MVM MÁTRA GÉP Kft.
MGEP-SZ2021/79

INFORMÁCIÓBIZTONSÁGI ÉS INFOKOMMUNIKÁCIÓS SZABÁLYZAT

A szabályzat előírásai megfelelnek az alábbi központi szabályozó dokumentumoknak, illetve tulajdonosi előírásoknak:

- 2026. április 29-én kiadott	KIE-20 Az MVM Csoport infokommunikációs központi irányelve
- 2025. június 26-án kiadott	KIE-17 Az MVM Csoport információbiztonsági és rendkívüli helyzetkezelési központi irányelve
- 2026. április 29-én kiadott	KER-20-01-02-03-04-05 Az MVM Csoport központi eljárásrendjei
- 2024. december 13-án kiadott	KER-17-02-03 Az MVM Csoport központi eljárásrendjei

Készítette: Információbiztonsági felelős

A szabályzatot jóváhagyom, alkalmazását 2026. június 19-től elrendelem.

Fonyódi Ákos
ügyvezető

1. TARTALOMJEGYZÉK

2. A szabályozás célja

Jelen szabályzat funkcionális célja az MVM Mátra Gép Kft.-nél (a továbbiakban: Társaság):

- egységes szemléletben meghatározni a felhasználók és az információtechnológiai rendszerek viszonyát az informatikai rendszerek által kezelt adatok, információk bizalmasságának, sértetlenségének, rendelkezésre állásának megőrzése érdekében;
- a Társaság ügyviteli működési környezetébe kerülő, illetve ott keletkező adatok, információk informatikai rendszere(ke)n történő adatfeldolgozásával szemben támasztott biztonsági követelmények rögzítése;
- az informatikai, valamint kommunikációs berendezések (hardver) és alkalmazott rendszerek (szoftver) biztonságának elősegítése;
- a felhasználók által a számítástechnikai eszközök, hálózatok, rendszerek, szoftverek és az internet felhasználása során alkalmazandó biztonsági követelményrendszer meghatározása,
- azon alapvető biztonsági normák és működési keretek meghatározása, amelyek érvényesítésével a Társaság az elfogadható minimumra csökkentheti az információkezelés nem kívánt (működésre negatív hatást kifejtő) következményeit;
- az adatbiztonsággal kapcsolatos szerepek, feladat- és felelősségi körök rögzítése;
- meghatározni az informatikai és ügyviteli célú elektronikus hírközlés, digitalizáció és üzleti intelligencia funkció egységes keretrendszerét, az annak kialakításához, hatékony működtetéséhez, ellenőrzéséhez, fejlesztéséhez szükséges elvárásokat és követelményeket.

A jelen szabályzat rendelkezéseit minden üzemszerűen használt ügyviteli rendszer és munkafolyamat esetében teljeskörűen, a releváns kockázatokkal arányos módon szükséges alkalmazni.

3. A szabályzat hatálya

3.1. Időbeli hatály

Jelen szabályzat jóváhagyásától hatályon kívül helyezésig alkalmazandó. Jelen szabályzat mellékletei a szabályzat egységes, elválaszthatatlan részét képezik.

3.2. Személyi hatály

A jelen szabályzat személyi hatálya kiterjed:

- a Társaság valamennyi szervezeti egységére és munkavállalójára, akik informatikai és/vagy telekommunikációs eszközt használnak;
- a Társaság által igénybe vett ügyviteli informatikai rendszerekkel, szolgáltatásokkal összefüggésben, a Társasággal szerződéses jogviszonyba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (a továbbiakban: külső személy), a velük kötött szerződésben, illetve a titoktartási nyilatkozatban rögzített mértékben;
- a Társaság által igénybe vett IT rendszereket használó, a rendszerekhez és alkalmazásokhoz bármilyen hozzáféréssel rendelkező természetes vagy jogi személyre, a velük kötött szerződésben, illetve a titoktartási nyilatkozatban rögzített mértékben.

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

3.3. Tárgyi hatály

A jelen szabályzat hatálya kiterjed a Társaság tulajdonában vagy használatában lévő informatikai rendszerekben előforduló adatokra, információkra, a Társaság tulajdonában vagy használatában lévő informatikai rendszerek teljes életciklusára (tervezés, fejlesztés, beszerzés, bevezetés, üzemeltetés, kivonás), valamint az informatikai és az elektronikus hírközlés, digitalizáció keretszabályaira.

4. Kapcsolódó főbb szabályzatok, hivatkozások

A jelen szabályzatban foglaltak a mindenkor hatályos jogszabályokban rögzítettekkel összhangban, azzal együttesen alkalmazandók.

- 1992. évi LXVI törvény a polgárok személyes adatainak nyilvántartásáról
- 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról
- 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
- 346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról
- 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/GDPR; hatályos: 2016.04.27-tól)

A jelen szabályzat összhangban van a KIE-17 és KIE-20 MVM Csoport információbiztonsági és rendkívüli helyzetkezelési (a továbbiakban: KIE-17), valamint infokommunikációs (a továbbiakban: KIE-20) központi irányelveivel.

5. Fogalmak, meghatározások

A jelen szabályzat fogalommeghatározásait az 1. sz. melléklet tartalmazza.

6. A szabályzat tárgya, tartalma

6.1. Az informatikai, információbiztonsági rendszer

Jelen szabályzat egységes rendszerbe foglalja a Társaság információtechnológiai biztonsági, információbiztonsági tevékenységeit, feladatait, továbbá kialakítja a Társaságban az ilyen irányú tevékenységeinek monitoring és koordinatív funkcióját, képessé téve így a Társaságot az IT biztonságot és üzletmenet folytonosságot fenyegető veszélyekkel szembeni szervezett védekezésre.

Az információbiztonsággal kapcsolatos általános követelmények elemeit jelen szabályzat 2. sz. melléklete tartalmazza.

6.1.1. Az informatikai, információbiztonsági biztonsági rendszer célja és kialakítása

A Társaság információbiztonsági rendszert köteles működtetni, melynek célja a Társaság által használt információk és információs rendszerek azonosítása, azok információbiztonsági kockázatainak felmérése, kockázatarányos védelmi intézkedések bevezetése és folyamatok kialakítása, valamint azok hatékony menedzsmentje.

6.1.2. Az információbiztonsági rendszer szabályzati környezete

Az információbiztonsági rendszer működtetésének alapja a megfelelően kialakított szabályozási környezet. Az MVM Csoporton belül az információbiztonság egységes és egyenszilárdságú kezelése érdekében jelen szabályzat információbiztonsági előírásai kötelezően betartandó követelményeket jelentenek a Társaságra nézve.

6.2. A Társaság besorolása információbiztonsági kategóriákba

Az MVM Csoportba tartozó társaságokat információbiztonsági szempontból információbiztonsági kategóriákba kell sorolni. A Társaság információbiztonsági kategóriákba történő besorolása a társasági információbiztonsági felelős által történik. A Társaság besorolását évente felül kell vizsgálni. A társasági információbiztonsági felelős által kitöltött és aláírt, a „Társasági besoroló kérdőív információbiztonsági kategóriákba” tárgyú kérdőívet minden év január 31-ig meg kell küldeni az MVM Zrt. Csoportszintű biztonsági igazgatóság kijelölt kapcsolattartója részére. A kérdőív mintáját a jelen szabályzat 1. sz. formanyomtatványa tartalmazza.

A Társaságnak a saját kategóriájának megfelelő információbiztonsági intézkedéseket kell megvalósítania a KIE-17 és KIE-20 alapján megfogalmazott ajánlásban rögzítettek szerint. Opcionális jelleggel a Társaságnak bármikor lehetősége van az adott információbiztonsági kategóriától való magasabb szintű eltérésre, felső vezetői jóváhagyás mellett. Az ajánlásban előírtnál alacsonyabb információbiztonsági szint irányába viszont indokolt esetben az MVM Zrt. információbiztonsági és kríziskezelési osztályvezető előzetes jóváhagyását követően az MVM Zrt. csoportszintű biztonsági igazgatójának külön engedélye alapján lehet eljárni.

6.3. Az információbiztonság szervezete

Az információbiztonsági, IT biztonsági követelmények teljesítéséhez, az előírt kontrollok megvalósításához és karbantartásához elengedhetetlen a felelős szereplők mind csoportszinten, mind társasági szinten történő kijelölésére, valamint feladataik és felelősségük meghatározásra kerülnek. A kijelölt felelősök munkaköri leírása tartalmazza a betöltött szerepkörükkel kapcsolatos feladatokat. A kijelölt felelősnek rendelkeznie kell helyettessel, aki távolléte, illetve elérhetetlensége esetén a hiányzó személy feladat és hatáskörének megfelelően köteles eljárni.

A Társaság köteles a szervezeti és működési szabályzatában rögzíteni az információbiztonsággal és rendkívüli helyzetkezeléssel, valamint az infokommunikációval kapcsolatos felelősségi köröket és feladatokat, illetve azok ellátásának formáját.

A Társaság az információbiztonsággal kapcsolatos feladatainak elvégzését, valamint az információbiztonsági felelős tevékenységének ellátását - a vonatkozó szolgáltatási (SLA) szerződés megkötésével - a munkaszervezetébe nem tartozó, külső szolgáltató, illetve szolgáltatás igénybevételével biztosítja.

A felelősségi szerepkörökről, szervezeti egységekről és feladataikról a Társaságnak tájékoztatási kötelezettsége van az MVM Zrt. csoportszintű biztonsági igazgatója felé.

6.3.1. Társasági szintű közreműködők

- A Társaság első számú vezetője (a továbbiakban: Ügyvezető)
- Számítástechnikai főmunkatárs
- Információbiztonsági felelős (IBF)
- Ügyvezető által megbízott más személy(ek)

6.3.2. Információbiztonsági felelős és kinevezésének folyamata

Az információbiztonsági felelős a Társaság vonatkozásában ellátja az elektronikus információs rendszer biztonságáért felelős személy - a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvényben foglalt - feladatait, valamint segíti és szakmailag támogatja az Ügyvezetőt a kiberbiztonsággal kapcsolatos törvényi kötelezettségeinek teljesítésében.

Az információbiztonsági felelősről az Ügyvezető dönt, egyben megküldi az MVM Zrt. információbiztonsági és kríziskezelési osztályvezetőnek felterjesztésre (előzetes jóváhagyásra), aki továbbítja az MVM Zrt. csoportszintű biztonsági igazgató számára jóváhagyásra. Az eredményről a Társaság tájékoztatja a tulajdonosi joggyakorlót. Az Ügyvezető intézkedik az információbiztonsági felelős adatainak - a nemzeti kiberbiztonsági hatóságnál történő - hatósági nyilvántartásba vételéről is. Az információbiztonsági felelős részletes feladatait és a vele szemben támasztott követelményeket a jelen szabályzat 3. sz. melléklete tartalmazza.

6.3.3. Csoportszintű közreműködők

Az MVM Zrt. szabályozza a KIE-17 ÉS KIE-20 központi irányelvek alapján az információbiztonsággal és infokommunikációval kapcsolatos szervezetek kialakítását, a vonatkozó felelősségek és feladatok meghatározását.

6.4. Az információ védelme

Annak érdekében, hogy az információ védelme a Társaságon belül egységes legyen, és a szükséges és elégséges információbiztonsági követelmények, kontrollok meghatározhatóak legyenek, a Társaságnak végre kell hajtania, vagy hajtatnia a következőket:

- adatvagyon felmérés,
- kockázatelemzés készítése,
- adatvagyon elemek biztonsági osztályba sorolása,
- informatikai rendszerek biztonsági osztályba sorolása,
- hozzáférés és jogosultság menedzsment folyamatok működtetése.

6.4.1. Adatvagyon felmérése

A szükséges védelmi intézkedések meghatározásához azonosítani kell azon adatvagyon elemeket, melyeket védeni szükséges.

A védelmi intézkedések meghatározásának alapja a kockázatelemzés elkészítése, melynek feltétele, hogy a Társaság az adatvagyon felmérés keretein belül azonosítsa a folyamataiban keletkezett, vagy a folyamatai által használt adatvagyon elemeken túl az azokhoz kapcsolódó erőforrásokat is, illetve felmérje, hogy milyen hatása van annak, ha az adatvagyon elem bizalmassága, sértetlensége és rendelkezésre állása sérül. Az adatvagyon gazdálkodási keretrendszer létrehozásával és működtetésével kapcsolatos elvárásokat a jelen szabályzat 4. sz. melléklete tartalmazza.

6.4.2. Kockázatok azonosítása és kezelése

A védelmi intézkedések meghatározásának alapja az információbiztonsági kockázatelemzés elkészítése, mely tartalmazza a Társaságnál azonosított aktuális információbiztonsági kockázatokat, vagyis az adatvagyon elemet érintő sérülékenységeket, az azokat kihasználó fenyegetéseket, azok bekövetkezési valószínűségét és becsült hatását. A későbbiekben bevezetendő védelmi intézkedéseket és eljárásokat ezeknek megfelelően kell kialakítani.

6.4.3. Adatvagyon elemek személyes adatköri minősítése

Az adatvagyonból a KIE-16 Az MVM Csoport személyes adatkezelési és adatvédelmi irányelvének megfelelően meg kell határozni a személyes adatkezelésekben érintett adatok körét.

6.5. Hozzáférés-menedzsment, jogosultságok felügyelete és kezelése

6.5.1. Jogosultságkezelés folyamat biztonsága - minimumhozzáférés alkalmazásának elve

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 annak észlelésekor, de legkésőbb a felhasználói felülvizsgálat során.

A jogosultság kezelést kötelező egységes szabályok mentén működtetni a Társaság összes rendszerére vonatkozóan. A jogosultságkezelési folyamat hatókörébe tartoznak:

- az IT Szolgáltató(k) (Microsoft-365, MVMI) által biztosított rendszerek,
- bármely egyéb ügyviteli IT szolgáltatást nyújtó szolgáltató rendszerei,
- valamint a saját üzemeltetésű IT rendszerek.

A jogosultságok igénylésének-, változtatásának folyamata email-en keresztül történik, mellékletként küldött formanyomtatványok segítségével.

A Társaság az alábbi formanyomtatványokat alkalmazza:

- Jogosultság biztosítása (aktívba visszatérő) - ügyv.int. - MINTA.docx
- Jogosultság biztosítása (első mindenkinek) - ügyv.int. - MINTA.docx
- Jogosultság biztosítása (POSZEIDON miatt) - ügyv.int MINTA.docx
- Jogosultság biztosítása (új belépő) - ügyv.int. - MINTA.docx
- Jogosultság biztosításának visszavonása (jogiba kerülő) - ügyv.int. - MINTA.docx
- Jogosultság biztosításának visszavonása (megszűnő) - ügyv.int. - MINTA.docx
- Jogosultságok felülvizsgálata.docx

A nyomtatványok az IBIR rendszerben az alábbi könyvtárban találhatóak:

OneDrive - MVM Mátra Gép Kft\Kiberbiztonság\02 IBIR\009 Jogosultságkezelés\001 Nyomtatványok

6.5.2. Jogosultság nyilvántartás

A Társaság a kiosztott jogosultságokról historikus nyilvántartást vezet az alábbi helyen:

OneDrive - MVM Mátra Gép Kft\Kiberbiztonság\02 IBIR\009 Jogosultságkezelés\Mátra Gép jogosultsag_nyilvantartas_v1.0.0.xlsx

6.5.3. Jogosultság kiadása és visszavonása

A Társaságnak több olyan rendszere van, amelyben jogosultságkezelés történik. Minden rendszerben elkülönítetten történik a jogosultságok kezelése melyeket a Számítástechnikai főmunkatárs végez. A Társaságnak az összes rendszerre vonatkozó központi jogosultágkezelő rendszere nincs.

A jogosultságkezelési folyamatba bevont, illetve jogosultságkezeléssel bíró rendszereket a rendszernyilvántartás (CMDB) tartalmazza.

6.5.3.1. Jogosultság igénylés és kiadás folyamata - beléptetés

Jogosultság igénylés- és kiadási folyamatot új munkatárs beléptetésekor, illetve meglévő munkatárs új munkakörbe való áthelyezése esetén kell indítani az alábbiak szerint:

- Jogosultság igény ***feladása*** email küldése a Számítástechnikai főmunkatársnak. A levélben benne kell lennie az alábbiaknak:
  - Felhasználó, akinek a jogosultsági szerepköröket kérik;
  - Kért jogosultság, szerepkör;
  - Jóváhagyó munkahelyi vezető;
- Amennyiben a jogosultság kérést a felhasználó területi vezetője küldte, úgy a Számítástechnikai főmunkatárs ezt jóváhagyott kérésnek tekinti és külön további jóváhagyás nélkül beállítja a jogosultságot.

Jogosultságkérést az igénylő felhasználó és munkahelyi vezetők kezdeményezhetnek.

- A jogosultságok beállítását/beállíttatását a Számítástechnikai főmunkatársi közvetlenül végzi, amennyiben a jóváhagyás és a kért jogosultság a szokásos jogosultsági rend szerint, a meglévő szerepkörökkel került feladásra.
- Amennyiben a jogosultság kérést a felhasználó területi vezetője küldte, úgy a Számítástechnikai főmunkatárs ezt jóváhagyott kérésnek tekinti és külön további jóváhagyás nélkül beállítja a jogosultságot.
- Kérdéses vagy aggályos jogosultság kérés esetén a Számítástechnikai főmunkatárs kikéri területi vezető vagy az Ügyvezető vagy az IBF jóváhagyását.
- A jogosultság igénylési folyamat visszajelzés emailben történő elküldésével ér véget.

6.5.3.2. Jogosultság változtatás folyamata - munkakör változás

A jogosultság változtatási folyamat megegyezik a *6.5.3.1 Jogosultság igénylés és kiadás folyamata - beléptetés* pontban leírt jogosultság kérései folyamattal. Jogosultságváltoztatásnak minősülnek:

- a jogosultság tényleges változtatása;
- jogosultság szüneteltetése;

6.5.3.3. Jogosultság visszavonás folyamata – kiléptetés

Jogosultság visszavonási folyamatot meglévő munkatárs kiléptetése esetén kell indítani az alábbiak szerint:

- Jogosultság visszavonási igény ***feladása*** a Számítástechnikai főmunkatársnak küldött email formájában történik. A levélben benne kell lennie az alábbiaknak:
  - Felhasználó, akinek a jogosultsági szerepköreinek visszavonását kérik;
  - Visszavonandó jogosultságok, szerepkörök, vagy az összes jogosultság visszavonásának kérése;
  - Jóváhagyó munkahelyi vezető;
- Amennyiben a jogosultság kérést a felhasználó területi vezetője küldte, úgy a Számítástechnikai főmunkatárs ezt jóváhagyott kérésnek tekinti és külön további jóváhagyás nélkül visszavonja a felhasználó jogosultságait
- Jogosultsági és/vagy eszközigény ***visszavonása***
- A jogosultság visszavonási folyamat a visszajelzés továbbításával ér véget.

Amennyiben a munkatárssal kötött kilépési megállapodás ezt kifejezetten tartalmazza a Társaság kontrollált mentési lehetőséget biztosíthat a kilépő dolgozónak egyes, szigorúan meghatározott és ellenőrzött adattartalmak mentésére és átadására. Ez minden esetben az IBF és/vagy az Ügyvezető egyedi jóváhagyásához van kötve. Az adattartalmakról való egyedi mentéseket a Számítástechnikai főmunkatárs végzi szigorúan az IBF utasításai alapján.

Indokolt esetben - tipikusan fegyelmi eljárás esetén - a Számítástechnikai főmunkatárs egyedileg egyeztet az adott felhasználó jogosultságainak időzített és összehangolt visszavonásáról.

A kiléptetett munkatárs céges adattartalmú postafiókja és egyéb központilag tárolt céges adattartalmú állományai megőrzésre kerülhetnek a mindenkori vonatkozó adatkezelési jogszabályoknak megfelelően. Kilépés esetén az Ügyvezető dönt az adattartalom megőrzéséről. Ezek biztonsági okból való visszaállítását az Ügyvezető vagy az IBF kezdeményezheti. A visszaállítást a Számítástechnikai főmunkatárs végzi.

6.5.4. <u>Privilegizált fiókok kezelésének szabályai</u>

A Társaságnál dolgozó olyan informatikai dolgozóknak (pl. Számítástechnikai főmunkatárs) aki(k) egyes munkáihoz privilegizált (Rendszergazda, Admin, Root) jogosultságú felhasználói fiók használata szükséges, két felhasználói fiókkal kell rendelkezniük. Az egyik egy normál jogú felhasználói fiók, a másik privilegizált felhasználói fiók.

A privilegizált jogosultságú felhasználói fiók kizárólag e jogosultságot igénylő munkákhoz használható. Minden egyéb, privilegizált jogosultságot nem igénylő munkához normál felhasználói fiókot kell használni.

A IT rendszerek alapértelmezett privilegizált jogosultságú (Rendszergazda, Admin, Root) fiókjai le vannak tiltva, azok nincsenek használatban.

A rendszerekben kell lenniük az alapértelmezettek helyett létrehozott vészhelyzeti privilegizált felhasználóknak. Ezek hozzáférési adatai, illetve minden egyéb központilag használatos jelszó központi borítékos megoldással és/vagy biztonságos jelszótároló alkalmazásba kerül tárolásra. A zárt boríték(ok) az Ügyvezető széfjében lehetnek elhelyezve, a biztonságos jelszótároló alkalmazáshoz jelszavát is ez tartalmazza. A kettő együtt konzisztens biztonsági rendszert képez.

6.5.5. <u>Jogosultságok felülvizsgálati folyamata</u>

A Társaság a felhasználói jogosultságokat éves gyakorisággal felülvizsgálja A jogosultság felülvizsgálatokat a Számítástechnikai főmunkatárs végzi, dokumentált folyamatban. A feltárt eltéréseket jegyzőkönyvezi, illetve elvégzi a nem szükséges jogosultság visszavonását.

