A készüléket tilos nyilvános helyen felügyelet nélkül, látható helyen hagyni, növelve az eltulajdonítás kockázatát.
- A készülékbe tilos magántulajdonú SIM kártyát helyezni.
- Be kell állítani, hogy harminc (30) másodperc tétlenséget követően a mobil készülékek képernyőjének zárolása automatikusan megtörténjen.

- Készülék eltulajdonítása esetén jelen Szabályzat 5.17. alfejezetében leírtak szerint kell eljárni.
- A készülék elvesztésének bejelentését követően, a Társaság mobileszköz-menedzsment rendszerének hiányában az OWA-n keresztül az eszköz távoli törlése (amennyiben lehetséges), illetve azonnali jelszóváltoztatás szükséges a felhasználó által. A Társaság mobileszköz-menedzsment rendszer alkalmazása esetén pedig az informatikai szolgáltató munkatársa – amennyiben az eszköz nyomkövetése nem lehetséges, vagy nem indokolt – távolról azonnal letiltja a jelentett készüléket és távolról törli a Társaság konténer tartalmát/visszaállítja a gyári beállításokat. Amennyiben az eszköz nyomkövetése engedélyezett, a bejelentést követően előzetesen megkísérlésre kerül az eszköz lokációjának azonosítása. Egyéb, az eszközzel kapcsolatos incidensek kivizsgálásába és kezelésébe a biztonsági szolgáltató bevonása szükséges.
- Az eszközök elvesztése, eltulajdonítása, rongálódása esetén a munkavállaló az 5.6.3. pontban foglaltak szerint szankcionálható, amennyiben a káresemény a felhasználónak felróható módon történt a károkozás, illetve annak információbiztonsági relevanciája van.

Leadás, rendszerből való kivonás

- A Társaságtól távozó munkavállalónak a kilépés napján, vagy mobil eszköz csere esetén le kell adnia a céges mobiltelefonját/tabletjét.
- Az eszköz leadásáról átadás-átvételi nyilatkozat kell, hogy készüljön, illetve annak a „sétáló papíron" is rögzítésre kell kerülnie.
- A leadott készüléket a biztonsági szolgáltató munkatársai veszik át a felhasználótól vagy az illetékes szakterülettől, akik gondoskodnak az eszköz visszaállíthatatlan törléséről, szükség esetén image-eléséről, valamint a készülék állapotától függően felkészítik azt a következő felhasználó számára.
- Az eszközön tárolt esetleges magánjellegű információk (kontaktok, képek, alkalmazások, stb.) eltávolítása a felhasználó feladata és felelőssége. Sem a biztonsági szolgáltatónak, sem az informatikai szolgáltatónak nem kötelessége az eszközön tárolt adatok kimentése a felhasználó számára. Továbbá a felhasználó magánjellegű adatainak kompromittálódása, elvesztése esetén semmilyen kártérítési igénnyel nem élhet, az eszközön tárolt privát adatokért a Társaság, az informatikai és a biztonsági szolgáltató semmilyen felelősséget nem vállal.
- Amennyiben incidens gyanúja merül fel, az eszköz vizsgálatát a visszaállíthatatlan törlés előtt a biztonsági szolgáltató végzi el az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció elrendelésére.

5.16. Külső közreműködők, harmadik fél hozzáférése

A külső partnerrel kötött szerződésnek kell tartalmaznia a szervezeti szintű információbiztonsági követelményeket és megfelelő szintű titoktartási nyilatkozatokat, melyek formai és tartalmi elemeit a Társaság jogi szakterülete ellenőrzi, meglétét az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció auditok keretében ellenőrizheti.

Az információbiztonsági szabályozás szempontjából külső közreműködőnek/harmadik félnek tekintendő minden olyan külső szervezet, szerződéses partner, akinek tevékenysége indokolttá teszi az MVM Csoport, vagy annak bármely társaságának csoportszintű belső használatú és annál magasabb minősítésű adataihoz vagy bármely informatikai rendszeréhez történő hozzáférést. Ilyen módon külső szereplőnek minősülnek az MVM Csoport társaságainak alvállalkozói, szerződéses partnerei, valamint az MVMH domain-be nem tartozó társaságok, a hatóságok, valamint a média, továbbá társasági belső használatú, illetve annál magasabb kategóriába sorolt adatok esetén az MVM Csoport többi társasága is harmadik félnek 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 5.5. alfejezet).

5.16.1. Külső felek közreműködésével kapcsolatos általános szabályok

Csoportszintű belső használatú, illetve annál magasabb minősítésű adatot külső félnek továbbítani, vagy ahhoz hozzáférést biztosítani csak jogszabályi kötelezettség, illetve szerződéses kapcsolat vagy a Társaság Ügyvezetőinek meghatalmazása alapján lehet, kizárólag az adott feladattal összefüggésben, az ahhoz szükséges mértékben, formában és tartalomban, a megfelelő jogosultság és felhatalmazás alapján, az abban meghatározott időtartam alatt. A harmadik fél jogosultságáról, illetve az adatok, információk kezeléséhez szükséges feltételek rendelkezésre állásáról (pl. titoktartási nyilatkozat) a továbbítás/betekintés lehetővé tétele előtt meg kell győződni az érintett adatgazda bevonásával.

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

Szerződéses partnerek esetében (a továbbiakban ide értendőek a Társaság Ügyvezetői általi meghatalmazással rendelkezők) a szerződésnek tartalmaznia kell a szerződéses jogviszony alatt fennálló információbiztonsági követelményeket, valamint titoktartási megállapodást, illetve indokolt esetben egyéb információbiztonsági nyilatkozatot. A szerződésben, vagy az abban előírt formában, nevesíteni kell minden külső személyt, aki a Társaság adataihoz, információihoz, információs illetve 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 a jelen Szabályzatban meghatározottak szerint.

Abban az esetben, ha a harmadik fél munkavégzéséhez csak MVM Csoport-os e-mail címmel rendelkezik, és annak használati szabályai más nyilatkozatban, szerződésben nem rögzítettek szükség van a MOB-BSz-17-NY-01 formanyomtatvány kitöltésére és aláírására.

A szerződés/megállapodás információbiztonsági követelményeinek tartalmaznia kell a következőket:

- információk bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzési követelményei, a külső szereplőkre vonatkozó általános információbiztonsági előírások,
- elektronikus levelezés, fájlok titkosításának szabályai,
- papír alapú dokumentumok kezelésének információbiztonsági szabályai,
- amennyiben értelmezhető, a látogatókra vonatkozó fizikai biztonsági szabályokat,
- amennyiben értelmezhető, hozzáférés módja a belső IT- és információs rendszerekhez, a hozzáférés szabályai és a felhasználó felelősségei,
- amennyiben értelmezhető, dokumentumok és adathordozók átadásának, cseréjének és kezelésének információbiztonsági követelményei és az ezzel kapcsolatos felhasználói felelősségek,
- a Társaság információbiztonsági ellenőrzésének lehetőségét és feltételeit,
- a szerződésben foglalt információbiztonsági követelmények megszegéséből származó szankciókat,
- szerződés megszűnésekor vagy lejártakor az információk és átadott információhordozók visszaadásának, a szerződéses partner adathordozóján lévő információk megsemmisítésének követelményei.

A szerződésben ki kell térni a harmadik félnél 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, illetve a beszerzési eljárás és a szerződés előkészítése során már az első nem nyilvános információ kiadása előtt a külső partnerrel egyoldalú, előzetes titoktartási nyilatkozatot kell aláírattatni a szerződés megkötése előtt átadott adatokra vonatkozóan is.
- A titoktartási nyilatkozatot/nyilatkozatokat mind szervezet, mind magánszemély szinten alá kell íratni.
- Amennyiben a külső fél saját munkaszerződésében kívánja szabályozni a titoktartási kötelezettséget, a szerződésben jeleznie kell azt, illetve ebben az esetben a szervezet vezetője vállalja a teljes felelősséget a titoktartásra vonatkozóan. Ettől függetlenül bizalmas és szigorúan bizalmas adatok külső féllel történő megosztása előtt a Társaság megkövetelheti személyre szóló titoktartási nyilatkozatok aláírását.
- A szerződéses partner alvállalkozóit is titoktartási kötelezettség kell, hogy kötelezze.

Az információbiztonsági követelmények társaság oldali betartásáért a szerződésben nevesített képviselő(k) felel(nek). Az információbiztonsági követelmények betartását a társasági információbiztonsági felelős ellenőrzi.

5.16.2. Adatok átadása harmadik félnek

Adatok átadása harmadik félnek csak az 5.16.1. pontban rögzített feltételek teljesítését követően, a szerződésben meghatározott módon lehetséges.

Papír alapú dokumentumok átadása esetén törekedni kell a személyes átadásra, illetve a dokumentum továbbításakor figyelembe kell venni az 5.4. alfejezetben rögzített követelményeket.

Elektronikus dokumentumok átadásánál az 5.11. alfejezetben rögzített titkosítási eljárást kell követni az elektronikus levelezés során, illetve nagy mennyiségű adat átadása esetén preferálni kell a titkosított adathordozók használatát.

A szerződéses partnernek lehetővé kell tennie a biztonságtudatos munkavégzés feltételeinek megteremtését, továbbá a munkakör ellátásához szükséges, megfelelő biztonsági feltételekkel rendelkező eszközök biztosítását. Amennyiben a szerződéses partner a rögzített feltételek teljesítését nem tudja garantálni, vagy az átadott adatok biztonsági besorolása megköveteli, a Társaság a munkavégzés idejére munkaállomást és/vagy projektszobát biztosíthat.

Az adatok előírásoknak megfelelően történő átadása mind a Társaság, mind a szerződött külső fél felelőssége. A nem-megfelelő adatátadásból származó károkért az érintett felhasználók mind társasági, mind szerződött partneri oldalon szankcionálhatók az 5.6.3. pontban meghatározottak szerint.

5.16.3. Ideiglenes belépési jogosultság adása harmadik félnek

Amennyiben a szerződött külső féllel való munka indokolja (projekt időtartama, intenzitása), a külső szereplők számára igényelhető ideiglenes belépőkártya. Az ideiglenes belépő igénylése és használata során az 5.5. alfejezet előírásait kell figyelembe venni. Az ideiglenes belépőkártya engedélyezéséről a projekt vezetője, illetve a társasági információbiztonsági felelős hozza meg a döntést.

5.16.4. Hozzáférési jogosultság biztosítása informatikai rendszerhez

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, illetve munkaállomás és a szükséges informatikai rendszerekhez jogosultság igénylésére.

A Társaság informatikai rendszeréhez külső partnernek biztosított 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 jogosultságot az adatgazda, valamint az MVM Zrt. Csoportszintű Biztonsági Igazgatója adhat, az 5.5. alfejezetben foglaltak szerint. A jogosultság kiadását és a lejárat határidejét írásban kell rögzíteni.

Minden harmadik félnek a hozzáférési jogosultság kiadása előtt meg kell ismernie jelen Szabályzatot 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. Ennek érdekében, amely rendszernél lehetséges, automatikus lejáratot kell beállítani, illetve a szerződés megszűnésével egyidejűleg, azonnal vissza kell vonni a kiadott jogosultságokat. A jogosultságok határidejének megfelelő kezelése a szerződésben érintett szervezeti egység vezetőjének felelőssége. A társasági információbiztonsági felelős ezt saját hatáskörben ellenőrizheti.

A hozzáférési jogosultság megújításáért a fogadó fél felel, év végi törlését a Társaság ellenkező esetben végrehajtja.

Külső szereplőknek hordozható informatikai eszköz (laptop, USB adattároló, stb.) akkor adható, ha ez szerepel a szerződésben, és az eszközzel elszámolási kötelezettsége van, de preferált a helyi, asztali munkaállomások használata.

Külső szereplők nem szerezhetnek a Társaság számítógépes hálózatán semmilyen privilegizált (pl. adminisztrátori) jogosultságokat, kivéve amennyiben informatikai rendszer üzemeltetése az alvállalkozói együttműködés tárgya. Ebben az esetben a kiemelt jogosultságot dokumentálni kell, illetve a kiemelt jogosultság csak az aktuális munkavégzés időtartamára adható ki, üzleti adatok érintettsége esetén adatgazdai jóváhagyás mellett. A szerződésben részletesen szükséges továbbá annak szabályozása, hogy a külső partner rendszergazdai jogai mire jogosítják fel, továbbá ezek kontrollja és monitoringja hogyan történik.

A dokumentumok és adathordozók, valamint az informatikai hálózathoz (annak részeihez, illetve meghatározott alkalmazásokhoz) történő hozzáférési felhasználói azonosítók és jelszavak átadása és visszavétele történjen megfelelően jóváhagyott és dokumentáltan igazolható módon.

A külső szereplőknek az informatikai rendszerhez adott felhasználói azonosítók nyilvántartása legyen naprakész, kontrollja és monitorozása folyamatos kell, hogy legyen – ezek nyilvántartása a Társaság informatikai szolgáltatásokért felelős szervezetének a feladata.

A Társaság által biztosított eszközökön, illetve a Társaság területén a jelen Szabályzatban rögzített biztonsági előírások betartása kötelező.

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

5.16.5. Projektszoba, adatszoba

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

A projektszobával kapcsolatos alapvető elvárásokat a MOB-BSz-17-M-13 melléklet tartalmazza.

5.16.6. Ellenőrzések

A jelen fejezetben rögzített, harmadik félre vonatkozó információbiztonsági előírásokat a társasági információbiztonsági felelős jelen Szabályzatban rögzítettek szerint köteles ellenőrizni.

A harmadik féllel kötött szerződésben részletesen dokumentálni kell az ellenőrzés gyakoriságát, a vizsgálat tárgyát, illetve a vizsgálat módját.

Eltérés esetén a hiányosság vagy nem-megfelelőség kezelésére határidőt kell kiszabni, melynek leteltét követően a társasági információbiztonsági felelős visszaellenőrzést végez az érintett pontokon.

Az ellenőrzésekről jelentést kell készíteni, melyet mind a harmadik fél képviselője, mind az adott vállalkozóért felelős terület vezetője felé meg kell küldeni. Súlyos, vagy folyamatosan fennálló nem-megfelelőség vagy hiányosság azonosítása esetén a társasági információbiztonsági felelősnek tájékoztatnia kell a felettesét, illetve a Társaság Ügyvezetőit is.

5.17. Incidenskezelés

Az információbiztonsági incidenskezelés célja az információbiztonságot, a szervezet erőforrásainak, folyamatainak, információbiztonsági kontrolljainak működését veszélyeztető, illetve a rendeltetésszerűtől eltérő események figyelése, információbiztonsági incidensek azonosítása, kezelése, valamint az incidens lezárását követően a tanulságok levonása és védelmi intézkedések meghatározása az incidensek okának megszüntetésére a további bekövetkezési gyakoriság és/vagy hatás csökkentése céljából.

A Társaság minden munkavállalójának és külső partnerének kötelessége az általa tapasztalt biztonsági eseményt, vagy általa feltárt biztonsági sebezhetőséget haladéktalanul jelenteni a jelen Szabályzatban, illetve a kapcsolódó MOB-BSz-17-FU-03 folyamatutasításban foglaltak szerint.

Az incidens jelentésének elmulasztása az incidens jellegétől és mértékétől függően szankcionálható! A lehetséges szankciókat az 5.6.3. pont tartalmazza.

Jelen Szabályzat az információbiztonsági események/incidensek alábbi típusait különbözteti meg (meghatározásukat a MOB-BSz-17-M-02 melléklet tartalmazza):

- Információbiztonsági esemény
- Információbiztonsági incidens
- Rendkívüli esemény
  - Üzletfolytonossági esemény
  - Katasztrófa esemény

Jelen fejezet az információbiztonsági események és incidensek jelentésével és kezelésével kapcsolatban fogalmaz meg előírásokat. A rendkívüli események jelentésének és kezelésének rendjét jelen Szabályzat 5.18. alfejezete és a MOB-BSz-17-FU-03 folyamatutasítás tartalmazza.

5.17.1. Információbiztonsági események és incidensek típusai

Az információbiztonsági eseményeket és incidenseket a következő három kategóriába sorolhatjuk be:

- **Informatikai biztonsági esemény/incidens**: Informatikai eseménynek/incidensnek tekinthető minden, az informatikai eszközökkel kapcsolatban felmerülő, hardveres vagy szoftveres meghibásodás, probléma, a megszokottól eltérő, rendellenes működés (pl. vírusfertőzés, adathalász támadás, adathordozó/mobil eszköz elvesztése, jelszó kompromittálódása, stb.).
- **Fizikai biztonsági esemény/incidens**: A fizikai biztonsági események/incidensek közé sorolhatók a biztonságtechnikai eszközöket, biztonsági előírásokat érintő események és

incidensek (pl. beléptető rendszer meghibásodása, nem rendeltetésszerű használata, biztonsági előírások szándékos megsértése, illetéktelen behatolás, lopás, stb.).

- **Egyéb információbiztonsági esemény/incidens:** Idetartoznak azon információbiztonsági események vagy incidensek, melyek nem sorolhatók be egyik fent említett kategóriába sem (pl. bizalmas dokumentumok elvesztése, kompromittálódása, adatkezelésre vonatkozó szabályok megsértése, gyanús telefonhívások, stb.).

5.17.2. Információbiztonsági események és incidensek jelentése

Minden munkavállaló kötelessége az általa észlelt információbiztonsági eseményt vagy incidenst az illetékes személyek felé jelenteni.

A csoportszintű (kettő vagy több társaságot érintő) incidensről az információkat (pl. jegyzőkönyv, adatlap, stb.) továbbítani kell az MVM Zrt. Csoportszintű Biztonsági Igazgatóságra. Minden bejelentett incidenst dokumentálni szükséges.

Az értesítendők köre az esemény/incidens típusától függően a következő lehet:

Információbiztonsági esemény/incidens típusa	Értesítendők köre	Tájékoztatás szükséges
Informatikai biztonsági esemény/incidens	• Közvetlen felettes • REVIR ügyeletes* • Ügyviteli rendszer esetében informatikai szolgáltató HelpDesk-je • Technológiai rendszer esetében helyi üzemeltetés	• Információbiztonsági felelős • Adatgazda • Bűncselekmény esetén felső vezetés • REVIR Központi Ügyelet*
Fizikai biztonsági esemény/incidens	• Közvetlen felettes • REVIR ügyeletes* • Biztonsági őr vagy • Biztonsági szolgáltató kapcsolattartója • Biztonsági referens	• Információbiztonsági felelős • Adatgazda • Bűncselekmény esetén felső vezetés • REVIR Központi Ügyelet*
Egyéb információbiztonsági esemény/incidens	• Közvetlen felettes • REVIR ügyeletes* • Információbiztonsági felelős	• Adatgazda • Bűncselekmény esetén felső vezetés • REVIR Központi Ügyelet*

*A REVIR jelentésköteles események nem kizárólagos (indikatív) listáját a MOB-BSz-17-FU-05-M-04 melléklet tartalmazza.

Előfordulhat, hogy az információbiztonsági eseményt vagy incidenst először az informatikai vagy biztonsági szolgáltató észleli, ebben az esetben az eseményt/incidenst észlelő szolgáltató kötelessége, hogy haladéktalanul tájékoztassa a társasági információbiztonsági felelőst az eseményről/incidensről.

Amennyiben szükséges, az incidenst a hatályos jogszabályok szerint jelenteni kell az illetékes hatóságok felé is, a vonatkozó jogszabályokban megkövetelt határidőn belül.

Az incidensek jelentésére az alábbi általános előírások vonatkoznak:

- Az információbiztonsági eseményeket, illetve incidensek gyanúját haladéktalanul jelenteni kell az értesítendő személyek körében meghatározott szereplőknek.
- Az incidensek jelentése a következő felületeken történhet:
  - e-mailen: informaciobiztonsag@mvm.hu
    helpdesk@mvmi.hu
    diszpecser@mvm-bszk.hu
    revir@mvm-bszk.hu (REVIR jelentésköteles események)
  - telefonhívással:
    +36/20 887-3137, +36/20 887-3138; +36/20 887-3139
    +36/75 501-919
    +36/80 205-251;+36/30 438-6692 (REVIR jelentésköteles események)
  - személyesen a társasági információbiztonsági felelősénél.
- Az információbiztonsági események/incidensek jelentését minden esetben dokumentált formában is meg kell tenni, mely lehet:
  - elektronikus levél
  - jegyzőkönyv (lehet rendszerben rögzített is)
  - hangrögzítés (telefonhívás esetén)
- Az információbiztonsági eseményeket és incidenseket minden esetben oly módon kell jelenteni, hogy az ne keltsen pánikot a munkatársak között (nem szükséges kör-email írása, ezt a társasági információbiztonsági felelős az események kivizsgálása során megteszi).
- A felhasználónak a jelentést követően – amennyiben más utasítást nem kap - az incidenssel teendője nincsen, az észlelt esemény, illetve incidens kezelése és kivizsgálása nem az észlelő felhasználó feladata, viszont az incidens kivizsgálásába információszolgáltatás végett a társasági információbiztonsági felelős bevonhatja, mely esetben kötelessége együttműködnie, illetve az esetlegesen szükséges eszközöket átadnia.
- Bűncselekmények, illetve egyéb, hatóságok felé jelentésköteles események azonosítása esetén a hatóságokkal való kapcsolatfelvétel a csoportszintű biztonsági igazgató feladata.
- Amennyiben a felhasználó nem jelenti az általa észlelt incidenst, és emiatt a szervezetet kár éri, a munkavállaló felelősségre vonható az 5.6.3. pontban foglaltak szerint.
- Amennyiben az incidens nem csoportszintű, de más társaságot is érinthet, a társasági információbiztonsági felelősnek haladéktalanul fel kell vennie a kapcsolatot az érintett társaság információbiztonsági felelősével, és be kell vonnia az incidens kezelésébe.

Az információbiztonsági események és incidensek jelentésének eljárásrendjét, valamint a jelentés tartalmát a MOB-BSz-17-FU-03 folyamatutasítás tartalmazza.

5.17.3. Információbiztonsági események és incidensek kezelése

Az információbiztonsági események és incidensek kezelése során mind az incidens elhárítása, mind kivizsgálása megtörténik. Ezen feladatok végrehajtása egy társaságot érintő információbiztonsági esemény vagy incidens bekövetkezése esetén a következő szereplők feladata:

Információbiztonsági esemény/incidens típusa	Felelős	Közreműködő
Informatikai biztonsági esemény/incidens	• Ügyviteli rendszer esetében informatikai szolgáltató • Technológiai rendszer esetében helyi üzemeltetés	• Információbiztonsági felelős • Biztonsági szolgáltató, amennyiben indokolt • Közvetlenül érintett felek, amennyiben szükséges • Hatóságok, amennyiben indokolt
Fizikai biztonsági esemény/incidens	• Biztonsági szolgáltató	• Információbiztonsági felelős • Közvetlenül érintett felek, amennyiben szükséges • Hatóságok, amennyiben indokolt
Egyéb információbiztonsági esemény/incidens	• Információbiztonsági felelős	• Biztonsági szolgáltató, amennyiben indokolt • Informatikai szolgáltató, amennyiben indokolt • Közvetlenül érintett felek, amennyiben szükséges • Hatóságok, amennyiben indokolt

Amennyiben az esemény vagy incidens a Társaságon belül kezelhető, a társasági információbiztonsági felelőse koordinálja annak elhárítását és kivizsgálását. Az informatikai szolgáltató és a biztonsági szolgáltató, mint közreműködő, bevonását a MOB-BSz-17-FU-03 folyamatutasításban foglalt események esetén szükséges megtenni (pl. fertőzött adathordozó vizsgálata, stb.).

Több társaságot is érintő, vagy jelentős incidens esetén a Társaság vagy az informatikai szolgáltató az esemény/incidens kivizsgálást a biztonsági szolgáltató felé eszkalálhatja a MOB-BSz-17-FU-03 folyamatutasításban foglaltak szerint.

A teljes vállalatcsoportot érintő incidens esetén az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkció magához vonhatja az incidens kezelésével kapcsolatos döntési jogokat, illetve az incidens kivizsgálásának irányítását.

Amennyiben az információbiztonsági esemény vagy incidens kezelése során indokolt, a hatóságok bevonásának lépéseit a MOB-BSz-17-FU-03 folyamatutasítás tartalmazza.

Amennyiben az információbiztonsági esemény vagy incidens az üzletmenet folytonosságát veszélyezteti, vagy akadályozza, életbe kell léptetni az üzletfolytonossági és erőforrás-helyreállítási terveket, és az incidenst rendkívüli eseményként kell kezelni a hivatkozott szabályzat szerint.

Az információbiztonsági esemény/incidens elhárítására tett lépéseket folyamatosan jegyzőkönyvezni kell, illetve az elhárítással egyidejűleg meg kell kezdeni az incidens kivizsgálását.

Bizonyítékok gyűjtése

Az incidensek kivizsgálásához a társasági információbiztonsági felelőse, illetve a vizsgálatba bevont egyéb felek (informatikai és biztonsági szolgáltatók) jogosultak bizonyítékok gyűjtésére.

Abban az esetben, amennyiben az incidens bűncselekménynek minősül, a bizonyítékok gyűjtését kizárólag a hatóságok végezhetik el.

Az informatikai és biztonsági szolgáltató köteles a társasági információbiztonsági felelősnek vagy az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkciónak – annak kérése alapján – rendelkezésére bocsátani az adott incidenssel kapcsolatos, kizárólag az érintett társaságra vonatkozó adatokat (pl. naplóállományok, stb.).

A bizonyítékok gyűjtésének lehetséges módjai az MVM Csoporton belül:

- Naplófájlok vizsgálata a vizsgálatban érintett rendszereken (beleértve a beléptető rendszert is).
- Az alkalmazott monitorozó eszközök által rögzített, az incidenssel kapcsolatos információk.
- Incidensben érintett informatikai eszközök (beleértve az okostelefonokat), illetve azokról készített image-ek vizsgálata.
- Megalapozott gyanú esetén az incidensben érintett felhasználó a Társaság által biztosított elektronikus levelezésébe történő betekintés.
- Kamerás megfigyelő rendszer felvételeinek megtekintése.

Informatikai eszközöket, rendszereket érintő incidensek esetén az informatikai szolgáltatónak, a biztonsági rendszereket illetően pedig a biztonsági szolgáltatónak van adatszolgáltatási kötelezettsége az érintett társaság felé az incidenssel kapcsolatban.

A gyűjtött információk szigorúan bizalmas információnak minősülnek, kezelésük az 5.4. alfejezetben foglaltak szerint történhet. Hozzáférési jogosultsággal kizárólag a vizsgálatba bevont személyek, valamint a Társaság Ügyvezetői és általuk felhatalmazott személyek rendelkezhetnek.

Az incidens kivizsgálása során gyűjtött bizonyítékokat jegyzőkönyvben rögzíteni kell.

5.17.4. Információbiztonsági események és incidensek lezárása

Az információbiztonsági esemény vagy incidens kezelése abban az esetben tekinthető lezártnak, amennyiben az incidensre való reagálás, elhárítás megtörtént, további károk okozása elhanyagolható, valamint a bizonyítékok gyűjtése és vizsgálata lezárult, az esemény kivizsgálása megtörtént, a szükséges megállapításokat a szakértők megtették és a következtetéseket levonták.

Dokumentálás

Az információbiztonsági esemény/incidens elhárításának lépéseit, illetve kivizsgálásának eredményeit dokumentált módon rögzíteni kell. A dokumentáció lehet jegyzőkönyv, vagy valamely erre a célra alkalmazható informatikai rendszer is. A dokumentáció tartalma információbiztonsági esemény/incidens típusoktól és az eset súlyosságától függően eltérő lehet, de mindenképpen rögzíteni kell a következőket:

- esemény/incidens jelentésének időpontja,
- esemény/incidens bejelentőjének neve, munkahelye, beosztása,
- esemény/incidens jellege, leírása,
- esemény/incidens bejelentést fogadó neve, munkahelye, beosztása,
- kezelésben résztvevő szervezeti egységek, személyek,
- esemény/incidens becsült hatása, kockázatai, ismert okozott/lehetséges károk,
- esemény/incidens hatása más társaságokra, illetve rendszerekre,
- elhárítás, illetve kivizsgálás megkezdésének ideje,
- elhárítás során tett intézkedések (napló),

- gyűjtött bizonyítékok (részletes felsorolás),
- kivizsgálás eredménye, tapasztalatok,
- javasolt védelmi intézkedések, javító intézkedések a hasonló jellegű incidensek elkerülése végett,
- elhárítás értékelése, szükséges utómunkálatok,
- lezárás dátuma,
- érintett felek aláírása.

Tájékoztatás

Az incidens elhárításáról írásban (elektronikus levél, Intranet hír, felugró ablak) tájékoztatni kell az elhárításban, illetve kivizsgálásban résztvevőket, valamint szükség esetén az érintett munkatársakat. A tájékoztató csak a szükséges és elégséges mértékben kell, hogy tartalmazza az incidenssel kapcsolatos információkat, az események, illetve vizsgálati eredmények részletes megosztása tilos.

5.17.5. Rendszeres riportok készítése

Az információbiztonsági eseményekről és incidensekről mind társasági, mind csoportszinten rendszeres riportot kell készíteni, illetve a statisztikákat elemezni.

Incidens riportok

A társasági információbiztonsági felelős az alábbiakban meghatározott rendszeres időközönként riportot készít az elmúlt időszak Társaságot érintő incidenseiről és elemzi azokat, valamint összehasonlítja a korábbi időszakok információbiztonsági eseményeinek/incidenseinek statisztikáival.

A Társaság az információbiztonsági besorolása szerint bizonyos időközönként riportot készít. Az elemzés szempontjai a következők:

- gyakoriság, ismétlődés,
- kárkövetkezmény, okozott hatás,
- érintett erőforrások,
- érintett társaságok,
- becsült bekövetkezési idő és bejelentés között eltelt idő,
- bejelentés ideje és az elhárítás megkezdése között eltelt idő,
- elhárításra fordított idő,
- kivizsgálások során azonosított javító intézkedések megvalósításának státusza.

A társasági információbiztonsági felelőse a riport készítéséhez a rendelkezésre álló esemény/incidens dokumentációkon túl az informatikai szolgáltató, a biztonsági szolgáltató, és szükség esetén a Társaság REVIR ügyeletese által rendelkezésre bocsátott adatokat használja fel.

A riportok alapján ki kell vizsgálni minden gyanús eseményt. Gyanús eseménynek minősül például, ha egy incidens magas gyakorisággal következik be, vagy a vártnál nagyobb kárkövetkezménnyel vagy visszaállítási idővel kell számolni, de az is gyanúra adhat okot, ha bizonyos felhasználók esetében nő a különféle bejelentések száma.

Az elkészített riportot a Társaság felső vezetése elé kell tárni a további intézkedésekről való döntés meghozatala érdekében. Amennyiben gyanús esemény kerül azonosításra, a további vizsgálatok tételéhez tájékoztatni kell az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkciót, valamint bevonásra kerülhet az incidens jellegétől függően az informatikai és biztonsági szolgáltató is.

A Társaságnál bekövetkezett incidensekről a MOB-BSz-17-NY-02 formanyomtatványban foglalt sablon szerint éves szinten jelentést kell tenni az MVM Zrt. Csoportszintű Biztonsági Igazgatónak, melyet minden év január 31-ig meg kell küldeni az előző időszakra vonatkozóan.

5.17.6. Incidensjelentés és kezelés oktatása, visszamérése

Az információbiztonsági események és incidensek jelentésének, valamint kezelésének szabályait, előírásait a biztonságtudatossági oktatások keretein belül minden munkavállaló számára oktatni kell.

Az információbiztonsági események és incidensek jelentésének és kezelésének folyamatát a társasági információbiztonsági felelőse saját hatáskörben bármikor, csoportszinten az MVM Zrt. Csoportszintű Biztonsági Igazgatóság ellenőrizheti. Az ellenőrzés beépíthető az éves audit programba, illetve Social Engineering auditok keretein belül is végrehajtható.

A visszamérést a Társaság saját hatáskörben végzi, és annak eredményéről tájékoztatja az MVM Zrt. Csoportszintű Biztonsági Igazgatóságát.