6.5.6. Technikai felhasználók és kiemelt jogosultságot igénylő szoftverek hozzáférés kezelésének szabályai – Ügyviteli rendszerek

Azon rendszerek esetében, amelyeknél személyhez nem kötött technikai felhasználók létrehozása szükséges (pl. automatikusan lefutó task-ok végrehajtására), a fejlesztőnek/üzemeltetőnek:

- A technikai felhasználók jogosultságainak kiadási folyamatába be kell vonnia a Társaság IBF-ét.
- Technikai felhasználó létrehozása és jogosultságokkal való ellátása az IBF jóváhagyását követően végezhető el.
- Pontos nyilvántartást kell vezetnie a technikai felhasználókról, azok tevékenységéről, jogosultságairól.
- Meg kell osztania a technikai felhasználók nyilvántartását az IBF-el.
- Gondoskodni kell a technika felhasználók adatainak biztonságos tárolásáról.
- Az fentieken túl minden egyéb szükséges esetben további információkat kell szolgáltatnia a technikai felhasználókról az IBF felhívására.
- Időszakos, vagy periodikus aktiválású technikai felhasználók létrehozása esetén minden egyes aktiválásról tájékoztatni kell legalább az IBF-et.

A technikai felhasználók hozzáférési adatait tartalmazó nyilvántartásokat:

- lepecsételt, aláírt borítékban, páncélszekrényben, és/vagy
- megfelelően titkosított jelszótároló alkalmazásban/adatbázisban kell tárolni.

A technikai felhasználók nyilvántartásaihoz a Számítástechnikai főmunkatárs és az IBF közösen fér hozzá. A nyilvántartáshoz való hozzáféréseket és végzett műveleteket naplózni kell, ahol ez technológiailag lehetséges.

Technikai felhasználóval természetes személyként a napi jellegű munkavégzés tilos!

6.6. Rendszerhozzáférés, autentikáció, fiókzárolási szabályok

6.6.1. Rendszerhasználat jelzése

A Társaság IT rendszerei használatának megkezdésekor, a bejelentkezést követően a rendszer figyelmeztető üzenetet küld a felhasználó számára, mely az alábbi információkat tartalmazza:

- a felhasználó a Társaság elektronikus információs rendszerét használja;
- a rendszerhasználat, felhasználói aktivitás megfigyelésre, rögzítésre, naplózásra kerülhet;
- a rendszer jogosulatlan használata tilos és büntetőjogi és/vagy polgári jogi felelősségre vonással járhat;
- a rendszer használatának megkezdése egyben a fentiek tudomásul vételét jelenti.

6.6.2. Felhasználói hitelesítési szabályok, bejelentkezési eljárások és szabályok kötelező alkalmazása, az autentikáció módja

A Társaság a kritikus rendszerek esetén autentikációs megoldásokat használ, amelynek biztonsági előírásai a következők.

A Társaság által üzemeltetett egyes egyéb, nem kritikus rendszerek esetében - melyek nem AD integráltak - egyedi autentikációs megoldások vannak kialakítva, amelyek kezelését az adott rendszer kulcsfelhasználói végzik. Ezen rendszerek esetén, azok korlátai miatt, az autentikációs biztonsági előírások nem, vagy csak korlátozottan valósulnak meg, amelyet a Társaság ismert és felvállalt kockázatként kezel.

A Társaság rendszereihez hitelesítés nélkül nem lehet hozzáférni, azok nem használhatóak hitelesítés nélkül.

6.6.3. Általános autentikációs szabályok és hitelesítési információk védelme

Az alkalmazandó jelszavak esetén, amennyiben ez technológiailag lehetséges, az összes alkalmazott autentikációs rendszernek (Active Directory) ki kell kényszerítenie a jelszavakra vonatkozó előírásokat.

Amennyiben az előírt komplexitás az adott rendszer esetén nem kényszeríthető ki, úgy a felhasználónak kell figyelmet fordítani az előírások alkalmazására.

6.6.4. Kezdeti jelszó

A felhasználó a véletlenszerűen generált kezdeti jelszavát a Számítástechnikai főmunkatárstól kapja.

A kezdeti jelszót a felhasználónak az első bejelentkezés során meg kell változtatnia, melyet a rendszerek automatikusan kikényszerítenek, amennyiben a rendszer képességei ezt lehetővé teszik. Amennyiben egy adott rendszer képességei nem teszik lehetővé a kezdeti jelszó kötelező megváltoztatásának kikényszerítését, úgy adminisztratív kiegészítő kontrollokkal kell gondoskodni a kontroll minél teljeskörűbb megvalósításáról. A Számítástechnikai főmunkatárs felelőssége, hogy a kontrol az általa üzemeltetett rendszerek alapértelmezett és/vagy kezdeti jelszóira is érvényesítésre kerüljön.

6.6.5. Jelszópolitika

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

- minimum 10 karakter hosszúságú (kikényszerített, ahol lehetséges),
- 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-, különösen a Társaságon kívüli rendszerekhez javasolt eltérő jelszavakat használni, amennyiben ez lehetséges,
- az utolsó 5 jelszó nem használható fel újra, az újra felhasználást - a rendszerek kikényszerítik,
- 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 Társaság IT Biztonsági szakterület által támogatott alkalmazások használhatóak, egyedi, privát megoldások nem,
- az egymást követő jelszavak legalább 1 karakterben térjenek el (különbözőség).

A jelszavakat és a felhasználói fiókokat tilos más felhasználóval megosztani, még a rendszergazdáknak sem adhatók át. Minden fióknak egyértelműen hozzárendelve kell lennie egy adott természetes személyhez, mint felhasználóhoz. Több felhasználói fiókkal kizárólag a privilegizált jogosultságú felhasználók rendelkezhetnek (normál jogosultságú fiók a napi munkához és privilegizált fiók a rendszergazda jellegű munkákhoz).

6.6.6. Sikertelen bejelentkezés

A Társaság minden rendszertípus esetén egységesen szabályozza a sikertelen bejelentkezési kísérletek maximális számát, amelyet túllépve a felhasználói fiók zárolásra kerül az adott rendszerben, ahol ez lehetséges.

Az sikertelen bejelentkezési kísérletek száma egységesen egymást követő 5 bejelentkezési kísérlet.

6.6.6.1. IT rendszerek fiókzárolásának feloldása

IT rendszerek esetén a Számítástechnikai főmunkatársat kell megkeresniük a felhasználóknak a fiókzárolás feloldásához személyesen, telefonon, vagy emailben.

6.6.6.2. Jelszavak élettartama

A jelszavak rendszeres cseréje az IT rendszerek esetében kikényszerített módon, 180 naponta automatikusan valósul meg.

Egyéb rendszerek esetén törekedni kell a jelszavak rendszeres cseréjére. A jelszót javasolt legfeljebb 180 naponta cserélni.

A jelszót haladéktalanul meg kell változtatni minden olyan esetben, amikor fennáll annak gyanúja, illetve lehetősége, hogy ismertté vált, kompromittálódott. A felhasználók minden ilyen gyanú esetén kötelesek azonnal értesíteni a Számítástechnikai főmunkatársat.

6.6.7. Erős, illetve kétfaktoros autentikáció

Megerősített (pl. kétfaktoros) autentikáció alkalmazása szükséges minden olyan rendszer esetében, melyben fennállhat szigorúan bizalmas adatok tárolásának lehetősége, vagy nagy mennyiségben tartalmaznak bizalmas információkat.

A Társaság kétfaktoros autentikációt követel meg az alábbi rendszerek esetén:

- O365 kiemelt fiókok levelezés és tárhelyhozzáférés,
- VPN hozzáférési jogosultsággal rendelkező felhasználók

A fentiekről a Számítástechnikai főmunkatárs vezet részletes nyilvántartást.

6.6.8. Hitelesítés nélkül végrehajtható tevékenységek

A Társaságnál nincs olyan rendszer, vagy tevékenység, amelyben hitelesítés nélkül végezhető tevékenység lenne.

6.6.9. Külső rendszerekhez való hozzáférés szabályai

Külső rendszerhez kizárólag a munkavégzéssel összegfüggésben, a Társaság a Számítástechnikai főmunkatárs és/vagy az IBF jóváhagyását követően lehet hozzáférni.

A hozzáférés technológiai kialakítását, a külső rendszerhez való hozzáféréshez céges fiók regisztrálását a Számítástechnikai főmunkatársnak és/vagy az IBF-nek jóvá kell hagynia.

Külső rendszerekhez való hozzáféréseket a Számítástechnikai főmunkatárs tartja nyilván.

6.7. Munkatársak toborzásának, kiválasztásának biztonsági követelményei

6.7.1. Belépést megelőző szabályok munkavállaló előzetes ellenőrzése

A Társaság az egyes munkavégzésre irányuló bármilyen jogviszony létrejötte előtt, a jelöltek alkalmazását megelőzően HR átvilágítást végezhet. Az átvilágítást - a Társasággal kötött szolgáltatási (SLA) szerződés alapján - az MVM Services Zrt., illetve érintett szervezeti egysége, mint külső szolgáltató (a továbbiakban: Munkaügyi iroda) hajtja végre.

6.7.1.1. Munkakörök biztonsági besorolása

Minden belépő, vagy munkakört váltó munkavállaló munkakörét azonosítani kell. A munkakör azonosítását a Munkaügyi iroda végzi a Társaság Munkakör Katalógusa alapján. A Munkakör

Katalógust a Munkaügyi iroda tartja karban. Amennyiben az adott munkakör még nem szerepel a Munkakör Katalógusban, úgy azt fel kell venni oda.

A Társaság három munkakör biztonsági kockázati besorolási szintet alkalmaz, amelyek az alábbiak:

Besorolás megnevezése	Munkakörök	Munkakör biztonsági kockázati besorolási szint kódja
MAGAS KOCKÁZATÚ munkakör	Felsővezetők Középvezetők Operatív vezetők	3
ALAP KOCKÁZATÚ munkakör	Céges informatikai eszközt használó fizikai, szellemi, vagy mindkét típusú munkát végző munkavállalók	2
ALACSONY KOCKÁZATÚ munkakör	Informatikai eszközt nem használó fizikai munkát végző munkavállalók	1

6.7.1.2. MAGAS (3-as) kockázatú munkakör azonosítása és biztonsági besorolása

Magas kockázatú (3) munkakörként olyan munkakör azonosítható, amelyben törvény vagy a Társaság büntetlen előélet hiányában a foglalkoztatást jelen alfejezetben foglalt szabályok szerint kizárja.

Az adott munkakör biztonsági kockázati besorolási szintjéhez kötelezően elvégzendő összes vizsgálati lépést az „***MVM MG Munkakör besorolás v1.0.0.xlsx Biztonsági besorolás”*** munkalapja tartalmazza. Magas kockázatú (3) munkakör esetén az ehhez a kategóriához tartozó, a táblázatban felsorolt összes ellenőrzést el kell végezni.

Az ellenőrzéseket a Munkaügyi iroda végzi. A Munkaügyi iroda szúrópróbaszerű ismételt ellenőrzést végezhet, amennyiben ezt az IBF, vagy munkavállalót alkalmazni szándékozó szervezeti egység ezt indokoltnak látja.

6.7.1.3. ALAP (2-es) és ALACSONY (1-es) kockázatú munkakörök és biztonsági besorolása

Alap kockázatú (2) munkakörként olyan munkakör azonosítható, amelyben törvény vagy a Társaság büntetlen előélet hiányában a foglalkoztatást jelen alfejezetben foglalt szabályok szerint kizárja.

Az adott munkakör biztonsági kockázati besorolási szintjéhez kötelezően elvégzendő összes vizsgálati lépést az „***MVM MG Munkakör besorolás v1.0.0.xlsx Biztonsági besorolás”*** munkalapja tartalmazza. Alap kockázatú (2) munkakör esetén az ehhez a kategóriához tartozó, a táblázatban felsorolt összes ellenőrzést kell elvégezni

Alap (2) és alacsony (1) kockázatú munkakör esetén az ehhez a kategóriához tartozó, a táblázatban felsorolt összes alapellenőrzést javasolt elvégezni.

Az ellenőrzéseket a Munkaügyi iroda végzi. A Munkaügyi iroda szúrópróbaszerű ismételt ellenőrzést végezhet, amennyiben ezt az IBF, vagy munkavállalót alkalmazni szándékozó Szakterület ezt indokoltnak látja.

6.7.1.4. Egy munkakör minősítésének rendkívüli felülvizsgálata

Munkakör és biztonsági besorolásának változtatása írásban kezdeményezhető, megfelelő indoklással alátámasztva. Munkakör biztonsági besorolásának változtatásról a Munkaügyi iroda dönt, az írásbeli kérelem beérkezésétől számított 1 hónapon belül, a rendelkezésre álló információk alapján az Ügyvezető jóváhagyásával.

6.7.2. Munkatársak beléptetésének IT biztonsági követelményei

6.7.2.1. Általános biztonsági követelmények

A Társaság vele munkavégzésre irányuló szerződéses jogviszonyba kerülő bármely természetes személy számára

- a munkaszerződésben vagy a megbízási szerződésben,
- a munkaköri leírásban,
- külön tájékoztatókban,
- szabályzatokban,
- oktatási anyagokban

határozza meg az informatikai és információbiztonsági követelményeket, kötelezettségeket, valamint ezekben hívja fel a figyelmet ezek megszegésének lehetséges következményeire.

A Társaság minden munkatársa, szerződéses partnere csak előzetes titoktartási nyilatkozat aláírását követően férhet hozzá a munkakörének, megbízásának megfelelő jogosultságokkal a Társaság informatikai rendszereihez és adataihoz.

A nyilatkozat aláírására új belépők esetén a munkakezdést megelőzően megtartott ***Információbiztonsági Oktatást*** követően kerül sor.

A munkavállaló munkakörének, megbízásának ellátásához szükséges jogosultságok az *6.5.3 Jogosultság kiadása és visszavonása* pontban leírt folyamat szerint igényelhetők.

A próbaidős munkavállaló a próbaidő alatt csak megfelelő felügyelet mellett dolgozhat a Társaság vállalati adatvagyonához hozzáférő rendszereken.

6.8. Munkaviszony megszűnésének, munkakör megváltoztatásának feltételei (kiléptetés, átléptetés)

6.8.1. Felelősségek a munkaviszony megszűnésekor

A távozó munkavállaló nem jogosult munkavégzése során keletkezett, vagy általa kezelt a Társaság adatvagyoni körébe tartozó adatok további birtoklására. Azokat el nem viheti, a Társaság, mint munkáltató hozzájárulása nélkül sértetlenségüket és rendelkezésre állásukat nem változtathatja meg, róluk magáncélú másolatot nem készíthet. A korlátozás betartását a Társaság technikai úton ellenőrizheti. Jelen pontban rögzített szabály bizonyítható megszegése esetén, a biztonsági igazgató kezdeményezésére a Társaság eljárást indíthat.

6.8.2. Információbiztonsági relevanciával bíró vagyontárgyak visszaszolgáltatása

Valamennyi munkavállalónak, a vele megkötött szerződésben meghatározottak szerint a Társaság számára vissza kell szolgáltatnia a Társaság valamennyi, birtokában lévő, információbiztonsági relevanciával bíró vagyontárgyát (adathordozók, számítógép, mobiltelefon stb.). A vagyontárgyak visszaszolgáltatásáért a kilépő munkavállaló és az adott szervezeti egység vezetője a felelős. A visszavételi folyamatot az IBF ellenőrizheti.

6.8.2.1. IT eszközleadás

Számítástechnikai eszközök számítógépek (asztali PC, laptop) és USB adathordozók esetén a munkavállaló feladata leadni az eszközt. Az eszköz adatmentesítését/adattörlését a Számítástechnikai főmunkatárs végzi, amennyiben erre szükség van.

6.8.2.2. IT eszköz megvásárlása

IT eszköz megvásárlása egyedi engedélyezés alapján történhet a Társaság vagy a munkavállaló kezdeményezésére. Az IT eszköz tulajdonjoga kizárólag nem visszavonható adatmentesítést/adattörlés végzését követően adható át. Ennek folyamata:

- Az IT eszköz megvásárlását a Társaság engedélyezi, valamely szakterület kezdeményezése alapján.
- Amennyiben az eszköz IT biztonsági relevanciával bír, úgy az érintett munkavállaló köteles az eszközt átadni a Számítástechnikai főmunkatársnak adatmentesítés/végleges adattörlés céljából.
- A Számítástechnikai főmunkatárs gondoskodik az IT eszköz adattartalmának végleges, nem visszaállítható törléséről.

Amennyiben egy eszközről az adattartalom nem távolítható el visszavonhatatlanul, úgy az eszköz

- nem vonható ki a Társasági célú használatból,
- nem értékesíthető,
- nem adományozható el.

Ilyen esetekben a selejtezési eljárás végén az eszközt megbízható módon, dokumentált folyamatban meg kell semmisíteni.

6.9. Fegyelmi eljárás és alkalmazható szankciók

A Társaság gondoskodik arról, hogy szükséges esetben olyan fegyelmi eljárás működjön, amely kiterjed az információbiztonsággal kapcsolatos fegyelmi vétségekre is.

A Társaság olyan folyamattal rendelkezik a kiléptetési folyamat IT biztonsági tennivalóira vonatkozóan, amelyben össze kell hangolnia a következőket:

- a felmondás közlése,
- a jogosultságok időzített visszavonása/felfüggesztése,
- a kiléptetési folyamatban szereppel bíró munkatársak megfelelő és előzetes tájékoztatása.

A Munka Törvénykönyve, a Polgári Törvénykönyv, illetve a Büntető Törvénykönyv alapján a munkavállaló, vagy bármilyen munkavégzésre irányuló jogviszonyban munkát végző természetes, vagy jogi személy a munkavégzésre irányuló jogviszonyból származó kötelezettségének vétkes megszegése esetén kötelezhető az okozott kár megtérítésére, amennyiben nem a vonatkozó szabályozásokban előírtak szerint járt el, és a káresemény a munkát végző vétkes magatartásának következményeként azonosítható.

Bizonyos információbiztonsági követelmények megszegése esetén a Társaság fenntartja a jogot bizonyítékként felhasználható adatok, információk (pl. rendszernaplók, videófelvételek stb.) előzetes, folyamatos, vagy utólagos gyűjtésére és elemzésére.

6.10. IT biztonságtudatossági oktatás

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

IT biztonsági oktatást kell szervezni az alábbi esetekben:

- Rendszeresen, évente legalább egy alkalommal ismétlő jelleggel, minden munkavállaló részére, a munkavállalók biztonságtudatossági szintjének folyamatos fenntartása és javítása érdekében.
- Eseti jelleggel a következő események bekövetkezése során:
  - Jelen szabályzat kialakítása, illetve jelentős módosulása esetén minden érintett részére.
  - Új munkavállaló belépésekor az új belépő részére.
  - Incidens bekövetkezését és kivizsgálását követően az érintettek részére, amennyiben az Ügyvezető vagy az IBF indokoltnak látja az ismétlő képzést.

Az oktatások megszervezése és lebonyolítása az IBF/vagy a Számítástechnikai főmunkatárs feladata, együttműködve a Munkaügyi iroda munkatársaival.

Az oktatáson résztvevőknek az oktatást követően vizsgázniuk kell az oktatáson elhangzottakból. A vizsga szervezését és lebonyolítását az IBF a Számítástechnikai főmunkatárssal közösen végzi.

A rendszeres oktatás esetében meg kell határozni különböző oktatási célcsoportokat (például felső vezetés, adminisztrációs terület, üzemeltetés stb.) és az oktatási tematikát. A célcsoportok kialakításakor figyelembe kell venni a célcsoportra jellemző speciális fenyegetéseket, valamint a célcsoport által használt adatok biztonsági besorolását.

6.11. Külső közreműködők, harmadik fél hozzáférése

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

Az információbiztonsági szabályozás szempontjából külső közreműködőnek, harmadik félnek tekintendő minden olyan külső szervezet, szerződéses partner, akinek tevékenysége indokolttá a Társaság bármely informatikai rendszeréhez, illetve belső használatú vagy annál magasabb minősítésű adataihoz történő hozzáférést.

Ilyen módon külső közreműködőnek minősülnek a Társaság alvállalkozói, szerződéses partnerei, valamint az MVM Csoporton kívül eső cégek, a hatóságok.

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 ***6.11.2 Adatok átadása, vagy*** *adathozzáférés biztosítása harmadik fél* fejezet).

6.11.1. Külső felek közreműködésével kapcsolatos általános szabályok

6.11.1.1. Külső közreműködő bevonásának feltételei

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

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

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

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

6.11.1.2. Szerződésben szabályozandó alapkövetelmények

Szerződéses partnerek esetében (a továbbiakban ide értendőek az Ügyvezető általi meghatalmazással rendelkezők) a szerződésnek tartalmaznia kell:

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

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

6.11.1.3. Szerződésben szabályozandó információbiztonsági követelmények

A szerződés vagy megállapodás információbiztonsági követelményeinek tartalmaznia kell a következőket:

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

6.11.1.4. Külső közreműködők személyi változásainak kezelése

A szerződésekben, vagy azok mellékleteiben minden esetben meg kell nevezni a külső közreműködők hozzáféréssel rendelkező, munkavégző munkatársait, illetve változások esetén ki kell térni a külső közreműködőnél történő személyi változások kezelésére, illetve ezek haladéktalan bejelentésére.

Rögzíteni kell továbbá az egyéb alvállalkozók bevonására vonatkozó információbiztonsági szabályokat, ez esetben a fővállalkozó felel az alvállalkozó tevékenységéért információbiztonsági szempontból is.

A szerződés/megállapodás titoktartási nyilatkozatával kapcsolatos előírások a következők:

- Az együttműködés, a beszerzési eljárás és a szerződés előkészítése során már az első nem nyilvános információ átadása előtt a külső partner bevont képviselőivel egyoldalú, előzetes titoktartási nyilatkozatot kell aláírattatni a szerződés megkötése előtt átadott adatokra vonatkozóan is.
- A titoktartási nyilatkozatokat az adott jogviszonynak megfelelően szervezet és magánszemély szintjén egyaránt alá kell íratni.
- A szerződésben kötelezően elő kell írni, hogy a külső fél minden munkavállalóját, érintett szerződéses partnerét, alvállalkozóját titoktartásra kötelezze a legalább a szerződésben előírt hatókörben.

Az információbiztonsági követelmények Társaság oldali betartásáért a szerződésben nevesített Társasági képviselők felelnek. Az információbiztonsági követelmények betartását a Társaság keretein belül az IBF ellenőrizheti.

6.11.2. Adatok átadása, vagy adathozzáférés biztosítása harmadik fél számára

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

Adatok átadása harmadik félnek csak az ***6.11.1. Külső felek közreműködésével kapcsolatos általános szabályok*** fejezetben rögzített feltételek teljesítését követően, a szerződésben meghatározott módon lehetséges.

Papír alapú dokumentumok átadása esetén törekedni kell a személyes átadásra, továbbá a dokumentum továbbításakor, átadásakor meg kell felelni a ***6.11.1. Külső felek közreműködésével kapcsolatos általános szabályok*** fejezetben, rögzített követelményeknek.

Elektronikus dokumentumok átadásánál a ***6.18 Elektronikus kommunikáció biztonsága*** fejezetben rögzített titkosítási eljárásokat kell követni az elektronikus levelezés során, illetve nagy mennyiségű adat átadása esetén preferálni kell a titkosított adathordozók használatát.

A szerződéses partnernek biztosítana kell saját munkavégzői számára:

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

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

- munkaállomást,
- projektszobát,
- VPN hozzáférést,
- biztonságos állománycsere megoldást

biztosíthat.

Az adatok biztonságos módon való átadása a Társaság és a szerződött külső fél közös felelőssége. A nem megfelelő adatátadásból származó károkért az érintett természetes és jogi személyek a Társaság és a szerződött partner oldalán egyaránt felelősségre vonhatók a ***6.9 Fegyelmi eljárás és alkalmazható szankciók*** pontban meghatározottak szerint.

6.11.3. Határozott időre szóló belépési jogosultság adása harmadik félnek

Amennyiben a szerződött külső féllel való munka indokolja (pl. projekt, tartós vagy rendszeres munkavégzés), a külső szereplők számára igényelhető ideiglenes belépőkártya.

6.11.4. Külső szereplők IT rendszerekhez való hozzáférése

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

6.11.4.1. Külső szereplők IT rendszerekhez való hozzáférési jogosultságai

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

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

A külső partnernek részére a Társaság informatikai rendszeréhez adott felhasználói azonosítók csak azokhoz az információkhoz és olyan mértékben adhatnak hozzáférést és jogosultsági szintet, amennyi az együttműködés során a munkavégzéshez feltétlen szükséges. Harmadik fél hozzáférési jogosultságáról az adatgazda, valamint a Számítástechnikai főmunkatárs dönthet a *6.5 Hozzáférés-menedzsment, jogosultságok felügyelete és kezelése* fejezetben foglaltak szerint. A jogosultság kiadását és a lejárat határidejét írásban kell rögzíteni.

Minden harmadik félnek a hozzáférési jogosultság kiadása előtt meg kell ismernie a 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. Amely rendszernél lehetséges, automatikus lejáratot kell beállítani, illetve a szerződés megszűnésével egyidejűleg vissza kell vonni a kiadott jogosultságokat. A jogosultságok határidőjének megfelelő kezelése a szerződésben érintett szervezeti egység vezetőjének felelőssége. A Számítástechnikai főmunkatárs ezt saját hatáskörében, rendszeresen, legalább évi egy alkalommal ellenőrzi.

A hozzáférési jogosultság megújításáért a Társaság fogadó szervezeti egysége felel, év végi törlését a Számítástechnikai főmunkatárs automatikusan kezdeményezi, illetve hajtja végre.

6.11.4.2. Külső szereplők IT rendszerekhez való privilegizált jogosultságai

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

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

6.11.5. Külső szereplőknek való informatikai eszköz átadása

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

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

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

6.11.6. Projektszoba, adatszoba

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

A projektszoba lehet fizikai jellegű vagy elektronikus adatszoba.

6.11.7. Ellenőrzések

Jelen fejezetben rögzített, harmadik félre vonatkozó információbiztonsági előírásokat a Számítástechnikai főmunkatárs a jelen szabályzatban foglaltak alapján köteles ellenőrizni.

Harmadik féllel kötött szerződésben

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

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

Az ellenőrzésekről jelentést kell készíteni, melyet a harmadik fél képviselője és az adott vállalkozóért felelős terület vezetője felé egyaránt meg kell küldeni. Súlyos, vagy folyamatosan fennálló nem-megfelelés vagy hiányosság azonosítása esetén az IBF, illetve a Számítástechnikai főmunkatárs tájékoztatja az Ügyvezetőt, amennyiben ez indokolt.

6.12. Fizikai biztonság

6.12.1. Területek védelme, biztosítása

A Társaság területén kamerarendszer működik, amelynek működéséért a Számítástechnikai főmunkatárs felelős.

A kamerarendszernek csak rögzítési funkciója van. A felvételek visszanézésére jogosultakat külön lista tartalmazza.

6.12.2. Irodák, helyiségek és egyéb létesítmények védelme

A Társaság által használt területek, épületek és azok helyiségei a fizikai és környezeti biztonság szempontjából az alábbi biztonsági zónába sorolhatóak:

Nyilvános területek

A Társaság mindazon területei, helyiségei, amelyek látogatók számára nyilvánosak, ugyanakkor a Társaság szempontjából magánterületnek minősülnek.

Irodai terület kategória

Csak a Társaság munkavállalói, külső partnerek - külön engedély alapján - belépésre jogosult munkavállalói, illetve vendégek csak kísérettel léphetnek be.

Fokozottan védett kategória

Fokozottan védett helyiségnek kell tekinteni azokat a helyiségeket, ahol bizalmas adatok feldolgozására, tárolására alkalmazott kiegészítő informatikai erőforrások találhatók, valamint ide sorolandók az ügyvezetői, illetve felsővezetői irodák, helyiségek. Az ide tartozó helyiségeket zárható ajtóval kell ellátni.

Fokozottan védett kategóriába a következő helyiségeket kell sorolni:

- az aktív hálózati elemek elhelyezésére és üzemelésére szolgáló helyiségek, szekrények;
- használaton kívüli, adathordozót tartalmazó IT eszközök tárolására szolgáló helyiségek;
- ügyvezetői iroda, valamint a biztonsági tevékenység során keletkező dokumentumok (adathordozók, nyomtatványok stb.) és technikai eszközök tárolására kijelölt helyiség.

Kiemelten védett kategória

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

Kiemelten védett (zárt) helyiségekbe csak ellenőrzött módon és csak az arra jogosult személyek juthatnak be. A bejutás és benntartózkodás során kíséretet kell biztosítani a külső személyek részére. Ebbe a kategóriába az alábbi helyiségek tartoznak:

- Vagyonvédelmi informatikai eszközök elhelyezésére használt helyiség (továbbiakban: szerverszoba).

6.13. Iratkezelés rendje

Az iratkezelés rendjét a Társaság mindenkor hatályos Iratkezelési szabályzata tartalmazza.

6.14. Informatikai rendszerek fejlesztése, beszerzése

A Társaságnak a folyamatai megfelelő ellátásához az informatikai és telekommunikációs rendszereiket - az üzleti igényekkel összhangban és a változó biztonsági igényeknek megfelelően - folyamatosan fejlesztenie kell. Az informatikai rendszerek fejlesztése kapcsán külön szükséges kezelni az ügyviteli és a technológiai rendszereket.

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

- **Belső fejlesztésű** rendszerek: A Társaság által fejlesztett ügyviteli vagy technológiai alkalmazások.

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

A külső fejlesztésű rendszerek szerződése tartalmazza a telepítési és használati feltételeket, valamint a fejlesztési lehetőségeket, verziókövetést. Ebben az esetben a fejlesztővel/szállítóval kötött szerződésben kell kitérni az IT biztonsági követelményekre, melyet az IBF ellenőriz.

6.14.1. Általános irányelvek informatikai rendszerek fejlesztésére, beszerzésére vonatkozóan

Az informatikai rendszerek fejlesztését a következő IT biztonsági követelmények szerint kell végrehajtani.

6.14.1.1. Igények azonosítása

Az új igény egyeztetése során be kell vonni az IBF-et az új rendszerrel vagy fejlesztéssel kapcsolatos kockázatok korai feltárása végett. Az információbiztonsági szempontú véleményezésnek, jóváhagyásnak minden esetben dokumentált módon kell megtörténnie.

6.14.1.2. Fejlesztési terv készítése és jóváhagyása

A fejlesztési terv elkészítésénél minden esetben figyelembe kell venni az IT biztonsági követelmények biztosítását, meghatározni az információbiztonsági kockázatokat, ezért a dokumentum összeállításába az IBF-et is be kell vonni. Az IBF bevonásának elmaradásából származó károkért a fejlesztési projekt vezetője felelős. Fejlesztés csak abban az esetben kerülhet megkezdésre, amennyiben az Ügyvezető jóváhagyta a fejlesztési tervet.

6.14.1.3. Fejlesztés megvalósítása

Belső fejlesztés esetén az informatikai szolgáltatónak vagy a fejlesztésben érintett más társaságnak, vagy a Társaság fejlesztésben érintett szervezeti egységének fejlesztési módszertannal/szabályzattal kell rendelkeznie, mely dokumentálja a fejlesztések megvalósításának menetét, szabályait, kitérve az IT biztonsági követelményekre.

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

Felhő alapú rendszerek igénybevételének igénye esetén a rendszer bevezetése előtt az információbiztonsági felelősnek ellenőriznie kell a szolgáltató IT biztonsági megoldásainak megfelelőségét (interjú, vagy dokumentum vizsgálat). Ajánlása alapján az Ügyvezető hagyja jóvá a rendszerben tárolt/kezelt adatok körét, figyelembe véve az adatok besorolását. Az ellenőrzés eredményét dokumentált módon rögzíteni kell, a dokumentáció tárolása az 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.

6.14.1.4. Tesztelés

A fejlesztés során minden tételnek van tesztelési időszaka, csak a jóváhagyott release 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, melyek az éles rendszerből vett adatok anonimizálásával/deperszonalizálásával kerülnek előállításra.
- Az éles rendszer elkülönül a fejlesztői és teszt környezettől.
-

Éles környezetben csak a tesztelt, jóváhagyott kiadások kerülhetnek implementálásra. 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 társasági fejlesztés esetén az Ügyvezető, illetve az általa kijelölt személy bármikor ellenőrizheti.

6.14.1.5. 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 gondoskodni kell az IT biztonsági szempontból megfelelő működtetésről, karbantartásról.

6.14.2. Változáskövetés

A Társaságnak, mint informatikai rendszert üzemeltető társaságnak rendelkeznie kell olyan informatikai rendszerrel, illetve szabályozással, amely lehetővé teszi a megfelelő változáskövetés és változáskezelés fenntartását.

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

Minden tervezett változtatásról igényt kell küldeni a Társaság információbiztonsági felelősének is. Különösen figyelemmel kell kísérni az immateriális javakként számontartott szoftverek frissítése esetén az éves upgrade-t.

Az igény megérkezését követően az IBF feladata megvizsgálni az igény létjogosultságát, illetve megvalósíthatóságát IT biztonsági szempontok figyelembevételével. Az igény jóváhagyása az Ügyvezető hatáskörébe tartozik.

Az igény megvalósítását követően az eredmény és a végrehajtás ideje alatt készült dokumentáció megfelelőségét IT biztonsági szempontból az IBF ellenőrzi, majd ajánlása alapján, megfelelőség esetén az Ügyvezető jóváhagyja.

Amennyiben az eredmény nem megfelelő, a változás nem tekintendő lezártnak, a kért módosításokat a megfelelő dokumentáció mellett el kell végezni.

6.15. Elektronikus Informatikai Rendszerek (EIR-ek) üzemeltetése

Az alábbi fejezet az informatikai rendszerek bevezetését követően, azok működtetésével és karbantartásával kapcsolatban határoz meg IT biztonsági követelményeket.

6.15.1. Elektronikus Informatikai Rendszerek biztonsági osztályba sorolása

Az információs rendszerek biztonsági osztályba sorolása kötelező. A biztonsági osztályba sorolást az elektronikus információs rendszerek biztonsági osztályba sorolására vonatkozó jogszabály követelményeinek megfelelően szükséges végrehajtani. Az információs rendszerek 1-3. (ALAP, JELENTŐS, MAGAS) biztonsági osztályba sorolását az információs rendszerben kezelt adatok jellege és mennyisége, illetve a rendszer funkciói határozzák meg. A biztonsági osztályba sorolást a Társaság információbiztonsági felelősének ajánlása alapján az Ügyvezető hagyja jóvá.

Az informatikai rendszerek működtetésének, üzemeltetésének általános IT biztonsági követelményei a következők, jelen szabályzat fejezeteiben részletezett módon:

- minden rendszerben biztosítani kell a naplózást, legalább a rendszer által nyújtott naplózási technológiai lehetőségek határáig;
- ügyviteli rendszerek esetében a naplózáson túl biztosítani kell a kiemelt felhasználó monitoring lehetőségét;
- minden rendszerben biztosítani kell az adatok archiválását, ahol ezt az adattartalom indokolja;
- minden olyan rendszerről biztonsági mentések készítése szükséges, ahol a rendszer kritikussága, vagy az adattartalom ezt indokolja;
- minden rendszer esetén végre kell hajtani a rendszerre előírt karbantartási feladatokat;
- minden olyan rendszer esetén, amelynél a rendszer kritikussága, az adattartalom, vagy a rendszer funkcionalitása ezt indokolja sérülékenység vizsgálatokat kell lefolytatni a KIE-17 ÉS KIE-20 előírásainak megfelelően;
- a rendszereket üzemeltető felhasználók esetében be kell tartani a jogosultsági előírásokat.

Az ügyviteli informatikai eszközök IT biztonsági szempontból megfelelő működtetéséért a Számítástechnikai főmunkatárs felel, az IT biztonsági követelmények teljesülését az IBF rendszeresen ellenőrizheti, illetve külső auditok alkalmával ellenőriztetheti.

6.15.2. Ügyviteli informatikai eszközök

A Társaság alábbiakban részletezett ügyviteli informatikai eszközeit a Számítástechnikai főmunkatárs üzemelteti. Az eszközök működtetésére a következő IT biztonsági előírások vonatkoznak.

6.15.2.1. Munkaállomások

A Társaság minden ügyviteli területen dolgozó munkavállalója számára biztosít asztali munkaállomást és/vagy laptopot. A Társaság belső hálózatára csak a Számítástechnikai főmunkatárs által üzemeltetett munkaállomások csatlakoztathatók.

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 munkaállomásokra vonatkozó kontrollokat ügyviteli területen a Számítástechnikai főmunkatárs biztosítja, így a frissítések kiküldése is az ő felelőssége és feladata. A hardveres és szoftveres karbantartás, hibaelhárítás szintén a Számítástechnikai főmunkatárs felelőssége és feladata.

Alapértelmezetten az ügyviteli munkaállomásokon az optikai meghajtók és az USB portok csak olvasható (read-only) módban üzemeltethetőek. Adatok kiírására csak az IBF ajánlása alapján, az Ügyvezető által jóváhagyott titkosított adathordozók használhatóak - kizárólag indokolt esetben - a munkavégzés során.

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. Erre a célra a fájlszerver adott megosztásait kell alkalmazni. Amennyiben a lokális tárolás elkerülhetetlen, úgy biztosítani kell, hogy a számítógép háttértárolója titkosított legyen BitLocker alkalmazásával.

Biztonsági okokból tiltani kell, hogy a felhasználók a munkaállomásokon tudjanak mappát megosztani.

6.15.2.2. Szerverek

Az ügyviteli szerver üzemeltetését a Számítástechnikai főmunkatárs végzi.

A szerverekkel kapcsolatos feladatok, melyeket jelen szabályzat pontjai tartalmaznak részletesebben a következők:

- Karbantartás;
- Naplózás;
- Archiválás;
- Biztonsági mentések.

6.15.2.3. Egyéb eszközök

A Társaság egyéb ügyviteli IT erőforrásai közé sorolhatók a nyomtatók, faxok, scannerek. Ezek speciális biztonsági követelményei az alábbiak:

6.15.2.4. Nyomtatás

A Társaságnál elsősorban 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.

Bizalmas dokumentumok esetén, 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 a Számítástechnikai főmunkatársat kell értesíteni, és a nyomtatást egy másik eszközön végrehajtani; saját, otthoni eszközök használata nem megengedett.

6.15.2.5. Scannelés

A központi nyomtatók scannerként is funkcionálnak. A scannelt 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 végeztével ügyelni kell arra, hogy az eredeti dokumentumok ne maradjanak az eszközben.

6.15.2.6. Alkalmazások telepítése

A Társaság tulajdonát képező munkaállomásokra szoftverek csak adminisztrátori jogosultsággal telepíthetőek, mellyel az átlagfelhasználók nem rendelkezhetnek. A hordozható, un. portable alkalmazások használata alapértelmezetten tiltott, az ilyen szoftverek igénylési folyamata megegyezik a nem standard szoftverekével.

Az IBF a munkaállomásokra telepített alkalmazásokat évente egy alkalommal felülvizsgálja.

6.15.3. **Bejelenetkezési rendszerüzenet**

A Társaság főbb rendszerei bejelentkezést követően az alábbi üzenet kiírásával jelzik a rendszerhasználatot:

„A felhasználó a Társaság elektronikus információs rendszerét használja.

A rendszerhasználat, felhasználói aktivitás megfigyelésre, rögzítésre kerülhet.

A rendszer jogosulatlan használata tilos és büntetőjogi és/vagy polgári jogi következménnyel járhat;

A rendszer használatának megkezdése egyben a fentiek tudomásul vételt jelenti.”

6.15.4. **Az authentikáció módja**

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

6.15.4.1. Jelszókezelés

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

- minimum 10 karakter hosszúságú (rendszer kikényszeríti)
- kis- és nagybetűket, számokat és speciális karaktereket (@, &, #, stb.) tartalmaz (rendszer kikényszeríti)
- a jelszónak nem lehet része a felhasználó természetes neve, felhasználói neve, email címe
- ne legyen személyhez köthető információ (pl. név, születési dátum, kedvenc márka stb.)
- különböző rendszerekhez (kiváltképp vállalaton 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.

Elfelejtett, lezárolt jelszavak esetén, új jelszót a Számítástechnikai főmunkatárstól lehet igényelni. A jelszavakat tilos más felhasználóval megosztani, még a rendszergazdának sem adhatók át. A jelszót haladéktalanul meg kell változtatni minden olyan esetben, amikor fennáll annak gyanúja, illetve lehetősége, hogy ismertté vált, kompromittálódott.

6.15.5. Karbantartás

A biztonsági kockázatok csökkentése érdekében a Társaság mind a munkaállomások, mind a szerverek karbantartásáról rendszeresen kell, hogy gondoskodjon.

A munkaállomások (asztali számítógépek és laptopok) karbantartásáról a Számítástechnikai főmunkatárs gondoskodik, valamint az ügyviteli szerverek karbantartásáért is felel. A felhasználónak az eszközök karbantartásával kapcsolatban annyi feladata van, hogy ne akadályozza meg a szükséges frissítések telepítését, illetve kérés esetén működjön együtt a Számítástechnikai főmunkatárssal. 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.

Amennyiben a karbantartás vagy hibajavítás során az eszköz külső szervizbe történő szállítása indokolt, gondoskodni kell arról, hogy belső, bizalmas adatok ne kerüljenek vállalaton kívülre. Az informatikai eszközök szervizbe szállításáért a Számítástechnikai főmunkatárs felel

6.15.6. Naplózás

A Társaság által üzemeltetett informatikai ügyviteli rendszert naplózni kell, minden olyan rendszeren, amely ezt technológiai szempontból lehetővé teszi. A naplókat a Társaságnak 1 évig meg kell őriznie. A naplózott rendszereket, illetve a naplózás szabályait dokumentáltan rögzíteni kell.

6.15.6.1. Alapvető naplózási követelmények

A rendkívüli és a biztonságot fenyegető eseményeket eseménynaplóba kell bejegyezni és azt a bizonyíthatóság érdekében 1 évig meg kell őrizni.

- Az elszámoltathatóság és felülvizsgálhatóság érdekében a naplózási rendszert úgy kell kialakítani, hogy abból utólag megállapíthatóak legyenek az informatikai rendszerben bekövetkezett fontosabb események, különös tekintettel azokra, amelyek a rendszer biztonságát érintik. Ezáltal ellenőrizni lehet a hozzáférések jogosultságát, meg lehet állapítani a felelősséget, valamint az illetéktelen hozzáférést vagy az arra tett kísérletet.