5.18. Rendkívüli helyzetkezelési rendszer

A rendkívüli helyzetkezelési rendszer célja a Társaság működése tekintetében kritikus funkciók folytonosságának biztosítása, illetve egy előre nem látott kockázati esemény bekövetkezése esetén a hatás minimalizálása.

A Társaság rendkívüli helyzetkezelési tevékenysége kiterjed az üzletfolytonossági események és a krízis események kezelésére ennek érdekében a Társaság rendkívüli helyzetkezelési rendszere magában foglalja a rendkívüli helyzetkezelési tervek, védelmi intézkedések kialakítását és alkalmazását.

A dominóhatás megelőzése, kezelése, az üzletmenet elvárt szinten történő fenntartása, a normál üzletmenet visszaállítása, a rendkívüli helyzetkezelési eljárások összehangolása érdekében a Társaság együttműködik az MVM Csoport más társaságaival, az MVM Zrt. irányítása szerint.

5.18.1. A rendkívüli helyzetkezelés szervezeti háttere

A következőkben bemutatásra kerül a Társaság rendkívüli helyzetkezelési szervezeti háttere, mely a társasági szintű feladatok ellátását biztosítja. A szereplők felelősek a jelen Szabályzat és a kapcsolódó folyamatutasítások szerint hatáskörükbe tartozó feladatokért. Az egyes szereplők feladatairól szóló kivonatot a MOB-BSz-17-M-16 melléklet tartalmazza.

<u>Társaság Ügyvezetői</u>

A Társaság Ügyvezetői, mint a Társaság első számú vezetői, felelősek a rendkívüli helyzetkezelési rendszer legfelsőbb szintű támogatásának biztosításáért, így a szükséges erőforrások és menedzsment szintű támogatás biztosításáért.

<u>Társasági biztonsági funkcióért felelős vezető</u>

A biztonsági vezető felelős a rendkívüli helyzetkezelési rendszer kialakításának, fejlesztésének szakmai támogatásáért, felső szintű koordinálásáért, erőforrás biztosításáért.

<u>Társasági üzletfolytonossági felelős</u>

A társasági üzletfolytonossági felelős, mint kijelölt szerepkör, felelős a rendkívüli helyzetkezelési feladatok koordinálásáért, valamint felelős a rendkívüli helyzetkezelési rendszer kialakításáért és karbantartásáért. A kiemelt feladatokról és a szükséges kompetenciákról a KIE-17-M-04 Társasági üzletfolytonossági felelős melléklet rendelkezik.

<u>Társasági Krízis Team</u>

A Társasági Krízis Team, mint összehívható testület, felelős a rendkívüli helyzetkezelés irányításáért, koordinálásáért. Akkor szükséges összehívni, amennyiben a rendkívüli esemény jellege és súlyossága, vagyis az esemény krízis szintje megköveteli. A krízis szintekre

vonatkozóan részletes leírás a KIE-17-M-01 Meghatározások mellékletben a „Krízis szintek" címszó alatt található.

Állandó tagjai:

- Társaság Ügyvezetői (vezető).

A rendkívüli helyzet jellegéből fakadóan a Társasági Krízis Team tagjai bevonhatnak további vezetőket/szakértőket a Társasági Krízis Team-be. A testület vezetője a Társaság Ügyvezetése.

Társasági REVIR ügyeletes

A társasági REVIR ügyeletes, mint kijelölt szerepkör, felelős a rendkívüli eseményről szóló információkat jelenteni a REVIR Központi Ügyelet (MOB-BSz-17-M-14) útján a Rendkívüli Események Figyelőszolgálata részére. A szerepkör heti váltásban (hétfőn 10 órától a következő hétfő 10 óráig) kerül betöltésre, melyet havonta előre meg kell küldeni a REVIR Központi Ügyelet részére. A beosztás elkészítését a társasági üzletfolytonossági felelős koordinálja, egyezteti a társasági REVIR ügyeletessel/ügyeletesekkel, és terjeszti fel jóváhagyásra a Társaság Ügyvezetői részére. (D-08)

Folyamatgazda

Rendelkezik a felelőssége alá tartozó folyamatok átfogó ismeretével, így biztosítani képes a folyamatok minőségi kritériumoknak való megfeleltetését. Ennek köszönhetően a hatáskörébe tartozó folyamatok tekintetében szakmai támogatást nyújt a rendkívüli helyzetkezelési rendszer kialakítása és eseti, illetve rendszeres felülvizsgálta során.

Erőforrásgazda

Felelős a Társaság tulajdonában, vagy rendelkezési jogosultságában álló erőforrások (például emberi erőforrás, technikai erőforrás, informatikai erőforrás stb.) tervezéséért, működtetéséért, helyreállításáért. A hatáskörébe tartozó kritikus erőforrások tekintetében folyamatos szakértői támogatást biztosít a rendkívüli helyzetek proaktív és reaktív kezelésében.

Folyamatszponzor

Rendelkezik a folyamatok erőforrás és vezetői szintű támogatásához szükséges felhatalmazással. Feladata és szerepe a kritikus folyamatok esetében kiemelt.

Munkavállalók

A Társaság munkavállalóinak szerepe a rendkívüli helyzetkezeléssel kapcsolatosan a munkakörüktől függően lehet általános vagy speciális.

5.18.2. Rendkívüli helyzet felkészülés

A MOB-BSz-17-FU-04 folyamatutasítás tartalmazza a rendkívüli helyzetkezelési rendszer kialakításához és működtetéséhez szükséges, az úgynevezett felkészülési időszakban végrehajtandó feladatokat. A rendkívüli helyzet felkészülés folyamat során meghozandó döntések:

- Döntés az üzletfolytonossági felmérési terv jóváhagyásáról (D-09)
- Döntés a kritikus folyamat lista jóváhagyásáról (D-10)
- Döntés a feltárt kockázatok kezeléséről, az alkalmazott kockázatkezelési stratégiáról, a védelmi intézkedések bevezetéséről és alkalmazásáról, a maradványkockázatok elfogadásáról (D-11)
- Döntés a rendkívüli helyzetkezelési rendszer általános és speciális ismereteire vonatkozó oktatás, tematika, tananyag jóváhagyásáról (D-12)
- Döntés a tesztelés eredménye alapján javasolt védelmi intézkedési listáról (D-13)
- Döntés a Társaság éves értékelő jóváhagyásáról (D-14)

Az üzletfolytonossági rendszer kialakításának, működtetésének és karbantartásának módszertanát a MOB-BSz-17-M-15 melléklet tartalmazza.

A felkészülési időszak feladata a rendkívüli helyzetkezelési rendszer kialakítása, valamint rendszeres karbantartása annak érdekében, hogy egy rendkívüli esemény bekövetkezése után a kiesett vagy sérült kritikus üzleti folyamatok és erőforrások a lehető legkisebb kiesési időn belül helyreállíthatóak, helyettesíthetőek legyenek.

A rendkívüli helyzetkezelés felkészülési feladatai magukban foglalják az alábbiakat:

- A rendkívüli helyzetkezeléshez szükséges szervezeti és szabályozási keretek kialakítását.
- A rendkívüli helyzetkezelési tervek elkészítését megelőző elemzések elvégzését, üzleti hatáselemzés készítését és kockázatelemzés végrehajtását.
- A rendkívüli helyzetkezelési tervek elkészítését, oktatását, tesztelését.
- A rendkívüli helyzetkezelési dokumentáció felülvizsgálatát és karbantartását.
- A rendkívüli események jelentésével kapcsolatos eljárási és szervezési rend kialakítását és működtetését, valamint a rendkívüli események jelentését.
- A rendkívüli helyzetkezeléséhez szükséges kompetenciák megszerzését.
- A rendkívüli helyzetkezeléshez szükséges erőforrások beszerzését, készletezését.
- Az erőforrások pótlásához, helyettesítéséhez szükséges infrastrukturális elemek tartalékolási politikájának és krízistűrővé tételének végrehajtását.
- Biztonsági mentések rendszeres készítését és megfelelő tárolását.

A Társaság részére humán erőforrás szolgáltatást nyújtó szakterület feladata gondoskodni a naprakész munkaköri nyilvántartás rendelkezésre állásának biztosításáról, melynek segítségével a rendkívüli helyzetkezelési feladatok elvégzéséhez kapcsolódó helyettesítések könnyen azonosíthatók. A személyi változások, illetve a helyettesítési rend dokumentálása a Társaság részére humán erőforrás szolgáltatást nyújtó szervezeti egység/funkció vezetőjének felelőssége.

5.18.3. Rendkívüli helyzet bejelentése

A MOB-BSz-17-FU-05 folyamatutasítás tartalmazza a bekövetkezett rendkívüli események szervezett jelentési rendjét, a kezelésben kompetens felek közötti információáramlás érdekében végrehajtandó feladatokat.

A folyamatutasítás biztosítja – a hozzá tartozó formanyomtatványok és mellékletekkel együtt – hogy a bekövetkező rendkívüli eseményekkel kapcsolatos információk egységes és egycsatornás módon, szervezett és ellenőrzött keretek között, a lehető legrövidebb időn belül eljussanak a REVIR Központi Ügyeleten keresztül az MVM Zrt. Rendkívüli Események Figyelőszolgálata, valamint a rendkívüli események kezelésében illetékes szervezetekhez, személyekhez, valamint azokhoz, akiket a rendkívüli esemény közvetve érint.

5.18.4. Rendkívüli helyzet kezelése

A MOB-BSz-17-FU-06 folyamatutasítás tartalmazza a bekövetkezett rendkívüli események szervezett kezelési rendjét, a kezelésben érintettek által végrehajtandó feladatokat. A rendkívüli helyzet kezelése folyamat során meghozandó döntések:

- Döntés a társasági Krízis Team összehívásáról (D-15)
- Döntés a rendkívüli helyzetkezelés irányításának átvételéről, koordinálásáról (D-16)
- Döntés a rendkívüli helyzetkezelés irányításában csoportszintű eseménynél (D-17)
- Döntés a rendkívüli minősítésű időszak elrendeléséről (D-18)
- Döntés a rendkívüli helyzetkezelési tervek alkalmazásáról (D-19)

- Döntés a normál működési rendre való visszaállásról (D-20)
- Döntés a rendkívüli minősítésű időszak lezárásáról (D-21)
- Döntés a társasági rendkívüli esemény kezelési jegyzőkönyv jóváhagyásáról (D-22).

A Társaság feladatai a csoportszintű koordináció során:

- Rendkívüli, valamint egyéb jelentésköteles események jelzése a REVIR Központi Ügyelet felé.
- Társasági Krízis Team összehívása (amennyiben annak feltételei fennállnak).
- Dominóhatás érvényesülésének vizsgálata (ellenőrizi, hogy az adott folyamat kiesése, a káresemény érint-e más társaságot) és ennek jelzése (Társasági Krízis Team vezetője köteles azt haladéktalanul jelezni az érintett társaság vezetője és a REVIR Központi Ügyelet felé).
- Együttműködés a dominóhatással érintett társaságokkal, hogy biztosított legyen a rendkívüli helyzetkezelési intézkedéseik összhangja, valamint ezen társaságok közötti kommunikáció tartalmáról és eredményéről tájékoztatást adni a REVIR Központi Ügyeleten keresztül a Rendkívüli Események Figyelőszolgálata, illetve a Csoportszintű Krízis Team felé.
- Emberi élet és társasági/MVM Csoport vagyon mentése, megóvása.
- A rendkívüli helyzet kezeléshez rendelkezésre álló, vagy abba bevonható erőforrásokkal gazdálkodni a károk optimális mérséklésének érdekében.
- A Társaság kritikus folyamatai üzletfolytonossági működésének biztosítása.
- Rendkívüli helyzet kezelési tervek alkalmazása szükség esetén.
- A rendkívüli esemény okozta károk elhárítása, hatásainak csökkentése.
- Rendkívüli helyzet kezelése.
- Javaslattétel a Csoportszintű Krízis Team összehívására (amennyiben annak feltételei fennállnak).
- A védelmi igazgatási szervek munkájának támogatása.
- A rendkívüli helyzetkezelés dokumentálása és tájékoztatás nyújtása a REVIR Központi Ügyelet részére.
- Rendkívüli esemény kezelését kiértékelő jegyzőkönyv készítése és megküldése az MVM Zrt. részére.

5.18.5. Dokumentáció tárolása

A rendkívüli helyzetkezelési rendszer dokumentációjának tárolása során biztosítania kell, hogy a dokumentumok krízisesemény bekövetkezésekor is elérhetőek legyenek. Ennek megfelelően a dokumentumok hozzáférhetőségét biztosítani kell a székház elérhetetlensége, szerverhiba, tűz stb. esetén is. Ezért a dokumentumokat több helyen, illetve elektronikus és nyomatott formában is el kell tárolni legalább az alábbiak szerint:

- nyomtatott példány:
  - Társaság Ügyvezetői(teljes dokumentáció)
  - Társaság üzletfolytonossági felelősnél (teljes dokumentáció)
  - Folyamatgazdáknál (vonatkozó tervek)
  - Erőforrásgazdáknál (vonatkozó tervek)
- elektronikus példány:
  - Társaság Ügyvezetői (teljes dokumentáció, külső adathordozón is)
  - Társaság üzletfolytonossági felelősnél (teljes dokumentáció, külső adathordozón is)
  - Folyamatgazdáknál (vonatkozó tervek, külső adathordozón is)
  - Erőforrásgazdáknál (vonatkozó tervek, külső adathordozón is)

A tervek érintettjeinek kötelező saját példánnyal rendelkeznie a legfrissebb dokumentumból. A dokumentumokat szükség esetén könnyen elérhető, de illetéktelenek elől elzárt helyen kell tárolni a dokumentumok kezelésére vonatkozó szabályok betartásával.

5.19. Társasági kötelezettségek a csoportszintű központi monitoring során

A csoportszintű központi monitoring során a Társaság támogatja az MVM Zrt.-t az alábbiak ellenőrzésében:

- A rendkívüli helyzetkezelési tervek és a rendkívüli helyzetekre vonatkozó egyéb szabályzatok a központi szabályozó dokumentumokban lefektetett elvárásoknak megfelelnek-e, naprakészek-e, mikor kerültek alkalmazásra és milyen eredménnyel, mikor kerültek utoljára tesztelésre és milyen eredménnyel.
- Biztosított-e a rendkívüli helyzetkezelési teendők oktatása, az érintett munkatársak tisztában vannak-e a feladataikkal.
- Az egyes társaságok naprakészen tartják-e és ellenőrzik-e a rendkívüli helyzetkezelési tervek által elvárt eszközrendszert és az erőforrások rendelkezésre állását.

A Társaság implementálja az MVM Zrt. módosítási igényeit.

5.20. Alternatív telephely

Legalább a kritikusnak minősített folyamatok esetében, az üzletfolytonossági kockázatelemzés során szükséges vizsgálni a telephely, mint erőforrás, kiesését. Szükség esetén alternatív telephelyet kell kialakítani. Az alternatív telephellyel kapcsolatos elvárásokat a folyamatgazda határozza meg, majd a társaság üzletfolytonossági felelős véleményezi és terjeszti fel jóváhagyásra a Társaság Ügyvezetői részére. (D-23)

Az alternatív telephely vizsgálatakor az alábbi jellemzőket mindenképp figyelembe kell venni:

- Elérhetőség.
- Rendelkezésre állás.
- Kapacitás, befogadóképesség.
- Biztonsági követelmények.
- Infrastruktúra.

5.21. Krízis Központ

A Társaságnak vizsgálnia kell, hogy a rendkívüli események kezelésének irányítására, a menedzsment és a Társasági Krízis Team működésének támogatására a munkavégzés eredeti helyén, illetve szükség esetén, alternatív telephelyen, Krízis Központot működtessen-e. Szükség esetén Krízis Központot kell kialakítani. A Krízis Központtal kapcsolatos elvárásokat a társasági üzletfolytonossági felelős határozza meg és terjeszti fel jóváhagyásra a Társaság Ügyvezetői részére. (D-24) A Krízis Központban megtalálhatónak kell lennie a Társasági Krízis Team számára mindazon eszközpark és technológia, amely szükséges a rendkívüli helyzet fizikai és kommunikációs kezeléséhez.

5.22. REVIR

A Rendkívüli Események Vezetői Információs Rendszer (REVIR) a rendkívüli eseményekkel kapcsolatos hatékony információáramlást, dokumentálást és döntéshozatalt támogató rendszere az MVM Csoportnak.

5.23. Audit, felülvizsgálat

Az auditok, felülvizsgálatok célja meggyőződni arról, hogy a szükséges kontrollok kialakítása megtörtént, illetve a bevezetett védelmi intézkedések megfelelően működnek, valamint új kockázatok azonosíthatóak-e.

5.23.1. Információbiztonsági belső auditok

Az információbiztonsági auditok mind az ügyviteli, mind a technológiai rendszerekre kiterjednek az audit célja, hatóköre szerinti meghatározásban. Az információbiztonsági auditok a MOB-BSz-17-FU-07 folyamatutasításban vannak részletezve. A belső információbiztonsági auditok végrehajtása folyamat során meghozandó döntések:

- Döntés az audit tervről (D-25).

5.23.2. Sérülékenység vizsgálatok

A sérülékenység vizsgálatok célja az informatikai rendszerek sérülékenységeinek, gyenge pontjainak azonosítása, illetve az azok jelentette kockázatok feltárása és kezelési lehetőségeik vizsgálata.

A Társaság ügyviteli informatikai rendszerének sérülékenység vizsgálatát csak az informatikai szolgáltató vagy az általa megbízott vállalkozó hajthatja végre, a vizsgálatról a Társaság Ügyvezetői döntenek, az MVM Zrt. Csoportszintű Biztonsági Igazgató előzetes jóváhagyásával (D-26). Információbiztonsági szempontból rendkívüli esetekben az informatikai szolgáltatóval egyeztetve a társasági információbiztonsági felelős vagy a Társaság által megbízott vállalkozó a Társaság Ügyvezetőinek jóváhagyásával hajthatja végre azt, az MVM Zrt. Csoportszintű Biztonsági Igazgató előzetes jóváhagyásával.

Üzemviteli rendszerekkel kapcsolatos sérülékenységi vizsgálatok végrehajtása a Társaság felelőssége, melyet szintén a Társaság Ügyvezetői hagynak jóvá, az MVM Zrt. Csoportszintű Biztonsági Igazgató előzetes jóváhagyásával (D-27).

Az üzemviteli rendszereken rendszeres sérülékenység vizsgálatot kell végrehajtani, valamint új üzemviteli rendszer alkalmazása vagy bevezetése esetén is.

A sérülékenység vizsgálatoknak ki kell terjedniük minden, az MVM Csoport által alkalmazott, az informatikai szolgáltató, a biztonsági szolgáltató, illetve a Társaság által üzemeltetett ügyviteli és technológiai rendszerekre egyaránt, az üzemeltető által végzett és a társasági információbiztonsági felelős által benyújtott kockázatelemzés alapján kijelölt rendszerekre vonatkozóan. A sérülékenység vizsgálat kiterjedhet a teljes infrastruktúrára, illetve adott kijelölt alkalmazásokra egyaránt. A vizsgálatok célja és hatóköre auditonként eltérő lehet, ezeket a sérülékenység vizsgálat megkezdése előtt, dokumentált módon rögzíteni kell.

A sérülékenység vizsgálatoknak az alábbiakra kell kiterjedniük az audit hatókörétől függően:

- külső támadások lehetőségeinek azonosítása,
- belső támadások lehetőségeinek azonosítása,
- nem megfelelő beállítások, konfigurációk azonosítása,
- hálózati eszközök sérülékenységei,
- informatikai rendszerek, alkalmazások sérülékenységei,
- adatbázisok sérülékenységei,
- felhasználók, illetve környezet sérülékenységei.

Ügyviteli rendszerek esetében az informatikai szolgáltató felelőssége a sérülékenység vizsgálatok rendszeres, ütemezett végrehajtása.

A sérülékenység vizsgálat lehet belső végrehajtású, automatikus tesztelés, amennyiben a Társaság rendelkezik a megfelelő eszközökkel, illetve külső fél által végrehajtott független audit

is. Külső fél által végrehajtott sérülékenység vizsgálat lehet a biztonsági szolgáltató által végrehajtott audit, vagy a biztonsági szolgáltató kontrollja alatt álló harmadik fél által végrehajtott penetrációs teszt is. Külső fél bevonása esetén a MOB-BSz-17-NY-03 formanyomtatvány kitöltése és aláírása szükséges a vizsgálatok megkezdése előtt.

5.23.3. Üzletfolytonossági és rendkívüli helyzetkezelési auditok

Az üzletfolytonossági és rendkívüli helyzetkezelési auditok célja a Társaság üzletfolytonossági és rendkívüli helyzetkezelési rendszer elemeinek mind szabályozói, mind gyakorlati oldalú vizsgálata, a nem-megfelelősségek feltárása, és a rendszer hatékonyságát növelő, fejlesztését elősegítő intézkedési javaslatok megfogalmazása.

Az auditok során ellenőrizni kell a Társaságra vonatkozó rendkívüli helyzetkezelési tervek és a rendkívüli helyzetekre vonatkozó egyéb szabályozók tekintetében:

- a központi lefektetett elvárásoknak történő megfelelést,
- frissítések gyakoriságát,
- mikor kerültek alkalmazásra és milyen eredménnyel,
- mikor kerültek legutóbb tesztelésre és milyen eredménnyel,
- biztosított-e a rendkívüli helyzetkezelési teendők oktatása és milyen formában,
- az érintett munkatársak tisztában vannak-e a feladataikkal,
- a társaságok naprakészen tartják-e és ellenőrzik-e a rendkívüli helyzetkezelési tervek által elvárt eszközrendszert és biztosított-e a tervekben rögzített erőforrások rendelkezésre állása.

6. Kapcsolódó folyamatutasítások

- MOB-FU-17-01 Az MVM Mobiliti Kft. Társasági információbiztonsági rendszer kialakítása és működtetése című folyamatutasítása
- MOB-FU-17-02 Az MVM Mobiliti Kft. Társasági jogosultságok információbiztonsági kezelése című folyamatutasítása
- MOB-FU-17-03 Az MVM Mobiliti Kft. Társasági információbiztonsági események és incidensek jelentése, kezelése című folyamatutasítása
- MOB-FU-17-04 Az MVM Mobiliti Kft. Társasági rendkívüli helyzetkezelés felkészülési feladatai című folyamatutasítása
- MOB-FU-17-05 Az MVM Mobiliti Kft. Társasági rendkívüli helyzet bejelentése című folyamatutasítása
- MOB-FU-17-06 Az MVM Mobiliti Kft. Társasági rendkívüli helyzet kezelése című folyamatutasítása
- MOB-FU-17-07 Az MVM Mobiliti Kft. Társasági belső információbiztonsági auditok végrehajtása című folyamatutasítása

7. Hatályon kívül helyezés

Nincs hatályon kívül helyezendő dokumentum.

8. Mellékletek és formanyomtatványok

- MOB-BSz-17-M-01 Az MVM Mobiliti Kft. Információbiztonsági és rendkívüli helyzetkezelési belső szabályzatának hivatkozásai
- MOB-BSz-17-M-02 Az MVM Mobiliti Kft. Információbiztonsági és rendkívüli helyzetkezelési belső szabályzatának meghatározásai
- MOB-BSz-17-M-03 Az MVM Mobiliti Kft. Információbiztonsági Politikája
- MOB-BSz-17-M-04 Az MVM Mobiliti Kft. Információbiztonsági Stratégiája
- MOB-BSz-17-M-05 Az MVM Mobiliti Kft. információbiztonsági kockázatelemzésének módszertani követelményei

- MOB-BSz-17-M-06 A Társasági információbiztonsági követelmények megszegésének esetei és szankcionálásának szempontjai
- MOB-BSz-17-M-07 Az MVM Mobiliti Kft. esetében alkalmazott adatbiztonsági kategóriák
- MOB-BSz-17-M-08 A Társasági adatok kezelésére vonatkozó információbiztonsági követelmények
- MOB-BSz-17-M-09 A Társasági dokumentumok nagy mennyiségű szállításának információbiztonsági követelményei
- MOB-BSz-17-M-10 Az MVM Mobiliti Kft. felhő alapú rendszereinek információbiztonsági vizsgálati szempontjai
- MOB-BSz-17-M-11 Vezeték nélküli hálózatok és kapcsolódó jogosultságok a Társaságon belül
- MOB-BSz-17-M-12 A Társaságon belül tiltott internetes oldalak
- MOB-BSz-17-M-13 A Társasági projektszoba, illetve adatszoba általános információbiztonsági követelményei
- MOB-BSz-17-M-14 REVIR Központi Ügyelet elérhetőségei
- MOB-BSz-17-M-15 Üzletfolytonossági módszertan
- MOB-BSz-17-M-16 Rendkívüli helyzetkezelési rendszer szereplői és feladatai
- MOB-BSz-17-M-17 Információbiztonsági és rendkívüli helyzetkezelési Döntési Hatásköri Lista
- MOB-BSz-17-NY-01 Elektronikus levelezés használatának szabályai és tudomásul vételi nyilatkozat külső fél részére
- MOB-BSz-17-NY-02 Társasági incidens riport az MVM Zrt. Csoportszintű Biztonsági Igazgatósága részére adott időszakra vonatkozóan
- MOB-BSz-17-NY-03 Hozzájárulási nyilatkozat sérülékenység vizsgálat végrehajtásához

A KIE-17 Az MVM Csoport információbiztonsági és rendkívüli helyzetkezelési központi irányelvében szereplő mellékletek és formanyomtatványok jelen Szabályzat végrehajtása során kötelezően alkalmazandóak.

MÓDOSÍTÁS NYILVÁNTARTÓLAP

MÓDOSÍTÁSOK		
MÓDOSÍTÁS SZÁMA	**MÓDOSÍTÁS DÁTUMA**	**MÓDOSÍTÁS LEÍRÁSA (JELLEGE)**

AZ MVM MOBILITI KFT. INFORMÁCIÓBIZTONSÁGI ÉS RENDKÍVÜLI HELYZETKEZELÉSI BELSŐ SZABÁLYZATÁNAK HIVATKOZÁSAI

- MSZ EN ISO 9001:2015 Minőségirányítási rendszerek. Követelmények
- MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonsági irányítási rendszerek. Követelmények
- Az Európai parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)
- 2009. évi CLV. törvény a minősített adat védelméről
- 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- 2013. évi V. törvény a Polgári Törvénykönyvről
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról
  234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról
- 1995. évi LIII. törvény a környezet védelmének általános szabályairól
- 2007. évi LXXXVI. törvény a villamos energiáról
  280/2016. (IX. 21.) Korm. rendelet a villamosenergia-rendszer jelentős zavara és a villamosenergia-ellátási válsághelyzet esetén szükséges intézkedésekről
- 2008. évi XL. törvény a földgázellátásról
- 110/2020. (IV. 14.) Korm. rendelet a földgázvételezés korlátozásáról, a földgáz biztonsági készlet felhasználásáról, valamint a földgázellátási válsághelyzet esetén szükséges egyéb intézkedésekről
- a magyar villamos energia rendszer üzemi szabályzata (3069/2014. számú MEKH határozattal jóváhagyva)
- a magyar földgázrendszer üzemi és kereskedelmi szabályzata (505/2016. számú MEKH határozattal jóváhagyva)
- 4/2016. (VII. 28.) NMHH rendelet az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszeréről, valamint a szolgáltatók bejelentési és kapcsolattartási kötelezettségeiről
- 1324/2011. (IX. 22.) Korm. határozat a kormányügyeleti rendszer létrehozásáról
- 39/2019. (X. 31.) ITM utasítás a kormányügyeleti rendszer minisztériumi feladatainak meghatározásáról.
- Az MVM Csoport Információbiztonsági és rendkívüli helyzetkezelési központi irányelve (KIE-17)

AZ MVM MOBILITI KFT. INFORMÁCIÓBIZTONSÁGI ÉS RENDKÍVÜLI HELYZETKEZELÉSI BELSŐ SZABÁLYZATÁNAK MEGHATÁROZÁSAI

Active Directory (AD)
Az AD a Microsoft egyes hálózati szolgáltatásainak gyűjtőneve. Fő célja a számítógépek részére autentikációs és autorizációs szolgáltatások nyújtása, lehetővé téve a hálózat minden publikált erőforrásának (fájlok, megosztások, perifériák, kapcsolatok, adatbázisok, felhasználók, csoportok stb.) központosított adminisztrálását.

Adat
Az adat tények, fogalmak, eligazítások olyan formai megjelenése, amely alkalmas az emberi vagy az automatikus eszközök által történő értelmezésre, vagy feldolgozásra.

Adatbiztonsági osztály (adatbesorolási kategória)
Az adatok kategorizálása érzékenységük szerint.

Adatfeldolgozó
Az a személy vagy szervezet, aki/amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi.

Adatgazda
Annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik. Minden társaságnál szükséges az adatgazdák kijelölése.

Adatkör
Logikailag egy egységbe sorolható adatok halmaza (pl. munkaszerződések).

Adatszivárgást megelőző rendszer (DLP rendszer)
Olyan informatikai rendszerek, melyek észlelik, és lehetőség szerint megakadályozzák a bizalmas információk jogosulatlan használatát, illetve továbbítását. A DLP (Data Loss Prevention) szoftver és megoldás olyan informatikai védelmi rendszert jelent, amely azonosítja, monitorozza és megvédi a bizalmas adatokat, mind a végpontok, a hálózat és az adattárolók tekintetében. Ez a védelem átfogó tartalom alapú vizsgálattal, az adatfolyamok biztonsági elemzésével (a létrehozó jogosultságai, az adatok tárgya, az időzítés, címzett/célállomás, stb.), és egy központosított menedzsment rendszer segítségével történik.

Adatvagyon
A társaság tulajdonában lévő, a társaság működése során létrehozott, feldolgozott, tárolt és továbbított információhalmaz.

Adatvagyon felmérés
A folyamatok által használt adatvagyon elemek, valamint az azokhoz kapcsolódó, a további vizsgálatokhoz és kezeléshez tartozó paraméterek azonosítása, mely vonatkozik a társaság papír alapú és elektronikus adatvagyonára egyaránt.

Adatvagyon leltár
Az adatvagyon felmérés eredményét tartalmazó adatbázis vagy dokumentum, mely tartalmazza a társaság védendő adatait.

Adatvesztési tolerancia (Recovery Point Objective - RPO)
Egy rendkívüli esemény bekövetkezésétől visszafelé számított időtartam, melyre vonatkozóan az üzleti terület elviseli, tolerálja az adatvesztést. Az adatok mentését úgy kell megoldani, hogy adatvesztés csak ezen időtartamon belül következhet be.

Alapjogosultság
Azon jogosultságok összessége, melyek elengedhetetlenek ahhoz, hogy a munkavállaló hozzáférjen a munkája ellátásához szükséges alapvető informatikai rendszerekhez.

Alternatív folyamat
A társaság folyamatának megszakadása esetén, az üzletfolytonossági tervekben foglaltak alapján végrehajtandó, előre meghatározott és elfogadott szinten történő működést lehetővé tevő helyettesítő folyamat, annak részletes lépései az ellátáshoz szükséges eszközök, ezen erőforrások és felelősök megjelölésével.

Alternatív folyamat fenntarthatósági ideje
Az üzletfolytonossági tervben foglalt alternatív működési folyamat előre meghatározott szinten történő működtetésének, fenntartásának maximális időkerete.

Alternatív telephely
Olyan működési helyszín, amely alkalmas a társaság kritikus folyamatának fenntartására egy előre meghatározott és elfogadott működési szinten, amennyiben annak esetleges megszakadását a munkavégzés eredeti helyének, vagy támogató infrastruktúrájának elérhetetlensége vagy működésképtelensége okozza.

Authentikáció
Az a folyamat, amely során a rendszer ellenőrzi a felhasználó személyazonosságát (pl. felhasználónév és jelszó bekérésével).

Authorizáció
Annak ellenőrzése, hogy az adott felhasználónak van-e jogosultsága az adott tevékenység végrehajtására (pl. programok telepítése).

Beléptető rendszer
Olyan rendszer, mely biztosítja, hogy az adott biztonsági zónába csak azonosítás után és a megfelelő jogosultsággal rendelkezők léphessenek be, valamint a beléptetés ellenőrizhető legyen.

Biometrikus azonosítás
A biometrikus azonosítás arra irányul, hogy a személyeket egyedi fizikai jellemzőik alapján azonosítsa. Előnye, hogy nem szükséges egyéb olyan azonosító eszköz, ami elveszíthető vagy ellopható. Ezen túlmenően megnehezíti az egyén azonosságának hamisítását, ezzel növelve a biztonságot.

Bizalmasság (confidentiality)
Annak biztosítása, hogy az adatokhoz, információkhoz csak az arra jogosultak és csak a jogosultságuk szintje szerint férhetnek hozzá, ismerhetik meg, használhatják fel, illetve rendelkezhetnek felhasználásáról.

Biztonsági zóna
Olyan, fizikailag jól elhatárolható terület, mely az ott tárolt, kezelt, vagy éppen elhangzott információk biztonsági besorolásának függvényében került kialakításra.

Biztonsági szolgáltató központ
MVM BSZK Biztonsági Szolgáltató Központ Zártkörűen Működő Részvénytársaság (MVM BSZK Zrt.)

Csoportszintű informatikai szolgáltató
MVM Informatika Zártkörűen Működő Részvénytársaság (MVMI Zrt.)

Csoportszintű információbiztonsági fórum
Évente 2 alkalommal összehívott fórum, melynek célja, hogy résztvevői megvitassák az elmúlt időszak információbiztonsági eseményeit, megosszák egymással tapasztalataikat, beszámoljanak a csoportszintű, illetve társasági célok megvalósulásáról, egyeztessék a következő időszak vállalatcsoportot érintő feladatait.

Csoportszintű Krízis Team (CSKT)
Az MVM Zrt.-ben alakuló, a rendkívüli helyzet kezelésének irányítását vagy az elhárítás csoportszintű koordinációját (üzletfolytonossággal kapcsolatos folyamatok, illetve társaságok közötti koordinációt) végző, a társasági Krízis Team munkáját a központi funkciók támogatásával segítő, az egyedi igényekre reagálni képes, ezért összetétele tekintetében rugalmas testület.

Csoportszintű üzletfolytonossági módszertan
Tartalmazza társaságnál egységesen alkalmazandó elvek alapján az üzletfolytonossági dokumentáció kidolgozásához, karbantartásához, oktatásához és teszteléséhez szükséges részletes lépéseket, feladatokat valamint segédleteket.

Dedikált USB eszköz
Az MVM Csoport társaságai által adatok vállalaton belüli/kívüli továbbítására kizárólagosan alkalmazható, központilag, az informatikai szolgáltató által biztosított és menedzselt, AD-hoz rendelt hordozható adattároló (pl. pendrive, külső merevlemez).

Demilitarizált zóna (DMZ)
Olyan fizikai vagy logikai alhálózat, ami egy szervezet belső szolgáltatásait tartalmazza és tárja fel egy nagyobb, nem megbízható hálózatnak, általában az internetnek. A DMZ célja, hogy egy plusz biztonsági réteget biztosítson a szervezet helyi hálózatának (LAN), így egy esetleges külső támadónak csak a DMZ-ben található elemekhez lehet hozzáférése, nem az egész hálózathoz.

Detektív védelmi intézkedés
A szabálysértések, információbiztonsági incidensek felderítésére irányuló cselekmények, kontrollok, eszközök.

Direct Access (DA) / Távoli hozzáférés
Az MVMI Zrt. által e célra biztosított hordozható eszközökön a Direct Access alkalmazása teszi lehetővé a felhasználó számára a munkavégzéshez szükséges társasági adatok és rendszerek távoli elérését.

Dominóhatás
Adott társaság működése során bekövetkező olyan rendkívüli esemény, amely a vele kapcsolatban álló társaságokra, szervezetekre, szervezeti egységekre átterjedve a rendkívüli helyzet kialakulásának valószínűségét és lehetőségét megnöveli, vagy a bekövetkezett rendkívüli eseménnyel kapcsolatos következményeket súlyosbítja.

DPO: Data Protection Officer
A GDPR 37-39. cikke szerinti adatvédelmi tisztviselő(k).

Egyéb biztonsági esemény
Azon információbiztonsági események, melyek nem sorolhatók be sem a fizikai, sem az informatikai biztonsági kategóriába.

Egyéb biztonsági incidens
Azon információbiztonsági incidensek, melyek nem sorolhatók be sem a fizikai, sem az informatikai biztonsági kategóriába.

Elektronikus archiválás
Az adott informatikai rendszerből háttér tároló(k)ra kerülnek átmozgatásra konzisztensen és hitelesen az adatok.

Elszámoltathatóság (számonkérhetőség - accountability)
Annak biztosítása, hogy az adott felhasználó által végzett tevékenységek egyértelműen az adott felhasználóra legyenek visszavezethetők.

Erőforrás gazda
Társaság, vagy a társaság kijelölt vezetője, aki a társaság tulajdonában, vagy rendelkezési jogosultságában álló erőforrások (például emberi erőforrás, technikai erőforrás, informatikai erőforrás stb.) tervezéséért, működtetéséért, helyreállításáért felelősséggel tartozik.

Erőforrás helyreállítási terv (Disaster Recovery Plan - DRP)
Olyan dokumentum (cselekvési terv), ami részletes leírást tartalmaz egy rendkívüli esemény miatt kiesett/meghibásodott erőforrás helyreállítása érdekében szükséges teendőkről, feladatokról.

Erős/több faktoros authentikáció
Többlépcsős/multifaktoros (MFA) azonosítás, mely során a felhasználók a felhasználónév-jelszó páros mellett egyéb eszközök alkalmazásával is azonosítják magukat, például tokennel, vagy SMS-ben kapott kód megadásával.

Értesítési lista
A társaságok által folyamatosan karbantartott jegyzék, melyben valamennyi rendkívüli helyzetben feladat-, vagy hatáskörrel rendelkező személy és szervezeti egység elérhetőségei (név, beosztás, e-mail cím, vezetékes és mobilszám) egy helyen megtalálhatóak.

Esemény
Minden olyan állapotváltozás, amelynek jelentősége van a folyamatok, a szolgáltatások menedzsmentjében és amelyek a folyamatot működtetők, illetve a szolgáltatásokat nyújtó részéről beavatkozást igényel és gyakran vezet naplózandó incidensekhez.

Fizikai biztonsági esemény
Olyan állapot előfordulása, amely a biztonsági szabályzat lehetséges megsértésére, vagy a védelmi intézkedések hiányára vagy nem-megfelelő működésére, vagy a biztonsággal összefüggő, korábban nem ismert helyzetre utal és fennállása fizikai biztonsági incidenshez vezethet. Fizikai biztonsági esemény esetében konkrét károkozás nem történt, de fennáll a lehetősége, hogy az esemény kezelésének elmulasztása esetén a szervezet kárt szenved egy későbbi támadás során.

Fizikai biztonsági incidens
Nem kívánt vagy nem várt, egyedi vagy sorozatos fizikai biztonsági események, amelyek nagy valószínűséggel veszélyeztetik a védett létesítményben tevékenykedő személyeket, erőforrásokat és vagyonelemeket, ezzel tényleges vagy feltételezhető kárt okozva a társaság számára.

Folyamatgazda
A minőségügyi és szabályozási szabályzat definiálja a folyamatgazda fogalmát.

Forensic labor
Olyan informatikai laboratórium, ahol informatikai és információbiztonsági események/incidensek kivizsgálása lehetséges szakértők által dokumentált körülmények között.

Földgáz üzemzavar
A GET. 3.§-a értelmében minden olyan a földgáz termelését, tárolását, szállítását, elosztását korlátozó vagy megszüntető esemény, amelynek oka az együttműködő földgázrendszer normál üzemmenettől eltérő olyan működése, amelynek következménye veszélyeztetés vagy földgázellátási zavar, és amely egy vagy több felhasználó földgázellátásának szünetelését okozza.

Földgázellátási válsághelyzet
A GET. 97. § (1) bekezdése értelmében az az esemény, amely a személyeket, vagyontárgyaikat, a természetet, a környezetet vagy a felhasználók jelentős részének ellátását veszélyezteti. Földgázellátási válsághelyzetet a következő események válthatnak ki:

- a földgázellátás és földgázfelhasználás egyensúlya oly mértékben felbomlik, hogy azt a szokásos egyensúlytartási eszközökkel már nem lehet helyreállítani,
- a földgáz-felhasználási igények meghaladják a beszerzés lehetőségeit, illetve
- ezek közvetlen veszélye fenyeget.

Földgázellátási zavar
A GET. 96. § (1) bekezdése értelmében minden olyan, a földgázellátási válsághelyzetet el nem érő mértékű, jellemzően területi (regionális) zavar, amely az elosztó- és szállító hálózat, valamint a földgáztároló üzembiztonságát, szabályozhatóságát vagy együttműködő képességét súlyosan veszélyezteti, és amely következtében az együttműködő földgázrendszer egyensúlya csak egyes felhasználók földgázvételezésének korlátozásával biztosítható.

HelpDesk
Az MVMI Zrt. Ügyfélszolgálati Osztálya, amely támogatja informatikai kérdésekben a munkavállalókat.

Helyreállítási idő (Recovery Time Objective – RTO)
Az az időtartam, amennyi idő alatt a kiesett erőforrás, vagy szolgáltatás helyreállítandó rendkívüli esemény bekövetkezte után, figyelemmel az alternatív folyamat fenntarthatósági idejére is (számítása: maximálisan elfogadható kiesési idő és a visszaállítási idő különbsége).

Helyreállítási terv
Azon intézkedések rendszerezett, tervezett együttes végrehajtását leíró műszaki szemléletű dokumentum, amelyekkel a társaság a rendkívüli esemény bekövetkezése után a lehető leghamarabb képes - az általa nyújtott, vagy menedzselt - kiesett szolgáltatások, erőforrások, működési feltételek eredeti állapotba történő helyreállítására. Tartalmazza az eredeti szolgáltatás, vagy erőforrás helyreállításának, vagy cseréjének, illetve beüzemelésének és ellenőrzésének lépéseit felelősökkel.

Hitelesség (authenticity)
Annak biztosítása, hogy egy tárgy vagy erőforrás azonossága az, aminek állítják. A hitelesség olyan entitásokra vonatkozik, mint a felhasználók, a folyamatok, a rendszerek és az információ.

Image
Informatikai eszköz adatait tartalmazó komplett biztonsági mentés.

Információbiztonság (information security)
Az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzésére; továbbá egyéb tulajdonságok, mint a hitelesség, az elszámoltathatóság, a letagadhatatlanság és a megbízhatóság biztosítására irányuló gyakorlat, tevékenységek, folyamatok halmaza.

Információbiztonsági esemény
Olyan állapot előfordulása, amely az információbiztonsági szabályzat lehetséges megsértésére, vagy a védelmi intézkedések hiányára vagy nem-megfelelő működésére, vagy az információbiztonsággal összefüggő, korábban nem ismert helyzetre utal és fennállása információbiztonsági incidenshez vezethet. Információbiztonsági esemény esetében konkrét károkozás nem történt, de fennáll a lehetősége, hogy az esemény kezelésének elmulasztása esetén a szervezet kárt szenved egy későbbi támadás vagy meghibásodás során.

Információbiztonsági incidens
Nem kívánt vagy nem várt, egyedi vagy sorozatos információbiztonsági események, amelyek nagy valószínűséggel veszélyeztetik az üzleti tevékenységet és fenyegetik az információk biztonságát, ezzel kárt okozva a társaság számára.

Információbiztonsági politika
Az információbiztonsági rendszer magas szintű dokumentuma, mely a biztonsági célok és alapelvek meghatározása mellett kinyilvánítja a felső vezetés információbiztonság iránti elkötelezettségét is.

Információbiztonsági rendszer
Olyan folyamatok összefüggő halmaza, melynek célja a társaság(ok) által használt információk és információs rendszerek azonosítása, azok információbiztonsági kockázatainak felmérése, kockázatarányos védelmi intézkedések bevezetése és folyamatok kialakítása, valamint azok hatékony menedzsmentje.

Információbiztonsági stratégia
Az információbiztonsági politikában meghatározott célok elérésének módját, a megvalósítandó védelmi intézkedések bevezetésének lépéseit, 3-5 év távlatában tartalmazó dokumentum.

Információbiztonsági szabályzat
Az információbiztonsági szabályokat, az alkalmazott védelmi intézkedéseket, követelményeket és felelősségeket tartalmazó dokumentum.

Inkrementális mentés
Növekményes adatmentés (biztonsági másolat készítése). Az inkrementális mentés alkalmazása esetén nem kerül elmentésre minden adat, hanem csak azok, amelyek egy korábbi mentés óta megváltoztak.

Irányfigyelés
Olyan beléptető rendszer technológia, hogy egy bizonyos személy csak akkor léphet ki egy zónából, ha előtte be is lépett.

Jogosultság menedzsment rendszer
A jogosultságok kiadására, módosítására és nyilvántartására, valamint azok felülvizsgálatára szolgáló informatikai rendszer vagy folyamat.

Katasztrófaesemény
A veszélyhelyzet kihirdetésére alkalmas, illetve e helyzet kihirdetését el nem érő mértékű olyan állapot vagy helyzet, amely emberek életét, egészségét, anyagi értékeiket, a lakosság alapvető ellátását, a természeti környezetet, a természeti értékeket olyan módon vagy mértékben veszélyezteti, károsítja, hogy a kár megelőzése, elhárítása vagy a következmények felszámolása meghaladja az erre rendelt szervezetek előírt együttműködési rendben történő védekezési lehetőségeit, és különleges intézkedések bevezetését, valamint az önkormányzatok és az állami szervek folyamatos és szigorúan összehangolt együttműködését, illetve nemzetközi segítség igénybevételét igényli.

Kiemelt jogosultsággal rendelkező felhasználók
Kiemelt jogosultsággal rendelkező felhasználók elsősorban a rendszeradminisztrátori feladatokat ellátó üzemeltetők, de ide értendő bármilyen adminisztrátori, illetve az olyan többletjogosultsággal rendelkező felhasználó (pl. Sharepoint oldal adminisztrátora), aki többletjogosultsága révén magasabb kockázatot jelent az általa kezelt és feldolgozott adatok bizalmasságának, sértetlenségének, illetve rendelkezésre állásának biztosítására.

Kiesési idő
Egy vagy több tevékenység (folyamat) megszakadásának időtartama.

Kockázat
Valamely fenyegetés megvalósulásának lehetősége, fenyegetettség mértéke, amely egy fenyegetés bekövetkezési gyakoriságának (bekövetkezési valószínűségének) és az ezáltal okozott kár nagyságának a függvénye.

Kockázatelemzés
Az információk és a hozzájuk kapcsolódó erőforrások értékének, sérülékenységének, fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.

Kockázat elfogadó stratégia
Alkalmazása a kis bekövetkezési valószínűségű, kis üzleti hatású kockázatok (pl. a fűtés meghibásodása vagy nyomtató, fax kiesése) esetén javasolt. Ezen kockázatok hatásának mértéke kellően alacsony ahhoz, hogy csökkentése érdekében a továbbiakban közvetlen intézkedésre nincs szükség.

Kockázatfedezeti stratégia
A kockázat tudomásul vételét és a pénzügyileg mérhető kockázatok kezelését jelenti arra vonatkozó biztosítások kötésével, erre szakosodott biztosító társaságokkal.

Kockázatkezelés
A kockázatok bekövetkezési gyakoriságának és/vagy bekövetkezéskori hatásának csökkentésére irányuló védelmi intézkedések kidolgozása, melynek feladata a fenyegetettségek elleni kockázatarányos védekezés.

Kockázatmegelőző stratégia
Proaktív kockázatkezelési stratégia, amely az előre nem jelezhető kockázatok, károsító hatások bekövetkezésének valószínűségét a lehető legkisebbre korlátozza.

Kompenzáló kontroll
Olyan védelmi intézkedés, amely ideiglenesen vagy véglegesen egy másik védelmi intézkedést helyettesít, illetve csökkenti a meglévő vagy potenciálisan fellépő, hibákat és hiányosságokat eredményező kontroll gyengeséget.

Kontroll
Lásd Védelmi intézkedés.

Kormányügyeleti tájékoztatást igénylő rendkívüli esemény
A kormányügyeleti rendszer minisztériumi feladatainak meghatározásáról szóló 39/2019. (X. 31.) ITM utasítás 2. § szerinti rendkívüli esemény:

- mindaz az előre nem látott veszély, vagy bekövetkezett esemény, amely a Magyarországot érintő potenciális vagy tényleges hatásában alkalmas az élet, a testi épség, az egészség, a vagyoni javak, a pénzügyi és a gazdasági ellátó rendszerek, a közigazgatási infrastruktúra, a természeti vagy az épített környezet olyan mérvű károsítására, továbbá a köznyugalom és a társadalom működésének olyan súlyos megzavarására, amely nagyságrendjénél fogva kormányzati fellépést igényel vagy igényelhet, függetlenül attól, hogy a konkrét helyzet eléri-e az Alaptörvény 48-53. cikkében

foglalt minősített időszak szintjét, vagy azt az ország határain belül vagy kívül keletkezett ok váltja ki;
- az NFM utasítás 1. mellékletében szereplő, a nemzeti fejlesztési miniszter vezetése, irányítása és felügyelete alatt álló szervekre (mint ágazati biztonsági ügyeletekre) vonatkozó,
- rendkívüli eseményeket tartalmazó jegyzékben foglaltak szerint.

Korrektív védelmi intézkedés
A szabálysértések, információbiztonsági incidensek bekövetkezése utáni elhárításra irányuló cselekmények, kontrollok, eszközök.

Környezeti káresemény
A rendkívüli esemény, melyből fakadóan bármely környezeti elemet többletterhelés éri vagy nagy valószínűséggel érheti, illetve többlet hulladékképződés keletkezik, vagy nagy valószínűséggel keletkezhet, különösen a jogszabályban szabályozott küszöbértéket elérő felszíni vizek szennyezése, földtani közeg- és felszín alatti vizek szennyezése, légszennyezés, zajártalom.

Kriptográfiai eszközök
Titkosítást lehetővé tevő eszközök, melyek alkalmazásával csökkenthető a kezelt adatok bizalmasságának sérülése. Kriptográfiai eszköz például a teljes merevlemez titkosítás, jelszavas tömörítés, stb.

Kritikus folyamat
Azok a társasági folyamatok, amelyek kiesésekor bizonyos kárhatások előre meghatározott mértékű bekövetkezésére lehet számítani.

Kritikus időszak
Az üzleti terület által meghatározott időintervallum, a naptári év egy adott szakasza, vagy ismétlődően előforduló időpont, illetve egy prioritást élvező tevékenység végrehajtásának időszaka, amely alatt a társaság kritikus folyamata nem sérülhet, vagy működésének megszakadása nem fogadható el.

Kritikus munkakör
Olyan munkakör, amely az MVM Csoportban alkalmazott adatbiztonsági kategóriákba definiáltaknak megfelelően a 4-es Társasági bizalmas adatok és az 5-ös Társasági szigorúan bizalmas adatok szintjéhez hozzáfér, vagy ahhoz jogosultságot tud adni. Továbbá kritikus munkakört töltenek be a társaság kritikus folyamatainak működtetéséhez nélkülözhetetlen munkakörök.

Krízis Központ
Olyan működési helyszín, amely alkalmas a Csoportszintű Krízis Team és Válságkommunikációs Team működésének támogatására a munkavégzés eredeti helyén, vagy az alternatív telephelyen az eredeti helyszín, vagy annak egyes részeinek, támogató infrastruktúrájának elérhetetlensége esetén. A Krízis Központban megtalálható a Csoportszintű Krízis Team és a Válságkommunikációs Team számára mindazon eszköz és technológia, amely szükséges a rendkívüli helyzet fizikai és kommunikációs kezeléséhez.

Krízis szintek
A rendkívüli helyzet besorolása annak jellege és súlyossága alapján, amely rögzíti a kezelésbe bevonandó szereplőket. A REVIR Központi Ügyeletet minden szint esetében köteles tájékoztatni az érintett társaság.

1. szint (Helyi): Olyan rendkívüli esemény, amely kezelése érdekében nem szükséges a társasági Krízis Team összehívása, a Krízis Koordinátor bevonása. Az esemény hatása az érintett társaságon belül, egy adott területet, szervezeti egységet érint, a társaság képes saját erőforrásaival, a belső automatizmusai mentén kezelni az eseményt.
2. szint (Társasági): Olyan rendkívüli esemény, amely kezelése érdekében szükséges a társasági Krízis Team összehívása, a Krízis Koordinátor bevonása. Az esemény hatása az

érintett társaságon belül marad, a társaság képes saját erőforrásaival kezelni az eseményt. Az MVM Zrt. illetékes kijelölt vezető munkatársa, vagy illetékes REVIR Tanácsadója rendelkezésre áll, elemzi és segíti a helyzet megoldását, vagy a Rendkívüli Események Figyelőszolgálatának döntése alapján a társasági Krízis Team-be vagy a Krízis Koordinátor mellé delegálva közvetlenül segíti az esemény kezelését.

3. szint (Csoport): Olyan rendkívüli esemény, amely kezelése érdekében szükséges a Csoportszintű Krízis Team összehívása. Az esemény hatása a vállalatcsoport több társaságát érinti, dominóhatást okoz, az érintett társaság nem, de a vállalatcsoport képes saját erőforrásaival kezelni az eseményt. A megalakuló Csoportszintű Krízis Team is végezheti a rendkívüli esemény kezelésének irányítását, vagy a védekezés csoportszintű koordinálását.
4. szint (Állami): Olyan rendkívüli esemény, amely kezelése érdekében szükséges az állami védelmi igazgatási vagy központi kormányzati szerveknek átadni az irányítást, mert a társasági Krízis Team, a Krízis Koordinátor vagy a Csoportszintű Krízis Team nem képes saját erőforrásaival kezelni, vagy jogszabály alapján nem jogosult az esemény kezelésének irányítására. Az esemény hatása a vállalatcsoporton túlmutat (pl: nemzetgazdaság működését érintő, lakosságot vagy a vállalatcsoport területén kívüli környezetet érintő, országhatáron túlnyúló hatású, állami szervek összehangolt beavatkozását igénylő, stb.). A társasági Krízis Team, a Krízis Koordinátor, vagy a Csoportszintű Krízis Team az elhárításban, eseménykezelésben továbbra is szakmai támogatást nyújt az állami szervek részére.

Külső közreműködők
Külső szereplőnek minősül minden olyan, nem az adott társaság szervezetébe tartozó intézmény, szervezet, vállalkozás vagy egyén, aki jogszabályi előírás, kinyilvánított kölcsönös együttműködési szándék, vagy egyoldalú akarat alapján a társaság működésével kapcsolatban adatot, információt állít elő, ismer meg, kezel, publikál.

Letagadhatatlanság (non-repudiation)
Olyan garanciát jelent, amellyel valamely cselekmény, illetve esemény megtörténte oly módon bizonyítható, hogy azok később nem tagadhatóak le (pl. elektronikus aláírás használata által).

MAC address szűrés
A MAC address szűréssel lehetőség nyílik arra, hogy kizárólag az előre meghatározott fizikai címmel rendelkező eszközök számára legyen a LAN-hálózathoz hozzáférés, megakadályozva ezzel az idegen eszközök belső hálózathoz történő csatlakoztatását.

Malware (kártékony kód)
Rosszindulatú számítógépes programok összefoglaló neve. Ide tartoznak például a vírusok, férgek (worm), kémprogramok (spyware), agresszív reklámprogramok (adware), és a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök (rootkit).

Maradványkockázat
A maradványkockázat a kockázatkezelési stratégia ismeretében a védelmi intézkedések alkalmazását követően fennmaradó kockázat.

Maximálisan elfogadható kiesési idő (Maximum Tolerable Downtime –MTD)
Egy adott folyamat vonatkozásában meghatározott azon maximális időintervallum, amely még elfogadhatónak tekinthető a társaság üzletmenetének zavartalan, jelentős károk nélküli fenntartása szempontjából.

Mobil eszközök
Minden olyan számítástechnikai eszköz, amely fizikailag szabadon mozgatható és funkcionalitását betölti mozgás közben is. Ide sorolhatók a hordozható számítógépek, illetve a velük azonos adattárolási, adatkezelési és adatmegjelenítési funkciókkal bíró telekommunikációs

eszközök (pl. tablet, notebook, okostelefon, stb), valamint a hordozható adattárolók (pl. külső merevlemez, pendrive, stb.).

Mobil eszköz menedzsment (MDM - Mobile Device Management vagy EMM – Enterprise Mobility Management)
A mobil eszközök biztonságos használatának megteremtése érdekében alkalmazott központi irányítási és kontroll funkciókat biztosító megoldás, rendszer.

MVM Csoport
Az MVM Csoport Központi Irányítási Kódexe alapján azon heterogén jogi személyek összessége, melyekben az MVM Zrt. a Ptk. szerinti többségi befolyással rendelkezik, függetlenül attól, hogy adott jogi személy létesítése, illetve működése Magyarország vagy bármely más külföldi állam jogrendszere alapján történt.

Port security
Lásd MAC address szűrés.

Preventív védelmi intézkedés
A szabálysértések, információbiztonsági incidensek megelőzésére irányuló cselekmények, kontrollok, eszközök.

Prioritási lista
Tartalmazza a szabályzóban meghatározott jogosult által előre megállapított, illetve rendkívüli esemény bekövetkezésekor felülvizsgált azon kritikus társasági, vagy csoportszintű folyamatokat, illetve erőforrásokat vagy szolgáltatásokat, amelyek a csoportszintű üzletfolytonosság fenntartása, illetve a helyreállítások során prioritást kell, hogy élvezzenek. A prioritási körbe tartozó folyamatok, és erőforrások, szolgáltatások megállapítása során figyelemmel kell lenni:

- a kritikus folyamatok, szolgáltatások kiesése esetén várható kárérték nagyságára,
- a kieséssel okozható dominóhatás terjedelmére,
- jogszabályi kötelezettség teljesítésére,
- energiaellátó rendszerek üzembiztonságának és működőképességének fenntartására,
- technológiai rendszerek műszaki sajátosságaira,
- kritikus időszakokra.

Release csomagok
Egy számítógépes szoftver, rendszerint fejlesztési fázisában, a javításokat, módosításokat, frissítéseket tartalmazó kiadás.

Rendelkezésre állás (availability)
Annak biztosítása, hogy az adatok szükség esetén az arra jogosult személy számára a megfelelő helyen, megfelelő időn belül, a megfelelő minőségben elérhetőek legyenek.

Rendkívüli esemény
(Rendkívüli helyzet) Minden olyan, a rendeltetésszerű működéstől jelentősen eltérő, nem várt esemény, vagy körülmény, amely személyek életét, testi épségét, illetve anyagi javakat tekintve súlyos következményekre vezetett, vagy reális veszélye van annak, hogy vezetni fog, illetve a társaság, vagy a vállalatcsoport működésében komoly zavart okoz vagy okozhat, és amely beavatkozást igényel. A rendkívüli eseményeknek két típusát különböztetjük meg: üzletfolytonossági esemény és katasztrófa esemény.

Rendkívüli Események Figyelőszolgálata (REF)
Az MVM Zrt. műszaki vezérigazgató-helyettes irányítása alatt álló stáb, amely átfogó ismeretekkel rendelkezik az MVM Csoport működési rendjét illetően, ezért hozzá valamennyi, az MVM Csoportot érintő rendkívüli eseményről, bármely időszakban a REVIR Központi Ügyeleten keresztül bejelentés érkezhet.

Rendkívüli Események Vezetői Információs Rendszere (REVIR)
A rendkívüli eseményekkel kapcsolatos hatékony információáramlást, folyamatosan rögzíthető dokumentálást és döntéshozatalt támogató tájékoztatási rendszer, amely működtetése informatikai és folyamatos elérhetőséget biztosító szervezeti támogatással valósul meg.

REVIR értesítési lista
A társaságok REVIR ügyeleteseinek beosztását, csoportszinten összesítetten tartalmazó lista, amelyet a társasági adatszolgáltatás alapján a REVIR Központi Ügyelet kezel.

REVIR jelentésköteles esemény
Azon rendkívüli események, amelyekkel kapcsolatos információkat és tájékoztatást a társasági REVIR Ügyeletesnek haladéktalanul, vagy a jelen szabályzóban meghatározott határidőig szükséges a REVIR Központi Ügyelet számára jelentenie.

REVIR Központi Ügyelet
A REVIR rendszerben kezelendő értesítések csoportszinten történő fogadásáról, rögzítéséről, naplózásáról, valamint az érintettek tájékoztatásáról folyamatosan 7/24 rendszerben gondoskodó, az MVM Csoport központi ügyeleti szolgálata, amelyet a biztonsági szolgáltató működtet. A REVIR jelentésköteles eseményekkel kapcsolatos információkat és tájékoztatást eljuttatja a Rendkívüli Események Figyelőszolgálata, valamint az ügyeletes REVIR tanácsadó részére. A REVIR Központi Ügyelet a tájékoztató rendszer működtetését, annak humán, technikai és informatikai hátterét a működéshez szükséges, mindenkor rendelkezésére álló kapacitások, eszközök és hálózatok felhasználásával és rendszeresített létszámával végzi. A REVIR Központi Ügyelet szakmai támogatását a társaságok egyes kijelölt munkavállalói, mint társasági REVIR ügyeletesek, illetve a REVIR tanácsadók végzik.

REVIR tanácsadó
Az MVM Zrt. döntési jogosultsággal felruházott munkavállalója, aki a rendkívüli esemény jellegéhez igazodóan illetékességi szakterületén, illetve beosztása szerinti időben információval és döntés előkészítéssel, javaslattal támogatja a Rendkívüli Események Figyelőszolgálata, a REVIR Központi Ügyelet, valamint a Csoportszintű Krízis Team munkáját, továbbá a rendkívüli eseménnyel érintett társaság irányában szakmai konzultációt biztosít, valamint delegálható a Társasági Krízis Teambe.

Rendkívüli események által érintett működési tevékenységek kategóriái

1) kommunikációs
   - média-érdeklődésre számot tartó, a vállalati imázst negatívan érintő események.
2) technológiai-működési
   - jogszabályokban, vagy szerződésekben előírt normál szintű működést akadályozó, veszélyeztető, korlátozó események (például nem tervezett üzemzavar, üzletfolytonossági esemény, jelentős zavar, válsághelyzet, felhasználói korlátozással járó események stb.).

3) biztonsági
   - vállalati – információs és fizikai - vagyonelemek, valamint munkavállalók ellen elkövetett szándékos vagy gondatlan cselekmények, vagy ezek kísérlete;
   - biztonsági előírások szándékos megsértése, vagy megkerülése;
   - fizikai biztonság tekintetében: biztonsági berendezések sérülése, vagy nem megfelelő működése;
   - információbiztonság tekintetében: vállalati adatvagyon bizalmasságának, sértetlenségének vagy rendelkezésre állásának sérülését, vagy annak veszélyeztetését okozó események;
   - humánbiztonsági: személyi sérülést és halált okozó események, munkavállalók által elkövetett vesztegetés, zsarolás, csalás vagy ezek kísérlete;
   - veszélyeztetettségi szint növelését eredményező események: természeti, vagy ipari havária események, terrorcselekmény, közveszéllyel fenyegetés).

4) környezeti
   - természeti környezetben kárt okozó események.

Rendkívüli-helyzet kezelés
Különleges, rendkívüli helyzetekben alkalmazott, illetve azokra felkészülő integrált vezetési folyamat (funkció). A szervezet elérhető belső és külső forrásait – időt, pénzt, szaktudást, munkaerőt, tárgyi és adminisztratív eszközöket stb. – felhasználva, azokat akár szokványos tevékenységüktől elvonva úgy csoportosítja újra, hogy

- rendkívüli helyzeteket felmérje, felismerje és tervet dolgozzon ki elkerülésükre vagy a bekövetkezett rendkívüli helyzet kezelésére,
- képessé tegye a vállalatot a hasonló jellegű helyzetek előre jelzésére,
- a fennálló rendkívüli helyzet romlását megakadályozza,
- a rendkívüli esemény bekövetkezését lehetőség szerint elhárítsa, vagy,
- negatív következményeit minimalizálja,
- a helyreállítást (szükség és lehetőség szerint) segítse.