- A naplózási rendszernek alkalmasnak kell lennie mindegyik felhasználó, vagy felhasználói csoport által végzett művelet szelektív regisztrálására. A következő eseményeket sikerességét és sikertelenségét feltétlenül naplózni kell:
    - rendszerindítások, leállítások;
    - rendszer óraállítások;
    - be és kijelentkezések;
    - programleállások;
    - az azonosítási és a hitelesítési mechanizmus használata;
    - hozzáférési jog érvényesítése azonosítóval ellátott erőforráshoz;
    - azonosítóval ellátott erőforrás létrehozása vagy törlése;
    - felhatalmazott személy műveletei, amelyek a rendszer biztonságát érintik.
- Kerüljön naplózásra a biztonságot érintő összes tevékenység az adott rendszer technológiai határain belül.
- A naplófájlok tartalmát megadott időosztással képernyőn és nyomtatón is meg lehessen jeleníteni.
- A naplóállományokat tilos megsemmisíteni, felülírni, módosítani: azokat archiválni kell.
- Rögzíteni kell a hibás bejelentkezési kísérletek számát az adott rendszer technológiai határain belül.
- Szükség van egy olyan nyilvántartásra, melyből lekérdezhető, hogy adott munkaállomáshoz | rendszerhez melyik felhasználói csoport és milyen joggal férhet hozzá; illetve egy olyan nyilvántartásra, melyből az kérdezhető le, hogy egy adott felhasználói csoport mely munkaállomáshoz | rendszerhez és milyen joggal férhet hozzá.
- A biztonsági eseménynapló (naplófájl) adatait védeni kell az illetéktelen hozzáféréstől.
- A rendszerben a biztonsági eseménynapló fájlok auditálásához szükséges eszközöknek lehetővé kell tenniük egy vagy több felhasználó tevékenységének szelektív vizsgálatát.
- Javasolt kialakítani a biztonság belső ellenőrzésének rendszerét, amely során meg kell határozni a felügyeleti és megelőzési tevékenységek eljárásrendjét.
- Az eseményrekordnak (bejegyzésnek) az adott rendszer technológiai határain belül a következő mezőket javasolt tartalmaznia:
    - felhasználónevet,
    - dátumot,
    - időpontot,
    - az esemény típusát,
    - az esemény sikerességét (sikeres, sikertelen).
    - A biztonsági naplóban a következő eseményeket kell rögzíteni:
    - rendszerindítást;
    - felhasználók be- és kijelentkezését;

- jogosultságok megváltozását felhasználóra és felhasználói csoportra vonatkozólag;
- biztonsági menedzsment rendszerre vonatkozó változásokat, beleértve a naplózási funkciókat is;
- naplózási szolgáltatás elindítását és leállítását.
- A biztonsági naplót a létrehozásától kezdve folyamatosan karban kell tartani, valamint védeni kell az illetéktelen módosítástól és törléstől, ezért ember számára olvasható formában is kell tárolni.

6.15.7. Archiválás

Az informatikai rendszerekben tárolt adatok esetén, a mindenkor hatályos adatvédelmi törvényeknek megfelelően, az archiválás végrehajtása a Számítástechnikai főmunkatárs feladata. Az archív adatokhoz csakis az Ügyvezető által kijelölt, érintett személy férhet hozzá. Az archivált anyagokat azok biztonsági besorolása szerint kell tárolni, kezelni.

Az archiválás biztonsági követelményeit, illetve az archivált anyagok megfelelő kezelését az IBF a jelen szabályzatban meghatározottak szerint, de legalább éves szinten egyszer kell, hogy ellenőrizze.

6.15.8. Adathordozók törlése

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

egyszerű törlés szükséges az alábbi esetekben:

- munkaállomások leadását követően
- 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 eltávolítható
- informatikai eszközök leselejtezését követő értékesítése, adományozása esetén

Munkaállomások, okostelefonok, tabletek és laptopok adatainak visszaállíthatatlan törlése előtt a leadott eszközökről indokolt esetben image-et kell készíteni a későbbi esetleges vizsgálatok végrehajtása céljából, ami a Számítástechnikai főmunkatárs feladata.

Az adathordozók fizikai megsemmisítését csak arra szakosodott szolgáltató végezheti az információbiztonsági felelős jelenlétében.

6.15.9. Biztonsági mentések

Biztonsági mentések készítése

A Társaságnak gondoskodnia kell az általa használt informatikai rendszerek biztonsági mentésének elkészítéséről. A biztonsági mentések készítése a Számítástechnikai főmunkatárs feladata.

A központi mentések nem terjednek ki a felhasználói munkaállomásokra, illetve mobil eszközökre. Ezen eszközökről a felhasználónak kell indokolt esetben a jelen szabályzatban foglalt biztonsági követelményeket betartva biztonsági mentést készítenie.

A központi biztonsági mentések készítését dokumentált módon, eljárásrendben vagy üzemeltetési utasításban kell rögzíteni. A mentések gyakorisága és típusa rendszerenként eltérő lehet.

A biztonsági mentések készítésével kapcsolatos általános IT biztonsági 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.

Biztonsági mentések visszaállítása

A biztonsági mentések visszaállítása a Számítástechnikai főmunkatárs feladata.

6.16. Hálózatbiztonság

A hálózatbiztonsággal kapcsolatos tevékenységeket, szabályozásokat a Társaság MGEP-SZ2021/63 Információtechnológiai (IT) üzemeltetési szabályzata tartalmazza.

6.17. WiFi hálózat használatának szabályai

A Társaság vezeték nélküli (WiFi) hálózatot biztosíthat:

- Saját belső WiFi: elsődlegesen a Társaság saját munkavállalói, másodlagosan bizonyos feltételek teljesülése esetén külsős munkavégzők részere.
- Vendég WiFi a Társaság telephelyein ideiglenesen, vagy tartósan dolgozó külső munkavégzők, partnerek számára.

6.17.1. Belső WiFi hálózatok

Belső, vezeték nélküli (WiFi) hálózat csak a Számítástechnikai főmunkatárs által létesíthető, az IBF által előírt biztonsági konfigurációt alkalmazva.

A belső, vezeték nélküli (WiFi) hálózathoz kizárólag Társasági eszközökkel lehet csatlakozni.

Technológiai rendszerek működéséhez csak abban az esetben létesíthető vezeték nélküli hálózati hozzáférés, ha az adott feladat egyéb módon nem oldható meg. Ilyen esetekben a vezeték nélküli hálózatok létesítésekor azokat belső vezeték nélküli hálózattal megegyező védelmi igényszintű hálózatként kell kezelni és annak megfelelő védelmi intézkedéseket kell megvalósítani ezen hálózatok üzemeltetése során.

Minden ilyen megoldás létesítése, módosítása kizárólag a Számítástechnikai főmunkatárs közreműködése mellett, annak biztonsági előírásait implementálva és annak jóváhagyását követően lehetséges.

Technológiai rendszerekhez létesített vezeték nélküli hozzáféréseket kizárólag a meghatározott célra, az elérhető biztonsági megoldások és intézkedések maximalizálása mellett lehet használni.

Tilos ezeket egyéb, nem a technológiához köthető célra megosztani, használni!

A belső WiFi hálózatra csatlakoztatott vállalati számítógépekkel ugyanazok belső IT erőforrások érhetőek el, mint a vezetékes hálózati csatlakozás esetében.

A belső WiFi hálózaton belül az mindenkor elérhető legmagasabb biztonsági szintű WiFi vállalati szintű biztonsági (autentikációs és titkosítási) protokollt kell alkalmazni.

A belső WiFi hálózati eszközöket rendszeresen, legalább évente javasolt ellenőrizni/ellenőriztetni kifejezetten vezetéknélküli hálózatot célzó behatolás/etikus hacking vizsgálattal.

6.17.2. Vendég WiFi

A vendég WiFi a Társaság telephelyein munkát végző egyes külsős munkavégzők számára lehet elérhető. A vendég WiFi szabadon hozzáférhető, korlátozott sávszélességű internet elérést szolgáltathat. A rá csatlakoztatott eszközökön az eszköz gazdájának felelőssége a megfelelő végpontvédelmi és biztonsági megoldások megléte és működtetése.

A Társaság semmilyen formában nem felel a vendég WiFi használatából adódó, a külsős munkavégző eszközével kapcsolatos bármely biztonsági incidensért.

A Társaság azon munkavállalóinak, akik jogosultak külső (pl. otthoni) WiFi használatára, egyes esetekben szükségük lehet a vendég WiFi hálózathoz való csatlakozásra. Ilyen esetekben értelemszerűen a külső WiFi használati szabályai érvényesek. A vendég WiFi belsős számítógépekkel való használatát kerülni kell.

A Társaság saját laptopjait, munkaállomásait és mobileszközeit tilos egyidejűleg a vendég WiFi-re és vezetékes megoldással a belső hálózatra csatlakoztatni!

Ennek betartásáról a Társaság adminisztratív és technológiai megoldásokkal is gondoskodhat.

A vendég WiFi hozzáférési adatait fél évente kell változtatni. Ennek elvégzése a Számítástechnikai főmunkatárs feladata.

6.17.3. Külső WiFi hálózathoz céges eszközökkel való csatlakozás előírásai

Külső helyszínen, vagy otthon történő munkavégzés céljából szükséges lehet külső, nem a Társaság, vagy IT Szolgálató által üzemeltetett vezeték nélküli (WiFi) hálózatok elérése. Mivel a külső vezeték nélküli hálózatok a Társaság és/vagy az IT Szolgáltató által nem kontrollálhatók, ezért használatukra szigorúbb előírások vonatkoznak.

Külső, vezeték nélküli hálózatnak tekintendők az alábbiak:

- mobil Internet (SIM, USB stick, mobil WiFi modem, mobil hotspot stb., még abban az esetben is, ha azt a Társaság bocsátja rendelkezésre),
- külső vezeték nélküli (WiFi) hálózat (otthoni vagy külső partner vállalat vendég WiFi hálózata),
- publikus vezeték nélküli hálózat (szálloda, kávézó stb. által biztosított ingyenes vagy fizetős WiFi hálózat),
- a Társaság saját vendég WiFi hálózati hozzáférése.

Munkavégzés céljából a publikus vezeték nélküli (WiFi) hálózatok használata (pl. szálloda, konferencia által biztosított) laptopok esetében kizárólag saját VPN használatával megengedett.

Publikus hálózatra csatlakozáskor a mindenkor legmagasabb biztonsági szintűnek számító WiFi biztonsági (autentikációs és titkosítási) protokollt kell alkalmazni. Amennyiben ez nem lehetséges, úgy kerülni kell az adott hálózat használatát.

Otthoni vagy mobil WiFi hálózat használata esetén fel kell hívni a munkavállalók figyelmét az eszközök megfelelő, biztonságos használat szabályaira.

A külső WiFi hálózatok csak a Társaság IT üzemeltetési szakterülete által biztonsági konfigurációval használható. A felhasználó nem kísérelheti meg a vállalati eszköz WiFi biztonsági konfigurációjának megváltoztatását. A nem szabványos (felhasználó által jogosulatlanul megváltoztatott) biztonsági konfigurációból eredő incidensekért a felhasználó felelős.

6.17.4. Egyidejű csatlakozás tilalma

A belső ügyviteli hálózatra vezetéken csatlakoztatott munkaállomásokról ezzel egyidejűleg külső hálózat felől (pl. mobil hotspot-on, elérhető-, nem a Tásasághoz tartozó külső WiFi hálózaton keresztül) VPN kapcsolatot létesíteni, vagy ezt megkísérelni tilos!

6.18. Elektronikus kommunikáció biztonsága

6.18.1. Nyilvános hálózatokon folytatott kommunikáció védelme (VPN)

A Társaság a nyilvános hálózatokon továbbított adatokat VPN megoldásokkal és Sharepoint alkalmazásával védi technológiai alapú visszaélésektől.

6.18.2. Általános titkosítási szabályok

Jelen szabályzat az elektronikus kommunikáció Társaságon belül elérhető eszközeire vonatkozóan tartalmaz előírásokat, úgy mint:

- elektronikus levelezés;
- azonnali üzenetküldő alkalmazások;
- videokonferencia;
- fájlmegosztó alkalmazások.

Ezen alkalmazások használata kizárólag az adatvédelmi és egyéb hatályos jogszabályi követelményeknek megfelelően, a Társaság előírásait és korlátozásait betartva, védelmi célú monitoring megvalósulása mellett megengedett az alábbiakban foglaltak szerint.

A jelen szabályzatban ismertetett szolgáltatások a Társasággal szerződéses jogviszonyban álló informatikai szolgáltatótól vehetők csak igénybe.

Külső, (szabadon hozzáférhető) kommunikációs megoldások (pl. alternatív üzenetküldő szolgáltatások) munkavégzés céljából való használata kizárólag az Számítástechnikai főmunkatárs vagy az IBF jóváhagyásával, a biztonsági követelmények teljesítése mellett valósulhat meg.

A Társaság az általa kezelt adatok bizalmasságát és sértetlenségét fenyegető kockázatok csökkentése érdekében kriptográfiai eszközöket alkalmazhat mind adatok tárolása, mind pedig azok továbbítása során a rendelkezésre álló technológiai lehetőségek által szabott kereteken belül, azokon a helyeken, ahol ezt az adattartalmak érzékenysége megkívánja.

Kriptográfiai megoldások alkalmazása kockázatarányosan, az elérhető technológiai megoldások képességeinek erejéig kötelező.

Technológiai (OT) rendszerek esetén speciális esetekben a kriptográfiai megoldások alkalmazása akkor is mellőzhető, ha a kriptográfiai megoldás veszélyezteti az OT rendszer működését, az adatátvitel sebességét, az adatok sértetlenségét és/vagy a rendszer rendelkezésre állását. Ilyen esetekben törekedni kell a megfelelő szintű kiegészítő/kompenzáló kontrollok alkalmazására, amennyiben erre technológiai, vagy adminisztratív stb. lehetőség rendelkezésre áll.

Kriptográfiai megoldások alkalmazása javasolt az alábbi esetekben:

- asztali munkaállomásokon, ahol a helyileg tárolt adattartalom ezt indokolja;
- hordozható számítógépen notebookon, ahol a helyileg tárolt adattartalom ezt indokolja;
- elektronikus kommunikációs csatornákon - amennyiben az adatcsomag elhagyja a Társaság területét, illetve a továbbított adattartalom ezt indokolja (elektronikus levelezés, chat, külső fájlmegosztó alkalmazások stb.),
- külső hordozható adathordókon - függetlenül attól, hogy az adathordozó elhagyja-e a Társaság területét,
- biztonsági mentések adathordozóin - függetlenül attól, hogy az adathordozó elhagyja-e a Társaság területét.

6.18.3. Elektronikus levelezés

A Társaság az elektronikus levelezési szolgáltatást csak és kizárólag munkavégzés céljából, a munkaköri leírásban rögzített feladatok hatékonyabb ellátásának érdekében biztosítja a munkavállalók, illetve szerződéses külső felek számára. Az elektronikus levelezés használatára a következő információbiztonsági szabályok vonatkoznak.

Általános alapelvek:

- A Társaság által a felhasználó rendelkezésére bocsátott e-mail cím a Társaság tulajdona. A címet és a mögötte álló levelező rendszert magán- és egyéb, a munkavégzéssel nem összefüggő célra használni tilos.
- Az elektronikus levelezés használati engedélye személyre szóló, azt (a technikai, illetve a csoportos e-mail cím kivételével) kizárólag a felhasználó saját maga veheti igénybe.
- A felhasználó saját felhasználói fiókjának, azonosítójának és jelszavának átadása más felhasználó részére tilos!
- A munkahelyi e-mail címmel magánjellegű regisztrációt tenni nem a munkavégzés céljával összeegyeztethető weboldalakon, online szolgáltatásban tilos!
- A külső levelezőrendszerek (pl. freemail.hu, gmail.com) használata munkavégzéssel összefüggő célból, szigorúan tilos!
- A Társaság által biztosított asztali és hordozható számítógépeken, mobileszközökön a társasági elektronikus levelezőkliensbe privát, külső szolgáltatók (pl. freemail.hu, gmail.com) fiókjának felcsatolása megengedett, de nem támogatott. Az ezek használatából származó károkért a felhasználó felel.
- Az incidensek kezelésének folyamatában, vagy ellenőrzési céllal
  - a felhasználó társasági eszközre felcsatolt magán elektronikus levelezésébe, vagy
  - a felhasználó társasági elektronikus levelezésébe

  a Számítástechnikai főmunkatárs vagy az IBF az Ügyvezető tájékoztatása mellett bekinthet.

Az e-mailek küldésére vonatkozó előírások:

- A feladó társasági felhasználó felelős az általa küldött e-mail tartalmáért információbiztonsági szempontból is.
- Más felhasználó nevében e-mailt küldeni tilos, kivéve a rendszerbeli meghatalmazási eljárás alkalmazásán keresztül!
- A leveleket mindig célzottan, és a munkavégzés céljához kapcsolódóan kell kiküldeni.
- Automatikus válaszüzenetek tartalmát minden esetben úgy kell meghatározni, hogy a benne megadott információkkal az értesített fél ne tudjon visszaélni.
- A vállalat levelezőrendszerében tiltott a kéretlen levelek („spam”), valamint az indokolatlan mértékű, munkavégzéssel össze nem függő tartalmak küldése.

- Nagyméretű fájlok küldése esetén, az informatikai szolgáltató által biztosított fájlküldő megoldás használata szükséges (amennyiben az rendelkezésre áll). Külső forrásból elérhető, hasonló jellegű oldalakra (pl. mammutmail, wetransfer), illetve fájlmegosztó portálokra (pl. Dropbox, GoogleDrive) társasági adatok feltöltése az Ügyvezető és/vagy a Számítástechnikai főmunkatárs és/vagy az IBF engedélyéhez és felelősségi köréhez kötődik.
- A bizalmas, érzékeny adatokat, információkat tartalmazó anyagokat minden esetben csak titkosítva lehet elküldeni:
    - Titkosításra képes alkalmazással (pl. 7Zip-pel) tömörítve és titkosítva, majd a levél csatolmányaként elküldve. A titkosítást a lehető legerősebb titkosítási algoritmussal kell végezni (pl. AES-256).
    - A levelező rendszer által támogatott, beépített titkosítása protokollok alkalmazásával (S/MIME, PGP stb.), amennyiben ez elérhető, vagy
    - Mindkét esetben figyelni rá, hogy a feloldáshoz szükséges jelszót, vagy a kulcsokat külön csatornán kell elküldeni.
- Minden email felhasználó köteles a Társaságtól kifelé menő leveleinél e-mail aláírást használni.

Az e-mailek fogadására vonatkozó irányelvek:

- Bizalmas információk továbbítását kérő elektronikus levelek esetében, mindig meg kell győződni az információkérés hitelességéről.
- **Ismeretlen, gyanús (potenciálisan veszélyt jelentő) feladótól érkezett csatolmányok, linkek megnyitása tilos!** Kérdéses tartalmak megnyitása esetén a felhasználónak azonnal a Számítástechnikai főmunkatárshoz 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 azt. Az abban lévő tartalmak, információk, adatok jogtalan megismerése és kezelése tilos!
- Külső vagy látszólag belső e-mail címről érkező, félrevezető tartalmú, feltehetően ártó szándékú e-mailek esetén azonnal jelenteni kell az eseményt a Számítástechnikai főmunkatársnak.

6.18.4. Távoli elérés szabályai

6.18.4.1. Távoli hozzáférés engedélyezése

A folyamatosan vagy ideiglenesen külső helyszínen dolgozó munkavállalók, munkavégzők számára a Társaság távoli hozzáférési megoldást biztosít. A távoli elérés az alábbi feltételek teljesülése esetén engedélyezhető:

- állandó munkaviszonnyal rendelkező munkavállalónak,
- határozott idejű munkaviszonnyal rendelkező munkavállaló esetében a munkavégzés időtartamára,
- próbaidő letöltését követően,

A távoli VPN hozzáféréssel rendelkező felhasználók jogosultsági megegyeznek a belső hálózati jogosultságokkal. Minden olyan belső erőforrást, megfelelő jogosultsággal elérnek, amelyekhez egyébként hozzáférési jogosultsággal rendelkeznek.

Távoli hozzáféréshez alapértelmezetten minden helyi hálózati hozzáréssel rendelkező felhasználó jogosult.

6.18.4.2. Távoli hozzáférés (VPN) technológiai előírásai

A Társaság belső ügyviteli hálózatához csatlakozni külső hálózatról kizárólag VPN kapcsolaton keresztül lehetséges a Társaság által előírt VPN megoldásokkal és konfigurációs beállításokkal.

Tilos a VPN hozzáférés

- beállításainak megváltoztatása és/vagy
- VPN hozzáférés önálló telepítése saját (nem a Társaság tulajdonában lévő) eszközön a Számítástechnikai főmunkatárs és/vagy az IBF külön engedélye nélkül.

Saját eszközre Társasági VPN-t kizárólag a Számítástechnikai főmunkatárs telepíthet.

A belső hálózatra csatlakoztatott munkaállomásokról egyidejűleg külső hálózat felől (pl. mobil hotspot-on, elérhető-, nem a Társasághoz tartozó külső WiFi hálózaton keresztül) VPN kapcsolatot létesíteni, vagy ezt megkísérelni tilos!

6.18.5. Internet használat

A Társaság a társasági informatika infrastruktúra által biztosított internet használatot elsősorban munkavégzés céljából, a munkaköri feladatok hatékonyabb ellátásának érdekében biztosítja. **A szolgáltatás magáncélra és egyéb, a munkavégzéssel nem összefüggő célokra történő felhasználása a Társaság által nem támogatott**.

Az Internet használat során betartandó információbiztonsági előírások:

- A felhasználói internet használati engedély személyre szóló, azt kizárólag a felhasználó saját maga veheti igénybe.
- A kliens számítógépen proxy, és egyéb anonimizálásra szolgáló alkalmazások (Pl. Tor Browser) futtatása tilos!
- A felhasználó internet-hozzáférésének más felhasználók részére nem központi módon történő megosztása vagy továbbszolgáltatása (a mobiltelefonok személyes AP szolgáltatása kivételével) tilos!
- A hálózati sávszélesség és erőforrások szükségesnél nagyobb, túlzott mértékű foglalása (pl. nagyméretű állományok indokolatlan letöltése, online video/audio folyamok háttérben futtatása) kerülendő.
- A munkatársaknak tilos az Internetről szoftverek (pl. „portable” alkalmazások) letöltése, futtatása. Amennyiben a felhasználónak a munka végzéséhez valamilyen speciális szoftver használata indokolt, azt a Számítástechnikai főmunkatársnak kell jeleznie.
- Tilos a gyanús (potenciálisan veszélyt jelentő) tartalmakra kattintás, nem ismert funkcióval bíró, felugró ablakok engedélyezése!
- Az Internet használat szabályainak tudatos megsértéséből származó károkért a felhasználó szankcionálható.