Rendkívüli helyzet kezelési terv
A társaság által rendkívüli időszakban alkalmazott tervek: különösen katasztrófa-terv, üzletfolytonossági terv, helyreállítási terv.

Rendkívüli minősítésű időszak
Az az időintervallum, amikor a társaság rendes működésének rendjét súlyos veszély fenyegeti, és a veszély elhárítása, illetve a következmények felszámolása érdekében rendkívüli eszközök, alternatív eljárások vehetők igénybe, mivel az arra jogosult a rendkívüli helyzet kezelésére vonatkozó szabályok alkalmazását életbe léptette.

Sebezhetőség
Lásd sérülékenység.

Sértetlenség (integrity)
Annak biztosítása, hogy az információ változatlan marad átvitel, illetve tárolás közben, illetve csak az arra jogosultak módosíthatják az adat tartalmát.

Sérülékenység (vulnerability)
Az informatikai rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat (pl. a sérülékenységek, sebezhetőségek kihasználásával a támadó magasabb jogosultsági szintet ér el, így át tudja venni az irányítást a kellő védelem nélküli rendszerek felett). A sérülékenységeket általában frissítésekkel lehet javítani.

Sérülékenység vizsgálat
Az informatikai rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása.

Social Engineering
A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.

Szabotázs
Rejtett, szándékos romboló tevékenység, amely a tervszerű munkavégzés megbénításával, a tevékenységek rejtett akadályozásával, végrehajtásának megtagadásával, elodázásával vagy tudatos félreértésével kívánja elérni célját.

Szolgáltatási incidens
Szolgáltatás kieséssel járó olyan incidens, amely nem kezelhető, vagy várhatóan nem kezelhető SLA sértés nélkül.

Szolgáltatás Folytonosság Menedzsment (Service Continuity Management - SCM)
Az Üzletfolytonossági Rendszer, valamint az Információbiztonsági Rendszer (IBIR) végrehajtását támogató folyamatrendszer, amelynek célja, hogy rendkívüli esemény bekövetkezése esetén a szükséges időn belül biztosítsa az üzleti kritikus folyamatok által alkalmazott szolgáltatások (például: biztonsági, informatikai, hálózati, számviteli, egyéb) és azokat közvetlenül támogató erőforrások rendelkezésre állását, helyreállítását és ennek érdekében szervezi a jelen szabályzóval összhangban a szolgáltatások és erőforrások kockázatainak felmérését és menedzselését, valamint szolgáltatás és erőforrás helyreállítási tervek készítését, továbbá azok tesztelését és alkalmazását.

Társasági biztonsági kategória
A Társaságot információbiztonsági szempontból előre meghatározott kritériumok alapján biztonsági kategóriákba kell sorolni, melynek eredményeképpen a saját kategóriájának megfelelő biztonsági védelmi intézkedéseket szükséges megvalósítania.

Társasági Információbiztonsági Felelős (IBF)
Az elektronikus információs rendszerek biztonságáért felelős megfelelő kompetenciákkal rendelkező személy. A tevékenységet az erre szakosodott belső szolgáltató is elláthatja. Az IBF feladatait és annak végrehajtását az éves információbiztonsági munkaterv alapján látja el a társaság védelmi igényszintbe sorolása alapján. Az IBF feladatait nem csak a kijelölt személy, hanem egy delegált szervezeti egység is elláthatja, azonban a felelősség az IBF-et terheli.

Társasági információbiztonsági fórum
Olyan a társaságon belül tartott szakmai értekezlet, ahol az információbiztonsággal kapcsolatos döntések támogatása, az ad-hoc/tervezett feladatok megvalósításának, valamint az elmúlt időszak információbiztonsági eseményeinek megvitatása történik. A fórum összehívása, levezetése, jegyzőkönyvezése a társasági információbiztonsági felelősnek a felelőssége. Állandó tagjai: társaság első számú vezetője, társasági IBF, társasági üzletfolytonossági felelős, Biztonsági szakterület vezető, Felső vezetés tagjai. Az ülés gyakorisága a társasági információbiztonsági besorolás szerint: emelt (legalább évente); magas (legalább félévente); speciális (legalább negyedévente). Eseti jelleggel a következő események során kell rendkívüli információbiztonsági fórumot összehívni:

- jelentős információbiztonsági incidens, illetve rendkívüli esemény bekövetkezése
- jelentős, az információbiztonsági szabályozást érintő szervezeti vagy folyamatban történő változás
- új erőforrás bevezetése (pl. informatikai rendszer), mely a jelenlegi működést, illetve információbiztonsági szabályozást jelentős mértékben érinti, befolyásolja
- kapcsolódó jogszabályokban, egyéb külső szabályozásban történő jelentős változások esetén
- a társaságot érintő információbiztonsági belső és külső auditokat megelőzően, illetve követően (tehát nem szolgáltatói adatszolgáltatással kapcsolatban)

Társasági Üzletfolytonossági Felelős
A társaság rendkívüli helyzetkezelési feladatainak koordinálásáért felelős megfelelő kompetenciákkal rendelkező személy. A tevékenységet az erre szakosodott belső szolgáltató is elláthatja. A társasági üzletfolytonossági felelős feladatait nem csak a kijelölt személy, hanem egy delegált szervezeti egység is elláthatja, azonban a felelősség a társasági üzletfolytonossági felelőst terheli.

Tartománynév (Domain)
A domain a számítógépek (kiszolgálók) azonosítására szolgáló névtartomány.

Technikai felhasználó
Bizonyos előre meghatározott funkció (pl. automatikusan lefutó task-ok végrehajtására) betöltésére, az informatikai rendszer üzemeltető által létrehozott, nem konkrét személyhez köthető felhasználó.

Tiszta asztal politika
Az irodában vagy tárgyalóban őrizetlenül, illetéktelenek számára hozzáférhető dokumentumtárolást hivatott elkerülni. Az asztalon mindig csak az éppen használt dokumentumok, adathordozók legyenek, melyeket nap végén zárható szekrényben kell elzárni.

Tiszta képernyő politika
Arra vonatkozik, hogy mások illetéktelenül ne szerezhessenek meg információt a számítógép monitoráról, illetve ne férhessenek hozzá a felhasználó fiókjához, amíg az magára hagyja a gépet. Ennek érdekében a munkaállomás elhagyása előtt zárolni szükséges a számítógépet (Windows+L).

Titkosítás
Az adatátvitelkor, vagy adattárolókon történő adat titkosítása esetén az adatokhoz csak az arra jogosultak férhetnek hozzá, a megfelelő kulcs (pl. jelszó) ismeretében.

Többletjogosultság
Az alapjogosultságokon túl igényelhető jogosultságok, beleértve a technológiai rendszerekhez való hozzáférést is.

Ügyviteli rendszer
Ide értjük az általános munkahelyi, ügyviteli, adminisztratív és egyéb irodai tevékenység kiszolgálásához és támogatásához szükséges informatikai rendszereket. Az ügyviteli rendszereket az MVM Csoport belső IT szolgáltatója (MVMI Zrt.) üzemelteti.

Üzletfolytonosság
A szervezet azon képessége, amely révén az üzleti működését megszakító, szokásostól eltérő váratlan helyzetekben fent tudja tartani üzleti működését egy előre meghatározott és elfogadott szinten.

Üzletfolytonosság-menedzsment
Olyan tevékenységek összessége, melyek célja, hogy a társaság eredményesen és hatékonyan legyen képes a működése során bekövetkező rendkívüli helyzetekben biztosítani az üzletfolytonosságot.

Üzletfolytonossági esemény, vagy helyzet
A normál üzleti működést megszakító, a szokásostól eltérő váratlan helyzet, működési zavar, amely elhárítására, felszámolására a társaságcsoport saját erejéből képes, és az üzletfolytonosság biztosítható, a társaság normál üzletmenete visszaállítható.

Üzletfolytonossági terv/akcióterv (Business Continuity Plan - BCP)
Olyan cselekvési terv, melynek célja elsősorban az információs/informatikai rendszerrel támogatott üzleti folyamatok, vagy a lehetőségekhez mérten legalább a kritikus folyamatok működőképességének biztosítása rendkívüli esemény bekövetkezése esetén. Ezek a tervek szorosan kapcsolódnak a vállalat üzleti folyamataihoz, azok kapcsolataihoz, működési és működtetési módjaihoz.

Védelmi intézkedés
A fenyegetettség bekövetkezési valószínűsége, illetve a bekövetkezéskor jelentkező kár csökkentésére fizikai, logikai vagy adminisztratív eszközökkel alkalmazott megoldás.

Villamosenergia-ellátási válsághelyzet
A VET 139. §-ának (1) bekezdésében meghatározott, a szükséghelyzetet, illetve veszélyhelyzetet el nem érő mértékű, a személyeket, vagyontárgyaikat, a természetet, a környezetet, illetőleg a felhasználók jelentős részének ellátását közvetlenül veszélyeztető villamosenergia-ellátási zavar. Válsághelyzetet különösen a következő események válthatnak ki:

- tartós erőművi, illetőleg a határon keresztül beszállított villamos energia hiánya,
- tartós elsődleges energiaforrás hiány,

- az ország vagy országrész villamosenergia-ellátásában több napon át hiányt okozó környezetszennyezés, illetőleg vezetékek üzemszünete,
- a felhasználók ellátásának zavara.

Villamosenergia-krízis
A jelentős zavar, a válsághelyzet veszélye valamint a válsághelyzet.

Villamosenergia-rendszer jelentős zavara
A VET. 138. § (1) bekezdése értelmében a villamosenergia-ellátási válsághelyzetet el nem érő mértékű üzemi hiba, amelynek során a villamosenergia-rendszer erőműveiben vagy közcélú hálózatain olyan, a villamosenergia-ellátási szabályzatokban meghatározott esemény következik be, amely a villamos energia termelését, termelési készségét, átvitelét, elosztását, szolgáltatását vagy felhasználását jelentősen korlátozza vagy megszünteti, illetőleg a villamosenergia-rendszer üzembiztonságát, szabályozhatóságát vagy együttműködő képességét súlyosan veszélyezteti.
Az Üzemi Szabályzat értelmében a Villamosenergia-rendszer jelentős zavara az az üzemzavari állapot, amely részben vagy egészben ellehetetlenítette a tervszerű menetrendi szállításokat(átvitelt), a kiegyenlítő szabályozás teljesítését, és amely üzemzavari állapot csak rendkívüli intézkedésekkel (üzemzavari tartalékok igénybe vétele, export-import menetrend módosítása, nemzetközi kisegítés kérése, felhasználói korlátozás elrendelése vagy annak automatikus bekövetkezése) révén hárítható el.

Villamos üzemzavar
Az Üzemi Szabályzat értelmében olyan üzemi hiba, amelynek során a VER erőműveiben vagy hálózatain a villamos energia termelését, termelési készségét, átvitelét, elosztását, szolgáltatását, kereskedelmét vagy felhasználását korlátozó, illetve megszüntető, vagy az energiarendszer üzembiztonságát súlyosan veszélyeztető esemény következik be.

Visszaállítási idő (Work recovery Time – WRT)
Az az időintervallum, amely az üzleti terület számára szükséges a rendkívüli esemény bekövetkezése esetén a kiesett erőforrás, vagy szolgáltatás helyreállításától számítva, a helyettesítő alternatív folyamati működésről a normál működés szerinti üzleti folyamati működésre történő visszatérésig (magában foglalja a helyreállított erőforrás, szolgáltatás funkcionális megfelelőségének az üzleti terület által elvégzett ellenőrzését is).

Visszaállíthatatlan törlés
Olyan adatmegsemmisítési eljárás, melynek során a törölt adatok labor körülmények között sem állíthatóak helyre.

VPN (Virtual Private Network – virtuális magánhálózat)
Távoli elérésre használt technológia, az interneten keresztül alakít ki egy biztonságos „csatornát" a társaság informatikai hálózata felé. A VPN-en keresztül kapcsolódott számítógép úgy viselkedik, mintha közvetlenül az adott hálózatba lenne kötve, a keresztülmenő adatok titkosított adatcsomagokba vannak becsomagolva, nem láthatók az eredeti hálózaton.

WiFi (Wireless Fidelity) hálózat
Vezeték nélküli hálózat. A különböző vezeték nélküli hálózatokat azonosítójuk (SSID) alapján lehet megkülönböztetni. A hálózatokra való felcsatlakozás lehet authentikációhoz kötött.

WPA (WiFi Protected Access)
A Wi-Fi Protected Access a vezeték nélküli hálózatoknak (WiFi) egy biztonságos protokollja.

WPS (WiFi Protected Setup)
A vezeték nélküli útválasztók egyik opcionális kényelmi szolgáltatása. E funkció elsősorban azok számára készült, akik nem járatosak a számítógépes hálózatok világában és a routerek/útválasztók, valamint hozzáférési pontok menürendszerében, beállításaiban. A WPS ugyan megkönnyíti a csatlakozást a vezeték nélküli hálózatokhoz, azonban több jelentős biztonsági kockázattal is jár.

AZ MVM MOBILITI KFT. INFORMÁCIÓBIZTONSÁGI POLITIKÁJA

Az MVM Mobiliti Kft. (a továbbiakban: Társaság) vezetősége elkötelezett, hogy az MVM Csoport által biztosított szolgáltatásokat a legmodernebb technológiák felhasználásával, magas színvonalon, biztonságosan működő szolgáltatások igénybevételével alkalmazza, valamint, hogy a szükséges információbiztonsági folyamatokat és szükséges erőforrásokat költséghatékonyan biztosítsa. A Csoport által kezelt adatok és információk kiemelt értéket képviselő vagyonelemek, melyet védeni kell a különböző fenyegetések ellen, ezért a Társaság törekszik arra, hogy az információs vagyonelemek védelme időben folyamatosan megvalósuljon, valamint, hogy az üzleti információk bizalmassága, sértetlensége és rendelkezésre állása biztosított legyen.

A cél magas szinten támogatni és szabályozni a Társaság alapfeladatainak zavartalan ellátásához szükséges adatvédelmi és információbiztonsági alapelveket.
A Társaság elkötelezett a vonatkozó törvényi, és az irányadó szabványokban foglalt előírásoknak történő maximális megfelelés iránt.

A Társaság felső vezetése a politikában megfogalmazott elvek és követelmények teljesítését elvárja a Társaság összes munkatársától, beszállítóitól és minden egyéb érdekelt féltől. Az információbiztonsági politika hatálya kiterjed a Társaság valamennyi folyamatára és szervezeti egységre, és igénybe vett elektronikus információs rendszereire, mely magában foglalja az adathordozókat, alkalmazásokat, szoftvereket, hardver elemeket, és papír alapú dokumentumokat.

Célkitűzések

Az elszámoltathatóság, illetve az integritás és bizalmas jelleg adatvédelmi elvéből fakadóan az egyes adatkezelési tevékenységek teljes folyamata dokumentált és visszakövethető kell, hogy legyen a Társaság által használt rendszerekben. Az üzleti információkhoz csak a munkájukhoz szükséges mértékben és ideig férhessenek hozzá az arra felhatalmazott személyek. Az adat és információ bármely megjelenési formájára - legyen az papír alapú, elektronikus vagy akár szóban elhangzott – érvényesíteni kell a jelen politikában foglaltakat.

Alapelvek

Bizalmasság: A kezelt információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

Sértetlenség: Az információ tartalma és tulajdonságai az elvárttal megegyeznek. Az információ az elvárt forrásból származik tehát hiteles, a származás ellenőrizhető, megállapítható (letagadhatatlan), illetve az elektronikus információs rendszer elemei rendeltetésének megfelelően használható.

Rendelkezésre állás: Az információ az elektronikus információs rendszerben elérhető az arra jogosult személy számára.

Védelem teljeskörűsége: A védelem alapelveit a fizikai, logikai és adminisztratív (szabályozás) területeken kell érvényesíteni.

Védelem zártsága: az összes valószínűsíthető fenyegetés ellen megelőző védelmi intézkedés történik, ezek összeségében szerves egységet / egészet alkotnak.

Védelem kockázat arányossága: a védelem mértéke és költsége a felmért kockázatokkal arányosak. Cél a szükséges és elégséges költséggel elérni a maximális védelmet.

Védelem folyamatossága: A védelem folytonosságának alapelve, hogy az információ keletkezésétől, teljes életciklusán át a végleges törlés / megsemmisítésig a védelmet folyamatosan biztosítani kell. A kialakított védelmi intézkedések időben megszakítás nélkül fennállnak.

AZ MVM MOBILITI KFT. INFORMÁCIÓBIZTONSÁGI STRATÉGIÁJA

Napjainkban az információ értéke már sokkal nagyobb jelentőséggel bír, mint maga az eszköz, melyen a védendő adatok szerepelnek, ezáltal az információ az MVM Mobiliti Kft. (a továbbiakban: Társaság) vagyona részét képezi. Az információ bizalmasságának, sértetlenségének vagy rendelkezésre állásának sérülése akár jelentős károkat is okozhat mind a Társaság, mind a teljes vállalatcsoport számára, ezáltal veszélyeztetve az üzleti célok elérését. Mindemellett elmondható, hogy az információbiztonsági fenyegetések egyre változatosabb és szélesebb skálája jelenik meg, melyeket profitorientált támadók, anyagi haszonszerzés céljából hajtanak végre.

Megtervezett és jól működő információvédelemmel lehet garantálni a Társaság üzleti adatvagyonát, működését, hatékonyságát, üzleti titkok, a személyes adatok védelmét, továbbá az MVM cégcsoport jó hírnevének, gazdasági eredményeinek védelmét.

A biztonság megerősítésének szervezeti, személyi, technikai, szabályozási összetevői vannak. Az információs rendszerek biztonsága ellen irányuló veszélyforrások közül – a nemzetközi és hazai tapasztalatok alapján – fontos helyen állnak a szervezeten belüli humán veszélyek, a véletlen emberi hibák és a rosszindulatú szándékos károkozások. A humán terület eljárásai kiemelt fontosságúak (a személyek kiválasztása, motiváltság megteremtése, oktatás, ellenőrzés, elbocsátás kezelése) az információbiztonság terén. A veszélyek csökkentése érdekében az elfogadott és széleskörűen alkalmazott nemzetközi és hazai biztonsági követelményeket kell érvényre juttatni.

Az információbiztonság megteremtésének célja a Társaság üzleti céljainak eléréséhez, a törvények betartása, folyamatok hatékony működése, az üzleti információk védelmének megteremtése adatszivárgások, információbiztonsági kockázatok minimalizálása.

A Társaság elkötelezett az információbiztonság folyamatos fejlesztésében és fenntartásában, összhangban a vállalatcsoport információbiztonsági céljaival.

Információbiztonsági célok a következők:

- az üzleti információk igényeknek megfelelő rendelkezésre állása,
- az üzleti információk a szükséges mértékben történő megosztása, hozzáférés biztosítása
- az üzleti információk hitelességének, valódiságának biztosítása,
- kockázatarányos, költséghatékony védelmi intézkedések és folyamatok bevezetése,
- az információbiztonsági támadások bekövetkezési valószínűségét minimalizálni,
- az esetlegesen bekövetkezett információbiztonsági incidensek okozta károk mértékét minimalizálni,

Információbiztonsági stratégia hatóköre kiterjed:

- a Társaság összes informatikai rendszerére, és igénybe vett szolgáltatásokra, a kezelt (vagyis feldolgozott, továbbított, tárolt) adatvagyonra;
- papír és más fizikai adathordozókra;
- az informatikai rendszerek, igénybe vett szolgáltatások és adathordozók teljes életciklusára (fejlesztés, bevezetés, működés, leállítás);
- az egyes rendszerelemekért, adathordozókért felelős külső és belső szervezetekre;
- a megelőzés, ellenőrzés és szabályozás rendszerére;
- az informatikai rendszerelemek, adathordozók védelmét biztosító szervezeti, szabályozási, fizikai és logikai összetevőire.

Információbiztonság alapjai a Társaságban

Az MVM Mobiliti Kft. az információbiztonsági gyakorlatot tekintve az alábbiakra építkezik:

A Társaság Szervezeti és Működési Szabályzata alapján:

Ügyvezetők feladatai és hatásköre

- működési hatékonyságjavító és fejlesztési programok/intézkedések kidolgozása, illetve bevezetése
- felelős a Társaság hosszú távú, eredményes, gazdaságos és biztonságos működéséért

Vezetők általános kötelezettsége, felelőssége

- bizalmas információk, üzleti titkok az irányadó jogszabályok, csoportszintű és belső szabályok szerint megőrzése, kezelése
- üzemeltetési és biztonsági területekkel összefüggő felügyelet és menedzsment
- a Társaság mindenkori működtetését és fejlődését elősegítő, ügymeneti, folyamatkezelési, információs, jelentési, adminisztrációs és dokumentációs rendszerek fejlesztése, bevezetése, működtetése, felülvizsgálata, módosítása
- a kiszervezett gazdasági, IT és egyéb funkciók felügyelete

Társaság valamennyi munkavállalója köteles:

- az üzleti titokra vonatkozó előírások betartása
- megőrizni a munkája során tudomására jutott üzleti titkokat (ideértve különösen a munkáltató piaci pozícióját, vagy más egyéb olyan kérdést és információt)

A Társaság rendelkezik Minőség Irányítási Rendszer (MIR) kézikönyvvel, amit a jövőben kíván működtetni és fenntartani. Az információvédelmet elősegítő eljárásrendek, működési folyamatok az Minőség Irányítási Rendszerben:

- szervezeti szerepek és felelősségek
- üzleti és IT folyamatok
- változtatások tervezése
- munkatársak ismeret, kompetencia fejlesztése
- kockázatelemzés
- belső és külső auditálás, vezetőségi átvizsgálás
- fejlesztés

A Társaság igénybe veszi a cégcsoporton belül működő információbiztonsági folyamatokat és szolgáltatásokat (MVM BSZK, MVM Services, MVM Informatika).

A Társaság a következő tanúsítvánnyal rendelkezik:

- MSZ EN ISO 9001: 2015 - Minőségirányítási Rendszer

A Társaság meghatározott eljárásrendeket, folyamatleírásokat alapján kezeli ügymeneteit. A folyamatokban meghatározott lépésekben kezeli üzleti információkat. A fő üzleti folyamatok:

- E-SZAB-4 Értékesítés
- E-SZAB-5 Töltési szolgáltatás
- E-SZAB-6 Kereskedelmi üzemeltetés

A Társaság alkalmazza az MVM csoport információbiztonsági irányelveit:

- KIE-16 Az MVM Csoport személyes adatkezelési és adatvédelmi központi irányelve
- KIE-17 Az MVM Csoport információbiztonsági és rendkívüli helyzetkezelési központi irányelve

AZ MVM MOBILITI KFT. INFORMÁCIÓBIZTONSÁGI KOCKÁZATELEMZÉSÉNEK MÓDSZERTANI KÖVETELMÉNYEI

Tartalom

1. A dokumentum célja

Jelen dokumentum célja az információbiztonsági kockázatelemzés végrehajtási lépéseihez kapcsolódó követelmények dokumentálása. További szempont a kialakításkor, hogy a kockázatelemzés támogassa a későbbi projektek (adatszivárgás elleni védelem, mobil eszköz menedzsment, stb.) sikeres megvalósítását.

A kockázatelemzés végrehajtásának következtében megvalósíthatóvá válik:

- A riportálás és visszacsatolás folyamata az MVM Csoporton belül.
- A valóságot jobban modellező, kockázatarányos védelmi intézkedések bevezetése és működtetése (pl.: egyazon kategóriába tartozó adatokat az informatikai szolgáltató egységesen, az egyenszilárdságot biztosítva védelmezzen, míg egy másik, kevésbé jelentős adatkategóriába tartozó adatokra kevésbé költséges kontrollokat érvényesíthessen).
- A társasági védelmi intézkedések definiálása.

2. Általános követelmények

A módszertannak az alábbi követelményeknek kell megfelelnie:

- A módszertannak az ügyviteli rendszerek mellett ki kell terjedniük a technológiai rendszerekben tárolt, kezelt adatokra is, illetve az azokat érintő kockázatok azonosítására is.
- Az információbiztonsági kockázatelemzés módszertan alapján elkészített információbiztonsági kockázatelemzésnek **alkalmasnak kell lennie mind az ISO 27001** követelményeinek teljesítésére, **mind a számlázási rendszer audit követelményeinek** (2013. évi L. törvény és kapcsolódó rendeletei) teljesítésére.
- A módszertannak figyelembe kell vennie a kockázatelemzéssel kapcsolatos nemzetközi szabályokat, ajánlásokat és a legjobb gyakorlatokat, igazodva az érintett iparági szegmenshez.
- A módszertannak figyelembe kell vennie az üzletmenet-folytonosság menedzsment rendszer bevezetése során kialakított üzleti hatáselemzés módszertant, a kapcsolódási pontok azonosításra kell, hogy kerüljenek a dokumentumok, illetve folyamatok között.

3. Információbiztonsági kockázatelemzés módszertan

Az információbiztonsági kockázatelemzésnek az adatvagyon felmérésen kell alapulnia.

3.1. Egyéb kapcsolódó kockázatelemzések azonosítása és kezelése

Az információbiztonsági kockázatelemzés mellett a Társaság más kockázatelemzéseket is készíthet (pl.: üzleti kockázatelemzés, pénzügyi kockázatelemzés, üzletfolytonossági kockázatelemzés, stb.), ezeket az információbiztonsági kockázatelemzés módszertanának elkészítése során figyelembe kell venni, illetve a kapcsolódási pontokat azonosítani kell.

Az általános információbiztonsági kockázatelemzésen túl a Társaságnak lehetősége van szűkítettebb kockázatelemzések készítésére, például sérülékenység vizsgálatok, egyéb speciális auditok során. Ezen eredményeket az általános információbiztonsági kockázatelemzésbe, annak felülvizsgálata során, legalább magas szinten bele kell építeni.

3.2. Információbiztonsági kockázatelemzés végrehajtása

A Társaság a kockázatelemzés végrehajtása előtt módszertant készít jelen dokumentum követelményei alapján, melyet a társasági információbiztonsági felelősnek kell jóváhagynia. A

módszertan az információbiztonsági kockázatelemzés végrehajtásának lépései és részletes leírása mellett tartalmazza az alkalmazott segédleteket, úgymint:

- vizsgálandó fenyegetések listája
- lehetséges sérülékenységek listája
- releváns bekövetkezési gyakoriságok és hatások
- a felmérés során alkalmazott kárérték-táblázat
    - kártípusok
    - kárérték skála
    - kockázati szint meghatározás.

Az információbiztonsági kockázatelemzés során fel kell tárni az adatvagyon felmérésben azonosított adatokat, illetve az üzleti hatáselemzés során értékelt folyamatokat és a hozzájuk kapcsolódó erőforrásokat érintő kockázatokat, vagyis a releváns fenyegetéseket, azok bekövetkezési gyakoriságát, továbbá a bekövetkezés során – legrosszabb esetet feltételezve – keletkezett kár mértékét és típusát, valamint a fenyegetések bekövetkezéséhez vezető sérülékenységeket. Az elemzés során a kockázatokat három szempont szerint kell vizsgálni annak megfelelően, hogy az adatok

- bizalmassága,
- sértetlensége,
- rendelkezésre állása sérül.

Az értékelés során figyelembe kell venni a társaságnál jelenleg hatályban lévő védelmi intézkedéseket is, melyek célja a kockázatok bekövetkezési valószínűségének és/vagy hatásának csökkentése.

A kockázatelemzést dokumentálni szükséges, akár egy meghatározott informatikai rendszerben.

3.3. Azonosított kockázatok kezelése

A kockázatelemzés elkészítését követően meg kell határozni azon lehetséges védelmi intézkedéseket, melyekkel az adott kockázat bekövetkezési valószínűsége és/vagy hatása csökkenthető. A védelmi intézkedés javaslatokat, és az azokról született döntést dokumentálni szükséges, akár egy meghatározott informatikai rendszerben

Az azonosított kockázatok kezelésének módja a következő lehet:

- Védelmi intézkedések bevezetése az azonosított kockázat(ok) bekövetkezési valószínűségének, vagy bekövetkezés esetén okozott hatásának csökkentésére. A bevezetendő védelmi intézkedések lehetnek:
    - Preventív (megelőző) védelmi intézkedések
    - Detektív (észlelő) védelmi intézkedések
    - Korrektív (javító) védelmi intézkedések
- Az azonosított kockázatok átruházása harmadik félre
- Az azonosított kockázat(ok) felvállalása

A kockázatelemzésben az azonosított kockázatok mellett javaslat készül a kockázatok kezelésére irányuló kockázatcsökkentő intézkedésekre, melyeket az adatgazda és a társasági információbiztonsági felelős – szükség esetén egyéb kapcsolódó szervezeti egységek/funkciók által – értékel, és javaslatot tesz a megvalósítandó védelmi intézkedésekre, vagy kompenzáló kontrollokra.

Az értékelés szempontjai a következők:

- védelmi intézkedés becsült költsége szembe állítva az azonos maximális kárhatással

- védelmi intézkedés megvalósíthatóságának időtávlata szembe állítva a bekövetkezési gyakorisággal/valószínűséggel
- ideiglenes vagy állandó kompenzáló kontroll lehetőségek

A javasolt védelmi intézkedéseket a kockázatelemzés eredményével együtt az társasági információbiztonsági felelős összesíti és terjeszti fel döntésre. A kockázatok kezeléséről, illetve a javasolt védelmi intézkedések bevezetéséről és alkalmazásáról a Társaság Ügyvezetői hozzák meg a döntést határozat formájában.

Azon kockázatok, melyek csökkentésére a felső vezetés nem tervezi védelmi intézkedés bevezetését, felvállalt kockázatnak tekintendők. A kockázat felvállalására az adatgazda és a társasági információbiztonsági felelős tesz írásbeli javaslatot. A felvállalt kockázatokról nyilatkozni szükséges, ennek elfogadása a Társaság Ügyvezetőinek a felelőssége.

3.4. Védelmi intézkedések tervezése és megvalósítása

Amennyiben a kockázatkezelés módjaként valamilyen védelmi intézkedés bevezetése kerül kiválasztásra, a választott védelmi intézkedések körét dokumentált módon rögzíteni és tervezni kell. A védelmi intézkedés javaslatok mellett előzetesen értékelni kell a 3.5 pontban rögzítettek szerint a maradványkockázatokat, illetve a védelmi intézkedés javaslatok indokoltságát (bekövetkezési gyakoriság, bekövetkezéskori kárhatás vagy mindkettő csökkentése, becsült erőforrás ráfordítás vizsgálata, stb.).

A védelmi intézkedések az alábbi típusúak lehetnek:
- fizikai kontrollok
- adminisztratív kontrollok
- logikai/technológiai kontrollok

A kiválasztott védelmi intézkedés tervezését magas szinten dokumentáltan rögzíteni kell a visszaellenőrizhetőség biztosítása céljából.
A védelmi intézkedések bevezetését megelőzően vagy kiegészítően kompenzáló kontrollok bevezetése lehet indokolt, melyeket szintén dokumentált módon rögzíteni kell.
A védelmi intézkedéseket dokumentálni szükséges, akár egy meghatározott informatikai rendszerben.

3.5. Maradványkockázatok azonosítása és elfogadása

Azon kockázatok esetén, melyek valamilyen védelmi intézkedés bevezetésével vagy tervezésével kezelésre kerülnek, azonosításra kerülnek a védelmi intézkedések bevezetése után fennmaradó, a továbbiakban már nem csökkenthető kockázatok, melyek rögzítésre kerülnek a maradványkockázatok listáján. A maradványkockázatok elfogadására az adatgazda és a társasági információbiztonsági felelős tesz írásbeli javaslatot. Az elfogadott maradványkockázatokról nyilatkozni szükséges, ennek elfogadása a Társaság Ügyvezetőinek a felelőssége.