6.18.6. Azonnali üzenetküldő alkalmazások

A Társaságon belüli a O365 Teams alkalmazásának használata, az azonnali üzenetküldési szolgáltatás használata támogatott. Más külső forrásból elérhető szolgáltatás (pl. Viber, Facebook messenger, stb.) igénybevétele munkavégzéshez nem engedélyezett.

6.18.1. Videokonferencia

Munkavégzéssel összefüggő videokonferencia hívások lebonyolítására kizárólag a Társaság által biztosított eszközök használhatóak a támogatott azonnali üzenetküldő alkalmazások lehetőségei mellett. Társasági szinten videokonferencia hívásokhoz a Microsoft Teams használata preferált.

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

6.18.2. Külső fájlmegosztó alkalmazások használatának szabályai

A külső fájlmegosztó alkalmazások (pl. DropBox, Google Drive, MammutMail) használata munkavégzéssel összefüggő célra, a Számítástechnikai főmunkatárs és/vagy az IBF jóváhagyásával lehetséges. A hozzájárulást

- egyszeri, időszakos, vagy folyamatos használatra,
- kizárólag és dedikáltan adott célhoz rendelve,
- a regisztrációs adatokat nyilvántartásba véve engedélyezheti.

A fiók kizárólag a meghatározott munkavégzési célra használható, azt magánjellegű, vagy nem szorosan a munkával összefüggő célra használni nem megengedett.

Magán fiók munkavégzési célra nem használható.

Az MVM Csoport tagjai, valamint egyes szerződött beszállítók, szolgáltatók által biztosított fájlmegosztó megoldások (Pl. Sharepoint) támogatottak és az általános IT biztonsági előírások betartásával használhatóak.

6.19. Alkalmazott kriptográfiai eszközök, megoldások

6.19.1. Kriptográfiai kulcsok kezelése

A Társaság által alkalmazott titkosítási megoldások kulcskezelése az alkalmazásokban integráltan, illetve külső alkalmazások használatával valósul meg (pl. KeePass), minden esetben és helyen, ahol kulcskezelés szükséges. A kulcskezelést a Számítástechnikai főmunkatárs végzi.

6.19.2. Teljes merevlemez titkosítás

A felhasználóknak kiadott hordozható és asztali számítógépek összes adattárolóját titkosítani javasolt mindenhol, ahol a helyileg tárolt adattartalom ezt indokolja. Javasolt a BitLocker használata.

- Technológiai (OT) rendszerek esetében törekedni kell az adattartalom titkosítására, ahol a helyileg tárolt adattartalom ezt indokolja.
- A teljes merevlemez titkosítás telepítése a Számítástechnikai főmunkatárs feladata.
- A teljes merevlemez titkosítás helyreállítási kulcsait a Számítástechnikai főmunkatárs tárolja, biztonságos, titkosított és mentett adatbázisban (pl. KeePass).
- A központilag alkalmazott rendszertől eltérő titkosítása megoldás ügyviteli (IT) rendszerek esetén a Számítástechnikai főmunkatárs és/vagy az IBF jóváhagyásával alkalmazható.

6.19.3. Hordozható adattárolók titkosítása

Amennyiben érzékeny adatot a vállalaton belül, vállalaton kívüli helyszínre, vagy külsős félnek szükséges továbbítani, és a továbbítás módja más, ellenőrizhető és biztonságos módon nem megoldható, olyan titkosított hordozható adattároló alkalmazása szükséges, melyet a Számítástechnikai főmunkatárs vagy az IBF jóváhagyott. Amennyiben a titkosítás megvalósítása nem lehetséges, megfelelő kompenzáló kontrollok alkalmazása szükséges (pl. mentési adattárolók szállítása esetén).

A titkosítatlan adathordozókon tárolt érzékeny vállalati adatok kompromittálódásáért az eszközt használó munkavállaló felel.

6.19.4. Fájltitkosító alkalmazások használata

Harmadik felekkel történő, érzékeny adattartalmat érintő fájlcsere esetén az adatok elektronikusan csak titkosított formában, vagy titkosított csatornán adhatók.

Ettől eltérni csak a Számítástechnikai főmunkatárs és/vagy az IBF jóváhagyását követően lehet. A fájltitkosító megoldás telepítését, karbantartását, valamint a felhasználók támogatását a Számítástechnikai főmunkatárs végzi. A megfelelő megoldás kiválasztása a Számítástechnikai főmunkatárs és/vagy az IBF felelőssége, az alkalmazás telepítését és karbantartását a Számítástechnikai főmunkatárs végzi.

A titkosítás elmulasztásából adódó károkért a felhasználó felelősségre vonható.

A titkosítani kívánt csatolmányok jelszavas tömörítésekor javasolt a minél „erősebb” (min. 12 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 küldjék ugyanazon csatornán a kulcsot, mint amelyen a titkosított adattartalom került elküldésre.

6.20. Nyilvános információk közzétételének szabályai

A Társaság a nyilvános információkat zárt folyamatban teszi közzé, amelyet külön ***Nyilvános adat közzétételi eljárásban*** szabályozza.

6.21. Általános naplózási előírások

6.21.1. A naplógyűjtésbe és elemzésbe való bevonás általános szabályai

A Társaság minden informatikai rendszerén naplógyűjtést és elemzést kell működtetni, illetve minden olyan rendszert be kell vonni, amelyek esetében:

- erre technológiai lehetőség van, illetve
- a rendszer kritikussága ezt indokolja.

6.21.2. A naplózás általános biztonsági követelményei

- A biztonsági eseményre utaló naplóbejegyzéseket naplókat rendszeresen, de legalább havonta egy alkalommal ellenőrizni kell.
- Gondoskodni kell a naplók rendszeres archiválásáról.
- A biztonsági eseménynaplókat védeni kell az illetéktelen hozzáféréstől, módosítástól, részleges, vagy teljes törléstől.
- Tilos megkísérelni a naplóállományok megsemmisítését, felülírását, módosítását.

A fentiekért a Számítástechnikai főmunkatárs felelős.

6.21.3. Naplóforrások bevonásának szabályai

A naplózásba bevonandó/bevonható rendszerek alábbi naplótípusait kell bevonni a naplógyűjtési és elemzési folyamatba:

- **Tranzakcionális naplók:** az adott rendszerben végzett tranzakciók visszakövetéséhez szükséges események és tranzakcionális hibák visszakereshetőségéhez szükséges naplók;
- **Üzemeltetési naplók:** az üzemeltetési tevékenységeket, üzemeltetési eseményeket és hibákat rögzítő naplók;
- **Biztonsági naplók:** a biztonsági eseményeket rögzítő naplók;

Az elszámoltathatóság és visszakereshetőség érdekében törekedni kell olyan naplózási rend és rendszer kialakítására, hogy a lehető legszélesebb körben legyenek vizsgálhatóak az informatikai rendszerben bekövetkezett fontosabb események, különös tekintettel azokra, amelyek a rendszer biztonságát érintik.

6.21.4. A naplók elemzésének alapelvei

- Javasolt a naplók rendszeres elemzése a biztonsági és egyéb események felderítése, megelőzése érdekében.
- A biztonsági eseménynaplók vizsgálatához és elemzéséhez szükséges eszközöknek lehetővé kell tenniük egy vagy több felhasználó tevékenységének szelektív vizsgálatát.

6.21.5. Rendszernaplózás és monitoring

A Társaság rendszerei naplóinak gyűjtését az IT Szolgáltató végzi, aki alapvetően a naplók gyűjtéséért felel.

6.21.6. Naplógyűjtő rendszer üzemeltetése

A Társaságnak nincs dedikált naplógyűjtő és elemző célrendszere. A naplók gyűjtése a helyi On Premise rendszerekben, illetve Microsoft Azure Office 365 rendszerben történik. A helyi rendszerekben a naplógyűjtés Windows operációs rendszerek eseménynaplóiba történik.

6.21.7. Naplóbejegyzések védelme

A keletkező naplóbejegyzések védelméről a Számítástechnikai főmunkatárs gondoskodik az üzemeltetési környezetben elérhető technológiai lehetőségek határain belül.

6.21.8. Általános naplózási tartalmi követelmények

- Törekedni kell
    - a biztonságot érintő összes tevékenység naplózására,
    - a rendszerek működését rögzítő fő események naplózására,
    - a célrendszerek tranzakcionális és egyéb belső eseményeinek naplózására.
- Rögzíteni javasolt a jelszócserék fő információit.
- Egy naplóbejegyzésnek legalább a következő mezőket javasolt tartalmaznia:
    - felhasználónév,
    - dátum & időpont,
    - az esemény típusa,
    - rendszer azonosítója,
    - naplóbejegyzés típusa/jellege (rendszer, OS, applikáció, adatbázis, biztonsági, célrendszer tranzakció stb.),
    - az esemény sikeressége (sikeres, sikertelen, amennyiben ez értelmezhető),
    - rendszerindítás és leállítás (ahol értelmezhető),

- felhasználók be- és kijelentkezése,
- jogosultságok megváltozása felhasználóra, felhasználói csoportra stb.,
- a naplózási és biztonsági menedzsment rendszerre vonatkozó változásokat, beleértve a naplózási funkciókat is,
- naplózási szolgáltatás elindítását és leállítását,
- rendszerhibák és korrekciós intézkedések,
- programindítások és leállások, leállítások,
- azonosítási és hitelesítési mechanizmus használata,
- hozzáférési jog érvényesítése azonosítóval ellátott erőforráshoz,
- adatállományok és kimeneti adatok kezelésének visszaigazolása,
- azonosítóval ellátott erőforrás létrehozása vagy törlése,
- felhatalmazott fiókok műveletei, amelyek a rendszer biztonságát érintik.

A fentieket az üzemeltetési környezetben, illetve a célrendszerben elérhető technológiai lehetőségek határain belül kell alkalmazni.

6.21.9. Kiemelt jogosultságú felhasználók tevékenységéről szóló naplók

A kiemelt jogosultságú felhasználók tevékenységéről keletkező naplóbejegyzéseket lehetőség szerint olyan jogosultságokkal kell védeni, hogy azokon a naplózott felhasználók semmilyen módosítást, részleges-, vagy teljes törlést ne tudjanak végezni, azokhoz legfeljebb olvasási joggal férhessenek hozzá.

A kiemelt jogosultsággal rendelkező felhasználók tevékenységét, illetve az erről készült naplóbejegyzéseket az IBF, illetve az Ügyvezető külön értesítés nélkül jogosult bármikor elemezni, ellenőrizni. A Számítástechnikai főmunkatárs az ellenőrzésben köteles teljes körűen együttműködni.

A fentieket az üzemeltetési környezetben, illetve a célrendszerben elérhető technológiai lehetőségek határain belül kell alkalmazni.

6.21.1. Központi időszinkronizálás

Az IT Szolgáltató felelőssége, hogy az IT infrastruktúra minden általa üzemeltetett eleme egyetlen központi forráshoz szinkronizálja a rendszeridőt.

6.22. Mobil eszközök használata

A Társaság a felhasználók munkavégzésének könnyítése és rugalmasabbá, hatékonyabbá tétele érdekében mobil informatikai és kommunikációs eszközöket biztosít. Munkavégzési célra kizárólag társasági tulajdonban álló eszköz biztosítható, melyen elsősorban a munkavégzéshez szükséges, vagy szervesen ahhoz tartozó adatok tárolhatók, kezelhetők.

Amennyiben a munkavállaló magánjellegű adatokat tárolna a mobil eszközön, azok kompromittálódása, elvesztése esetén semmilyen kártérítési igénnyel nem élhet, a társasági eszközön tárolt privát jellegű adatokért a Társaság semmilyen felelősséget nem vállal.

Jelen szabályzat érvényes a Társaság által a felhasználók részére, munkavégzés céljából biztosított minden hordozható számítógépre, 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 alábbiakban az egyes mobil eszközök használatára vonatkozó előírások kerülnek rögzítésre eszköz típusonkénti bontásban.

6.22.1. Notebook használatával kapcsolatos információbiztonsági követelmények

Kiadás

- Az eszközök belépéskori átvételéről, illetve kilépéskori leadásáról a felhasználónak a megfelelő jóváhagyásokkal kell rendelkeznie. Az eszköz az állománybavételi bizonylat aláírásával kerül a felhasználó nevére.
- A felhasználók a Társaság hálózatához (társasági domain-hez) távolról csakis VPN megoldás alkalmazásával csatlakozhatnak a **Távoli elérés** pontban meghatározottak szerint, ennek hiányában a hálózati alkalmazások nem érhetők el.

Használat

- A notebookok használatának felhasználókra vonatkozó szabályai a jelen pontban foglalt kiegészítésekkel megegyeznek a munkaállomások általános használati szabályaival.
- A Társaság tulajdonát képező notebookokat a munkavállaló saját felelősségére magával viheti, vagy a munkaidő lejártával bent hagyhatja a társasági telephelyen (objektumban)a következő feltételekkel:
- Munkaidőn kívül a notebookokat kikapcsolt állapotban, elzártan (pl. zárt szekrényben vagy bezárt irodában) kell elhelyezni.
- A notebookok őrizetlenül hagyása még zárt autóban is kerülendő. Amennyiben ez nem megoldható, az eszközt nem látható, nehezen elérhető helyre kell helyezni. Az autóban őrizetlenül hagyott eszköz ellopása esetén a felelősség és a kár megtérítése a munkavállalót terheli.
- A notebookot a lakhelyétől eltérő helyszínen (pl. szálloda, konferencia helyszíne) csak harmadik fél számára hozzá nem férhető, biztonsági zárral ellátott helyen elhelyezve és kikapcsolt állapotban lehet őrizetlenül hagyni.
- Külföldi kiküldetés esetén a munkavállaló által kivinni kívánt eszközöket, illetve adatokat az IBF-el egyeztetni szükséges, indokolt esetben (pl. EU-n, vagy NATO tagállamon kívüli országba történő utazás során) az információbiztonsági felelős által meghatározott, az Ügyvezető által jóváhagyott 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 szankcionálható.

Karbantartás

- A Társaság által biztosított eszközökön a felhasználónak karbantartási feladata nincsen, a szükséges hardveres és szoftveres karbantartást a Számítástechnikai főmunkatárs végzi.
- Az eszköz használója a berendezés meghibásodását, rendellenes működését minden esetben jelenteni köteles a Számítástechnikai főmunkatárs felé, aki megkísérli a javítást, ha ez nem sikerül, továbbítja a külső szervíz felé. Az átadásról átadás-átvételi nyilatkozatot kell készíteni. Amennyiben a meghibásodás az eszköz nem rendeltetésszerű használatából fakad, a felhasználó szankcionálható.

Leadás, rendszerből való kivonás

- A munkavállaló kilépési szándéka esetén az erre illetékes munkatárs ellenőrzi, hogy a kilépő munkavállalónak milyen eszközöket szükséges visszaszolgáltatnia és erről értesíti a munkavállalót, a Számítástechnikai főmunkatárs pedig ellenőrizheti, hogy a kilépő felhasználó esetében szükség van-e információbiztonsági ellenőrzésre, felmerült-e valamilyen információbiztonsági incidens gyanúja. Az ellenőrzés során, az eszköz háttértáráról vizsgálati másolat készíthető.

- Ezután az eszköz egy másik felhasználó nevére kerül egy névről-névre átadási bizonylat alapján, amit mind az átadó, mind az átvevő aláír.
- A leadott eszközt - amennyiben biztonsági incidens gyanúja nem merült fel - a Számítástechnikai főmunkatárs alaphelyzetbe állítja (helyreállíthatatlan adattörlést követően újra telepíti az operációs rendszert, majd érvényesíti az aktuális beállításokat).
- Leselejtezett eszközök esetében - munkavállalói értékesítés előtt is - mindenképpen szükséges az eszközön levő adatok visszaállíthatatlan törlése és az eszköz részleges alaphelyzetbe állítása (gyári előtelepített operációs rendszer újra telepítése).

6.22.2. Hordozható adattárolók kezelésének információbiztonsági szabályai

A Társaság munkavállalóinak lehetőségük van hordozható adattárolók, USB, vagy egyéb engedélyezett interfészen keresztül csatlakoztatott adathordozók (pl. pendrive, külső merevlemez, memóriakártya) használatára, amennyiben adatot a Társaságon kívüli helyszínre, vagy külső félnek szükséges továbbítani.

Munkavégzés céljából csak a Társaság által biztosított, a következő IT biztonsági feltételeket teljesítő titkosított, vagy titkosítható adathordozók használhatók:

- az eszköz az alkalmazott végpontvédelmi rendszerrel, illetve egyéb vírusvédelmi megoldásokkal képes legyen együttműködni,
- az adathordozó egyedileg beazonosítható legyen,
- az eszköz szoftveres (pl. Bitlocker), hardveres vagy kombinált titkosítást biztosítson,
- a titkosítás legalább AES 256 bit-es legyen,
- kikényszeríthető legyen a társasági jelszóelőírásoknak megfelelő jelszó,
- számkódos eszköz esetén legalább 6 karakteres kódot kérjen az eszköz.

Valamennyi felhasználónak törekednie kell dedikált, személyhez rendelt USB adathordozó használatára. A dedikált USB eszköz a Társaság tulajdonát kell képezze. Az eszközzel kapcsolatos IT biztonsági 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.

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

Kiadás

- Ügyviteli és technológiai rendszerek esetében adattároló eszközt igényelni az adott terület vezetőjén keresztül, az Ügyvezető jóváhagyásával lehetséges.
- Dedikált USB adattároló eszközt próbaidős munkavállaló csak a közvetlen munkahelyi vezetője és az Ügyvezető jóváhagyásával kaphat.

Használat

- Amennyiben az eszköz kóddal vagy jelszóval rendelkezik, be kell tartani a 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.
- A Társaság által biztosított hordozható eszközökön semmilyen illegális szoftver vagy fájl (pl. zene, kép, film stb.) nem tárolható, törekedni kell továbbá a magáncélú használat minimalizálására.

- A Társaság által biztosított hordozható eszközök eltulajdonítása, rongálódása esetén a munkavállaló 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 Számítástechnikai főmunkatársnak, aki gondoskodik a megsemmisítésről.
- A leselejtezendő, használaton kívüli vagy javítható módon meghibásodott adathordozó eszközökről az adatokat nem visszaállítható módon kell törölni. A speciális törlést a Számítástechnikai főmunkatárs végzi.
- Állandó használatú eszköz a munkavállaló kilépésekor történő átadást a névről névre átadás-átvételi bizonylaton kell igazolni.
- Amennyiben incidens gyanúja merül fel, az eszköz a felhasználó általi törlés előtt lefoglalható a Számítástechnikai főmunkatárs által.

6.22.3. Mobiltelefon, okostelefon, tablet használatának információbiztonsági szabályai

A Társaság munkavállalói részére biztosíthat mobil-, illetve okostelefonokat, valamint tableteket, amennyiben munkavégzésükhöz ilyen jellegű eszközök szükségesek. A Társaságnak adminisztratív módon kell kikényszerítenie a mobil eszközök biztonságos használatát.

A társasági elektronikus levelezés, illetve társasági alkalmazások és a belső hálózat elérését biztosító WiFi hálózat csak a Társaság által biztosított eszközön állítható be. A jelen fejezetbe sorolt mobil eszközök és a szerverek közötti adatkommunikáció kizárólag biztonságos, titkosított csatornán történhet. A társasági belső hálózatra 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

- A készülék és SIM kártya kiadását az Ügyvezető engedélyezi és a Számítástechnikai főmunkatárs hajtja végre.
- A felhasználó számára kiadott eszközökről a Társaság naprakész nyilvántartást vezet, az átadás-átvételről jegyzőkönyv kell készüljön.
- Az eszközön tárolt adatokhoz történő jogosulatlan hozzáférés megakadályozása céljából a társasági adatok elérését biztosító domain autentikáción túl a mobil eszközök további hozzáférési védelemmel - legalább egy 4 számjegyű kód megadásának kikényszerítésével - kell, hogy kerüljenek ellátásra.

Használat

- A felhasználó felelőssége, hogy az eszközön megfelelően megválasztott számzár-kódot, illetve lehetőség szerint ujjlenyomat vagy egyéb biometrikus azonosítást állítson be. Az alkalmazott kódra vonatkozó információbiztonsági követelmények a következők:
  - nem lehet egyszerű, egymás után következő, illetve ismétlődő számsorozat (pl. 0000, 1234)
  - ne legyen szorosan a felhasználó személyéhez kapcsolódó szám (pl. születési dátum)
  - amennyiben lehetséges, válasszunk minél hosszabb számzárkódot
  - kerüljük a számzárkód felírását, különösképpen könnyen hozzáférhető helyen való tárolását.

- 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).
- Az okostelefonokon és tableteken is érvényesek az alkalmazások telepítésére, illetve az elektronikus levelezés szabályaira vonatkozó előírások.
- 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 Számítástechnikai főmunkatárs tudja elkészíteni a mentést, illetve a visszatöltést.
- A készüléket tilos nyilvános helyen felügyelet nélkül, látható helyen hagyni, növelve az eltulajdonítás kockázatát.
- Be kell állítani, hogy harminc (30) másodperc tétlenséget követően a mobil készülékek képernyőjének zárolása automatikusan megtörténjen.
- Készülék eltulajdonítása esetén haladéktalanul – a rendelkezésre álló lehetőségekhez mérten – értesíteni kell az IBF-et.
- A készülék elvesztésének bejelentését követően, azonnali jelszóváltoztatás szükséges a felhasználó által. Távolról azonnal letiltja a jelentett készüléket és távolról törli a társasági konténer tartalmát/visszaállítja a gyári beállításokat. Mivel az eszköz nyomkövetése a beazonosíthatóság érdekében engedélyezett, a bejelentést követően előzetesen megkísérlésre kerül az eszköz lokációjának azonosítása.
- Az eszközök elvesztése, eltulajdonítása, rongálódása esetén a munkavállaló 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 átadaása a névről-névre átadási bizonylat aláírásával történik.
- A leadott készüléket a Társaságnál az erre kijelölt munkatárs veszi át a felhasználótól vagy az illetékes szakterülettől, aki gondoskodik 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 az IBF-nek, sem a Számítástechnikai főmunkatársnak 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 semmilyen felelősséget nem vállal.
- Amennyiben incidens gyanúja merül fel, az eszköz vizsgálatát a visszaállíthatatlan törlés előtt az Ügyvezető rendelheti el.

A mobiltelefon és mobilinternet használattal kapcsolatos további szabályokat a KIE-20 M-04 melléklete tartalmazza.

6.23. Incidenskezelés

Informatikai biztonsági 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.).

Ide sorolhatók azon események vagy incidensek is, melyek nem sorolhatók be egyértelműen az informatikai biztonsági esemény/incidens kategóriába (pl. bizalmas dokumentumok elvesztése, kompromittálódása, személyes adatok kezelésére vonatkozó szabályok megsértése, stb.).

A Társaság minden munkavállalójának és külső partnerének kötelessége az általa tapasztalt biztonsági eseményt, vagy általa feltárt biztonsági sebezhetőséget haladéktalanul jelenteni a Számítástechnikai főmunkatársnak és/vagy az IBF-nek.

Az esemény/incidens fogadását, rögzítését és előzetes értékelést az esemény/incidens típusától függően a fogadó szakterület illetékes munkatársa végzi, de az illetékes szakterületi vezető a felelős a megvalósulásért.

A bejelentést fogadó kiértékeli és amennyiben rendkívüli eseményként, vagy incidenskét azonosítja, úgy az dokumentált formában rögzíti Az dokumentációs forma lehet:

a) e-mail
b) jegyzőkönyv
c) hangjegyzet (személyes vagy telefonos bejelentés esetén, amennyiben lehetséges)

A dokumentált bejelentésnek az alábbi információkat minden esetben tartalmaznia kell (nem ismert információk esetén „nincs adat” jelölés alkalmazandó):

a) Bejelentő adatai: neve, elsődleges munkáltatója, beosztása, elérhetőségei.
b) Esemény/incidens adatai: körülmények leírása, pontos időpont, helyszín, kiváltó ok, várható hatás/következmény, várható lefolyás, megtett intézkedések, értesítettek köre.
c) Bejelentést fogadó adatai: neve, elsődleges munkáltatója, beosztása, elérhetősége.

Az incidens jelentésének elmulasztása az incidens jellegétől és mértékétől függően szankcionálható. Információbiztonsági követelmények megszegésének eseteit és azok szankcióit a jelen szabályzat 5. sz. melléklete tartalmazza. Amennyiben a felhasználó nem jelenti az általa észlelt incidenst, és emiatt a Társaságot kár éri, a munkavállaló felelősségre vonható.

Bűncselekmények, illetve egyéb, hatóságok felé jelentésköteles események azonosítása esetén a hatóságokkal való kapcsolatfelvétel az Ügyvezető feladata.

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

Az események/incidensek elhárításával párhuzamosan megkezdődhet azok kivizsgálása. Amennyiben szükséges, elsőként el kell határolni az érintett eszközöket, mely lehetővé teszi a bizonyítékok eredeti állapotban történő konzerválását és begyűjtését.

Az elhatárolásért és a bizonyítékok összegyűjtéséért az esemény/incidens típusától függően az illetékes szakterületi vezető felel. A bizonyítékgyűjtés az esemény/incidens kezeléséért felelős illetékes szakterület munkatársainak feladata. A bizonyítékok gyűjtésére a Társaság IBF-e, illetve a vizsgálatba bevont egyéb felek (informatikai és biztonsági szolgáltató) is jogosultak.

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

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

Az incidens kivizsgálása során gyűjtött bizonyítékokat jegyzőkönyvben rögzíteni kell.

Az incidensek kivizsgálásának eredményét, a meghozott és végrehajtott intézkedéseket dokumentálni, jelentésben rögzíteni szükséges. A vizsgálat lezárásának tényét a vonatkozó jelentésben az Ügyvezető aláírásával igazolja.

Az incidens elhárításáról írásban (pl. e-mail) tájékoztatni kell az elhárításban, illetve kivizsgálásban résztvevőket, valamint az érintett munkatársakat.

Az IT biztonsági eseményekről és incidensekről társasági szinten rendszeres nyilvántartást kell vezetni. A Társaságot érintő incidensekről az Ügyvezető számára elemzés készül az alábbi szempontok alapján:

- gyakoriság, ismétlődés
- kárkövetkezmény, okozott hatás
- érintett erőforrások
- 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

Amennyiben az IT biztonsági 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.

6.24. Audit, felülvizsgálat

Az auditok, felülvizsgálatok célja, hogy a Társaság, továbbá az MVM Zrt. Csoportszintű Biztonsági Igazgatósága meggyőződhessen arról, hogy a szükséges kontrollok kialakítása megtörtént, a bevezetett védelmi intézkedések megfelelően működnek, az új kockázatok azonosíthatóak-e. Ezek feltárásának módjai az információbiztonsági auditok lefolytatása, valamint különböző sérülékenység vizsgálatok megvalósítása.

A Társaság információbiztonsági audit és felülvizsgálati feladatait, módszereit az MVM ajánlása alapján kell alkalmazni.

Az auditokon túl az MVM Services Zrt. Információbiztonsági és Kríziskezelési Osztály felé információbiztonsági adatszolgáltatási kötelezettsége áll fenn a Társaságnak. Adatszolgáltatási kötelezettség függetlenül attól fennáll, hogy a Társaságnál biztonsági audit kitűzésre került-e. Az adatszolgáltatás határidőre történő megküldése az IBF feladata és felelőssége.

A csoportszintű információbiztonsági auditok hatókörét, kiterjedését az MVM Zrt. csoportszintű szabályzó dokumentumai tartalmazzák. Az auditok az ügyviteli és a technológiai rendszerekre egyaránt kiterjednek, az audit célja és hatóköre szerinti meghatározásban.

7. INFOKOMMUNIKÁCIÓS ALAPELVEK ÉS KÖVETELMÉNYEK

7.1. Informatikai fejlesztések és szolgáltatások igénybevételének egységes alapelvei

A Társaság köteles csatlakozni a Csoportszintű IT Szolgáltatási Keretszerződéshez az üzleti informatikai szolgáltatóval (MVMI Zrt.) kötendő Csatlakozási Megállapodással, amennyiben az nem ütközik a Társaság Alapító Okiratában, vagy a vonatkozó jogszabályokban foglaltakkal, valamint a tulajdonosi szándékkal.

A Társaság köteles a csoportszintű üzleti informatikai szolgáltatások teljes lemondása esetén az üzleti informatikai szolgáltató és az informatika funkcionális terület bevonásával egyeztetni a szolgáltatás létrehozása érdekében felmerült ráfordítások kompenzálásáról, amennyiben azok a gazdasági élettartam lejárta előtt kerülnek lemondásra.

A tagvállalat és az üzleti informatikai szolgáltató közötti üzleti IT szolgáltatásokkal kapcsolatos viták rendezése ügyében döntéssel az informatikai funkcionális területi vezető (MVM Zrt. DIG) rendelkezik.

A Társaság köteles az üzemviteli informatikai eszközök és rendszerek, az üzemviteli szoftverlicencek esetén az informatika funkcionális területet rendszeresen, illetve a beszerzések indítása előtt, valamint végrehajtásról tájékoztatni.

A Társaság köteles adatot szolgáltatni az informatika funkcionális terület részére az üzleti és az üzemviteli informatikai témák - üzleti és az üzemviteli informatikai környezetükről, beszerzési és fejlesztési éves tervükről (Digitális Kormányzati Ügynökség Zrt. - DKÜ), az igénybe vett informatikai szolgáltatásaikról.

A Társaság köteles évente minimum egy alkalommal IT eszköz és IT szolgáltatás auditot lefolytatni.

Az üzleti informatikai szolgáltató által biztosított üzleti IT eszközök és szolgáltatások tekintetében az audit támogatására a Társaság köteles az üzleti informatikai szolgáltató (MVMI Zrt.) által biztosított audit megoldást (eVK) használni.

7.2. Ügyviteli célú elektronikus hírközlési szolgáltatások igénybevételének alapelvei

A Társaságok köteles csatlakozni a Csoportszintű Elektronikus Hírközlési Szolgáltatási Keretszerződéshez a csoporton belüli ügyviteli elektronikus hírközlési szolgáltatóval (MVM NET Zrt.) kötendő Egyedi Szolgáltatási Szerződéssel a KIE-20-M-02 melléklet 1.4. pont rendelkezéseivel összhangban, valamint a Csoportszintű Előfizetői Flotta Mobiltelefon Szolgáltatási Keretszerződéshez a csoporton kívüli szolgáltató céggel kötendő Egyedi Szolgáltatási Szerződéssel, amennyiben az nem ütközik a Társaság működési engedélyében (Alapító Okiratában), vagy a vonatkozó jogszabályokban foglaltakkal, valamint a tulajdonosi szándékkal.

A Társaság köteles figyelembe venni a mobil eszközök igénylése, beszerzése, logisztikája, SIM kártya kezelése és használata kapcsán a KIE-20-M-04 mellékletben leírtakat és az igénylésekhez a KIE-20-NY-01, KIE-20-NY-02, KIE-20-NY-03, illetve KIE-20-NY-04 formanyomtatványokat alkalmazni.

A Társaság köteles a csoportszintű ügyviteli elektronikus hírközlési szolgáltatások teljes lemondása esetén az MVM NET Zrt. és az informatika funkcionális terület bevonásával egyeztetni a szolgáltatás létrehozása érdekében felmerült ráfordítások kompenzálásáról, amennyiben azok a gazdasági élettartam lejárta előtt kerülnek lemondásra.

A Társaság köteles az Egyedi Szolgáltatási Szerződésekből, illetve a zárt felhasználói csoport tagjai részére nyújtott elektronikus hírközlési szolgáltatási szerződéseikből kiindulva összegyűjteni és megküldeni az informatika funkcionális terület részére a következő évben igénybe veendő ügyviteli elektronikus hírközlési szolgáltatási mennyiségeket a KER-20-01 központi eljárásrendben rögzítettek szerint a csoportszintű középtávú üzleti tervezési periódus kezdetén.

7.3. Üzleti intelligencia és adatvagyon gazdálkodás egységes alapelvei

A Társaság köteles csatlakozni a központi, vagy egy specifikus Business Intelligence Competence Centerhez (BICC), akikkel együttműködve zajlik a Business Intelligence (BI) igények kiszolgálása.

Üzleti informatikai rendszereket támogató BI megoldásokért a csoportszintű támogató szolgáltatások keretrendszere szerint az üzleti informatikai szolgáltató felel. Ettől eltérni DMB javaslatra ABIV jóváhagyással lehet, ebben az esetben a beszerzési folyamatba szakmai résztvevőként az ABIV bevonása szükséges.

Üzemviteli rendszereket támogató BI megoldásokért a Társaság felel, amely felelősséget az ABIV ezirányú kezdeményezésére átadhatja az MVMI Zrt. részére. A Társaság által használt üzemviteli rendszert támogató BI megoldások és termékek bevezetéséről és felelősségviseléséről az ABIV dönt.

A Társaság a BI jellegű működésükhöz szükséges szakértői, tanácsadási tevékenységekhez kapcsolódó kiadásokat üzleti tervében köteles rögzíteni, az ABIV tájékoztatása mellett.

8. Zárórendelkezés

Jelen szabályzat 2026. június 19. napján lép hatályba, ezzel egyidejűleg a 2025. augusztus 15. napján kiadott MGEP-SZ2021/79 Információbiztonsági és infokommunikációs szabályzat módosításra kerül.

Mellékletek

1. sz. melléklet:	Fogalommeghatározások
2. sz. melléklet:	Információbiztonsággal kapcsolatos általános elvárások (minimum elvárások)
3. sz. melléklet:	Információbiztonsági felelős feladatai és a vele szemben támasztott követelmények
4. sz. melléklet:	Adatvagyon gazdálkodási keretrendszer létrehozásával és működtetésével kapcsolatos elvárások
5. sz. melléklet:	Információbiztonsági követelmények megszegésének esetei és azok szankciói
6. sz. melléklet:	Információbiztonsági és Infokommunikációs DHL

Formanyomtatványok

1. sz. formanyomtatvány:	Társasági besoroló kérdőív információbiztonsági kategóriákba
2. sz. formanyomtatvány:	Nyilatkozat – társasági munkavállaló
3. sz. formanyomtatvány:	Nyilatkozat – külsős munkavállaló
4. sz. formanyomtatvány:	Nyilatkozat – mobiltelefon, mobilinternet használathoz

MÓDOSÍTÁS NYILVÁNTARTÓLAP		
Első hatálybalépés ideje: 2021-10-27.		
Ssz.	Módosítás dátuma	Módosítás leírása (jellege)
1.	2023. augusztus 14.	A KIE-20 központi irányelv változása miatti módosítások elvégzése.
2.	2024. április 30.	A KIE-20 központi irányelv változása miatti módosítások elvégzése.
3.	2024. október 14.	KER-20-01-02-03-04-05 Az MVM Csoport központi eljárásrendjeinek változása miatti módosítások elvégzése.
4.	2025. február 11.	KIE-17 központi irányelv változása, valamint a KER-17-02 és KER-17-03 központi eljárásrendek változása miatti módosítások elvégzése.
5.	2025. június 6.	A KIE-20 központi irányelv M-05 mellékletének változása miatti, valamint a 7/2025. sz. Belső ellenőrzési jelentés és intézkedési terv-ből adódó módosítások elvégzése.
6.	2025. augusztus 15.	KIE-17 központi irányelv változása miatti módosítások elvégzése.
7.	2026. június 19.	A KIE-20 központi irányelv, valamint a KER-20-01-02-03-04-05 központi eljárásrendek változása miatti módosítások elvégzése.

Fogalommeghatározások

ABIV: Adatmenedzsment és BI vezető
Adat: tények, fogalmak, eligazítások olyan formai megjelenése, amely alkalmas az emberi vagy az automatikus eszközök által történő értelmezésre, vagy feldolgozásra.
Adatgazda: Az adatgazda felelős az adatkör adatminőségéért, hozzáférési (olvasás, szerkesztés) jogosultságok jóváhagyásáért és az adatok felhasználásának módjáért, karbantartásáért és az azokat leíró metaadatok megfelelőségéért. Az adatgazdák legfőbb feladatai olyan folyamatok, irányelvek és szabályok (adatszótárak) kialakítása és felügyelete, melyek biztosítják a hatáskörükbe tartozó adatkörök értelmezhetőségét, köztük lévő összefüggések áttekinthetőségét, ami lehetővé teszi a hatékony üzleti hasznosíthatóságot.
Adatkör: Adatelemek szervezett gyűjteménye, amelyek olyan önálló entitásokat írnak le, amelyek üzleti szempontból egy logikai csoportot alkotnak. Az adatkörök olyan adatelemeket tartalmaznak, amelyek az azokat kezelő alkalmazások és/vagy üzleti folyamatok működése okán szükségesek. Több adatgazda által kezelt adatköröket különböző adatköröknek tekintünk, annak ellenére is, ha nevükben és/vagy kezelt adatelemeikben részben vagy egészben megegyeznek.
Adatvagyon: A társaság tulajdonában lévő, a társaság működése során létrehozott, feldolgozott, tárolt és továbbított adatok halmaza.
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 gazdálkodás: Az adatvagyon gazdálkodás alatt az adatvagyon felmérését, kezelését, fejlesztését, rendszerezését, valamint a benne rejlő üzleti lehetőségek kiaknázásának támogatását értjük. Az adatvagyon gazdálkodás részét képezi továbbá az adatok hozzáférésével, felhasználásával, szerkesztésével kapcsolatos tevékenységek biztonsági szempontból történő felügyelete.
Adatvagyon jegyzék: Az adatvagyon felmérés eredményét tartalmazó adatbázis vagy dokumentum, mely tartalmazza a társaság adatvagyonának elemeit, azok adatgazdáit, valamint az adatvagyon gazdálkodás és az információbiztonság szempontjából releváns adatokat
Adatvagyon leltár: Az adatvagyon felmérés eredményét tartalmazó adatbázis vagy dokumentum, mely tartalmazza a társaság védendő adatait.
Authentikáció: Az a folyamat, amely során a rendszer ellenőrzi a felhasználó személyazonosságát (pl. felhasználónév és jelszó bekérésével).
Biztonsági szolgáltató: Az MVM Csoport belső biztonsági szolgáltatója az MVM BSZK Zrt. és az MVM Services Zrt. egyes biztonsági szakterületei. A szolgáltatások részleteit a felek közötti szerződések, megállapodások tartalmazzák.
BI: Business Intelligence (Üzleti Intelligencia)
BICC: Business Intelligence Competence Center (Üzleti Intelligencia Központ)
Biztonsági zóna: Olyan, fizikailag jól elhatárolható terület, mely az ott tárolt, kezelt, vagy éppen elhangzott információk biztonsági besorolásának függvényében került kialakításra.
Digitalizációs Transzformációs Központ (DTK): az MVM Csoport stratégiai digitalizációs céljainak megvalósítását támogatja egy hatékony, csoportszintű IT digitalizációs és transzformációs irányítás kialakításán, valamint irányítási feladatainak ellátásán keresztül. A DTK az MVM Csoport üzleti architektúrájának, digitális fejlesztéseinek kialakításával kapcsolatban csoportszintű szakmai iránymutatásokat fogalmaz meg, a Vállalati Architektúra Iroda IT iránymutatásaival összhangban. A DTK támogatja a tagvállalatokat digitalizációs terveik kidolgozásában és megvalósításában.
DMB: Data Management Board (Adatgazdálkodásért felelős, MVM Csoport szintű testület)
DSO: Az MVM Csoport elosztó-hálózat üzemeltető társaságai

Esemény: Minden olyan állapotváltozás, amelynek jelentősége van a folyamatok és szolgáltatások menedzsmentjében, és amely a folyamatot működtetők, illetve a szolgáltatásokat nyújtók részéről beavatkozást igényel, és gyakran vezet naplózandó incidensekhez.
Egyedi Szolgáltatási Szerződés (ESZSZ): Az MVMI Zrt. és a cégcsoport társaságai között Egyedi Szolgáltatási Szerződések (ESZSZ) jönnek létre – külön egyedi informatikai szolgáltatási szerződés az MVMI Zrt.-vel és külön egyedi ügyviteli célú elektronikus hírközlési szolgáltatási szerződés az MVM NET Zrt.-vel –, amelyek tartalmazzák a megrendelő társaság által igénybe venni kívánt szolgáltatásokat és azok díjait rögzítő megállapodást az ICT Szolgáltatási Keretszerződések alapján.
EVK (Elektronikus Változáskezelési-lapokat Kezelő Alkalmazás): az üzleti informatikai szolgáltatással kapcsolatos felhasználói változás igények kezelésére (igénylés, módosítás, lemondás) szolgáló workflow alkalmazás.
Fejlesztési portfólió és kiemelt projektek funkció: Az MVM Zrt. Fejlesztési Portfólió és Kiemelt Projektek Osztályvezető (FPKPO)
ICT belső technológiai szolgáltatók: Az MVM Csoport társaságai, valamint az MVM Zrt. és/vagy a társaságok részvételével működő leányvállalatai részére üzleti informatikai szolgáltatásokat nyújtó MVMI Zrt. és csoporton belüli ügyviteli célú elektronikus hírközlési szolgáltatásokat (ez alól kizárólag az előfizetői flotta mobiltelefon szolgáltatás jelent kivételt) nyújtó MVM NET Zrt. Az MVMI Zrt. és az MVM NET Zrt. ezen szolgáltatások vonatkozásában a KIE-02-M-02 Az MVM Csoport támogató szolgáltatók listája rendelkezései szerinti támogató szolgáltatónak minősül, ha vele csoportszintű SLA keretszerződést kötött az MVM Zrt.
ICT funkciógazda: Egy adott ICT rendszer/szolgáltatás funkcionális megfelelőségének felügyeletéért felel, feladata az adott funkciókörre vonatkozóan az esetlegesen eltérő tagvállalati igények összehangolása, konszolidálása.
Incidens: Nem kívánt vagy nem várt, egyedi vagy sorozatos események, amelyek nagy valószínűséggel veszélyeztetik az üzleti tevékenységet és fenyegetik annak biztonságát, ezzel kárt okozva a társaság számára.
Informatika funkcionális terület: MVM Zrt. Általános vezérigazgató-helyettes / Csoporton belüli elektronikus hírközlés és informatikai, digitalizációs technológiák funkció.
Informatika funkcionális területi vezető: MVM Zrt. Digitalizációs igazgató (MVM Zrt. DIG)
Informatikai szolgáltató: Az MVM Csoport belső informatikai szolgáltatója az MVMI Informatika Zrt. A szolgáltatások részleteit a felek közötti szerződések, megállapodások tartalmazzák.
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 felelős (IBSZ): Az elektronikus információs rendszerek biztonságáért felelős személy.
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 kategória: Meghatározott kritériumok szerint definiált kategóriák, amelyekbe a társaságok adatszolgáltatás alapján kerülnek besorolásra az MVM Zrt. által.

A társaságoknak a saját kategóriájuknak megfelelő biztonsági védelmi intézkedéseket kell megvalósítaniuk. Az alkalmazott információbiztonsági kategóriákat és a szükséges védelmi intézkedéseket az MVM Zrt. belső szabályzatban rögzíti, erről a társaságokat a besorolás eredményével együtt tájékoztatja.

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

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

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 társaságok által használt információk és információs rendszerek azonosítása, azok információbiztonsági kockázatainak felmérése, kockázatarányos védelmi intézkedések bevezetése és folyamatok kialakítása, valamint azok hatékony menedzsmentje.