3.6. Információbiztonsági kockázatelemzés felülvizsgálata, frissítése

A kockázatelemzést, valamint a foganatosított védelmi intézkedések státuszát és megfelelőségét éves rendszerességgel felül kell vizsgálni. A felülvizsgálat végrehajtásának felelőse az társasági információbiztonsági felelős, aki a felülvizsgálat lefolytatásába más kapcsolódó szervezeti egységeket/funkciókat, illetve a biztonsági szolgáltatót, mint külső szakértőt bevonhatja.

A kockázatelemzés évközi, rendkívüli felülvizsgálata szükséges, amennyiben:

- az információkezelést és feldolgozást végző vagy támogató folyamatokban, illetve a kezelt adatok körében lényeges változás következik be,
- a Társaság tulajdonában vagy használatában lévő informatikai rendszerekben lényeges változás következik be,
- új fenyegetések vagy trendek jelennek meg, melyek vizsgálata szükséges,
- jelentős incidens bekövetkezése után, amennyiben a társasági információbiztonsági felelős azt indokoltnak látja.

A rendkívüli felülvizsgálat kezdeményezése a hivatkozott változások ismeretében a társasági információbiztonsági felelős felelőssége, aki a kapcsolódó szervezeti egységeket/funkciókat értesíti a rendkívüli felülvizsgálat szükségességéről.

A TÁRSASÁGI INFORMÁCIÓBIZTONSÁGI KÖVETELMÉNYEK MEGSZEGÉSÉNEK ESETEI ÉS SZANKCIONÁLÁSÁNAK SZEMPONTJAI

1. Az információbiztonsági követelmények megszegésének esetei

Szabályszegés típusa	Leírás	Szabályzati hivatkozás
Eszköz elvesztés, rongálás	Az eszköz értéke mellett a felhasználónak mérlegelnie kell az azon tárolt adatok bizalmasságának, sértetlenségének és/vagy rendelkezésre állásának sérüléséből származó károk lehetőségét is, és annak függvényében be kell tartania jelen szabályzat hordozható eszközök kezelésére vonatkozó pontjában foglaltakat (lásd 5.15 Mobil eszközök használata). A hordozható eszköz elvesztéséből származó esetleges információbiztonsági károkat a társasági információbiztonsági felelősének kell vizsgálnia, illetve a vizsgálat eredményét dokumentált módon rögzítenie kell. Amennyiben a munkavállalónak felróható módon az eszközön tárolt adatok kompromittálódnak, a keletkezett kárért az érintett felhasználó szankcionálható. A szankció mértékéről az eset kivizsgálását követően a munkáltatói jogkör gyakorlója hozza meg a döntést.	MOB-BSz-17 Az MVM Mobiliti Kft. Információbiztonsági és rendkívüli helyzetkezelési belső szabályzata 5.6.3. Munkavállalókra vonatkozó szankciók
Incidensek jelentésének elmulasztása	Amennyiben a munkavállaló a számára rendelkezésre bocsátott munkaeszköz működésében hibát észlel, rendellenes működést tapasztal (például a vírusvédelmi rendszer hibát jelez), azt azonnal jelentenie kell a HelpDesk-nek. Az ennek elmaradásából fakadó károkért a felhasználó szankcionálható. Minden olyan jellegű kár, mely egyértelműen azonosítható következménye egy be nem jelentett rendellenességnek vagy incidensnek, a felhasználót terheli.	MOB-BSz-17 Az MVM Mobiliti Kft. Információbiztonsági és rendkívüli helyzetkezelési belső szabályzata 5.6.3. Munkavállalókra vonatkozó szankciók

Eszköz nem rendeltetésszerű használata	A társasági információbiztonsági felelős bármikor jogosult ellenőrizni, hogy a munkavállalók a munkavégzésükhöz biztosított eszközöket rendeltetésszerűen, munkavégzés céljára használják-e, illetve betartják-e az információbiztonsági előírásokat. Az ellenőrzés tényét a Társaság nem köteles előzetesen bejelenteni, de törekednie kell arra, hogy az ne zavarja a napi munkamenetet. A vizsgálat keretein belül ellenőrizni lehet a következőket: • Indokolatlan magáncélú használat (például zene- és/vagy filmletöltés, játékok használata, magáncélú adatok tárolása) • Illetéktelen személyes adatok kezelése • Illegális szoftverek használata • Biztonsági beállítások megfelelősége, azok módosítása • Biztonsági incidens gyanúja esetén elektronikus levelezés, naplófájlok megtekintése	MOB-BSz-17 Az MVM Mobiliti Kft. Információbiztonsági és rendkívüli helyzetkezelési belső szabályzata 5.6.3. Munkavállalókra vonatkozó szankciók
Információbiztonsági előírások betartásának elmulasztása	Amennyiben a Társaság munkavállalója jelen szabályzatban rögzített felelősségi körének, feladatainak nem tesz eleget, a Társaság – a szándékos mulasztás, illetve a már okozott, valamint lehetséges károk figyelembe vételével – szankcionálhatja az érintett felhasználót.	MOB-BSz-17 Az MVM Mobiliti Kft. Információbiztonsági és rendkívüli helyzetkezelési belső szabályzata 5.6.3. Munkavállalókra vonatkozó szankciók
Internet használat	Az Internet használati engedély személyre szóló, azt kizárólag a felhasználó saját maga veheti igénybe.	MOB-BSz-17 Az MVM Mobiliti Kft. Információbiztonsági és rendkívüli helyzetkezelési belső szabályzata 5.14.2. Internet használat
	A kliens számítógépen proxy, VPN, és egyéb anonimizálásra szolgáló alkalmazások (Pl. Tor Browser) futtatása tilos.	
	A felhasználó internet-hozzáférésének más felhasználók részére nem központi módon történő megosztása vagy tovább szolgáltatása tilos.	
	A hálózati sávszélesség és erőforrások szükségesnél nagyobb, túlzott foglalása (pl. nagyméretű állományok indokolatlan letöltése) tilos. Az előírás megszegése esetén a felhasználó felettesét értesíti a szolgáltató, további intézkedés céljából.	
	Tilos a Társasághoz, vagy harmadik félhez kötődő kereskedelmi szoftverek, valamint jogvédett tartalmak feltöltése, letöltése, illetve továbbítása Internetes oldalakon.	
	A munkatársaknak tilos az Internetről szoftverek letöltése, futtatása. Amennyiben a felhasználónak valamilyen programra igénye merül fel, az informatikai szolgáltató felé kell jeleznie azt.	

	Tilos a gyanús tartalmakra kattintás, ismeretlen felugró ablakok engedélyezése. Amennyiben a felhasználó valamiben nem lenne biztos, az informatikai szolgáltató HelpDesk-jéhez, vagy az információbiztonsági területhez kell segítségért fordulnia.	
Beléptető rendszer	A beléptető rendszer nem rendeltetésszerű használata (pl. átmászás a forgóvilla alatt/fölött, több személy beengedése egy belépőkártyával, a belépőkártya kölcsönadása, stb.) szankciókat von maga után. A belépőkártya elvesztése esetén a munkavállaló köteles jelenteni az incidenst a társasági biztonsági területnek, valamint a Beléptető kártya Átadás-Átvételi nyomtatványban foglaltak szerint köteles befizetni az új kártya igénylésének összegét. Az incidens bejelentéséről, valamint az összeg befizetéséről jegyzőkönyv készül, az állandó belépőkártya pótlása kizárólag ezen jegyzőkönyv ellenében történhet meg. A Társaság biztonsági területe azonnal jelenti a bejelentett incidenst a beléptető rendszer üzemeltetőjének, akinek gondoskodnia kell a belépőkártya azonnali letiltásáról, ezzel megakadályozva az elveszett kártyával való esetleges visszaélést. Minden munkavállaló kötelessége továbbá, hogy a beléptető rendszer meghibásodását, nem megfelelő működését (pl. nem záródó ajtók) haladéktalanul jelezze a biztonsági szolgálat helyszíni munkatársainak, vagy a társasági biztonsági területnek. A beléptető rendszer rendeltetésszerű működését, valamint a belépőkártyák használatát a társasági információbiztonsági felelős évente legalább egy alkalommal kell, hogy ellenőrizze.	MOB-BSz-17 Az MVM Mobiliti Kft. Információbiztonsági és rendkívüli helyzetkezelési belső szabályzata 5.7.2 Alkalmazott eszközök és információbiztonsági követelményeik
Laptop használat	Az informatikai szolgáltató, illetve A Társaság tulajdonát képező laptopokat/notebookokat a munkavállaló hazaviheti, vagy a munkaidő lejártával bent hagyhatja az irodában a következő feltételekkel:	MOB-BSz-17 Az MVM Mobiliti Kft. Információbiztonsági és rendkívüli helyzetkezelési belső szabályzata 5.15.1. Laptop/notebook használatával kapcsolatos információbiztonsági követelmények
	Munkaidőn kívül a laptopokat/notebookokat zárt szekrényben vagy bezárt irodában kell elhelyezni.	
	A laptopok/notebookok őrizetlenül hagyása még zárt autóban is kerülendő. Amennyiben ez nem megoldható, az eszközt nem látható helyre kell helyezni. Az autóban őrizetlenül hagyott eszköz ellopása esetén a felelősség és a kár megtérítése a munkavállalót terheli. A laptopokat/notebookokat bekapcsolt állapotban szállítani tilos.	
	A laptopot/notebookot a munkavállaló őrizetlenül csak a saját lakhelyén belül hagyhatja, de ott is csak kikapcsolt vagy zárolt állapotban.	

	Külföldi kiküldetés esetén a munkavállaló által kivinni kívánt eszközöket, illetve adatokat a társasági információbiztonsági felelőssel és az érintett adatgazdával egyeztetni szükséges, indokolt esetben a társasági információbiztonsági felelős által meghatározott külön informatikai eszközök biztosítása szükséges a kiküldetés időtartamára.	
Szerződéses követelmények	A szerződés/megállapodás információbiztonsági követelményeinek megszegése.	MOB-BSz-17 Az MVM Mobiliti Kft. Információbiztonsági és rendkívüli helyzetkezelési belső szabályzata 5.16.1. Külső felek közreműködésével kapcsolatos általános szabályok

Szankcionálási szempontok

Amennyiben a munkavállaló felróható (szándékos vagy gondatlan) magatartásának következményeként megsérti a jelen szabályzatban foglalt rendelkezéseket és ezzel A Társaságnak kárt okoz, a munkavállaló szankcionálható.

A kár alapját a MOB-FU-17-04-M-02 Kárérték táblázat melléklet adja, jogi-, imázs- és működési kár függvényében, melynek jellege/ értéke alapján lehet:

- **Alacsony** besorolásúnak számít a minimális és csekély kárérték,
- **Közepes** besorolású a mérsékelt kárérték,
- **Magas** besorolású a jelentős és kritikus kárérték.

Az okozott kár értékét az érintett szakterület vagy szakterületek vezetői (közvetlen felettes, ill. a Társaság Ügyvezetői) és a társasági információbiztonsági felelős együttesen határozzák meg.

Ezen melléklet alapján érvényesített felelősségre vonás esetén a Munkavállaló egyéb kártérítési vagy jogi felelősség alól nem mentesül

1. Munkáltatói intézkedések (szankciók)

Az eljárás típusától függően az alábbi munkáltatói intézkedések (szankciók) róhatók ki:

	Gondatlan	Súlyosan gondatlan/Szándékos
Alacsony	Szóbeli figyelmeztetés és ismételt Információbiztonsági képzésben való részvétel (e-learning).	Írásbeli figyelmeztetés, (HR aktába bekerül) és személyre szabott, személyesen megtartott információbiztonsági, tematikus képzés, írásbeli és szóbeli számonkéréssel.
Közepes	Írásbeli figyelmeztetés, (HR aktába bekerül) és személyre szabott, személyesen megtartott információbiztonsági, tematikus képzés írásbeli és szóbeli számonkéréssel. Teljesítési feltétel sikeres vizsga.	Hátrányos jogkövetkezmény (fegyelmi eljárás) és személyre szabott, személyesen megtartott információbiztonsági, tematikus képzés, írásbeli és szóbeli számonkéréssel. Teljesítési feltétel sikeres vizsga. Indokolt esetben az informatikai rendszerekhez való hozzáférés felfüggesztése, korlátozása[1].
Magas	Hátrányos jogkövetkezmény (fegyelmi eljárás) és személyre szabott, személyesen megtartott információbiztonsági, tematikus képzés, írásbeli és szóbeli számonkéréssel. Teljesítési feltétel sikeres vizsga. Indokolt esetben az informatikai rendszerekhez való hozzáférés felfüggesztése, korlátozása[1]	Hátrányos jogkövetkezmény (fegyelmi eljárás) vagy a munkaviszony megszüntetése; Büntető feljelentés

[1]Megjegyzés: az informatikai rendszerekhez való hozzáférés újbóli biztosítása sikeres írásbeli és szóbeli vizsgát követően lehetséges.

2. A munkáltatói intézkedések döntéshozói

	Gondatlan	Súlyosan gondatlan/Szándékos
Alacsony	Közvetlen felettes vezető (D, V) Társasági információbiztonsági felelős (K)	Közvetlen felettes vezető (D, K, V) Társasági információbiztonsági felelős (V) HR (I)
Közepes	Közvetlen felettes vezető (D, K, V) Társasági információbiztonsági felelős (K, V) HR (I)	Közvetlen felettes vezető (K) Társaság Ügyvezetői (D) HR (V) Jog (K) Társasági információbiztonsági felelős (K, V)
Magas	Közvetlen felettes vezető (K) Társaság Ügyvezetői (D) HR (V) Jog (K) Társasági információbiztonsági felelős (K, V)	Közvetlen felettes vezető (K) Társaság Ügyvezetői (D) HR (V) Jog (K) Társasági információbiztonsági felelős (K)

A gondatlanságból elkövetett, információbiztonsági szabályzatban foglaltak megsértésének többszöri egymás utáni ismétlődése esetén, a társasági információbiztonsági felelős – a szabálysértő munkavállaló közvetlen vezetőjével egyeztetve – javaslatot tehet a Társaság Ügyvezetői részére a szándékos károkozás szankcióinak alkalmazására (indoklással és az alkalmazni javasolt szankció konkrét megjelölésével).

Magyarázat:

Rövidítés	Jelentés	Rövidítés	Jelentés	Rövidítés	Jelentés	Rövidítés	Jelentés
V	Végrehajt	D	Dönt	K	Közreműködik	I	Információt kap

AZ MVM MOBILITI KFT. ESETÉBEN ALKALMAZOTT ADATBIZTONSÁGI KATEGÓRIÁK

1. osztály – Nyilvános adatok: a Társaságon belül és kívül egyaránt szabadon kommunikálható, nyilvános forrásból is elérhető információk (pl. reklám és marketing anyagok, publikus jelentések, közérdekű adatok, tájékoztatók, stb.)

2. osztály - Csoportszintű belső használatú adatok: a csoporton belül, a társaságok között szabadon megosztható, azonban a csoporton – így a Társaságon – kívül nem kommunikálható, vagy csak az MVM Zrt. Csoportszintű Biztonsági Igazgatóság előzetes engedélyével kommunikálható információk (pl. belső telefonkönyv, csoportszintű kiadványok, csoportszintű szabályzatok, csoportszintű folyamatutasítások tartalma, csoportszintű oktatási anyagok, stb.), illetve ide tartoznak a máshová nem sorolható belső információk.

3. osztály - Társasági belső használatú adatok: a Társaságon belül szabadon megosztható, azonban a Társaságon kívül még csoportszinten sem kommunikálható, vagy csak abban az esetben, ha a társasági információbiztonsági felelős és az adatgazda előzetes engedélyt adott (pl. társasági fejlesztésekkel, projektekkel kapcsolatos információk, társasági szabályzatok, társasági folyamatutasítások tartalma, oktatási anyagok, stb.).

4. osztály - Társasági bizalmas adatok: a Társaságon belül is korlátozottan kommunikálható adatok köre. Hozzáférési jogosultsággal csak az adatgazda által meghatározott személyek rendelkezhetnek (pl. az egyes osztályok által kezelt adatok, ügyféladatok, személyes adatok, korlátozott hozzáférésű szabályzatok, stb.)

5. osztály - Társasági szigorúan bizalmas adatok: a Társaságon belül is korlátozottan kommunikálható adatok köre. Hozzáférési jogosultsággal csak a Társaság első számú vezetői által meghatározott személyek rendelkezhetnek (pl. munkaszerződések, béradatok, stb.).

A TÁRSASÁGI ADATOK KEZELÉSÉRE VONATKOZÓ INFORMÁCIÓBIZTONSÁGI KÖVETELMÉNYEK

Adat-biztonsági kategória	Tárolás	Továbbítás	Megsemmisítés
Nyilvános adatok	Nincsen speciális követelmény, bármilyen adathordozón, titkosítatlan formában tárolható.	Nincsen speciális követelmény, szabadon továbbítható.	Nincsen speciális követelmény, speciális megsemmisítést nem igényel.
Csoportszintű belső használatú adatok	Tiszta asztal, tiszta képernyő politika betartásával, papír alapú dokumentumokat a munkanap végén elzárt helyen kell tárolni, az elektronikus adatokat a fájlszerver közösen elérhető mappáiban lehet tárolni, illetve korlátozott hozzáférés biztosítása mellett titkosított adathordozón.	Csoporton belül speciális védelmi intézkedések nélkül továbbítható, csoporton kívül az adatgazda és a társasági információbiztonsági felelős dönt a speciális védelmi intézkedések szükségességéről: papír alapú dokumentumoknál ajánlott levélként való továbbítás, elektronikus dokumentumok esetén a társasági információbiztonsági felelős által jóváhagyott titkosítás alkalmazása szükséges csoporton kívüli továbbítás esetén.	A papír alapú dokumentumokat megsemmisítés céljából a megsemmisítendő iratokat gyűjtő konténerekben kell elhelyezni/iratmegsem-misítővel kell ledarálni. Az elektronikus adathordozókat a társasági információbiztonsági felelős részére kell leadni végleges törlés céljából.

Társasági belső használatú adatok	Tiszta asztal, tiszta képernyő politika betartásával, papír alapú dokumentumokat a munkanap végén elzárt helyen kell tárolni, az elektronikus adatokat a fájlszerver közösen elérhető mappáiban lehet tárolni, illetve korlátozott hozzáférés biztosítása mellett titkosított adathordozón.	Társaságon belül speciális védelmi intézkedések nélkül továbbítható, társaságon kívül (még csoporttag esetén is) az adatgazda a társasági információbiztonsági felelős bevonásával dönt a speciális védelmi intézkedések szükségességéről: papír alapú dokumentumoknál ajánlott levélként való vagy futár általi továbbítás, elektronikus dokumentumok esetén a társasági információbiztonsági felelős által támogatott titkosítás alkalmazása szükséges csoporton kívüli továbbítás esetén.	A papír alapú dokumentumokat megsemmisítés céljából a megsemmisítendő iratokat gyűjtő konténerekben kell elhelyezni/iratmegsemmisítővel kell ledarálni. Az elektronikus adathordozókat a társasági információbiztonsági felelős részére kell leadni végleges törlés céljából.
Társasági bizalmas adatok	Tiszta asztal, tiszta képernyő politika betartásával, papír alapú dokumentumokat használaton kívül elzárt helyen kell tárolni, az elektronikus adatokat a fájlszerver korlátozottan elérhető mappáiban lehet tárolni, illetve külső adathordozón titkosított formában.	Társaságon belül gondoskodni kell arról, hogy csak a hozzáférésre jogosult munkavállalók férjenek hozzá a továbbított adatokhoz (papír alapon: személyes átadás, lezárt boríték; elektronikus adatok esetében fájlszerver csoport szintű megosztás alkalmazása). Társaságon kívül papír alapú dokumentumok esetében tértivevényes levélként való, vagy belső futár általi továbbítás, elektronikus dokumentumok esetén a társasági információbiztonsági felelős által jóváhagyott titkosítás alkalmazása szükséges csoporton kívüli továbbítás esetén.	A papír alapú dokumentumokat megsemmisítés céljából a megsemmisítendő iratokat gyűjtő konténerekben kell elhelyezni/iratmegsemmisítővel kell ledarálni. Az elektronikus adathordozókat a társasági információbiztonsági felelős részére kell leadni végleges törlés céljából.

Társasági szigorúan bizalmas adatok	Tiszta asztal, tiszta képernyő politika betartásával, papír alapú dokumentumokat használaton kívül páncélszekrényben, vagy korlátozott hozzáférésű, biztonsági zónában elhelyezett, zárható szekrényben kell tárolni. Az elektronikus adatokat a fájlszerver korlátozottan elérhető mappáiban lehet tárolni.	Társaságon belül gondoskodni kell arról, hogy csak a hozzáférésre jogosult munkavállalók férjenek hozzá a továbbított adatokhoz (papír alapon: személyes átadás; elektronikus adatok esetében fájlszerver csoport szintű megosztás alkalmazása). Társaságon kívül papír alapú dokumentumok esetében a biztonsági szolgáltató általi továbbítás, vagy dokumentált (iktatott) személyes átadás, elektronikus dokumentumok esetén a társasági információbiztonsági felelős által jóváhagyott titkosítási eljárás szükséges minden esetben.	A papír alapú dokumentumokat iratmegsemmisítővel le kell darálni. Az elektronikus adathordozókat a társasági információbiztonsági felelős részére kell leadni végleges törlés céljából.

A TÁRSASÁGI DOKUMENTUMOK NAGY MENNYISÉGŰ SZÁLLÍTÁSÁNAK INFORMÁCIÓBIZTONSÁGI KÖVETELMÉNYEI

- A dokumentumokat átadó fél a dokumentumok dobozba rakása után a dobozt matricával is lezárja, melyet lepecsétel és aláír.
- A szállító ellenőrzi az átvett dobozon a lepecsételés és az aláírás sértetlenségét. Sérült vagy hiányos lezárás esetén nem veszi át a dobozt. Amennyiben sértetlen a lepecsételés, a szállító átveszi a dobozt, melyről átadás-átvételi jegyzőkönyv készül.
- A szállítás során a szállító felel a részére átadott dokumentumok bizalmasságának, sértetlenségének és rendelkezésre állásának megóvásáért, melynek érdekében betartja a következő szabályokat:
    - A dokumentumokat tartalmazó dobozokat nem hagyja felügyelet nélkül, a szállítás során folyamatos felügyeletet biztosít.
    - A dokumentumok szállításában a szállításra szolgáló jármű méretétől függően legalább 3 fő folyamatosan rendelkezésre áll.
    - A dobozokat a szállítás során a szállító nem bonthatja meg, tehát a pecsét nem sérülhet.
    - A szállító ügyel a nem szándékos sérülések elkerülésére (pl. beázás). Az ilyen jellegű károkért teljes mértékben a szállító felel.
    - A szállító a bepakolást követően egyenesen a célállomásra megy, köztes kitérőt nem tehet.
- Az átvevő fél a dobozok átvétele előtt ellenőrzi a pecsét és az aláírás sértetlenségét. Hiányzó, vagy sérült lepecsételés esetén jelenti az eseményt a társasági információbiztonsági felelősnek. Amennyiben a küldemény sértetlen, az átvételről átadás-átvételi jegyzőkönyv készül.
- Visszaszállításkor ugyanezen előírások betartása szükséges.

AZ MVM MOBILITI KFT. FELHŐ ALAPÚ RENDSZEREINEK INFORMÁCIÓBIZTONSÁGI VIZSGÁLATI SZEMPONTJAI

Felhő alapú rendszerek igénybevétele esetén – annak bevezetése előtt – szükséges, hogy az információbiztonsági területnek legyen lehetősége arra, hogy a szolgáltatást nyújtó fél belső szabályzatába, vagy annak kivonatába betekintést nyerjen, nyilatkozatokat, tanúsításokat kérjen, vagy más módon vizsgálatot folytasson a szolgáltatás – Társasági információbiztonsági szempontjainak – megfelelőségének ellenőrzése céljából.

A vizsgálatot az alábbiakban foglaltak szerint kell végrehajtani:

I. Belső szolgáltatókkal történő egyeztetés

A szolgáltatás bevezetése előtt az MVM Csoport informatikai és biztonsági szolgáltatójával egyaránt szükséges az alábbi szempontok egyeztetése.

1. Az igénybe venni kívánt szolgáltatásra van-e bármely belső szolgáltatónak alternatív megoldási javaslata? Amennyiben **igen**,
   - milyen mértékben és módon fedi le a Csoport szolgáltatója által nyújtott alternatíva az eredetileg igénybe venni kívánt szolgáltatást,
   - milyen feltételek szükségesek az alternatív megoldás bevezetéséhez,
   - milyen határidővel és milyen feltételekkel (költségek, garancia, SLA) tudja vállalni a szolgáltató az igénylés bevezetését/kivitelezését,
2. Amennyiben a belső szolgáltatók **nem** tudnak a bevezetni kívánt szolgáltatás/eszköz helyett alternatívával szolgálni, az alábbi információbiztonsági szempontok egyeztetése szükséges:
   - a bevezetni kívánt szolgáltatás/eszköz milyen mértékben és módon veszélyeztetheti a Társaság adatvagyonát kezelő infrastruktúrájának a bizalmasságát, sértetlenségét és a rendelkezésre állását, valamint a szolgálgatás bármilyen módon veszélyezteti-e az MVMI által üzemeltetett ügyviteli rendszert (kockázatelemzés készítése, lehetséges kockázatokra vonatkozó védelmi intézkedések meghatározása).
   - Milyen minősítésű adatok kerülnének a felhő alapú szolgáltatásban tárolásra, illetve feldolgozásra.

II. A bevezetni kívánt megoldás információbiztonsági vizsgálata

A vizsgálatot minimálisan a következő szempontrendszer szerint szükséges végrehajtani:

- Vizsgálni szükséges a szolgáltató tulajdonában lévő, általa bérelt, vagy más úton használatában lévő adatközpontjának/adatközpontjainak, valamint azok tartalékolásának földrajzi elhelyezkedését. Figyelemmel kell lenni a hatályos EU és hazai jogszabályi háttérre. Az elvárás érvényes az adatközpontok alternatív/tartalék telephelyének elhelyezkedésére vonatkozóan is.
- Vizsgálni kell a biztonsági mentéseket a társasági szabályzatban foglaltak alapján, illetve az előző pontban leírt adatvédelmi irányelvnek kell érvényesülnie a felhőben tárolt adatok

biztonsági mentésére vonatkozóan is, azzal a kitétellel, hogy a mentett adatok tárolási helyszíne ne legyen azonos az adatközponttal.

- A szolgáltatónak az általa biztosított szolgáltatás rendszeres sérülékenység-vizsgálatát kell biztosítania, annak érdekében, hogy a lehetséges biztonsági rések és az azokon keresztül fenyegető biztonsági események feltárása a lehető leghamarabb megtörténhessen. Magas szinten vizsgálni kell a sérülékenység-vizsgálatok jellegét és gyakoriságát, valamint az azok alapján tett védelmi intézkedés javaslatok kezelését, meglétük utóellenőrzését.
- Az üzletmenet-folytonossági és erőforrás helyreállítási tervek megléte és rendszeres tesztelése szintén az esetleges biztonsági kockázatok feltárása és kezelése miatt elengedhetetlen.
- Ellenőrizni kell a szolgáltató által saját rendszereiken elvégzett információbiztonsági auditok meglétét, gyakoriságát. A szolgáltatóval kötött megállapodásban szükséges annak rögzítése is, hogy az ügyfél az igénybe vett rendszereken milyen auditok elvégzésére jogosult, illetve a szolgáltató általi auditokról milyen adatszolgáltatást kap.
- A szolgáltatónak meg kell határoznia az ügyféladatok titkosítási módját, úgymint az adatok maszkolásának lehetőségét, ennek megfelelőségét ellenőrizni kell.
- A szolgáltatónak meg kell határoznia továbbá, milyen hálózati, alkalmazás, több faktoros autentikációs és egyéb IT biztonsági szolgáltatásokat nyújt az adatok védelme érdekében. Szükséges megvizsgálni annak lehetőségét, hogy van-e mód bizonyos adatokat helyben, bizonyos adatokat pedig a felhőben tárolni (Hibrid tárolási mód lehetséges-e.)
- Információt kell szerezni arról, hogy a szolgáltató a rendszer üzemeltetése során felhasználói tevékenység monitorozó szoftvert használ-e, és amennyiben igen, az erre használt eszköz/rendszer használatának módját is a szolgáltatói szerződésben szükséges rögzíteni, továbbá, a tárolt adatokról rendszeres auditok lefolytatását kérheti/végezheti az ügyfél
- Egyeztetni kell, hogy a szolgáltató milyen rendszerességgel, milyen adatokat tartalmazó riportokat ad át az ügyfél számára, illetve ezekhez kapcsolódó előírások hol vannak rögzítve.
- Információt kell szerezni arról, hogy az IT adminisztrátorok milyen, a felhőben tárolt ügyféladatokhoz és milyen mértékben férnek hozzá, illetve az ehhez kapcsolódó előírások hol van szabályozva.
- A szolgáltatás igénybevétele előtt a szolgáltató részéről szükséges az általuk használt szerződésminta megküldése az ügyfél részére, melyet mind jogi, mind információbiztonsági szempontokból szükséges vizsgálni (milyen információbiztonsági követelmények kerülnek benne rögzítésre).

III. Szolgáltatótól független vizsgálatok

- Milyen alternatív, elsősorban on-premise rendszerek állnak rendelkezésre hasonló funkcionalitással. (Amennyiben MVM Csoporton belül nincsen megfelelő alternatívát nyújtó szolgáltató.)
- Milyen egyéb információ-, esetleg humánbiztonsági kockázatai lehetnek az igényelt szolgáltatás/rendszer bevezetésének (pl. személyes adatok védelme).

A fentiek érvényesülésének mind jogi, mind műszaki garanciákkal kell érvényt szerezni.

VEZETÉK NÉLKÜLI HÁLÓZATOK ÉS KAPCSOLÓDÓ JOGOSULTSÁGOK A TÁRSASÁGON BELÜL

A Társaság informatikai szolgáltatótól igénybe vett vezeték nélküli hálózatának használatához kötött jogosultságok az alábbiak:

- **„employee-network":** az informatikai szolgáltató által biztosított hordozható számítógépekkel (notebookokkal) vehető igénybe a vezeték nélküli hálózati (WiFi) szolgáltatást megrendelő társaság(ok) telephelyén, melyek a központilag kiadott jogosultságok alapján automatikusan csatlakozhatnak a hálózathoz. Ebben az esetben a felhasználó alapjogosultságai szerinti teljes belső hálózat elérhető, ugyanúgy, mint a vezetékes kapcsolaton keresztül.
- **„guestnet":** azok a külső felek, szerződéses partnerek használhatják, akik nem rendelkeznek az informatikai szolgáltató által biztosított laptopokkal, mivel innen a belső hálózat nem elérhető, csakis Internet kapcsolat létesíthető. A hozzáférés határozott időre igényelhető az informatikai szolgáltatótól. A belépéshez szükséges felhasználónév-jelszó párost a felhasználó részére e-mailben küldi meg az informatikai szolgáltató.

A TÁRSASÁGON BELÜL TILTOTT INTERNETES OLDALAK

Az egyértelműen nem munkához köthető tartalmú Internetes oldalak látogatása tilos és technológiailag tiltottak is. Ezek a következő témakörű oldalak:

- Szexuális és pornográf tartalmú oldalak;
- Drogok használatát ismertető, támogató oldalak;
- MP3 és audio letöltési szolgáltatásokat tartalmazó oldalak;
- Online játék oldalak;
- Olyan weboldalak, amelyek az információbiztonság kijátszásához nyújtanak segítséget (kivéve ha a felhasználónak ez munkaköri kötelessége);
- Rasszizmust és gyűlöletet népszerűsítő oldalak;
- Alkoholt népszerűsítő és támogató oldalak;
- Erőszakot népszerűsítő oldalak;
- Fegyverekről, fegyverkereskedelemről és a kapcsolódó tárgyakról szóló oldalak;
- Illegális szoftverletöltő oldalak;
- Oldalak, melyek díjazzák a felhasználókat az internetes aktivitásukért;
- Kockázatos (kritikus vagy magas kategóriába tartozó), kártékony weboldalak, vagy nem kategorizált az MVM Zrt. Csoportszintű Biztonsági Igazgatóság Információbiztonsági és Kríziskezelési funkciója által egyedileg meghatározott korlátozások.

A TÁRSASÁGI PROJEKTSZOBA, ILLETVE ADATSZOBA ÁLTALÁNOS INFORMÁCIÓBIZTONSÁGI KÖVETELMÉNYEI

- A projektszobát, illetve adatszobát olyan helyiségben kell kialakítani, mely a társasági információbiztonsági felelős által meghatározott követelményeknek megfelel.
- A projektszoba/adatszoba nyitvatartási idejét a külső féllel kötött szerződésben rögzíteni kell. A nyitvatartási időnek összhangban kell lennie a társaság által alkalmazott munkarenddel. Nyitvatartási időn kívül a projektszobában tartózkodni tilos. Ettől eltérő működési rendet a társasági információbiztonsági felelős írásban engedélyezhet.
- A projektszobába/adatszobába való bejutás a külsős résztvevő részére is kizárólag a biztonsági szolgáltató által készített vendégkártya használatával és/vagy kulccsal lehetséges. Amennyiben állandó belépő igénylése nem indokolt (pl. a projektszoba kulccsal nyitható), vendégkártya átvételére a recepción/portaszolgálaton van lehetőség, melyet a munka végeztével/napvégén minden alkalommal le kell adni, s a következő alkalommal újra igényelni. Vendégkártya csak azon külsős résztvevők számára adható, akiknek fogadásáról, az épületben történő mozgásáról és a projektszobába és onnan történő kíséretéről a fogadó fél felelősséget vállal. Hosszabb távú (1 hónapot meghaladó) projekt esetén külsős résztvevő számára igényelhető ideiglenes belépőkártya.
- A projektszobába/adatszobába a külsős résztvevők közül kizárólag azon személyek léphetnek be, akik rendelkeznek titoktartási-, adott esetben Információbiztonsági nyilatkozattal, illetve akik a szerződésben nevesítésre kerültek.
- A projektszobában/adatszobában elhelyezett dokumentumok, információk eléréséhez kizárólag a projektszobában elhelyezett MVMH tartományi munkaállomás használható külső közreműködők által, hordozható eszköz kiadása nem megengedett számukra.
- A rendelkezésre bocsátott munkaállomással kapcsolatos követelmények a következők:
    - A külsős résztvevők számára egyedi MVMH-s azonosítót kell igényelni (közös bejelentkezési azonosító nem használható!).
    - A projektszobában/adatszobában elhelyezett dokumentumokról, információkról másolat semmilyen formában nem készíthető, ezért az adatszobában elhelyezett számítógépek kizárólag olvasási jogosultságot biztosítanak. Ezen túl, a kommunikációs portok letiltásra kerülnek, kizárólag azon közös meghajtó vagy rendszer érhető el róluk, amely a projekttel kapcsolatos dokumentumokat, információkat tartalmazza.
    - A rendelkezésre bocsátott adatok sokszorosításának elkerülése végett, tiltott a nyomtatási, továbbá a fénymásolási lehetőség is.
    - A projektszobában/adatszobában elhelyezett dokumentumok, információk megismerhetőségére elektronikus formában, Internet kapcsolat nélküli számítógépeken keresztül van lehetőség, bármilyen elektronikus küldés lehetőségének kizárásával.
    - A projektszobában/adatszobában rendelkezésre bocsátott MVMH-s tartományi gépeken szükséges a naplók rendszeres elemzése a társaság által meghatározott, alacsonyabb szintű szabályzatokban foglaltak szerint.

REVIR KÖZPONTI ÜGYELET ELÉRHETŐSÉGEI

REVIR Központi Ügyelet	
Telefon:	+36 80/205-251
Mobiltelefon	+36 30/438-6692
Fax (bejövő) Fax (kimenő)	+36 1/205-3285 +36 1/203-0133
E-mail:	revir@mvm.hu

Megjegyzés:

A +36 80/205-251 REVIR telefonszám (kimenő hívásnál megjelenő) hordozója a +36 1/203-0132 telefonszám.

A foglaltság elkerülése érdekében a fax küldeményt lehetőleg a bejövőként megjelölt fax számra célszerű küldeni. A két telefax vonal beszédhívás fogadására is alkalmas.

Fenti hívószámok foglaltsága vagy elérhetetlensége esetén a Központi Diszpécser Szolgálat telefonszámai is hívhatók:

+36 1/304-3137

+36 1/304-3139

ÜZLETFOLYTONOSSÁGI MÓDSZERTAN

Tartalom

1. A dokumentum célja

Jelen dokumentum célja, hogy meghatározza az MVM Mobiliti Kft. (a továbbiakban: Társaság) üzletfolytonossági rendszere kialakításának, működtetésének és karbantartásának magas szintű lépéseit és módszertanát, a központi előírások figyelembevételével. A dokumentum definiálja mindazokat a módszertani lépéseket, melyeken keresztül a Társaság meg kívánja valósítani a szervezetére vonatkozó üzletfolytonossági rendszer tervezést.

2. Az üzletfolytonossági tervezésről általában

A Társaság üzleti stratégiáját annak a feltételezésével alakítja ki, hogy üzleti folyamatai és az azok megvalósításához szükséges szolgáltatások, erőforrások folyamatosan működnek és a szervezetek üzleti döntéseiket is ennek alapul vételével hozzák meg. Minden olyan esemény, amely a Társaság fő profilját, tevékenységi körét meghatározó üzleti folyamatok működését veszélyezteti, jelentős esemény a szervezet életében, mivel veszélyezteti az üzleti célok elérését.

Az üzletfolytonossági intézkedések használatára akkor kerül sor, ha bekövetkezik egy olyan esemény, amelynek a következménye az üzletmenet fennakadása, egy vagy több kulcsfontosságú üzleti folyamat megszakadása. Az üzletfolytonossági tervezés elősegíti a szervezetek rugalmasságát, reakciókészségét egy esetlegesen előforduló krízishelyzet esetén, így biztosítva, hogy a szervezet céljai rendkívüli esemény bekövetkezése esetén is biztosítva, elérhetőek legyenek. Az üzletfolytonossági tervezés által lehetővé válik, hogy a szervezet fő tevékenységét, szolgáltatásait, termékeinek előállítását egy előre megállapodott szolgáltatási szint mellett és időn belül biztosítani tudja a folyamat megszakadása esetén is.

Az üzletfolytonossági tervezés megvalósításának indokoltsága:

- A krízishelyzet, erőforrás kiesés következtében fellépő pénzügyi és piaci veszteségek minimalizálása;
- Jó hírnév megóvása;
- Az ügyfelek, üzletfelek, tulajdonosok és hatóságok elvárásainak való megfelelés;
- Ügyfélbizalom növelése;
- A kulcsfontosságú folyamatok megfelelő szintű működésének fenntartása;
- A folyamatok kockázatarányos védelme;
- A szabályozási környezetnek való megfelelés;
- Gyorsabb reakció fennakadások esetén;
- Tudatos rendkívüli helyzet kezelés.

Az üzletfolytonossági menedzsment rendszer kialakítása során az alábbi szempontokat érdemes figyelembe venni:

2.1. Folyamatalapú szemlélet

Az üzletfolytonossági tervezés során a kritikus folyamatok meghatározásához, az alternatív folyamatok kidolgozásához nélkülözhetetlen a folyamatalapú szemléletmód alkalmazása, az üzletfolytonosság tervezését megelőzően a belső szabályzatok és folyamat leírások kidolgozása, ellenőrzése, oktatása, tesztelése (visszacsatolás), rendszeres felülvizsgálata.

2.2. Műszaki szemlélet

A tervezés során elengedhetetlen a kritikus folyamatokhoz kapcsolódó, üzletfolytonosság tervezés szempontjából kiemelt műszaki rendszerek, eszközök áttekintése. Ezek lehetnek különösen:

- az adott szolgáltató/termelő üzemben a szolgáltatáshoz/termeléshez használt technológiai berendezésekkel, eszközökkel.
- a folyamatok során használt infrastruktúra (pl.: ivóvíz szolgáltatás, fűtés, stb.), a használatban lévő és használaton kívüli épületek, valamint valamennyi épület közvetlen környezetére vonatkozó releváns információk,
- az informatikai és telekommunikációs rendszerek (pl.: levelező kiszolgáló, irodai hálózat, stb.),
- az egyéb, nem informatikai rendszerek, eszközök (pl.: beléptető rendszer, tűzjelzők, stb.),

Ezzel a szemlélettel könnyen azonosíthatók a kritikus erőforrások (például: humán erőforrások, IT erőforrások, stb.)

2.3. Pénzügyi szemlélet

Az üzletfolytonossági működés kialakítása során vizsgálni szükséges azt is, hogy milyen pénzügyi vonatkozása van az adott folyamat kiesésének. Ilyen vizsgálati szempontok lehetnek különösen:

- van-e megfelelő/elkülönített forrás a megelőzésre,
- felmerülhet-e igény a kiesés miatt bekövetkezett közvetlen károk megtérítésére, helyreállítási munkák finanszírozására,
- vannak-e olyan adatszolgáltatási kötelezettségek, amelyek elmulasztása pénzügyi szankciót von maga után,
- lehetnek-e a Társaságra vonatkozó – így pénzügyileg közvetve, vagy közvetlenül az MVM Csoportra ható – a jogszabályokban meghatározott szolgáltatási szint be nem tartása esetén előálló pénzügyi szankciók.

2.4. Humán szemlélet

Az üzletfolytonossági menedzsment humánerőforrás oldalról való megközelítése szintén elengedhetetlen:

- a folyamatok humán erőforrástól való függésének felmérése; a kritikus munkakörök meghatározása, jogosultságkezelés kialakítása;
- humán kockázat kezelési szempontok, eljárások alkalmazása;
- a hiányzó munkaerő pótlásának biztosítása;
- kritikus folyamatokhoz szükséges szakemberek rendkívüli minősítésű időszakban történő kiesésük esetén a helyettesítésükről vagy elhelyezésükről való gondoskodás;
- mind a megelőzési, mind a rendkívüli-helyzetkezelési időszakban a szükséges adatok, folyamatok monitoringja, a kapott információk folyamatos értékelése.

2.5. Kommunikációs, koordinációs szemlélet

Ez a nézőpont az MVM Csoport és a Társaság, mint tagvállalat kapcsolódását is szem előtt tartja. Jelen Szabályzatban foglalt szabályok definiálják, hogy egy vagy akár több társaságot üzletfolytonosság szempontjából érintő rendkívüli helyzet esetén milyen kommunikációs és koordinatív feladatai vannak a központnak, illetve a társaságok saját kommunikációs

szabályzatukban meghatározzák saját kommunikációs és együttműködési kötelezettségüket több vállalatot érintő rendkívüli helyzet esetén.

2.6. Dinamikus szabályozói környezet, rendszer

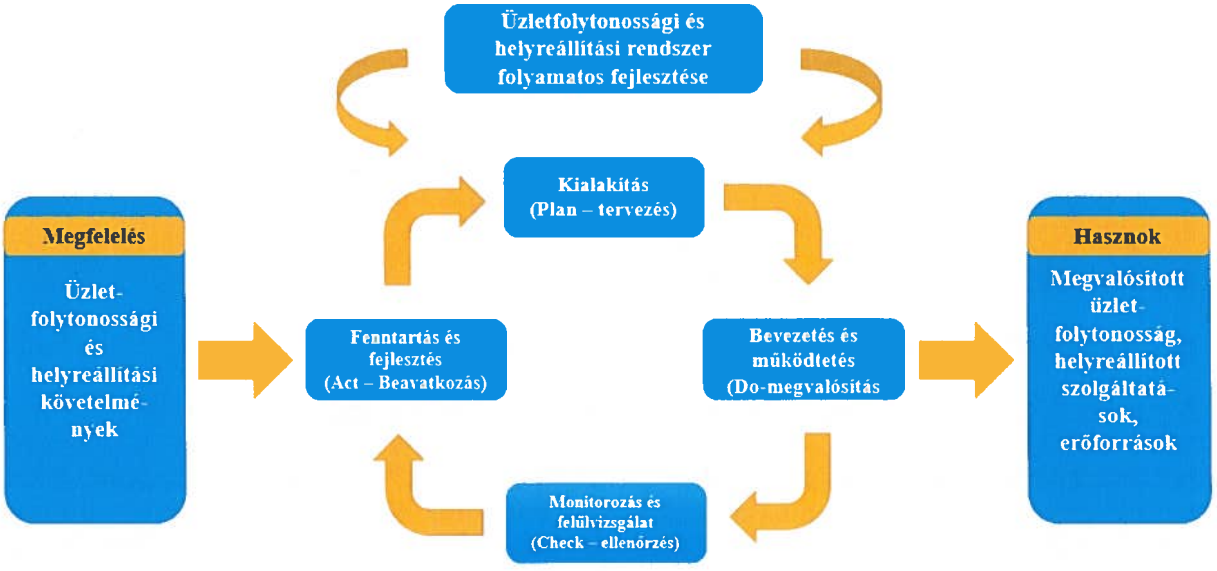
Amikor a vállalati működés folyamatos fejlesztését számtalan projekt célozza, valamint az adott társaság kritikus folyamataihoz kapcsolódó kritikus műszaki, informatikai rendszereket folyamatosan fejlesztik, nélkülözhetetlen feladat a folyamatos fejlesztések nyomon követése. – Szükséges a jelen kor követelményeinek megfelelő, és ez által a rendkívüli helyzet kezelési rendszerek fejlesztésekhez illesztését is folyamatosan biztosítani képes dinamikus szabályozói környezet működtetése, ezáltal minden változás idejében kezelésre kerül.

Új technológiák, rendszerek bevezetése esetén, vagy üzletfolytonossági szempontból kritikus eszközöket, rendszereket érintő beruházások esetén, a beruházási folyamat kötelező lépése ezen rendszerek, eszközök tekintetében szükséges üzleti hatáselemzés lebonyolítása, hogy ezen rendszerek és beruházások érintik, vagy befolyásolják e a kritikus folyamatok aktuális besorolását, illetve az őket támogató erőforrások függőségi jellemzőit, továbbá szükséges vizsgálni, hogy az ezen új rendszerek vagy beruházások által érintett más üzleti folyamatok besorolása és erőforrás függősége változik e (kritikus folyamatként értékelhetők lesznek e) a beruházás, vagy az új rendszer alkalmazása következtében.

Ha az új rendszer nem új szolgáltatáshoz, illetve nem új üzleti folyamat kiszolgálásához kerül bevezetésre, hanem pl. meglévő kiváltására az új rendszert szolgáltatónak a tervezés fázisában figyelembe kell vennie azon folyamatok üzleti hatáselemzését, amelyek az érintett szolgáltatást használni fogják. Ha új üzleti folyamat kiszolgálására kerül az új rendszer bevezetésre, akkor az adott folyamatra üzleti hatás-, és kockázatelemzést kell először elvégezni, amelynek eredményét figyelembe kell venni a rendszer tervezésekor.

3. Az üzletfolytonosság menedzsment rendszer működtetésének folyamata

Az üzletfolytonossági menedzsment rendszer kialakítása és működtetése – a nemzetközi irányelvekkel összhangban – meghatározható a PDCA (Plan-Do-Check-Act) modellnek megfelelően (lásd. ISO 22301:2012 Societal security – Business continuity management systems - requirements).



Tervezés (P)	A szervezet céljaihoz illeszkedő üzletfolytonossági stratégia, folyamatok, kontrollok definiálása
Megvalósítás (D)	Az üzletfolytonossági stratégia, folyamatok, kontrollok megvalósítása és működtetése
Ellenőrzés (C)	Az üzletfolytonossági stratégiával, célkitűzésekkel összevetve a megvalósulás felülvizsgálata, monitorozása.
Beavatkozás (A)	Az üzletfolytonossági intézkedések és tervek alkalmazása rendkívüli helyzetben, tapasztalatok alapján helyesbítő, módosító intézkedések.

4. Az üzletfolytonosság tervezéséhez és kialakításához szükséges előkészületek

Mielőtt megkezdődne az üzletfolytonosság tervezésének folyamata, szükséges, hogy a Társaság előre megtervezze és szabályozza a folyamat lépéseit, kijelölje a felelősöket annak érdekében, hogy ütemezett, koordinált, valamint ellenőrzött keretek mentén történjen a fejlesztés és működtetés.

Az üzletfolytonosság menedzsment rendszer bevezetésének egyik elsődleges lépése a feladatmegvalósítás terjedelmének (vizsgálat alá vont folyamatok és az elemzések időigénye) vizsgálata és ennek tükrében a végrehajtáshoz szükséges erőforrások (elemzéseket végző munkatársak létszáma) becslése.

A feladat összetettségéből adódóan szükséges egy írásbeli, jóváhagyott üzletfolytonossági felmérési terv készítése, amely rögzíti a tervezési folyamat:

- egyes lépéseit,
- összefüggéseit,
- a határidőket,
- a feladat elvégzéséhez szükséges (pl.: emberi, IT) erőforrásokat,
- a kapcsolódó felelősöket,
- a szükséges bemenő adatokat.

Az üzletfolytonossági felmérési tervet a feladat megkezdésétől kezdve folyamatosan aktualizálni szükséges.

Eredménytermék: Üzletfolytonossági felmérési terv

5. Az üzletfolytonossági tervezés módszertani keretei

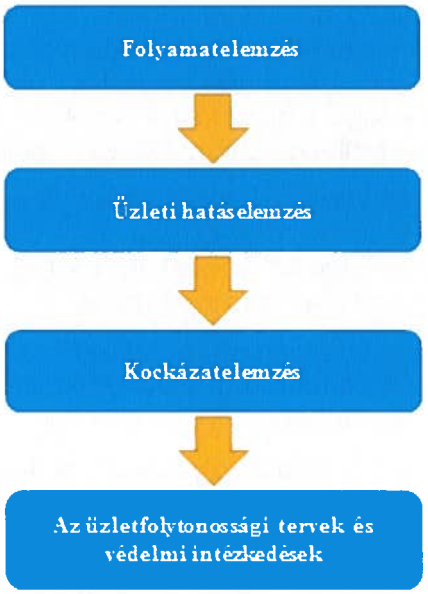
Az üzletfolytonossággal kapcsolatos feladatok megvalósításához, (pl.: a kritikus folyamatok felméréséhez, az interjúk, elemzések eredményeinek rögzítéséhez, a tesztelések és felülvizsgálatok tervezéséhez és dokumentálásához) előre elkészített formanyomtatványokat használunk. Ez segíti, hogy a begyűjtött nagy mennyiségű információ rendszerezett formában álljon rendelkezésre, segíti az áttekinthetőséget, a feldolgozást és a teljes körűséget (pl. minden folyamattal/szolgáltatással/erőforrással kapcsolatban azonos adatok álljanak rendelkezésre és minden adat elemzésre kerüljön, a tervezés és dokumentáció standard módon történjen). A rendkívüli helyzetkezelés szabályozói környezetének kialakítása során kárérték táblát kell készíteni, hogy az üzleti hatáselemzések konzisztens módon valósulhassanak meg. A táblát úgy kell kialakítani, hogy a Társaság szempontjából releváns kárjellegek (pl. anyagi, imázs, működési, stb.) és kárértékek (pl. minimális, mérsékelt, kritikus, stb.) mátrixa jöjjön létre. Az adatvagyon felmérés és az üzleti hatáselemzés során alkalmazható ugyanaz a kárérték tábla.

A formanyomtatványok, segédanyagok a Társaság MOB-BSz-17 Az MVM Mobiliti Kft. Információbiztonsági és rendkívüli helyzetkezelési belső szabályzatához kapcsolódó mellékletek és formanyomtatványok formájában kerülnek kiadásra.

Eredménytermék:

- Formanyomtatványok
- Kárérték tábla

6. Üzletfolytonossági tervezés folyamata



6.1. Folyamatok üzletfolytonossági felmérése

Az üzletfolytonossági felmérést javasolt a szervezet valamennyi folyamatára kiterjedően végrehajtani, célszerűen az adatvagyon felméréssel összehangoltan.

Az üzletfolytonossági felmérés célja az üzletfolytonossági szempontból kritikus folyamatok és az azok működésfolytonosságát veszélyeztető kockázatok megállapítása.

A folyamatok vizsgálatának ki kell terjednie annak értékelésére is, hogy a Társaság működési folyamatának zavara hatással van-e az MVM Csoport társaságainak működési folyamataira vagy a Társaság kritikus folyamataira. Az ilyen függések vizsgálatának célja a csoportszintű üzletfolytonosság biztosítása és a dominóhatás csökkentése.

A tervezés megkezdésekor a Társaság valamennyi működési folyamatát tartalmazó folyamatkatalógus alapján össze kell állítani az üzletfolytonossági felmérés által érintett folyamatok listáját szervezeti egység/folyamatgazda/folyamat bontásban. A folyamatok meghatározásánál irányadó lehet:

- mindenkor hatályos szervezeti és működési szabályzat,
- szervezeti ábra,
- folyamatmenedzsment rendszerben vagy a Társaság által más módon rögzített működési folyamatok és azok alapján készült folyamatleírások, belső eljárásrendek, szabályzatok, utasítások stb.
- Társaság kulcs irányító és támogató folyamatainak listája
- korábban már kritikus folyamatként értékelt folyamatok listája

Eredménytermék:

- Üzletfolytonossági tervezés által érintett folyamatok listája

Az üzletfolytonossági tervezés által érintett folyamatokra vonatkozó felmérés során az érintett folyamatokkal kapcsolatos azon információk összegyűjtését és rögzítését szükséges elvégezni, amelyek alapján megállapítható, hogy mely folyamatok tekinthetők a Társaság kritikus folyamatainak és milyen erőforrás kiesés vonható a kockázatértékelés körébe, melyik támogató erőforrás kiesésére érdemes akcióterveket kidolgozni.

A felmérés kiindulópontját az üzletfolytonossági tervezés által érintett folyamatok listája képezi.

Amennyiben az elemzésbe bevont folyamatok valamilyen dokumentált eljárásrendben szabályozva lettek, a szabályozó dokumentumokat (Szervezeti és Működési Szabályzat, a szervezeti ábra, a folyamatmenedzsment rendszerekben rögzített működési folyamatok és azok alapján készült folyamatleírások, belső eljárásrendek, utasítások stb) a személyes interjú lefolytatása előtt be kell kérni a folyamatgazdáktól. A dokumentumok átolvasása lehetőséget ad a folyamat megértésére, a felkészülésre, a vizsgálat szempontjából fontos adatok begyűjtésére.

Fontos kiemelni, hogy a személyes interjú lefolytatása semmiképpen nem maradhat el, mert előfordulhat, hogy az írásos szabályozó nem aktualizált illetve a valós működés esetlegesen eltérést mutathat a dokumentált eljáráshoz képest. Ilyen jellegű eltérés feltárása esetén az eltérés tényét jelezni kell és javaslatot kell tenni a módosításra.

A folyamatok üzletfolytonossági felmérése a MOB-FU-17-04-NY-01 formanyomtatványban foglaltak szerinti adattartalom folyamatgazda és/vagy az általa kijelölt személy általi kitöltése, illetve interjú lefolytatása mentén történik.

A személyes interjúk célja a működési folyamatok átvilágítása, a folyamat alapadatainak összegyűjtése, dokumentált eljárásrend esetén az adatok pontosítása.

A felméréseket javasolt folyamatgazdánként szervezni, azaz egy interjú keretében a folyamatgazdához tartozó összes kijelölt folyamat elemzésre kerülhet, illetve ennek megfelelően egy folyamatgazda több kérdőívet is kitölthet.

A kérdőív kitöltésében, illetve az interjún nem kell feltétlenül a folyamatgazdának részt vennie. A folyamatgazda kijelölhet más személyt is a kérdőív kitöltésére, illetve a megbeszélésen való aktív részvételre, fontos azonban, hogy az interjúalany vagy interjúalanyok operatív ismeretekkel rendelkezzenek a folyamatról. A folyamatgazdák rendelkeznek komplex rálátással az adott szakterületi folyamatokra, így a számukra meghatározott feladat- és hatáskörben biztosítani tudják a folyamatok szakmai elvárásoknak való megfelelését, valamint a folyamatok teljességének validálását (érvényesítő ellenőrzését) az azonosított külső és belső követelmények figyelembevételével.

A folyamat felmérésről készített kitöltött kérdőívet tartalmi megfelelőség szempontjából a folyamatgazda hagyja jóvá. **Abban az esetben, ha a folyamatfelmérésben a folyamatgazda által delegált személy vesz részt, a felmérés eredményének véglegesítése előtt a folyamatgazdának jóvá kell hagynia a delegált személy által közölt adatokat!**

A felmérés során az alábbi témákra szükséges kitérni:

6.1.1. Kritikus időszakok vizsgálata és maximálisan elfogadható kiesési idők meghatározása

Egyes folyamatok esetében előfordulhatnak kritikus időszakok (pl. törvényi kötelezettség határidős teljesítése miatt), amely időszakokban a maximálisan elfogadható kiesési idők rövidebbek lehetnek. **Amennyiben van ilyen kritikus időszak, ezt az adott folyamatnál rögzíteni kell, valamint a kárértékelést a kritikus időszakra vonatkozóan – mint legrosszabb lehetőségre – kell elvégezni.**

A felmérés során a kritikus időszakra vonatkozó maximálisan elfogadható kiesési időt is rögzíteni kell, megkülönböztetve a normál időszakra meghatározott azon időintervallumtól, amely alatt a folyamat megszakadása tolerálható.

6.1.2. Erőforrás függések mértékének vizsgálata – amennyiben adatvagyon felmérés során nem kerül azonosításra

Azonosítandó, hogy mely erőforrások meghibásodása, elérhetetlensége okozhatja a folyamat megszakadását. Az erőforrások rendszerezett formában történő dokumentálása segítséget nyújt a folyamatot érintő lehetséges kockázatok meghatározásához és ezáltal az alternatív folyamatok kidolgozásához.

Az elemzés során az alábbi függőségeket kell megvizsgálni:

- adat, adathordozó,
- humán erőforrás,
- IT rendszer,
- külső szolgáltató,
- egyéb erőforrás.

A folyamatokra vonatkozóan az üzletfolytonossági felmérés során az egyes erőforrásoktól való függőségek mértékének meghatározása szükséges, amely jelen módszertan alapján a következő lehet:

- Kis mértékű függés van
- Közepes mértékű függés van
- Teljes mértékű függés azonosítható

A függés mértékének megállapításához az alábbi táblázat nyújt segítséget.

Függés / Erőforrás típusa	Kis mértékű	Közepes mértékű	Teljes függőség
Humán erőforrásoktól	A humán erőforrás könnyen helyettesíthető más humán erőforrásokkal.	A humán erőforrás részben helyettesíthető más humán erőforrásokkal.	A humán erőforrás nem helyettesíthető más humán erőforrásokkal.
IT rendszerektől	Az adott folyamat manuálisan vagy más alkalmazással végrehajtható.	Az adott folyamat manuálisan vagy más alkalmazással részben végrehajtható.	Az adott folyamat manuálisan vagy más alkalmazással nem hajtható végre.
Külső szolgáltatóktól	Az adott folyamat a szolgáltató kiesése esetén végrehajtható.	Az adott folyamat a szolgáltató kiesése esetén részben végrehajtható.	Az adott folyamat a szolgáltató kiesése esetén nem hajtható végre.
Egyéb erőforrásoktól	Az erőforrás könnyen helyettesíthető más erőforrásokkal.	Az erőforrás részben helyettesíthető más erőforrásokkal.	Az erőforrás nem helyettesíthető más erőforrásokkal.

A függés mértékének definiálása azért fontos, mert egy teljes függésben lévő, mással nem helyettesíthető erőforrás kiesése okozhatja az érintett folyamat megszakadását, melyre valamilyen védelmi intézkedés kidolgozása és bevezetése válhat szükségessé, míg egy kis

függésben lévő erőforrás esetén a folyamat ezen eleme könnyen helyettesíthető másik erőforrással kiesés esetén.

6.1.3. Folyamat függések vizsgálata – amennyiben ARIS rendszerben nem azonosítható

Az egyes működési folyamatok nem csak az erőforrásoktól függhetnek, hanem más folyamatoktól is. A folyamatok közötti kapcsolódás két típusát különböztethetjük meg: vannak támogató, illetve kiszolgált folyamatok.

Támogató folyamatról akkor beszélünk, amikor egy másik (külső vagy belső társasági) működési folyamat valamilyen adatot, (rész-) eredményterméket ad át a vizsgált folyamatnak. A támogató folyamat leállása veszélyezteti a vizsgált folyamat megfelelő működését, és a függés mértékétől függően akár annak leállását is maga után vonhatja.

Kiszolgált folyamatról beszélünk, amennyiben egy másik működési folyamat a vizsgált folyamattól vár valamilyen adatot, (rész-) eredményterméket. Ebben az esetben a vizsgált folyamat megszakadása a kiszolgált folyamatra lehet negatív hatással, és a függés mértékétől függően akár annak leállását is maga után vonhatja.

A folyamatok közötti kapcsolódást az alábbi ábra szemlélteti:

A folyamat függések vonatkozásában is meg kell határozni azok mértékét, amely az alábbi táblázat szerint történik.

Függés / Erőforrás típusa	Kis mértékű	Közepes mértékű	Teljes függőség
Más folyamatoktól	Az adott folyamat függ másik folyamattól, de annak kiesése esetén is végrehajtható a folyamat.	Az adott folyamat függ másik folyamattól, amely kiesése esetén a folyamat egyes lépései nem hajthatók végre.	Az adott folyamat függ másik folyamattól, amely kiesése esetén a folyamat nem hajtható végre.

Fentieknek megfelelően minden folyamat vonatkozásában fel kell mérni, hogy milyen támogató folyamatot, illetve kiszolgált folyamatot kell figyelembe venni a folyamat felmérése során. Az eredmények alapján előfordulhat, hogy bizonyos, alacsonyabb kárértékkel rendelkező támogató folyamatokat magasabb besorolásúra kell módosítani annak következtében, hogy egy kritikus folyamatot szolgál ki, és ezáltal a kritikus folyamat működése nagymértékben függ annak működésétől, ezért nem elhanyagolandó a folyamatok közötti kapcsolódási pontok teljes körű és megfelelő feltérképezése.

Eredménytermék:

- kitöltött folyamatfelmérő kérdőív – üzletfolytonossági szempontból releváns folyamat adatok

6.2. Üzleti hatáselemzés révén a kritikus folyamatok meghatározása

Az üzletfolytonossági tervezés következő lépése az üzletfolytonossági szempontból kritikus működési folyamatok meghatározása. Ezek azok a folyamatok, amelyek kiesése a Társaság számára olyan következményekkel járhat, amely nem tolerálható, ebből következően az üzletfolytonossági tervezés során az adott folyamat kiesésére fel kell készülni: a folyamat rendkívüli helyzetben való folyamatos működése céljából intézkedéseket szükséges kidolgozni.

A hatáselemzés célja annak felmérése, hogy a vizsgált működési folyamat kiesése, megszakadása milyen következményekkel, kárral jár a szervezet életében. A hatáselemzés

során a folyamatgazda, illetve az általa kijelölt személy a gyakorlati tapasztalatok, a szabályozási környezet ismeretében, becslés alapján meghatározza az adott folyamat különböző kiesési időkön túli leállása esetén várható kárkövetkezményeket. A hatáselemzésnél azt vizsgáljuk, hogy a megengedett maximális kiesési időn túli leállás mekkora kárt okoz. A kárérték meghatározásánál a legrosszabb esetet kell számításba venni. Az egyes folyamatok esetében – a folyamat jellegétől függően – nem biztos, hogy minden felsorolt kárkövetkezmény relevánsnak tekinthető, ilyen esetben ezt a „nincs" értékkel kell jelölni.