IT governance: Digitalizációs és hírközlési üzleti megoldások fejlesztési funkció, akinek a feladata az üzletfejlesztési ötletek befogadása, az üzleti területtel ezek valódi üzleti igénnyé való kidolgozása. Az igények harmonizációja az üzleti és IT prioritásokkal, a csoportszintű projekt portfolió figyelembevétele mellett. Az **IT governance** támogatja, koordinálja és egyezteti az MVM Zrt. és az MVM Csoportba tartozó társaságok informatikai fejlesztéseinek, beruházásainak tervezését. Ellenőrzi, konszolidálja az ügyviteli és üzemviteli IT fejlesztési terveket. Felügyeli az IT fejlesztések végrehajtását, a tervek megvalósulását. Ennek keretében folyamatosan monitorozza az összes csoportszintű vagy kiemelt fontosságú informatikai fejlesztési projekt megvalósulását. Az **IT governance** kezeli az IT projekt portfoliót és működteti az MVM Csoport szintű igénykezelést és az IT projekt priorizálási fórumot.

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.

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

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.

Mobileszközök: mobiltelefon, ill. mobilinternet szolgáltatás igénybevételére alkalmas készülékek, olyan nem helyhez kötött IT/ICT eszközök, amelyek önerejükből képesek mobilkapcsolatot létesíteni (mobilinternet, WiFi, NFC, Bluetooth stb.) illetve adatokat tárolni, feldolgozni, továbbítani.

Mobilinternet: a mobilinternet készülék (mobil internet stick) és a SIM kártya együtt.

Mobilszolgáltatás: mobil-hangalapú, ill. mobilinternet szolgáltatások.

Mobiltelefon: MVM Csoport Társaságai által a munkavállalók részére biztosított vállalati mobiltelefon készülék és a SIM kártya együtt.

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 internet szolgáltatás: mobileszközre aktiválható internet csomag.
Projekt Irányító Bizottság (PIB): A Projekt Irányító Bizottság a projektek működését irányító vezető testület, melynek feladata a projekt eredményeinek áttekintése és elfogadása, valamint a projekt menetét jelentősen befolyásoló döntések meghozatala. **Projekt Operatív Bizottság (POB):** A Projekt Operatív Bizottság a projektek működését operatív szinten vezető testület, melynek feladata a projekt eredményeinek kidolgozása, operatív szintű elfogadása, valamint döntés előkészítő anyagok elkészítése.
Projekt Priorizációs Fórum (PPF): üzleti IT projektek kategorizálását és priorizálását támogató fórum.
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.
SIEM (Security Incident and Event Management): Bizonyos rendszerek gyűjtőfogalma. A SIEM rendszerek alapelve, hogy a vállalati környezetből a megfelelő adatokat több helyen is gyűjtve rendszerezze, és hogy átfogó képet kapjunk a tevékenységekről, ami megkönnyíti a követést, és aminek köszönhetően láthatóvá válnak azok a minták, amik különbözőek a megszokottaktól.
Társasági programkoordinátor (a továbbiakban TPK): A KIE-05 Az MVM Csoport projektek kezelésére vonatkozó központi irányelvében rögzítettek szerinti funkciót betöltő munkatárs.
Társasági szolgáltatás-vezető(k): Az üzleti informatikai és az ügyviteli célú elektronikus hírközlési szolgáltatásokat igénybe vevő társaság szolgáltatásvezetői munkakörökben foglalkoztatott munkavállalója/munkavállalói, ezek/ennek hiányában a szolgáltatásokat igénybe vevő társaság első számú vezetője által szolgáltatáskezelésre kijelölt személy(ek).
Technikai felhasználó: Bizonyos előre meghatározott funkció (pl. automatikusan lefutó taskok végrehajtására) betöltésére, az informatikai rendszer üzemeltető által létrehozott, nem konkrét személyhez köthető felhasználó.
Titkosítás: Az adatátvitelkor, vagy adattárolókon történő adat titkosítása esetén az adatokhoz csak az arra jogosultak férhetnek hozzá, a megfelelő kulcs (pl. jelszó) ismeretében.
TTT besorolás: Az MVM Csoportban a belső technológiai szolgáltató, valamint a társaságok által használt informatikai technológiák Támogatott, Tűrt, Tiltott (TTT) kategóriák egyikébe történő besorolása.
Tulajdonosi joggyakorló: az informatikai és csoporton belüli elektronikus hírközlési tevékenységből fakadó feladatok esetén az MVM Zrt. Általános vezérigazgató-helyettese –; a csoporton kívüli elektronikus hírközlési tevékenységből eredő feladatok esetén MVM Zrt. Műszaki vezérigazgató-helyettese).
Ügyviteli rendszer: Az MVM Csoporton belül ide értjük az általános munkahelyi, ügyviteli, adminisztratív és egyéb irodai tevékenység kiszolgálásához és támogatásához szükséges informatikai rendszereket. Az ügyviteli rendszereket a belső informatikai szolgáltató üzemelteti.
Üzemviteli rendszer: Az energia termelés és hálózati szolgáltatás biztonságát, üzembiztonságát és technológiai folyamatait közvetlenül támogató, illetve azokra közvetlenül hatást gyakorló irányítástechnikai beavatkozó, szabályozó, vezérlő, védelmi vagy egyéb funkciót ellátó rendszerek, továbbá ezen rendszerek által vagy független adatgyűjtők által technológiai paraméterekkel vagy adatokkal kiszolgált kapcsolódó rendszerek. (KIE-20)

Vállalatcsoporti programkoordinátor (a továbbiakban VPK): A KIE-05 Az MVM Csoport projektek kezelésére vonatkozó központi irányelvében meghatározottak szerinti funkciót betöltő munkatárs az MVM Zrt. vezérigazgató-helyettesi területein.
Vállalati Architektúra Menedzsment Csoport (VAI): Csoporton belüli elektronikus hírközlés és informatikai, digitalizációs technológiák feladatcsoport, amely működési rendjét a KIE-20-M-03 Vállalati Architektúra Menedzsment Csoport működési rendje című melléklet tartalmazza.
Vállalati Architektúra Menedzsment Csoport csoportvezető: Az MVM Services Zrt. Vállalati Architektúra Menedzsment Csoport vezetője
Változáskezelési Bizottság: Az SAP ERP, SRM és HCM rendszerekben felmerülő fejlesztési igények elbírálását és engedélyezését támogató bizottság.

Információbiztonsággal kapcsolatos általános elvárások

(minimum elvárások)

Az információbiztonsági rendszer

- Az információbiztonsági rendszer célja és kialakítása (Az információk és információs rendszerek azonosítása, kockázatainak felmérése, kockázatarányos védelmi intézkedések bevezetése és folyamatok kialakítása, valamint azok hatékony menedzsmentje)
- Az információbiztonsági rendszer szabályzati környezete (Az információbiztonsági rendszer működtetésének alapja a megfelelő szabályozási környezet. Elemei: információbiztonsági politika, -stratégia, -szabályzat és kapcsolódó folyamatutasítások)

Társaságok besorolása információbiztonsági kategóriába

- A társaság információbiztonsági kategóriájának megfelelő feladatok, követelmények teljesítése (Besorolási kérdőív kitöltése és benyújtása, a társasági információbiztonsági kategóriájának megállapítását követően a kapcsolódó követelmények következetes és szakmai teljesítése)

Az információbiztonság szervezete

- Csoportszintű közreműködők (REVIR Központi Ügyelet, Rendkívüli Események Figyelőszolgálata, REVIR tanácsadó, Csoportszintű Krízis Team, Csoportszintű Információbiztonsági Fórum)
- Társasági szintű közreműködők (védelmi igényszint szerint)
- Információbiztonsági felelős kinevezésének folyamata *(KIE-17 szerint)*

Az elektronikus információs rendszer védelme:

- elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell

a) az elektronikus információs rendszerben kezelt adatok, információk és az elektronikus információs rendszerek által nyújtott vagy azon keresztül elérhető szolgáltatások bizalmassága, sértetlensége és rendelkezésre állása, valamint

b) az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása vonatkozásában a zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet.

az elektronikus információs rendszer felett rendelkezési jogosultsággal rendelkező szervezet, az adatkezelő vagy az adatfeldolgozó által, adott cél érdekében

a) az adatok, információk kezelésére használt eszközök, ideértve a környezeti infrastruktúrát, a hardvert, a hálózatot és az adathordozókat

b) az adatok, információk kezelésére használt eljárások, ideértve a szabályozást, a szoftvert és a kapcsolódó folyamatokat, valamint

c) az a) és b) pontban foglaltakat kezelő személyek

együttesének védelmét is biztosítani szükséges.

Az információ védelme

- Adatvagyon felmérése (A szükséges védelmi intézkedések meghatározásához kell azonosítani azon adatvagyon elemeket, melyeket védeni szükséges.)
- Adatosztályozás (A társaságok által az elektronikus információs rendszerben kezelt adatok és információk biztonsági besorolása azok bizalmasságának, sértetlenségének és rendelkezésre állásának szempontjából.)

- Kockázatok azonosítása és kezelése (A védelmi intézkedések alapja a kockázatelemzés, feltétele, hogy az adatvagyon felmérés keretében a folyamatokban keletkezett, és/vagy használt elemeken túl, a kapcsolódó erőforrások azonosítása megtörténjen. Az adatvagyon elem bizalmassága, sértetlensége és rendelkezésre állása sérülésének hatásait fel kell mérni.)
- Adatvagyon elemek személyes adatköri minősítése *(KIE-16 szerint)*

Hozzáférés-menedzsment, jogosultság kezelés (A kezelt és tárolt adatok védelme érdekében minden alkalmazott informatikai rendszerben jogosultságkezelést kell biztosítani, melyet dokumentált módon szabályozni szükséges)

- Technikai felhasználók kezelése (IBF tájékoztatás, adatgazda jóváhagyása, nyilvántartás vezetése, periodikus aktiválás szabályai)

Szervezeti és személyi biztonság *(KIE-13 szerint)*

- Munkatársak beléptetésének információbiztonsági követelményei (jogosultság igénylés, munkavállalói felelősség, belépő tudatossági oktatás)
- Munkatársak kiléptetése/átléptetése (összeférhetetlenség, jogosultság kezelés, levelezés, archiválás, biztonsági incidens érintettség, eszközkezelés)
- Biztonságtudatossági oktatás (éves Csoportszintű Biztonságtudatossági Programhoz igazítva, szükség esetén további, specifikus tartalommal, az oktatások elmulasztása olyan biztonsági incidensként értelmezendő, amelyet csoportszinten kell kezelni)
- Munkavállalókra vonatkozó szankciók *(KER-17-02-M-01 melléklet szerint)*

Fizikai biztonság *(KIE-13 szerint)*

- Biztonsági zónák és követelményeik
- Alkalmazott eszközök és információbiztonsági követelményeik (beléptető rendszer, zárak, mechanikai védelem, kamerás megfigyelő rendszer, riasztórendszer)

Iratkezelés rendje

- Dokumentumok biztonsági osztályozása (nyilvános / csoportszintű belső használatú / társasági belső használatú / társasági bizalmas)
- Minősített adatok kezelése (2009. évi CLV. törvény a minősített adat védelméről)
- Dokumentumok kezelése (dokumentumok tárolására használt eszközök, szállítás biztonsági követelményei, archiválás és digitalizálás, selejtezés, megsemmisítés)

Informatikai rendszerek fejlesztése, beszerzése

- Általános irányelvek informatikai rendszerek fejlesztésére, beszerzésére vonatkozóan (igények azonosítása, fejlesztési terv készítése és jóváhagyása, fejlesztés megvalósítása, tesztelés, kiadás-élesítés)
- Változáskövetés (változáskövetés fenntartása, igény elbírálásának eredményei)

Informatikai rendszerek működtetése

- Ügyviteli informatikai eszközök (munkaállomások, szerverek, egyéb eszközök [scannelés, nyomtatás], alkalmazások telepítése)
- Technológiai informatikai eszközök (minden olyan munkaállomás, szerver, nyomtató, egyéb speciális eszköz, amely csak a társaság technológiai hálózatához kapcsolódik, az ügyviteli hálózathoz közvetlen kapcsolata – általában – nincsen)
- Az authentikáció módja (Jelszókezelés, erős és kétfaktoros authentikáció)
- Karbantartás (munkaállomások, szerverek karbantartása, karbantartási terv/napló)
- Naplózás (naplózandó rendszerek, naplózással kapcsolatos alapkövetelmények)

- Monitorozás (informatikai rendszerek monitorozása, kiemelt felhasználók monitorozásal, felhasználói tevékenységek monitorozása)
- Archiválás (archiválás gyakorisága, módja, archiválandó adatok)
- Adathordozók törlése (egyszeri és visszaállíthatatlan törlés esetei, fizikai megsemmisítés)
- Biztonsági mentések (biztonsági mentések készítése, visszaállítása)

Kriptográfiai eszközök használata

- Teljes merevlemez titkosítás (ügyviteli és üzemviteli rendszerek esetében kik a felelősök, milyen működés elvárt)
- Fájl titkosító alkalmazások használata (lehetséges esetek felsorolása, titkosítás erőssége, fajtája)
- Elektronikus levelezés vagy egyéb kommunikáció titkosítása *(kötelező/nem kötelező, milyen esetekben alkalmazandó)*
- Hordozható adattárolók titkosítása (dedikált adathordozók, nem titkosított adathordozók, technológiai rendszerek esetében alkalmazott adathordozók)

Hálózatbiztonság

- Külső hálózat (biztonsági osztályba sorolt adatok tárolása a hálózaton kívül, külső hálózathoz való csatlakozás feltételei)
- Belső hálózat (belső hálózat működésére vonatkozó információbiztonsági irányelvek)
- Vezeték nélküli hálózat (belső és külső vezeték nélküli hálózatok információbiztonsági szabályai)
- Távoli elérés (távoli elérést megvalósító technológia leírása, teljesülendő feltételek)

Vírusvédelem, rosszindulatú kódok elleni védelem

- Ügyviteli rendszerek vírusvédelme (vírusvédelmi rendszerrel szemben támasztott követelmények, egyéb vírusvédelmi intézkedések)
- Technológiai rendszerek vírusvédelme (technológiai rendszereken alkalmazott vírusvédelmi követelmények ismertetése)
- Mobil eszközök vírusvédelme (vállalati mobileszközök vírusvédelme, mikor szükséges, milyen követelményeknek kell megfelelni)
- Kártékony kódok kezelése (információbiztonsági események jelentése kártékony kódok észlelése esetén, esemény vizsgálatának menete, bevonandó közreműködő felek)

Elektronikus kommunikáció

- Elektronikus levelezés (általános alapelvek, e-mailek küldésére vonatkozó előírások, e-mailek fogadására vonatkozó irányelvek, távoli elérés szabályai)
- Internet használat (internet használat során betartandó információbiztonsági előírások)
- Azonnali üzenetküldő alkalmazások (engedélyezett/nem engedélyezett azonnali üzenetküldő platformok, központilag biztosított lehetőségek)
- Videokonferencia (szolgáltatás igénybevételének lehetőségei, ide vonatkozó szabályok)
- Fájlmegosztó alkalmazások (külső fájlmegosztó alkalmazások, belső fájlmegosztó szolgáltatások)

Mobil eszközök használata

- Laptop/notebook használatával kapcsolatos információbiztonsági követelmények *(használat, karbantartás, leadás és rendszerből való kivonás)*
- Hordozható adattárolók kezelésének információbiztonsági szabályai (kiadás, használat, karbantartás, leadás és rendszerből való kivonás)

- Mobiltelefon, okostelefon, tablet használatának információbiztonsági szabályai *(kiadás, használat, leadás és rendszerből való kivonás)*

Külső közreműködők, harmadik fél hozzáférése

- Külső felek közreműködésével kapcsolatos általános szabályok (szerződés/megállapodás információbiztonsági követelményei, titoktartási nyilatkozat követelményei)
- Adatok átadása harmadik félnek (papír alapú, elektronikus dokumentumok, szerződéses partnerekre vonatkozó szabályok)
- Ideiglenes belépési jogosultság adása harmadik félnek *(amennyiben indokolt, milyen feltételekkel adható)*
- Hozzáférési jogosultság biztosítása informatikai rendszerhez (azonosító létrehozása külsős személyeknek, jogosultságai, mennyi időre adható)
- Projektszoba, adatszoba (kialakítás feltételei, elvárások)
- Ellenőrzések (ki ellenőrzi, milyen időközönként, eltérés esetén mik a teendők)

Incidenskezelés (KER-17-02 eljárásrend szerint)

- Felkészülés az esemény/incidens kezelésére (információbiztonsági események és incidensek típusainak meghatározása, felelősök kijelölése)
- Információbiztonsági események és incidensek bejelentése *(bejelentési csatornák és felelősségek meghatározása)*
- Információbiztonsági események és incidensek kezelése (esemény/incidens fogadása, rögzítése, előzetes értékelése; esemény/incidens értékelése; esemény/incidens elhárításának indítása; érintett eszközök lehatárolása, bizonyítékok gyűjtése)
- Információbiztonsági események és incidensek lezárása *(jegyzőkönyv készítése, lezárás)*
- Rendszeres riportok készítése
- Incidensjelentés és -kezelés oktatása, visszamérése

Audit, felülvizsgálat (belső, csoportszintű, külső auditok, rendkívüli ellenőrzések)

Információbiztonsági felelős (IBF) feladatai és a vele szemben támasztott követelmények

Az információbiztonsági felelős az elektronikus információs rendszerek biztonságáért felelős, meghatározott kompetenciákkal rendelkező személy, aki éves információbiztonsági munkaterv alapján látja el a következő feladatokat:

- gondoskodik a Társaság elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról;
- gondoskodik a kockázatkezelési keretrendszer szerinti tevékenységek tervezéséről, szervezéséről, koordinálásáról, elvégzéséről és ellenőrzéséről;
- hatósági kijelölés esetén - előkészíti és a Társaság vezetőjének jóváhagyását követően megküldi a nemzeti kiberbiztonsági hatóság részére a Társaság információbiztonsági szabályzatát;
- a Társaság adatvagyonának besorolása és az adatok osztályozása;
- előkészíti a Társaság elektronikus információs rendszereinek biztonsági osztályba sorolását;
- megtartja vagy megszervezi a továbbképzésre kötelezett személyek részére jogszabályban előírt továbbképzéseket, információbiztonság tudatosítás és képzés keretében felméri a biztonságtudatossági szintet, beépíti a tapasztalt eseményeket és incidenseket az oktatásokba;
- felel a társasági szintű információbiztonsági fórum megszervezéséért és megtartásáért;
- véleményezi az elektronikus információs rendszerek biztonsága szempontjából a Társaság elektronikus információbiztonságot érintő szabályzatait és szerződéseit;
- folyamatos és tervezett ellenőrzéseket végez annak vizsgálatára, hogy a Társaság elektronikus információbiztonságra vonatkozó belső normáiban lévő előírások hogyan valósulnak meg, ennek megállapításait rendszeres írásos jelentésben rögzíti a Társaság vezetője számára,
- elkészíti és megküldi a társasági információbiztonsági éves értékelő jelentést;
- rendszeresen felülvizsgálja az információbiztonsági szabályzatot, kiemelt figyelemmel a naplózással, az adathordozók használatával, a jelszókezeléssel és külső csatlakozások hitelesítésével, a hozzáférés menedzsmenttel és jogosultságkezeléssel kapcsolatos szabályok megfelelőségére, betartására és ellenőrzésére;
- felülvizsgálja, hogy a Társaság elektronikus információbiztonságot érintő belső szabályzatai összhangban vannak-e a hatályos jogszabályokkal és a Társaság belső szabályozóival;
- az ellenőrzések és az esetleges incidensek tapasztalatai felhasználásával – a fejlesztendő területekre vonatkozó javaslatokat tartalmazó – biztonsági helyzetértékelést készít a Társaság vezetője számára;
- legalább évente megvizsgálja – a korábbi kiberbiztonsági auditok során az adott elektronikus információs rendszerre vonatkozó biztonsági osztályhoz kapcsolódó védelmi intézkedések értékelése során feltárt hiányosságok megszűntetésére készített intézkedési tervet és beszámolót készít a Társaság vezetője számára az előrehaladásról, amiben kiemeli az esetleges lemaradásokat és a rövid távon szükséges intézkedéseket;
- hatósági kijelölés esetén - kapcsolatot tart a nemzeti kiberbiztonsági hatósággal és a kiberbiztonsági incidenskezelő központtal, a Társaság elektronikus információs rendszerét érintő incidensről tájékoztatja az illetékes kiberbiztonsági. incidenskezelő központot;

- hatósági kijelölés esetén - együttműködik a Kszetv. szerinti kritikus társaság ellenálló képességéért felelős vezetővel, valamint a Vbö. szerinti ellenálló képességért felelős vezetővel;
- megvalósítja a dokumentált üzemeltetési eljárások és az üzemeltetési feladatok vizsgálatát, a kötelezettségek elhatárolását (informatikai szerepkörök összeférhetetlenségi mátrix),
- részt vesz az információbiztonsági auditok, felülvizsgálatok, belső auditok végrehajtásában;
- incidensekkel kapcsolatos riportok készítése;
- ellenőrzi a fizikai biztonsági intézkedések megfelelőségének, betartását;
- gondoskodik az informatikai rendszerek fejlesztésére, beszerzésére vonatkozóan változás-szabályozási eljárások, dokumentált változáskövetés megvalósításáról;
- hatósági kijelölés esetén - előkészíti és a Társaság vezetőjének egyetértésével kezdeményezi a nemzeti kiberbiztonsági hatóságnál a Társaság elektronikus információs rendszereivel kapcsolatos engedélyezési eljárásokat,
- külső partnerekkel összefüggő információbiztonsági kockázatok azonosítása, szerződésekben az információbiztonsági követelmények teljesülésének ellenőrzése;
- Ha az elektronikus információs rendszer biztonságáért *felelős személy* feladatait a Társaságon kívüli személy végzi, feladatait alapvető társaságoknéá legalább kéthavonta egy napon, fontos társaságoknál legalább háromhavonta egy napon – dokumentált módon – az érintett társaságnál való fizikai jelenlét mellett köteles ellátni.