Az üzleti hatáselemzés során a folyamatok kiesésének következtében becsült legmagasabb kárértékek elemzéséhez és ezáltal a folyamatok kritikussági besorolásában segítséget nyújt a MOB-FU-17-04-NY-02 formanyomtatvány, illetve a biztonsági szolgáltató által nyújtott támogató rendszer. Az üzleti hatáselemzést a módszertanhoz és a szabályozáshoz kapcsolódó nyomtatványokon szükséges rögzíteni.

Az üzleti hatáselemzés sablonban rögzített kárértékeket az adatvagyon felmérés megvalósításával felül kell vizsgálni és az üzleti hatáselemzés és adatvagyon felmérés során ugyanazt a kárértéktáblázatot kell használni.

A különböző maximális kiesési idők és a hozzájuk tartozó kárértékek tükrében, az alábbi módon kerülnek besorolásra a Társaság folyamatai, és kerülnek ezáltal meghatározásra a kritikus folyamatok.

A hatáselemzés eredményei alapján a folyamatok három kategóriába sorolhatók:

- Kritikus.
- Közepesen kritikus.
- Nem kritikus.

Kritikus

Kritikusnak tekinthetők azok a folyamatok, melyek kiesési hatása bármely kárjelleg vonatkozásában a kárérték-táblázat alapján:

- 2 nap vagy annál rövidebb kiesési idő esetén „kritikus".
- 4 óra vagy annál rövidebb kiesési idő esetén „jelentős".
- 30 perc kiesési idő esetén „mérsékelt".

A kritikus folyamatok tekintetében mindenképpen szükségszerű kockázatelemzés lefolytatása és ennek eredményeként védelmi intézkedések, üzletfolytonossági akciótervek kidolgozása, mely az adott folyamat folyamatosságát biztosítják.

Közepesen kritikus

Közepesen kritikusnak tekinthetők azok a folyamatok, melyek kiesési hatása bármely kárjelleg vonatkozásában a kárérték-táblázat alapján:

- 3 nap vagy annál hosszabb kiesési idő esetén „kritikus".
- 1 nap vagy annál hosszabb kiesési idő esetén „jelentős".
- 2 nap, 1 nap, 4 óra, 2 óra, 1 óra kiesési idő esetén „mérsékelt".
- 1 nap, 4 óra, 2 óra, 1 óra, 30 perc kiesési idő esetén „csekély".

A közepesen kritikus folyamatok tekintetében, javasolt (vezetői döntéstől függően) kockázatelemzés végrehajtása és ennek eredménye alapján védelmi intézkedések kidolgozása.

Nem kritikus

Nem kritikusak azok a folyamatok, melyek kiesési hatása bármely kárjelleg vonatkozásában a kárérték-táblázat alapján:

- 3 nap vagy annál hosszabb kiesési idő esetén „mérsékelt".
- 2 nap vagy annál hosszabb kiesési idő esetén „"csekély".

- 30 perc vagy annál hosszabb kiesési idő esetén „minimális" vagy „nincs".

A nem kritikus folyamatok tekintetében nem kell kockázatelemzést végezni és védelmi intézkedéseket kidolgozni.

Eredménytermék:

- Folyamatok kiesése esetén becsült kármértékek
- Társaság kritikus folyamatok listája

6.3. Üzletfolytonossági kockázatelemzés

Miután az üzleti hatáselemzés eredményeként a Társaság kritikus folyamatai megállapításra kerültek, az üzletfolytonossági kockázatelemzés fázisa következik, melynek során a folyamatokat érintő üzletfolytonossági kockázatok felmérésre kerülnek. Az üzletfolytonossági kockázatelemzés végrehajtására az információbiztonsági kockázatelemzéssel párhuzamosan is sor kerülhet.

Üzletfolytonosság szempontjából a kockázat annak a lehetősége, hogy valami előre nem látható, kedvezőtlen esemény történik (a veszély megvalósulásának lehetősége, adott esetben a katasztrófa vagy krízis bekövetkezésének esélye).

Az üzletfolytonossági célterületű kockázatelemzés célja annak felmérése, hogy az adott működési folyamat lefolyását milyen kockázatok érhetik, vagyis megvizsgáljuk, hogy melyek azok a lehetséges tényezők, események, amelyek a működési folyamat rendeltetésszerű lefolyását, erőforrás kiesésből fakadóan befolyásolhatják, az üzleti folyamatot támogató erőforrások kiesése milyen fenyegetések hatására, milyen sérülékenység fennállásával következhet be.

Az üzleti hatáselemzés során definiált kritikus folyamatok képezik elsősorban a kockázatelemzés hatókörét, de célszerű a közepesen kritikus folyamatok esetében is elvégezni a vizsgálatokat.

6.3.1. Üzletfolytonossági kockázatok azonosítása

A kockázatkezelési folyamat a releváns kockázatok azonosításával kezdődik. A folyamatgazdával vagy általa kijelölt személlyel azonosítás során a folyamat működtetése szempontjából releváns várható kockázatokról egy előzetes listát kell készíteni.

A kockázatelemzés során kiindulópontként vesszük a már számba vett erőforrás függések listáját, azaz a kockázatelemzés menetének elsődleges lépése, hogy felmérjük, hogy a vizsgált folyamat kapcsán az adott folyamati elemeket, erőforrásokat milyen kockázatot érhetik. Javasolt a kockázatokat folyamat/erőforrás/kockázat megnevezése bontásban rögzíteni.

A kockázatok azonosítását segíti a biztonsági relevanciájú kockázatok, veszélyek listája, amelynek összeállításához iránymutatást az MVM Zrt. Csoportszintű Biztonsági Igazgatósága nyújt.

A Társaság vagy az MVM Csoport központi kockázati univerzuma a kockázatok azonosításához szintén segítséget nyújthat.

Eredménytermék:

- Üzletfolytonossági kockázatlista folyamatonként

6.3.2. Kockázatok elemzése – amennyiben információbiztonsági kockázatelemzés keretein belül nem kerül megvalósításra

A beazonosítást követi az azonosított kockázatok elemzése, ami célirányosan figyelembe vesz és értékel minden a szervezet stratégiája és az ezt szolgáló rövidebb távú célok elérését befolyásoló, a kulcsfolyamat működtetése szempontjából releváns kockázati tényezőt. Mint a

kockázatmenedzsment folyamat minden szakaszának, ennek is folyamatosan meg kell történnie. Az újonnan beazonosított kockázati tényezőket elemezni, objektíven értékelni és osztályozni szükséges. Intézkedéseket csak akkor kell tenni, ha a kockázat egy bizonyos szintet elér.

Az elemzés esetében is több módszer közül választhatunk. Ennek egyik módja az ún. kockázati mátrix, amely jól szemlélteti a kockázati küszöb kérdésének problematikáját is. A térképen az egyes kockázati tényezőket a bekövetkezési valószínűségük és a hatásuk alapján helyezhetjük el. A kategóriákat a szervezet sajátosságainak ismeretében alakíthatjuk ki, például figyelembe vehetjük a kockázattűrési képességet. A kockázatokat folyamathoz és erőforráshoz rendelten rögzítjük.

A kockázatok elemzésénél két szempontot kell vizsgálni:

- a kockázat bekövetkezési valószínűsége,
- a kockázati esemény következtében keletkezett kár becsült nagysága.

A kockázatok elemzési munkafolyamatát támogató kockázati mátrix táblázat a MOB-FU-17-04-NY-02 formanyomtatvány „Kockázatelemzés" munkalapján található, míg a mátrix kitöltésének értékelő segéd táblázatai a „Segédlet (kockázatelemzés)" munkalapján.

A bekövetkezési valószínűség meghatározásánál az alábbi táblázatot vesszük alapul:

Sorrend	Bekövetkezési valószínűség	Várható bekövetkezési gyakoriság
1	**Nagyon ritka**	100 évben kevesebb, mint egyszer
2	**Ritka**	100 évben egyszer – 20 évben egyszer
3	**Nem túl gyakori**	20 évben egyszer – 5 évben egyszer
4	**Gyakori**	5 évben egyszer – 1 évben egyszer
5	**Állandósult**	Egyszer egy évben vagy többször

A kár becsült nagyságát az elfogadott kárérték táblázat segítségével határozzuk meg. Az okozott kárértékekre egységesen a következő szinteket határoztuk meg:

Sorrend	Kárérték szint
1	**Minimális**
2	**Csekély**
3	**Mérsékelt**
4	**Jelentős**
5	**Kritikus**

A **kockázati értéket** (a kockázati mátrix értékeit) a kárérték és bekövetkezési valószínűség értékeinek szorzatai adják. Ebből adódik, hogy a két (egytől ötig terjedő) intervallum-skála összeszorzásával a kockázat értékekre is egy intervallum-skálát kapunk, aminek minimum értéke =1, maximum értéke =25.

Ennek megfelelően a kapott kockázati értékű kockázati eseményeket a kockázati értékek kockázati szintekbe sorolásával azonnal értékelhetjük:

Kockázati szint	Pontszám alsó határa	Szín jelölés
Kis	1	
Közepes	8	
Nagy	15	

Az alábbi táblázat tartalmazza a különböző bekövetkezési valószínűségű és kárértéket okozó kockázati események kockázati értékeit, és egyben az azokhoz tartozó (színnel jelölt) kockázati besorolást is.

	Nagyon ritka (1)	Ritka (2)	Nem túl gyakori (3)	Gyakori (4)	Állandósult (5)
Minimális (1)	1	2	3	4	5
Csekély (2)	2	4	6	8	10
Mérsékelt (3)	3	6	9	12	15
Jelentős (4)	4	8	12	16	20
Kritikus (5)	5	10	15	20	25

Eredménytermék:

- Üzletfolytonossági kockázatlista folyamatonként kockázati értékekkel

6.3.3. Kockázatok kezelése

A kockázatok azonosítását és elemzését követően a kockázatmenedzsment következő lépése a kockázatok kezelése, mely során meg kell határozni azon lehetséges védelmi intézkedéseket, melyekkel az adott kockázat bekövetkezési valószínűsége és/vagy hatása csökkenthető. A védelmi intézkedés javaslatokat, és az azokról született döntést dokumentáltan rögzíteni kell (akár a kockázatelemzés elkészítésére szolgáló rendszerben).

Az azonosított kockázatok kezelésének módjai, vagyis az alkalmazott kockázatkezelési stratégiák a következők lehetnek:

- **Elkerülés:** A kockázat bekövetkezésének elkerülése. Például a tevékenység teljes elkerülésével, vagy egy teljesen más megközelítés alkalmazásával.
- **Áthárítás:** A kockázat áthárítása kezeléssel és felelősséggel együtt egy harmadik félnek, általában valamilyen kompenzációért. Például biztosításkötés.
- **Csökkentés:** A leggyakrabban alkalmazott stratégia. A kockázat bekövetkezésének és az abból eredő kár mértékének meghatározott toleranciaszint alá csökkentése, kontrollok kidolgozásával, bevezetésével. Például adatvesztés ellen biztonsági mentések alkalmazása. A kontrolloknak a fajtái a következők lehetnek:
  - Preventív (megelőző)
  - Detektív (észlelő)
  - Korrektív (javító)
- **Felvállalás:** A kockázat bekövetkezésének tudatos és dokumentált felvállalása.

A kockázatelemzésben az azonosított kockázatok mellett javaslat készül a kockázatok kezelésére irányuló kockázatcsökkentő intézkedésekre, melyeket a folyamatgazda vagy erőforrásgazda, és a társasági üzletfolytonossági felelős értékel. és javaslatot tesz a megvalósítandó védelmi intézkedésekre, vagy kompenzáló kontrollokra.

Az értékelés szempontjai a következők:

- védelmi intézkedés becsült költsége szembe állítva az azonos maximális kárhatással
- védelmi intézkedés megvalósíthatóságának időtávlata szembe állítva a bekövetkezési gyakorisággal/valószínűséggel
- ideiglenes vagy állandó kompenzáló kontroll lehetőségek

A javasolt védelmi intézkedéseket a kockázatelemzés eredményével együtt dokumentált módon kell továbbítani jóváhagyásra.

Azon kockázatok, melyek csökkentésére nincs tervben védelmi intézkedés bevezetése, felvállalt kockázatnak tekintendők. Kockázat felvállalására a folyamatgazda vagy erőforrásgazda, és a társasági üzletfolytonossági felelős tesz írásbeli javaslatot. A felvállalt kockázatokról nyilatkozni szükséges, ennek elfogadása a Stratégiai Bizottság felelőssége.

A több társaságot érintő közös kockázatok esetében a kockázatkezelés csoportszintű módjáról az érintett társaságok javaslata alapján az MVM Zrt. Csoportszintű Biztonsági Igazgatóság hozza meg a döntést és dokumentál feljegyzés formájában.

6.3.4. Védelmi intézkedések tervezése és megvalósítása

Amennyiben a kockázatkezelés módjaként valamilyen védelmi intézkedés bevezetése kerül kiválasztásra, a választott védelmi intézkedések körét dokumentált módon rögzíteni és tervezni kell. A védelmi intézkedés javaslatok mellett előzetesen értékelni kell a maradványkockázatokat, illetve a védelmi intézkedés javaslatok indokoltságát (bekövetkezési gyakoriság, bekövetkezéskori kárhatás vagy mindkettő csökkentése, becsült erőforrás ráfordítás vizsgálata, stb.).

A védelmi intézkedések az alábbi típusúak lehetnek:

- Adminisztratív védelem
- Fizikai védelem
- Technikai/Logikai védelem

A kiválasztott védelmi intézkedés tervezését magas szinten dokumentáltan rögzíteni kell a visszaellenőrizhetőség biztosítása céljából.

A védelmi intézkedések bevezetését megelőzően vagy kiegészítően kompenzáló kontrollok bevezetése lehet indokolt, melyeket szintén dokumentált módon rögzíteni kell. A védelmi intézkedések dokumentálása történet a kockázatelemzés készítését támogató rendszerben is.

6.3.5. Maradványkockázatok számítása

Azon kockázatok esetén, melyek valamilyen védelmi intézkedés bevezetésével vagy tervezésével kezelésre kerülnek, azonosításra kerülnek a védelmi intézkedések bevezetése után fennmaradó, a továbbiakban már nem csökkenthető kockázatok, melyek rögzítésre kerülnek a maradványkockázatok listáján. A maradványkockázatok elfogadására a folyamatgazda vagy erőforrásgazda és a társasági üzletfolytonossági felelős tesz írásbeli javaslatot. A maradványkockázatok elfogadásáról nyilatkozni szükséges, ennek elfogadása a Stratégiai Bizottság felelőssége.

Eredménytermék: Kockázati mátrix:

- Kockázatlista folyamatonként kockázati értékekkel és hatályban lévő vagy javasolt védelmi intézkedésekkel
- Maradványkockázatok folyamatonként.

6.4. Üzletfolytonossági tervek, egyéb védelmi intézkedések tervezése

Üzletfolytonossági szempontból az egyik elsődleges védelmi intézkedés javaslat az üzletfolytonossági tervek/akciótervek kidolgozása, de emellett más, informatikai és biztonsági relevanciájú, fizikai, logikai és/vagy adminisztratív védelmi intézkedés javaslatok is szerepet kapnak.

6.4.1. Üzletfolytonossági tervek

Az üzletfolytonossági tervek célja a kritikus üzleti folyamatok rendkívüli esemény bekövetkezése utáni fenntartása egy előre meghatározott szolgáltatási szinten.

Az üzletfolytonossági tervek az adott kritikus működési folyamat tekintetében helyettesítő folyamatokat tartalmaznak, azaz az adott működési folyamatra vonatkozóan alternatív dokumentált eljárásokat írnak elő a folyamatot támogató erőforrás kiesése okozta folyamat megszakadás esetére, az erőforrás eredeti állapotba történő helyreállításáig terjedő időre.

Az üzletfolytonossági tervek elkészítésénél a kockázatelemzésből azonosítani lehet, hogy a folyamat milyen okból eshet ki, és ezen helyzetekre kell forgatókönyvet, alternatív eljárást készíteni.

Az üzletfolytonossági tervek általános felépítését, tartalmi követelményeit a MOB-FU-17-04-NY-03 formanyomtatvány rögzíti.

Amennyiben az üzletfolytonossági rendszer működtetését támogató informatikai rendszer bevezetésre kerül, az abban alkalmazott megoldás segítségével is rögzíteni lehet az egyes akcióterveket, ezen esetben jelen módszertan aktualizálása indokolt.

Az üzletfolytonossági terv tartalmazza az alternatív folyamat lépések leírásán túl az alternatív folyamat működtetéséhez szükséges erőforrások és időkorlátok megjelölését, valamint az eredeti folyamatra, illetve a normál munkarendre való visszaállásig terjedő feladatokat is.

6.4.2. Egyéb védelmi intézkedések

Az üzletfolytonossági tervek mellett számos védelmi intézkedés alkalmazható, tervezhető annak érdekében, hogy a Társaság kritikus folyamatai egy előre meghatározott szinten tovább működjenek rendkívüli esemény bekövetkezése esetén.

Az üzleti hatáselemzés során beazonosított kritikus erőforrásokra (például informatikai erőforrások) és szolgáltatásokra vonatkozóan helyreállítási terveket szükséges kidolgozni. A helyreállítási tervek célja a kritikus üzleti folyamatokat támogató kritikus infrastruktúra, (például IT

infrastruktúra és az abban található adatok) rendkívüli esemény bekövetkezése utáni eredeti állapotba történő helyreállítása. A helyreállítási tervek az adott kritikus szolgáltatás, erőforrás helyreállításának lépéseit tartalmazzák. A helyreállítási tervek kialakítását az érintett erőforrásgazda végzi.

A helyreállítási lépések nem szükségszerűen azonosak a helyreállítás tesztelése és a valós vészhelyzetben végrehajtott helyreállítás során. A választott helyreállítási stratégia függvényében az általános működési és helyreállítási kockázatokat csökkentendő lehetséges, hogy tesztelés, gyakorlás során csak szűkített lépéssorozat végrehajtására kerül sor, de ezt a tényt és lépéssorozatot is rögzíteni kell az egyes akciótervekben.

A helyreállítási tervek általános felépítését, tartalmi elemeit a MOB-FU-17-04-NY-04 formanyomtatvány tartalmazza.

Ezeket a hatályban lévő vagy javasolt védelmi intézkedéseket a kockázatmenedzsment rendszerben a kockázatoknál javasolt rögzíteni.

Amennyiben az üzletfolytonossági rendszer működtetését támogató informatikai rendszer bevezetésre kerül, az abban alkalmazott megoldás segítségével is rögzíteni lehet az egyes akcióterveket, ezen esetben jelen módszertan aktualizálása indokolt.

7. Az üzletfolytonosság menedzsment rendszer működtetése és karbantartása

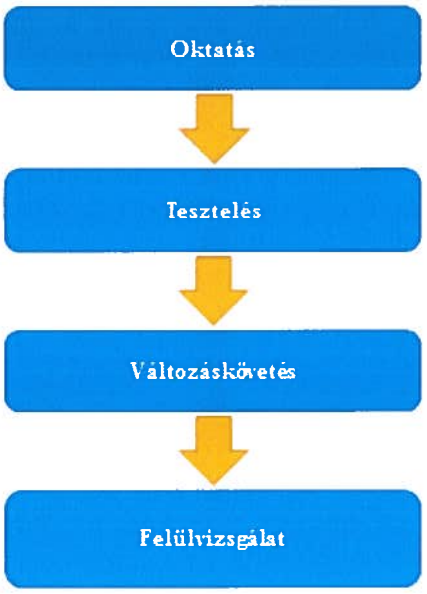
Az üzletfolytonossági rendszer megfelelő működésének és naprakészen tartásának biztosítása érdekében a Társaság a következő tevékenységeket hajtja végre:

- Az üzletfolytonossági rendszer és akciótervek oktatása;
- Az üzletfolytonossági tervek rendszeres tesztelése;
- Az üzletfolytonossági rendszert érintő változások figyelemmel kísérése, változáskövetés megvalósítása,
- Az üzletfolytonossági rendszer dokumentációjának rendszeres felülvizsgálata.

A Társaságnak oktatás keretében biztosítania kell, hogy az üzletfolytonossági rendszer működtetésében érintett munkavállalók megkapják a megfelelő információkat az üzletfolytonossági rendszerhez kapcsolódó felelősségükről, feladataikról.

A tesztelés képet ad arról, hogy az elméletben megalkotott alternatív eljárások a gyakorlatban, egy valós krízis vagy katasztrófahelyzet során mennyire alkalmazhatóak.

Az üzletfolytonossági rendszer működése dinamikus környezetben történik, ezért az üzletfolytonossági dokumentumok rendszeres felülvizsgálatáról és folyamatos karbantartásáról gondoskodni kell. Az üzletfolytonossági dokumentumok tekintetében gondoskodni kell az eseti változáskövetésről és a rendszeres időközönkénti átfogó felülvizsgálatról.



7.1. Üzletfolytonossági rendszer oktatása

Az oktatások megkezdése előtt oktatási tematikát kell készíteni az oktatás tartalmáról és ütemezéséről.

Az oktatási anyagok összeállítása és a képzések megtartása felelősségi körök szerint történik az alábbi bontásban:

- oktatás a Vezetők számára (felső- és középvezetés),
- oktatás a Végrehajtók (folyamatgazdák) számára,
- oktatás a BC/DR szakértők (akciócsoport tagok) számára.

Az üzletfolytonossági és erőforrás helyreállítási oktatás két részre különíthető el:

- általános üzletfolytonossági és erőforrás helyreállítási oktatás mindhárom célcsoport (vezetők, végrehajtók, BC/DR szakértők) részére,
- üzletfolytonossági és helyreállítási tervek gyakorlati oktatása a végrehajtók és a BC/DR szakértők számára.

Az üzletfolytonossági és erőforrás helyreállítási oktatás során első alkalommal, illetve az üzletfolytonossági rendszerben történt jelentősebb változások esetén személyes előadás keretein belül történő, tantermi oktatás preferált, míg az ismétlő oktatások, kevésbé jelentős változások kommunikálása e-learning rendszeren keresztüli oktatás vagy hírlevél, tájékoztató formájában is történhet.

Az oktatások megtörténtét arra alkalmas módon igazolni kell.

7.2. Üzletfolytonossági szabályok és tervek tesztelése

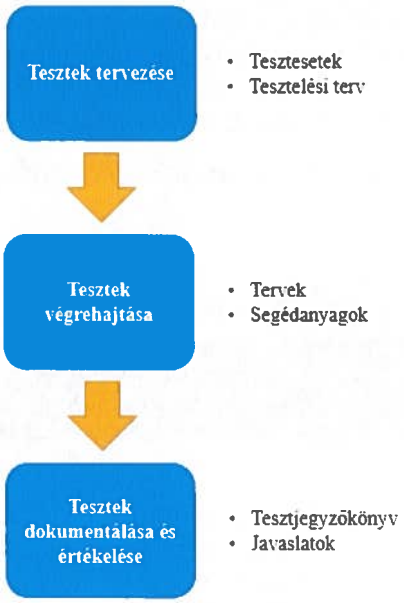
Az üzletfolytonossági tesztelés célja annak biztosítása, hogy az üzletfolytonossági tervek mindig az aktuális üzleti céloknak, üzleti folyamatoknak, az azokkal kapcsolatos tevékenységeknek és a rendelkezésre álló erőforrásoknak megfelelő intézkedéseket tartalmazzák.

A tesztelés képet ad arról, hogy az elméletben, a tervben megalkotott eljárások és lépései a gyakorlatban, egy valós rendkívüli esemény, vagy katasztrófahelyzet során mennyire alkalmazhatóak, a benne foglalt tevékenységek milyen hatékonysággal hajthatóak végre, mennyire felelnek meg az üzleti elvárásoknak, illetve a folyamatban részvevő szereplők mennyire vannak tisztában feladataikkal.

Amennyiben az üzletfolytonossági rendszer partnereket, szolgáltatókat is érint, a tesztelés során a velük való egyezmények szintén vizsgálatra kerülhetnek.

A tesztelés egyszerre szolgálja a kialakított üzletfolytonossági tervek használhatóságának vizsgálatát, illetve az érintettek ismereteinek bővítését, szerepük, felelősségük tudatosítását, az üzletmenet-folytonossággal kapcsolatban az oktatás során szerzett ismeretek frissítését.

A tesztelés végrehajtása a következő lépéseknek megfelelően történik:



7.2.1. Tesztelés tervezése

A tervek tesztelését tervezett módon kell végrehajtani, ezért a teszteket előre, dokumentált formában meg kell tervezni, a MOB-FU-17-04-NY-06 formanyomtatvány szerint.

A teszt céltűzései az alábbiak lehetnek:

- a tervek gyakorlati értékelése,
- a részletes tervekben megfogalmazott felkészülési, helyettesítési, incidenskezelési tevékenységek megfelelőségének vizsgálata,
- a tervek bármilyen hiányosságának feltárása,
- erőforrás tartalékok meglétének, tartalékolási szintjének ellenőrzése,
- értesítési, riasztási, kommunikációs megoldások működése, beleértve a kommunikációs eszközöket is,
- támogatói szerződésállomány felülvizsgálata (külső partnerekkel kötött szerződések, megállapodások elvárásoknak megfelelő alkalmazása).

A teszteket különféle típusokba lehet sorolni a bevont személyek száma, a szükséges erőforrások mennyisége és a teszt „életszerűsége" alapján:

- **Gondolati teszt:** előzetesen végig kell gondolni a végrehajtandó feladatokat, hogy kiderüljenek az esetleges hiányosságok, az előírt tevékenységek helyessége, megbízhatósága, kockázatai és erőforrásigényei. Ezt a teszttípust a legkönnyebb végrehajtani, a folyamatgazda, a folyamatszereplők és a társasági üzletfolytonossági felelős szükséges hozzá.
- **Bejárás**: a tervekben előírt technikai és üzleti feltételek (tartalékszerverek, kapcsolatok, nyomtatványok stb.) meglétének vizsgálata, általában helyszíni szemrevételezéssel.

- **Szimulációs teszt:** szimulációs tesztek segítségével minden úgy zajlik, mintha bekövetkezett volna egy tényleges rendkívüli esemény, amelynek a kiterjedése (az érintett folyamatok, erőforrások köre) a teszttervben kerül rögzítésre, azonban az erőforrások tényleges leállítása nem történik meg a teszt végrehajtása során. Célja az arról való meggyőződés, hogy adott feltételekkel az akcióterv folyamatai, illetve a helyreállítási feladatok a tervezett időn belül végrehajthatók-e.
- **Teljes megszakításos tesztelés:** az akcióterv teljes körű tesztelése minden üzleti terület és minden szükséges külső partner bevonásával. Az ilyen tesztek közelítik meg a legjobban a tényleges rendkívüli eseményt, mert a támogató erőforrások a tesztelés időtartamára ténylegesen leállításra kerülnek. Ezen teszttípus végrehajtása során a legmagasabb az üzleti folyamatokban keletkező zavar kockázata.

Bármely tesztelési típusról beszéljünk, a tesztelés eredménye tesztelési jegyzőkönyvben kerül rögzítésre.

A tesztelési típusokat az alábbi táblázat foglalja össze:

Tesztelési mód	Célok	Jellemzők	Előnyök	Hátrányok
Gondolati teszt és bejárás	Hibák feltárása és javítása, további igények összegyűjtése	Fizikailag nem végezzük el a lépéseket, csak végiggondoljuk	Gyorsan végrehajtható Nem jelent fennakadást a napi munkamenetben	Nem lehetünk biztosak benne, hogy minden hiányosságot azonosítottunk
Szimulációs tesztelés	Alternatív munkavégzés megvalósíthatós ágának kipróbálása	A tevékenységet az alternatív módon végezzük el, de nem állítjuk le az erőforrásokat	Nem okoz fennakadást a napi munkamenetben (maximum kis mértékben lassíthatja a folyamatot)	A visszaállítás nem kerül tesztelésre, mivel a fókusz az alternatív folyamaton van
Teljes megszakítás os tesztelés	Valós rendkívüli helyzet minél élethűbb megközelítése	Erőforrás tényleges leállítása és az alternatív folyamat szerinti működés	Sokkal hatékonyabban lehet azonosítani a nem-megfelelőségeket , mivel minden lépés tesztelésre kerül	A tényleges leállítás miatt fennakadás történhet a napi munkamenetben

A szimulációs és teljes megszakításos tesztelés kockázatainak csökkentése érdekében alaposan kidolgozott teszttervet kell készíteni. A tervezés során különös figyelmet kell fordítani a tesztelés típusára, illetve a teszt végrehajtásának idejére.

A teszteléseket úgy kell ütemezni (lehetőleg munkaidőn kívül), hogy azok a normál üzletmenetet a legkisebb mértékben akadályozzák.

Tesztelés szintjei

Attól függően, hogy a tesztelés hatóköre mely folyamatokra és erőforrásokra terjed ki, megkülönböztethetünk kommunikáció és értesítési lánc tesztelést, elemi, illetve integrációs tesztelést.

- **Kommunikáció, értesítési lánc tesztelése:** A kommunikációs teszt egyik célja az arról való meggyőződés, hogy a munkatársak ismerik a jelentésköteles eseményeket, azonosítani tudják az értesítendő személyeket és ismerik az elérhetőségeiket. Ezen tesztelés másik célja, hogy megállapítható legyen az értesítési lánc hatékonysága, vannak-e olyan értesítendő személyek, akik elérhetősége kevésbé valószínű, ezáltal az értesítési sorrend átalakítása lehet indokolt.
- **Elemi tesztelés:** Az elemi tesztelés célja egyetlen, adott folyamat akciótervének önmagában való működőképességének, logikai helytállóságának, tartalmi megfelelőségének ellenőrzése. Ebben az esetben a kapcsolódó folyamatok akciótervei nem kerülnek végrehajtásra, más folyamatok megszakadásának hatásait, illetve a kapcsolódó pontokat nem vizsgálják. Ebből eredően a hátránya, hogy egyszerre több folyamat megszakadása/több erőforrás kiesése esetén nem garantálható az akcióterv megfelelő működése.
- **Integrációs tesztelés:** Az integrációs tesztelés során több folyamat megszakadása/több erőforrás kiesésének hatása és akciótervének összhangja, végrehajthatósága kerül ellenőrzésre, ezáltal előnye, hogy az akciótervek közötti kapcsolat működőképessége is tesztelésre kerül. A tesztelés arra fekteti a hangsúlyt, hogy vannak-e olyan erőforrások, melyek egyszerre több alternatív folyamatot is ki kell, hogy szolgáljanak, és amennyiben igen, ez az akciótervek párhuzamos aktiválása során megfelelő kapacitással tud-e működni, valamint hogy az egyes alternatív folyamatok bemenő- és kimenő adatai megfelelő időben és minőségben rendelkezésre állnak-e az alternatív folyamatok működtetése során is.

7.2.2. Tesztelés végrehajtása

A tesztelés eredményeképpen lehetővé válik az üzletfolytonossági tervekben azonosított esetleges nem-megfelelőségek, hiányosságok javítása, a tervek finomhangolása, véglegesítése, a hatékony végrehajtás érdekében további javító intézkedések definiálása (pl. üzletfolytonossági akciótervek/erőforrás helyreállítási tervek módosítása, munkavállalók oktatása).

A tesztelésbe minden, az üzletfolytonossági tervekben felsorolt személy bevonása szükséges.

A szimulált rendkívüli esemény bekövetkezése esetén a bejelentéshez és kapcsolattartáshoz elengedhetetlen a kommunikációs lánc megfelelő alkalmazásának vizsgálata. A szimulációs tesztelés megfelelőségi kritériumai közé tartozik, hogy az értesítési elérhetőségek naprakészek, aktuálisak legyenek, valamint, hogy a vállalaton belüli és más érintett társaságok, külső felek irányába történő kommunikáció a megfelelő módon történjen. A tesztelés végrehajtása során az üzletfolytonossági tervben és a rendkívüli helyzet kezelési szabályzatban rögzített információáramlási feladatokat végre kell hajtani, kivéve, ha a tesztelési terv máshogyan rendelkezik. Elektronikus, írásbeli információáramlás esetén a levél tárgyának a ***Teszt*** elnevezést kell adni. Az elektronikus levelet a megfelelő információáramlás és a dokumentációs igény kielégítése érdekében a folyamat és erőforrásgazdának, valamint a társasági üzletfolytonossági felelősnek másolatban meg kell kapni. Telefonos, vagy személyes információátadás során tájékoztatni kell a másik felet, hogy jelenleg tesztelés történik és a közölt információk egy szimulált esetre vonatkoznak és nem valósak.

A tesztek végrehajtása attól függően, hogy közvetlenül az újonnan elkészített vagy módosított üzletfolytonossági terv kiadása előtt történik, vagy ismétlő jelleggel, a következőképpen történhet:

- **Közvetlenül az üzletfolytonossági terv kiadása előtt**: a tervek kialakítása vagy módosítása utáni első tesztek célja a terv működőképességének minél teljes körű tesztelése, a hibák, hiányosságok azonosítása, valamint a tervben érintett munkatársak gyakorlati oktatása. Az üzletfolytonossági terv csak akkor tekinthető véglegesnek, és abban az esetben kerülhet kiadásra, ha ezen teszt eredménye sikeresnek minősíthető. Az első tesztek során javasolt minden tesztelési típus megfelelő sorrendben történő végrehajtása.

- **Ismétlő jellegű, rendszeres tesztelés**: a későbbiekben, az üzletfolytonossági tervek bizonyos időszakonkénti rendszeres tesztelése történhet az érintettek előzetes értesítése nélkül. Javasolt tesztelési típus: szimulációs tesztelés (munkatársak tájékoztatásra kerülnek), teljes megszakításos tesztelés (munkatársak nem feltétlenül kerülnek tájékoztatásra).

A tesztben résztvevő munkatársak köre is változhat:

- **Csak kulcsszereplők**: közvetlenül az üzletfolytonossági tervek kiadása előtti teszt során döntés születhet arról, hogy első körben csak a kulcsszereplők teszteljék az üzletfolytonossági tervek működőképességét, a többi munkatárs pedig csak a véglegesnek tekinthető üzletfolytonossági akcióterv/erőforrás helyreállítási terv tesztelésébe kerüljön bevonásra.
- **Minden érintett munkatárs**: közvetlenül az üzletfolytonossági tervek kiadása utáni tesztek, illetve a rendszeres ismétlő jellegű tesztelés során javasolt, hogy az összes érintett személy részt vegyen a tesztelésben. Előnye, hogy több személy észrevétele, javaslata megjelenik, valamint hatékonyan alkalmazható az akciótervben leírtak gyakorlati oktatására.
- **Minden érintett munkatárs, kivéve kulcsszereplők**: a rendszeres ismétlő jellegű tesztelés során elképzelhetőek olyan tesztek, amikor a tervben érintett kulcsszereplőket kivonják a tesztelésből, annak érdekében, hogy azt vizsgálják, hogy a helyettesítést ellátó személyek hogyan hajtják végre a tervben leírtakat.

7.2.3. Tesztelés dokumentálása

A teszt eredményét a tesztelés során vezetett jegyzőkönyvek, naplók, egyéb eljárási „bizonyítások" alapján jegyzőkönyvekben kell dokumentálni.

A MOB-FU-17-04-NY-07 formanyomtatvány tartalmazza a tesztelés értékeléséhez és dokumentálásához szükségesen rögzítendő adatköröket.

A tesztelési jegyzőkönyvet jóvá kell hagyni és tájékoztatást kell adni a szabályzóban meghatározott személyek számára.

A kidolgozott üzletfolytonossági terveket a tesztelés eredményének (sikertelen vagy részben sikertelen), illetve tapasztalatainak függvényében módosítani, finomítani kell a felülvizsgálatok tanulságainak, a tapasztalt hiányok, eltérések ismeretében.

A végrehajtott teszt értékelése során tapasztalt eltérések, eredmények ismeretében, a jegyzőkönyvben fel kell tüntetni a feltárt hiányosságok pótlásáról, fejlesztésről szóló javaslatokat is.

7.3. Üzletfolytonossági rendszer felülvizsgálata

7.3.1. Üzletfolytonossági rendszer eseti felülvizsgálat

A Társaság működésében történő változások indukálhatják az üzletfolytonossági dokumentumok felülvizsgálatát. Az alábbi esetekben célszerű az üzletfolytonossági dokumentumokat eseti jelleggel felül kell vizsgálni:

- szervezeti működési folyamatok változása,
- új informatikai fejlesztések, bevezetések,
- szervezeti változások
- új kiszervezett tevékenységek, külső szolgáltatók
- Társaság működési folyamatát érintő, vagy tágabb működési környezetben rendkívüli esemény bekövetkezése.

A szabályzóban megjelölt személyek feladata és felelőssége annak ellenőrzése, vizsgálata, hogy szabályozási, szervezeti, munkaköri, személyi változások, erőforrás fejlesztések a szakterületükbe tartozó üzletfolytonossági terv-dokumentumokban okoznak e változást, azokat érintik-e. A változáskövetés eredményének megfelelően szükség esetén az üzletfolytonossági dokumentumokat módosítani kell. A változáskövetéssel kapcsolatban a szükséges módosítások megtétele a szabályzóban meghatározott személyek felelősségi körébe tartozik.

A felülvizsgálatról, változáskövetésről dokumentációt kell készíteni.

7.3.2. Üzletfolytonossági rendszer rendszeres felülvizsgálata

Az üzletfolytonossági dokumentumokat (folyamatelemzési, hatáselemzési, kockázatelemzési, tervezési dokumentumok) rendszeres időközönként átfogó felülvizsgálatnak kell alávetni a szabályzóban meghatározott időszakok szerint és felelősségi kör mentén.

A rendszeres, átfogó felülvizsgálat során ajánlott a lényegi dokumentációk áttekintését (pl. szabályzatok, üzleti hatáselemzések ismételt interjúkkal, tervek) felülvizsgálni.

A felülvizsgálat eredményének megfelelően szükség esetén az üzletfolytonossági dokumentumokat módosítani kell. A felülvizsgálattal kapcsolatban a szükséges módosítások megtétele a szabályzóban meghatározott személyek felelősségébe tartozik.

A folyamatgazda feladata és felelőssége annak ellenőrzése és vizsgálata, hogy szabályozási, szervezeti, munkaköri, személyi változások, erőforrás fejlesztések a hozzá tartozó dokumentumokban okoznak-e változást, azokat érintik-e, illetve magának a felülvizsgálatnak az elvégzése is az ő feladata.

A felülvizsgálatról, változáskövetésről dokumentációt kell készíteni.

RENDKÍVÜLI HELYZETKEZELÉSI RENDSZER SZEREPLŐI ÉS FELADATAI

Jelen dokumentum kivonatolja a rendkívüli helyzetkezelési rendszer szereplőit és feladatait.

1. Társaság Ügyvezetői

Feladatai felkészülési időszakban:

- Erőforrások és menedzsment szintű támogatás biztosítása.
- Döntés az üzletfolytonossági felmérési terv jóváhagyásáról.
- Döntés a társaság kritikus folyamat listájának jóváhagyásáról.
- Döntés a feltárt kockázatok kezeléséről, az alkalmazott kockázatkezelési stratégiáról, a védelmi intézkedések bevezetéséről és alkalmazásáról, a maradványkockázatok elfogadásáról.
- Döntés a tesztelés eredménye alapján javasolt védelmi intézkedési listáról.
- Döntés a társasági éves értékelő jelentés jóváhagyásáról.
- Döntés a társasági REVIR ügyeletesek havi beosztásának jóváhagyásáról.

Feladatai rendkívüli esemény kezelése esetén:

- Erőforrások és menedzsment szintű támogatás biztosítása.
- Döntés az EDR rendszeren keresztüli kommunikációról.
- Döntés a Társasági Krízis Team összehívásáról.
- Társasági Krízis Team összehívásának hiányában, a legmagasabb szintű döntések meghozatala a váratlan események kezelése kapcsán, melyek lehetnek (nem teljeskörű felsorolás):
    - Döntés a rendkívüli minősítésű időszak elrendeléséről.
    - Döntés a rendkívüli helyzetkezelési tervek alkalmazásáról.
    - Döntés a normál működési rendre való visszaállásról.
    - Döntés a rendkívüli minősítésű időszak lezárásáról.
- A rendkívüli helyzetkezelési tervek végrehajtásának koordinálása.
- Döntés a társasági rendkívüli esemény kezelési jegyzőkönyv jóváhagyásáról.
- Javasolhatja a Csoportszintű Krízis Team összehívását.

2. Társasági biztonsági funkcióért felelős vezető

Feladatai felkészülési időszakban:

- Erőforrások és menedzsment szintű támogatás biztosítása.
- A Társaság Ügyvezetői részére szakmai támogatás és javaslatok tétele rendkívüli helyzetkezelési ügyekben.

- A társasági rendkívüli helyzetkezelési rendszer kialakításának, fejlesztésének szakmai támogatása, felső szintű koordinálása.

Feladatai rendkívüli esemény kezelése esetén:

- Javasolhatja a Társasági Krízis Team összehívását.

3. Társasági Krízis Team

Feladatai felkészülési időszakban:

-

A Krízis szinttől függő társasági vagy csoportszintű feladatai rendkívüli esemény kezelése esetén:

- Döntés a rendkívüli helyzetkezelés irányításának átvételéről, koordinálásáról. (Ebben az esetben a Társasági Krízis Team a rendkívüli helyzetkezelés során az elsőszámú döntéshozó és irányító szervezet.) A legmagasabb szintű döntések a váratlan események kezelése kapcsán lehetnek (nem teljeskörű felsorolás):
    - Döntés a rendkívüli minősítésű időszak elrendeléséről.
    - Döntés a rendkívüli helyzetkezelési tervek alkalmazásáról.
    - Döntés a normál működési rendre való visszaállásról.
    - Döntés a rendkívüli minősítésű időszak lezárásáról.
- Döntés a rendkívüli helyzetkezelés irányításának átadásáról a Csoportszintű Krízis Team, részére, valamint a kezelés további támogatása.

4. Társasági REVIR ügyeletes

Feladatai felkészülési időszakban:

-

Feladatai rendkívüli esemény kezelése esetén:

- Gondoskodik a REVIR jelentésköteles események fogadásáról, rögzítéséről, naplózásáról.
- A REVIR jelentésköteles eseményekkel kapcsolatos információkat és tájékoztatást eljuttatja a REVIR Központi ügyelet részére.

5. Társasági üzletfolytonossági felelős

Feladatai felkészülési időszakban:

- Rendkívüli helyzetkezelés társasági és központi szabályozásának kialakítása.
- Rendkívüli helyzetkezelés szervezeti hátterének kialakítása.
- Rendkívüli helyzetkezelés szabályozásának felülvizsgálata.
- Döntés a rendkívüli helyzetkezelési rendszer általános és speciális ismereteire vonatkozó oktatás, tematika, tananyag jóváhagyásáról.

- Üzletfolytonossági felmérés megtervezése.
- Üzletfolytonossági folyamatfelmérés, erőforrás- és folyamatfüggések vizsgálatának koordinációja, társasági szintű összesítése.
- Üzleti hatáselemzések koordinációja, társasági szintű összesítése.
- Üzletfolytonossági kockázatok azonosítás, rögzítés és elemzés koordinációja, társasági szintű összesítése.
- Döntés a közepesen kritikus folyamatok kockázatelemzésének elvégzéséről.
- Egyes kockázatokhoz kapcsolódó javasolt kockázatkezelés, javasolt stratégia és javasolt kockázatkezelő védelmi intézkedések kidolgozásának koordinációja.
- Felterjesztés készítése a kockázatkezelésről a Stratégiai Bizottság részére. Üzletfolytonossági tervek kidolgozásának és védelmi intézkedések végrehajtásának koordinációja, társasági szintű összesítése.
- Értesítési lista kidolgozása.
- Rendkívüli helyzetkezelési rendszer általános ismereteire vonatkozó oktatás szervezése, tematika és tananyag készítése.
- Üzletfolytonossági és helyreállítási tervek tesztelési tervezésének, végrehajtásának, dokumentálásának koordinációja, társasági szintű összesítése.
- Felterjesztés készítése a tesztelés alapján készített javasolt védelmi intézkedési listáról a Stratégiai Bizottság részére.
- Csoportszintű tesztelés esetén összefoglaló jelentés készítése.
- Üzletfolytonossági és helyreállítási tervek felülvizsgálatának koordinációja.
- Társasági rendkívüli helyzetkezelési rendszer állapotáról szóló éves jelentés elkészítése.

Feladatai rendkívüli esemény kezelése esetén:

- Társasági rendkívüli esemény kezelési jegyzőkönyv elkészítése.
- Csoportszintű rendkívüli esemény kezelési jegyzőkönyv elkészítése.

6. Folyamatgazda

Feladatai felkészülési időszakban:

- Üzletfolytonossági folyamatfelmérés, és kapcsolódó erőforrás- és folyamatfüggések vizsgálata.
- Üzleti hatáselemzés elvégzése.
- Üzletfolytonossági kockázatok azonosítása, rögzítése és elemzése.
- Egyes kockázatokhoz kapcsolódó javasolt kockázatkezelés, javasolt stratégia és javasolt kockázatkezelő védelmi intézkedések kidolgozása.
- Maradványkockázatok számítása.
- Üzletfolytonossági tervek kidolgozása és védelmi intézkedések végrehajtása
- Rendkívüli helyzetkezelési rendszer speciális ismereteire vonatkozó oktatás szervezése, tematika és tananyag készítése.
- Üzletfolytonossági tesztelési terv elkészítése, végrehajtása, a tesztelés dokumentálása.
- Tesztelés eredménye alapján javasolt védelmi intézkedési lista készítése, a jóváhagyott lista megvalósítása.

- Üzletfolytonossági tervek felülvizsgálata.

Feladatai rendkívüli esemény kezelése esetén:

- Döntés-előkészítő információk gyűjtése és elemzése.
- Dominóhatás érvényesülésének vizsgálata (ellenőrzi, hogy adott folyamat kiesése, káresemény érint-e más társaságot), társasági REVIR ügyeletes haladéktalan értesítése dominóhatás fennállásáról.
- Rendkívüli helyzetkezelési tervek végrehajtását követő ellenőrzés, normál üzletmenetre történő visszaállás befejezésének jelzése a rendkívüli helyzetkezelésében résztvevők felé, emellett dokumentációs és utógondozási feladatok ellátása.

7. Erőforrásgazda

Feladatai felkészülési időszakban:

- Egyes kockázatokhoz kapcsolódó javasolt kockázatkezelés, javasolt stratégia és javasolt kockázatkezelő védelmi intézkedések kidolgozása.
- Helyreállítási tervek kidolgozása
- Rendkívüli helyzetkezelési rendszer speciális ismereteire vonatkozó oktatás szervezése, tematika és tananyag készítése.
- Helyreállítási tesztelési terv elkészítése, végrehajtása, a tesztelés dokumentálása.
- Tesztelés eredménye alapján javasolt védelmi intézkedési lista készítése, a jóváhagyott lista megvalósítása.
- Helyreállítási tervek felülvizsgálata.

Feladatai rendkívüli esemény kezelése esetén:

- Erőforrás helyreállítási/helyettesítési terv végrehajtását követő ellenőrzés, annak eredményéről a rendkívüli helyzetkezelésében résztvevők értesítése, emellett dokumentációs és utógondozási feladatok ellátása.

8. Folyamatszponzor

Feladatai felkészülési időszakban:

- A hozzá tartozó folyamatok erőforrás és vezetői szintű támogatásának biztosítása.
- Döntés a folyamat kritikussá minősítésének jóváhagyásáról.

9. Stratégiai Bizottság

Feladatai felkészülési időszakban:

-

10. Munkavállalók

Feladatai felkészülési időszakban:

- Részt vesz a megfelelő rendkívüli helyzetkezelési terv oktatásán, amennyiben érintett benne.
- Részt vesz a megfelelő rendkívüli helyzetkezelési terv tesztelésén, amennyiben érintett benne.
- Megismeri és megérti a rendszerben, a tervekben betöltött saját szerepét, feladatait, az ehhez szükséges információkat és kompetenciákat elsajátítja.
- Javaslatot tenni a rendszer vagy tervek fejlesztésére, javítására.
- Jelenteni az új kockázatokat.

Feladatai rendkívüli esemény kezelése esetén:

- Rendkívüli események észlelése esetén azonnali élet- és vagyonmentés megkezdése, és az elsődleges feladatok biztosítása, figyelemmel az érvényben lévő biztonsági, tűz-, munka- és balesetvédelmi előírásokra.
- Rendkívüli esemény jelentése a felettesnek és a REVIR Központi Ügyeletnek.
- Rendkívüli helyzetkezelési tervek életbe léptetését követően a vonatkozó feladatok tervszerű végrehajtása, a tervek végrehajtását koordináló vezetők folyamatos tájékoztatása, megtett intézkedések dokumentálása.

DÖNTÉS HATÁSKÖRI LISTA

Azonosító	Döntési hatáskör meghatározása	MVM Zrt. Szervezeti egységek vezetői					MVM Mobiliti Kft.					
		Vezérigazgató (VIG)	Csoportszintű Biztonsági Igazgató	Fizikai- és Humánbiztonsági	Információbiztonsági és Kríziskezelési	Megjegyzés	Ügyvezetés	Társasági üzletfolytonossági felelős	Társasági információbiztonsági felelős	Megjegyzés	Kapcsolódó központi DHL sor azonosítója	Kapcsolódó központi szabályozó azonosítója
MOB-BSz-17-D-01	Döntés a kockázatkezelési módszertanon alapuló kockázatkezelési feladatok végrehajtása kapcsán a nem a módszertanban meghatározott támogató IT eszköz azaz más szoftveres támogatás igénybevételéről.								D			
MOB-BSz-17-D-02	Döntés a kockázatok kezeléséről, javasolt védelmi intézkedések bevezetéséről, alkalmazásáról.								D			
MOB-BSz-17-D-03	Döntés a védelmi intézkedések bevezetésének ütemtervéről.								D			
MOB-BSz-17-D-04	Döntés a társasági információbiztonsági felelős és üzletfolytonossági felelős kinevezése ügyében.		EJ				D				KIE-17-1-D-02	KIE-17
MOB-BSz-17-D-05	Döntés az eltérő alapjogosultsági igénylésről.								D			
MOB-BSz-17-D-06	Döntés a jogosultság felfüggesztésének mellőzéséről.								D			
MOB-BSz-17-D-07	Döntés azonnali üzenetküldő alkalmazás kapcsán a külső felek felvételéről az IT szolgáltató által biztosított csevegő alkalmazás használata során.								D			
MOB-BSz-17-D-08	Döntés a társasági REVIR ügyeletes beosztásának ügyében.								D			
MOB-BSz-17-D-09	Döntés az üzletfolytonossági felmérési terv jóváhagyásáról.						D					
MOB-BSz-17-D-10	Döntés a kritikus folyamat lista jóváhagyásáról.						D					
MOB-BSz-17-D-11	Döntés a feltárt kockázatok kezeléséről, az alkalmazott kockázatkezelési stratégiáról, a védelmi intézkedések bevezetéséről és alkalmazásáról, a maradványkockázatok elfogadásáról.						D					
MOB-BSz-17-D-12	Döntés a rendkívüli helyzetkezelési rendszer általános és speciális ismereteire vonatkozó oktatás, tematika, tananyag jóváhagyásáról.							D				
MOB-BSz-17-D-13	Döntés a tesztelés eredménye alapján javasolt védelmi intézkedési listáról.								D			
MOB-BSz-17-D-14	Döntés a Társaság éves értékelő jelentésének jóváhagyásáról.						D					
MOB-BSz-17-D-15	Döntés a Társasági Krízis Team összehívásáról.								D			
MOB-BSz-17-D-16	Döntés a rendkívüli helyzetkezelés irányításának átvételéről, koordinálásáról.								D			
MOB-BSz-17-D-17	Döntés a rendkívüli helyzetkezelés irányításában csoportszintű eseménynél.	EJ							D		KIE-17-1-D-01	KIE-17
MOB-BSz-17-D-18	Döntés a rendkívüli minősítésű időszak elrendeléséről.								D			
MOB-BSz-17-D-19	Döntés a rendkívüli helyzetkezelési tervek alkalmazásáról.								D			
MOB-BSz-17-D-20	Döntés a normál működési rendre való visszaállásról.								D			
MOB-BSz-17-D-21	Döntés a rendkívüli minősítésű időszak lezárásáról.								D			
MOB-BSz-17-D-22	Döntés a társasági rendkívüli esemény kezelési jegyzőkönyv jóváhagyásáról.								D			
MOB-BSz-17-D-23	Döntés az alternatív telephely kialakításáról.						D					
MOB-BSz-17-D-24	Döntés a Krízis Központ kialakításáról.						D					
MOB-BSz-17-D-25	Döntés az auditterv jóváhagyásáról.								D			
MOB-BSz-17-D-26	Döntés a társaságok ügyviteli informatikai rendszerének sérülékenységi vizsgálatáról.		EJ						D		KIE-17-1-D-03	KIE-17
MOB-BSz-17-D-27	Döntés a társaságok üzemviteli rendszerének sérülékenységi vizsgálatáról.		EJ						D		KIE-17-1-D-04	KIE-17

ELEKTRONIKUS LEVELEZÉS HASZNÁLATÁNAK SZABÁLYAI ÉS TUDOMÁSUL VÉTELI NYILATKOZAT (KÜLSŐ FÉL RÉSZÉRE)

Társaság neve: .....
Társaság címe: .....
Társaság cégjegyzékszáma: .....

A Társaság tulajdonában álló (.....@mobiliti.hu) e-mail cím használatára jogosult azon felhasználó, aki

- A Társaság **állandó munkavállalója**.
- A Társasággal **szerződéses kapcsolatban álló külső munkavállaló**, vagy partner vállalat alkalmazottja, és a Társaságnál futó projekt indokolttá teszi a belső e-mail cím használatát, valamint ehhez a társasági információbiztonsági felelős hozzájárult.
- A Társasággal **szerződéses kapcsolatban nem álló külső partner, akinek tevékenysége indokolttá teszi a belsős cím használatát**, valamint ehhez a társasági információbiztonsági felelős hozzájárult, valamint jelen nyilatkozatot elfogadta, és az abban foglaltak tudomásulvételét aláírásával igazolta.

Az elektronikus levelezés (e-mail) használat szabályai a Társaság tulajdonában álló e-mail címekre vonatkozóan az alábbiak:

- A felhasználói fiók jelszavát a következők szerint kell képezni:
  - A jelszó nem lehet 8 karakternél rövidebb;
  - Tartalmaznia kell legalább egy kisbetűt, egy nagybetűt, egy számjegyet és/vagy speciális alfanumerikus karaktert (@, &, #, stb.);
  - Nem tartalmazhat utalást, részletet a felhasználónévre;
  - A jelszavakat 90 naponként meg kell változtatni;
  - A felhasználót 14 nappal a jelszó lejárat előtt a rendszer figyelmezteti a megújításra;
  - A változtatás után az új jelszót egy napig nem lehet megváltoztatni;
  - A rendszer a legutolsó 12 beállított jelszót tartja nyilván, melyeket a változtatáskor nem lehet újra beállítani;
  - A rendszer 15 próbálkozást enged a jelszó helyes bevitelére, majd 120 percre elérhetetlenné válik (átmenetileg zárolódik) a felhasználó
  - **A nem megfelelő jelszóválasztásból adódó esetleges visszaélésekért a felhasználó felelősségre vonható!**
- A rendszer a törölt elemeket 14 napig tárolja, utána véglegesen törlődnek a levelező rendszerből.
- Egy levélben a címzettek száma nem haladhatja meg a 250 darabot.
- A felhasználóknak lehetőségük van a levelezési szolgáltatás távoli, vállalaton kívüli elérésére is. Internet kapcsolaton keresztül a következő címen érhető el az Outlook Web Access (OWA) szolgáltatás:

  https://mail.mvm-informatika.hu/owa

  A megjelenő oldalon a vállalaton belül használt bejelentkezési tartomány\felhasználónév (pl.: MVMH\E0000) és jelszó megadása után lehet belépni a webes megjelenítésű levelező felületre.
  A levelezés ilyen módon történő eléréséhez VPN kapcsolat nem szükséges, ezért a felhasználó felelőssége, hogy gondoskodjon a következőkről:
  - Megfelelő erősségű jelszó választása és kezelése
  - Felügyelet nélkül hagyott munkaállomás zárolása/kikapcsolása, melyen az érintett e-mail cím beállításra kerül

  - OWA-ból való kijelentkezés munkavégzést követően
  - Jelszó mentésének tiltása OWA felületen
  - Megbízható, biztonságos internetkapcsolat alkalmazása
  - Adathalászatra és hasonló fenyegetésekre fordított fokozott figyelem.
- TILOS a lánclevelezés, a kéretlen levelek (spam), valamint az indokolatlan mértékű magáncélú tartalmak küldése.
- Csatolt állományként nem küldhetők:
  - futtatható állományok (pl. *.exe;*.bin; *bat; *.com; *.app; *.vb; *.vbs; *.js; *jar; *.ill; *.dll; *.dat fájltípusok);
  - hibásan tömörített fájlok;
  - nagyméretű nem tömörített fájlok.

  A rendszer a fentiekben felsorolt csatolmánnyal rendelkező leveleket csatolmány nélkül küldi el a címzett(ek)nek.
- Ajánlott a nagyméretű fájlokat tömöríteni (7ZIP használata támogatott), és levél csatolmányaként elküldeni.
- Bizalmas, érzékeny adatokat, információkat jelszóval védett tömörített állományban kell küldeni szervezeten kívülre, a 7ZIP program segítségével a levél csatolmányaként elektronikus levélben. A titkosítani kívánt csatolmányok jelszavas tömörítésekor javasolt a minél „erősebb" (min. 8 karakter hosszú, vegyes nagy- és kisbetű, szám, esetleg speciális karakterek alkalmazása) jelszó használata. A fogadó féllel (a levél címzettjével) a dekódoláshoz szükséges kulcs valamely más kommunikációs csatornán (pl. telefonon, szóban, SMS-ben vagy személyesen előre megállapodva) kerüljön megosztásra. Soha ne küldjük el ugyanabban a levélben a jelszót, mint amelyben a titkosított információ szerepel!
- „Üzleti Titok!" minősítésű dokumentum elektronikus úton nem továbbítható.
- Ismeretlen feladótól érkezett csatolmányok, linkek megnyitása esetén a társasági információbiztonsági felelőshöz vagy a Helpdesk-hez kell fordulni. További, a kérdéses file és weboldal vírusmentességének ellenőrzésére a www.virustotal.com weboldal ad lehetőséget. (A vizsgálathoz a csatolmányt megnyitás nélkül szükséges egy könyvtárba menteni, majd a Virustotal oldalán megadni az ellenőrizendő fájlt, illetve linket.)
- A felhasználó az elektronikus levelező rendszer használatával tudomásul veszi, hogy az általa használt @mobiliti.hu végződésű e-mail cím a Társaság tulajdona. Kötelezettséget vállal arra vonatkozóan, hogy azt kizárólag a Társaság érdekében végzett munkavégzéshez használja fel. Tudomásul veszi és hozzájárulását adja, hogy a Társaság által biztosított e-mail címet, illetve az annak használata során továbbított adatokat a Társaság meghatalmazottja ellenőrizze, valamint, hogy a munkavégzése során keletkezett elektronikus anyagok és a postafiók egész tartalma a Társaság tulajdonát képezik.

Alulírott .....

(születési hely: ..... , születési idő: ..... ,

anyja neve: ..... , személyi igazolvány száma: .....)

jelen nyilatkozat aláírásával kijelentem, hogy a fent rögzített előírásokat tudomásul vettem és a Társaság tulajdonát képező e-mail címem használata során betartom.

Kelt: ....., ...év .....hó ..... nap

.....

(név)

TÁRSASÁGI INCIDENS RIPORT AZ MVM ZRT. CSOPORTSZINTŰ BIZTONSÁGI IGAZGATÓSÁGA RÉSZÉRE ADOTT IDŐSZAKRA VONATKOZÓAN

A TÁRSASÁG ALAPADATAI	
Társaság neve	
Társaság biztonsági besorolása	
Információbiztonsági felelős neve	
Információbiztonsági felelős beosztása	
Információbiztonsági felelős szervezeti egysége	
Vizsgált időszak	

A VIZSGÁLT IDŐSZAKBAN TÖRTÉNT BIZTONSÁGI INCIDENSEK					
Incidens rövid leírása (érintett eszköz, esemény)	**Bekövetkezés időpontja**	**Elhárítás rövid leírása**	**Elhárításra fordított idő (óra)**	**Kárkövetkezmény, okozott hatás leírása**	**Javaslatok**

TÁRSASÁGI MEGJEGYZÉSEK

HOZZÁJÁRULÁSI NYILATKOZAT SÉRÜLÉKENYSÉG VIZSGÁLAT VÉGREHAJTÁSÁHOZ

Alulírott ..... [név], mint a(z) .....
.....
[társaság neve, címe, cégjegyzékszáma] képviseletében hozzájárulok ahhoz, hogy a(z)
.....
[a vizsgálatot végrehajtó társaság neve] munkatársai a(z) .....
[a tesztelni kívánt alkalmazás, szolgáltatás megnevezése] rendszeren sérülékenység vizsgálatot hajtsanak végre az alábbi eszközök és módszerek alkalmazásával:

- ..... [a sérülékenység vizsgálathoz használt eszközök megnevezése]
- ..... [a sérülékenység vizsgálathoz használt eszközök megnevezése]
- ..... [a sérülékenység vizsgálathoz használt eszközök megnevezése]

A sérülékenység vizsgálat végrehajtásához szükséges feladatokat a(z) ..... [felügyeletet ellátó társaság] által a kapcsolódó szerződésben rögzített feltételek betartásával és felügyelete mellett lehetséges végrehajtani.

Jelen nyilatkozattal elismerem, hogy a sérülékenység vizsgálat végrehajtása a tesztelni kívánt rendszer esetleges gyengeségeinek felderítésére irányul, így az elvégzése nem tartozik a számítógépes bűncselekmény kategóriájába.

A hozzájárulás a vizsgálatok lezárásig tartó, szerződésben rögzített időszakra vonatkozik.

A vizsgálatot végző társaság munkatársai a szakmailag elvárható legnagyobb gondossággal, óvatossággal kötelesek eljárni, hogy a rendszerben fennakadást, kárt ne okozzanak.

Az üzemeltetők elfogadják, hogy a legnagyobb gondosság mellett is előfordulhatnak üzemzavarok, ezért a szükséges előfeltételeket megteremtik (Pl. biztonsági mentés a rendszerben tárolt adatokról).

Az üzemeltetők biztosítják, hogy az egyeztetett időpontokban technikai módszerekkel szándékosan nem akadályozzák a vizsgálatok elvégzését.

Jelen Hozzájárulási nyilatkozat hatálya kizárólag a fent megnevezett rendszer sérülékenység vizsgálatára vonatkozik, az előzetesen egyeztetett előfeltételek biztosítása mellett.

Amennyiben a(z) ..... [társaság neve] a sérülékenység vizsgálatban vizsgált IT szolgáltatásokat hosting szolgáltató erőforrásaira alapozva működteti, akkor a(z) ..... [társaság neve] feladata a hosting szolgáltatóval való mindennemű kapcsolattartás, egyeztetés, esetlegesen szükséges jóváhagyás beszerzése is.

A vizsgálatot végrehajtó társaság szakértői kötelesek a vizsgálat megkezdése előtt a futtatáshoz szükséges feltételeket rögzíteni és a vizsgálat végrehajtását a delegált, MVM csoportba tartozó társaságokkal, illetve szakterületekkel egyeztetett időpontban, azok felügyelete mellett elvégezni.

Kelt: ....., ...év .....hó ..... nap

.....	.....
.....	.....
társasági szabályzatban meghatározott vezető neve és beosztása	**társasági szabályzatban meghatározott vezető neve és beosztása**