Információbiztonsági felelőssel szemben támasztott követelmények

- Minimum 3 év információbiztonsági területen szerzett tapasztalat

ÉS

- Elektronikus Információbiztonsági Vezető diploma (Nemzeti Közszolgálati Egyetem) VAGY
- Információbiztonsági szakmérnök/szakember oklevél VAGY
- CISA, CISM CISSP vagy CRISC minősítés megléte

ÉS

- Büntetlen előélet, vagy mentesülés a kapcsolódó hátrányok alól, hatósági erkölcsi bizonyítvány szerint

Adatvagyon gazdálkodási keretrendszer létrehozásával kapcsolatos elvárások

Az adatok védelme, az üzletmenet folytonosságának fenntartása kiemelt társasági érdek. Az adatok minősége meghatározza a stratégiai és operatív tervek megvalósításának alapjait a pontos információ és folyamat-adat kapcsolódás mentén, ezért a Társaság felé elvárás, hogy adatvagyon gazdálkodási keretrendszert hozzon létre.

1. Az adatvagyon gazdálkodási keretrendszer tartalma és célja

Az adatvagyon gazdálkodási keretrendszer működtetésének elsődleges célja, hogy az adat társasági erőforrásként legyen kezelve a menedzsment és az operáció minden szintjén. Ezt a célt a Társaság

- belső szabályozók kialakítása,
- evangelizáció, tudatosítás, képzések megvalósítása,
- adatkezelési folyamatok kialakítása,
- adatvagyon gazdálkodási keretrendszer (támogató szoftveres háttér) bevezetése,
- KPI-ok kialakítása, mérése és folyamatos monitorozása

mentén valósíthatja meg. Ennek érdekében az adatvagyon gazdálkodás keretrendszer kialakítása során arra kell törekedni, hogy a keretrendszer

- fenntartható,
- a társasági folyamatok minden szintjén beágyazott,
- mérhető eredményeket megvalósító

legyen.

1.1 Az adatvagyon gazdálkodási keretrendszer komponensei

Az adatvagyon gazdálkodási keretrendszer kötelező és ajánlott komponensekből épül fel, az alábbiak szerint:

Kötelező komponensek: a kötelező komponensek implementálását el kell végezni, és ezt követően éves nyilatkozattétel szükséges a komponensek karbantartásáról, státuszáról. Jelen melléklet módszertani javaslattal szolgál a felsorolt komponensek megvalósítására:

- A társasági adatvagyon felmérése, dokumentálása, az adatvagyon folyamatos karbantartása.
- Adatok kezelésére, hozzáférésére, biztonsági szempontjaira vonatkozó elvárások implementálása, monitorozása.

- Az adatkezeléssel kapcsolatos társasági szabályozásnak való megfelelés folyamatos biztosítása és kimutatása.

Ajánlott komponensek: a fenti elemeket kiegészítő, a teljeskörű adatvagyon gazdálkodáshoz ajánlott tevékenységek, társasági implementációs határidő nélkül:

- Az adatstratégia megtervezése, kommunikációja és kivitelezése.
- Üzleti adatszótár létrehozása.
- Adatminőségi és adat architektúrára vonatkozó irányelvek, elvárások, előírások létrehozása és végrehajtásuk monitorozása.
- Az adatminőségi elvárások, szabályok, valamint az adatkezelési irányelvek teljesülésének operatív támogatása, az adatgazdai tevékenység és adatokkal kapcsolatos döntéshozás aktív támogatása.
- Adatkezeléssel (adatbiztonság, adathozzáférés, adatminőség, törvényi megfelelőség, adatgazdai feladatok, társasági belső irányelvek, szabványok) kapcsolatos események azonosítása és értékelése, incidensek kezelése nyomon követése és megoldása, valamint a megoldási folyamattal kapcsolatos információk rendszerezett előállítása.
- Üzleti érték hozzárendelése az adatvagyon egyes elemeihez, ezáltal az adatvagyon értékének meghatározása, valamint folyamatok és módszerek definiálása az érték meghatározásához.
- Társasági adatvagyon hasznosításának meghatározása, kivitelezése.

1.2 Az adatvagyon gazdálkodási keretrendszertől elvárható eredmények

A fenti elvek mentén kialakított adatvagyon gazdálkodási keretrendszertől elvárható eredmények elsősorban az alábbi kategóriákba sorolhatók:

- Kockázatok csökkentése:
    - Általános kockázatok (törvényi előírásoknak való megfelelés, adatszolgáltatási kötelezettség teljesítése)
    - Reputációs kockázatok
    - Adatbiztonsági kockázatok
    - Személyes, bizalmas adatokkal kapcsolatos kockázatok

- Költségek csökkentése:
    - Adatminőséghez kapcsolódó költségek csökkentése: nem megfelelő adatminőségből eredő hibák javításának vagy megelőzésének többletköltsége, bekövetkezett hibák következményeként felmerülő költségek
    - Adatok rendelkezésre állása és értelmezése során felmerülő költségek: az adatok rendszerezése és nyilvántartása (adatkatalógus), valamint értelmezése (üzleti szótár) nyomán az adatvagyon magasabb szintű hasznosítása mellett az üzleti

folyamatok végrehajtásához szükséges adatok hozzáférésének, valamint a megfelelő adatok kiválasztásának költsége

- Adatok tárolása és kezelése kapcsán felmerülő költségek: adattárolás földi vagy felhő alapú egységekben, adatok mozgatása, mentése, visszaállítása során felmerülő költségek

- Bevétel növelése és az üzleti lehetőségek kiterjesztése:
  - Üzleti folyamatok felgyorsítása és egyszerűsítése, humánerőforrások felhasználásnak optimalizálása az adatok rendelkezésre állásának és/vagy megbízhatóságának növelése mentén
  - Döntések megalapozottságának erősítése, előkészítési folyamat gyorsítása
  - Meglévő termékek, szolgáltatások értékének növelése adat alapú kiegészítésekkel
  - Új, adat alapú termékek, szolgáltatások létrehozása, bevezetése

2. Módszertani javaslat a társasági adatvagyon gazdálkodás keretrendszer kötelező komponenseinek implementálására

Az 1. pontban leírt adatvagyon gazdálkodás keretrendszer kialakítása az Ügyvezető felelőssége. Amennyiben egy társaság még nem, vagy csak részben rendelkezik adatvagyon gazdálkodás keretrendszerrel, ebben a fejezetben leírt támpontok mentén javasolt azt kialakítani. Igény esetén a Digitalizációs IT portfólió, adatmenedzsment tanácsadást nyújt a társaságok számára az adatvagyon gazdálkodás keretrendszer kialakításának tervezésében. A Társaságnak kiemelt figyelmet kell fordítani a 3. pontban leírt adatszolgáltatási kötelezettségek teljesítésére.

Az adatvagyon gazdálkodás keretrendszernek kritikus pontja az adatvagyon felmérése és az adatvagyon jegyzék kialakítása, ezeket a feladatokat első számú prioritásként kell kezelni és kialakítani.

2.1 A társasági adatvagyon felmérése, dokumentálása, az adatvagyon folyamatos karbantartása

A társasági adatvagyon felmérésnek, majd ezt követően az adatvagyon folyamatos karbantartásának célja a fentiek tükrében meghatározni a használatban lévő kritikus adatköröket és azok tulajdonságait, továbbá meghatározni az adatkörökért felelős adatgazdákat, akik az adatok életciklusa során felügyelik és naprakészen tartják a felhasználásukat, adatbiztonsági és adatvédelmi besorolásukat. A Társaság működése szempontjából kritikusnak tekintendő adatkörök meghatározásáért az Ügyvezető felel.

Az adatvagyon felmérés végrehajtásához, valamint az adatvagyon folyamatos karbantartásához szükséges erőforrás allokálásáért az Ügyvezető felel.

Az adatvagyon felmérését, majd az adatvagyon jegyzék elkészítését követően az azonosított adatgazdák felelnek a jegyzék tételes karbantartásáért, a jegyzékben foglalt adatok minőségéért,

megbízhatóságáért. A Business Intelligence Competence Center (BICC) szakértői támogatást nyújtanak az adatvagyon felmérésben, annak szervezésében, illetve az adatvagyon gazdálkodással kapcsolatos oktatásban és tudásmegosztásban.

Általános esetben az adatvagyon felmérést a Társaságnak egyszer kell elvégeznie; ezt követően kötelessége az elkészült adatvagyon jegyzék naprakészen tartása, bárminemű adatvagyont értintő változások lekövetése és azok adatvagyon jegyzékben való aktualizálása.

Az adatvagyon jegyzék elkészítése kapcsán a Digitalizációs IT portfólió, adatmenedzsment bármikor írásbeli tájékoztatást kérhet a Társaságtól (pl. adatvagyon jegyzék elkészítésének státusza, magas szintű eredménye, részeredménye).

Az adatvagyon felelősöknek – adatgazdáknak – az adatkörök jegyzékét folyamatosan naprakészen kell tartani, különös figyelmet helyezve az alábbi tipikusan előforduló, de nem kizárólagos változásokra:

- az információkezelést és feldolgozást végző vagy támogató folyamatokban, illetve a kezelt adatok körében történő változás,
- a társaság tulajdonában vagy használatában lévő informatikai rendszerekben adatköröket érintő változás,
- a vonatkozó adatok körében külső vagy belső csoportszintű szabályozás indukál kárérték-minősítés, vagy adatbiztonsági kategória besorolás módosítására indokot,
- személyi vagy szervezeti változás eredményeképp szükségessé válik az adatgazdák felülvizsgálata.

2.1.1 Módszertani javaslat az adatvagyon felmérés végrehajtására és adatvagyon jegyzék kialakítására

2.1.1.1 szervezeti egység és/vagy szakterület kijelölése

Az Ügyvezető kijelöli a szervezet teljeskörű működését lefedő szervezeti egységeket és/vagy szakterületeket, majd kijelöli az adatvagyon jegyzék létrehozásában résztvevő személyeket. Az adatvagyon jegyzék elkészítése során a Társaság üzleti folyamatait és szervezeti egységeit teljeskörűen le kell fedni.

2.1.1.2 adatkörök meghatározása

Az adatköröket önállóan kezelő (az adott adatkör vonatkozásában külön adatgazdával rendelkező) szervezeti egységenként szükséges meghatározni, ezeket az adatvagyon jegyzékbe felvenni.

Az adatvagyon jegyzék elkészítése szempontjából releváns szervezeti egységek általában, de nem minden esetben egybeesnek a társaság szakterületi tagolásával.

E módszertan szerinti adatvagyon jegyzék elkészítése eredményezheti, hogy egy adatkörnek egy társaságon belül (szakterületenként, igazgatóságonként) több adatgazdája is lehet. Ilyen esetben külön sorban kell feltüntetni mind azon adatköröket, amelyek több szakterületen is előfordulnak, emiatt több adatgazdával rendelkeznek. Az adatkörök meghatározása során törekedni kell az adott szervezeti egység által használt adatkörök és folyamatok teljeskörű lefedésére. Az adatkörök és adatgazdák konszolidációját az adatvagyon jegyzék elkészítése után érdemes elvégezni.

2.1.1.3 adatgazdák meghatározása

Minden adatkörhöz szükséges adatgazdát kinevezni. Az adatgazda felelős a hozzá tartozó adatkör(ök) felmérésének végrehajtásáért és folyamatos karbantartásáért. Az adatgazdákat dokumentált módon az Ügyvezető jelöli ki (kijelölő okirat, munkaköri leírásban rögzített adatgazdai szerep, egyéb ezekkel egyenértékű dokumentált mód).

Az adatgazdákat két módszertan egyike szerint javasolt kijelölni:

- Pozíció szerint: adatgazda lehet egy szakterületi vezető, akinek kellő tudása van a szakterületet érintő adatkörökkel és azok forrásrendszereivel kapcsolatosan
- Funkcionális tudás szerint: adatgazda lehet egy olyan személy is, aki nem az adott szakterület vezetője, viszont rendelkezik a szakterületet vagy forrásrendszert érintő adatkörökről funkcionális és/vagy szakértői tudással

2.1.2 Az adatvagyon jegyzék kötelező tartalmi elemei

Az adatvagyon jegyzékben minden adatkörről minimum az alábbi információkat fel kell tüntetni:

- Társaság neve
- BICC vezető vagy BI felelős neve
- Szakterület megnevezése
- Adatkör neve
- Adatkör leírása
- Adatkört tároló rendszer neve (amennyiben fizikai megjelenésű adatkörökről van szó, az adatkör fizikai tárolási helye)
- Adatgazda neve
- Adatgazda pozíciója
- Adatkör tartalmaz-e személyes adatot (igen/nem)
- Adatkörök BSR – bizalmasság, sértetlenség, rendelkezésre állás – szerinti besorolása
- Adatkörök adatbiztonsági osztályok szerinti besorolása (lásd 2.2.2)

Igény esetén a társaságok az adatvagyon jegyzék elkészítéséhez a BICC-től mintadokumentumot igényelhetnek.

2.2 Adatok kezelésére, hozzáférésére, biztonsági szempontjaira vonatkozó elvárások implementálása, monitorozása

Az adatvagyon gazdálkodás keretrendszernek kötelező eleme az adatkörök besorolása BSR (bizalmasság, sértetlenség, rendelkezésre állás) és biztonsági szempontok szerint. Az adatkör jegyzékbe felvezetett adatköröket két dimenzió mentén szükséges besorolni:

2.2.1 BSR – bizalmaság, sértetlenség, rendelkezésre állás – szerinti besorolás:

- bizalmasság szerint: mekkora kárral néz szembe a Társaság, amennyiben egy adatkör
  - a szervezeten belül egy vagy több jogosulatlan személy számára megismerésre kerül
  - a szervezeten belül megismerésre kerül
  - az MVM Csoporton belül jogosulatlan személy által megismerésre kerül
  - Társadalmi nyilvánosságra kerül

- sértetlenség szerint: mekkora kárral néz szembe a Társaság, ha egy adatkör
  - egyedileg sérül/megváltozik
  - tömegesen sérül/megváltozik

- rendelkezésre állás szerint: mekkora kárral néz szembe a Társaság, ha egy adatkör
  - adatszolgáltatási igényt követően a türelmi időn túl nem áll rendelkezésre, valamint mennyi a türelmi idő

2.2.2 Adatbiztonság osztályok szerinti besorolás:

- 1. osztály - nyilvános adat: 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 Információbiztonság előzetes jóváhagyásával 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 - társaság belső használatú adatok: a Társaságon belül szabadon megosztható, azonban a Társaságon kívül még csoportszinten sem kommunikálható, vagy csak abban az esetben, ha az Információbiztonság és az adatgazda előzetes jóváhagyást 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.)

Minősített adatok köre: a 2009. évi CLV., a minősített adat védelméről szóló törvény értelmében nemzeti vagy külföldi minősített adatnak minősített adatkörök. Jelen adatkategóriával ezen szabályzat nem foglalkozik, ezen adatok kezelése külön törvényi szabályozás alá esik.

3. Adatszolgáltatás

A Társaság köteles az adatvagyon gazdálkodás keretrendszer kötelező komponenseiről a Digitalizációs IT portfólió, adatmenedzsment, valamint az Információbiztonság számára az alábbiak szerint adatot szolgáltatni:

- Az Ügyvezető minden év január 31-ig nyilatkozik az előző év adatvagyon gazdálkodás keretrendszer kötelező komponenseinek státuszáról. A nyilatkozatát e-mail formájában megküldi az Információbiztonság, valamint a Digitalizációs IT portfólió, adatmenedzsment számára minden év január 31-ig. A társasági adatvagyon jegyzéket, valamint az adatvagyon elemek BSR és biztonsági besorolását tartalmazó dokumentumot az Információbiztonság, valamint a Digitalizációs IT portfólió, adatmenedzsment számára felkérés esetén rendelkezésre kell bocsájtani.

Információbiztonsági követelmények megszegésének esetei és azok szankciói

1. Az információbiztonsági követelmények megszegésének esetei

Szabályszegés típusa	Leírás
Eszköz elvesztés, rongálás	A társasági belső szabályzat hordozható eszközök kezelésére vonatkozó rendelkezéseinek betartása nem csak az eszköz értéke miatt indokolt, hanem az azon tárolt adatok bizalmasságának, sértetlenségének és/vagy rendelkezésre állásának sérüléséből származó károk lehetősége miatt is. A hordozható eszköz elvesztéséből származó esetleges információbiztonsági károkat a társasági információbiztonsági felelősnek 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.
Események/Incidensek jelentésének elmulasztása	Amennyiben a munkavállaló az általa észlelt eseményt/incidenst nem jelenti, akkor ennek elmaradásából adódó károkért a munkavállaló szankcionálható.
Eszköz nem rendeltetésszerű használata	Amennyiben a munkavállaló a munkavégzéséhez biztosított eszközöket nem rendeltetésszerűen használja, akkor szankcionálható. Nem rendeltetésszerű használat lehet (nem kizárólagos felsorolás): • Indokolatlan magáncélú használat (például zene- és/vagy filmletöltés, játékok használata, magáncélú adatok tárolása) • Illetéktelen személyes adatok kezelése • Illegális és/vagy nem engedélyezett szoftverek használata • Biztonsági beállítások módosítása
Internet használat	Az internet használatának engedélyezése 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 munkavégzés céljából az indokoltnál nagyobb, túlzott foglalása (pl. nagyméretű állományok indokolatlan letöltése) tilos.

	A hálózati sávszélesség és erőforrások magáncélú használata 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 felhasználói szemmel is gyanúra okot adó 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, megrongálódása esetén a munkavállaló köteles jelenteni az incidenst a társasági biztonsági területnek. Az incidens bejelentéséről jegyzőkönyv készül, az állandó belépőkártya pótlása kizárólag ezen jegyzőkönyv ellenében történhet meg. A társasági biztonsági terület 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.
Laptop használat	Az informatikai szolgáltató, illetve a társaság tulajdonát képező laptopokat/notebookokat a munkavállaló a munkaidő lejártával bent hagyhatja az irodában a következő feltétellel: • Munkaidőn kívül a laptopot/notebookot zárt szekrényben vagy bezárt irodában kell elhelyezni. Illetve hazaviheti, szállíthatja az alábbi feltételekkel: • A laptop/notebook őrizetlenül hagyása még zárt autóban is tilos. Az autóban őrizetlenül hagyott eszköz ellopása esetén a felelősség és a kár megtérítése a munkavállalót terheli. • A laptopot/notebookot 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 a társasági információbiztonsági terület által meghatározott külön informatikai eszközök biztosítása szükséges a kiküldetés időtartamára. Amennyiben a fentieket a munkavállaló megszegi, akkor szankcionálható.
Szerződéses követelmények	A szerződés/megállapodás információbiztonsági követelményeinek megszegése.
Dokumentumok kompromittálódása, sérülése, elérhetetlensége	Papír alapú vagy elektronikus dokumentumok jogosulatlan megismerése, módosítása, rendelkezésre állásának megszakítása.
Oktatások elmulasztása	Az éves információbiztonsági oktatások elmulasztása, illetve el nem végeztetése incidensnek minősül, szankciót von maga után.
Egyéb	A felsoroltakon kívül felmerülő esetben a társasági információbiztonsági felelős megvizsgálja, hogy információbiztonsági szabálysértés történt-e, és szükséges-e a szankcionálás.

Szankcionálási szempontok

Amennyiben a munkavállaló felróható (szándékos vagy gondatlan) magatartásának következményeként megsérti a jelen szabályzatban foglalt rendelkezéseket, a munkavállaló szankcionálható.

Alapvetően a szabálysértéssel okozott kár mértéke szerint kerülnek a szankcionálások kategorizálásra.

A kár alapját a társaság kárérték táblázata adja, jogi-, imázs- és működési kár függvényében, melynek jellege/ értéke alapján az alábbi szabálysértési kategóriák lehetnek:

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

Az okozott kár kategóriáját, és a kárt nem okozó szabálysértés kategóriáját az érintett szakterület(ek) vezetői (közvetlen felettes, ill. a társaság első számú vezető) és a társaság biztonsági funkciójának vezetője együttesen határozzák meg.

Ezen melléklet alapján érvényesített felelősségre vonás nem mentesíti a Munkavállalót az egyéb kártérítési vagy jogi felelősség alól.

1. Munkáltatói intézkedések (szankciók)

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

	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 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 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 és/vagy a munkaviszony megszüntetése.

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

A munkáltatói intézkedések döntéshozói

	Gondatlan	Szándékos
Alacsony	Közvetlen felettes vezető (D, V) Társasági információbiztonsági felelős (K)	Közvetlen felettes vezető (D) Társasági információbiztonsági felelős (V) HR (K)
Közepes	Közvetlen felettes vezető (D) Társasági információbiztonsági felelős (V) HR (K)	Közvetlen felettes vezető (K) Társaság első számú vezetője (D) HR (K) Jog (K) Társasági biztonsági funkció vezetője (K) Társasági információbiztonsági felelős (V)

Magas	Közvetlen felettes vezető (K) Társaság első számú vezetője (D) HR (K) Jog (K) Társasági biztonsági funkció vezetője (K) Társasági információbiztonsági felelős (V)	Közvetlen felettes vezető (K) Társaság első számú vezetője (D) HR (K) Jog (K) Társasági biztonsági funkció vezetője (K) Társasági információbiztonsági felelős (V)

Az információbiztonsági szabályzatban foglaltak gondatlanságból, egymás után többször történő ismételt megsértése esetén, a társasági információbiztonsági felelős – a szabálysértő munkavállaló közvetlen vezetőjével egyeztetve – javaslatot tehet a társasági biztonsági funkció vezetője részére a szándékosság esetén fennálló szankciók 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

Információbiztonsági és Infokommunikációs Döntési Hatásköri Lista

Azonosító	Döntési hatáskör meghatározása	MVM Zrt.				MVM Mátra Gép Kft.				Megjegyzés	Kapcsolódó központi DHL sor azonosítója	Kapcsolódó központi szabályozó azonosítója
		(VIG) Vezérigazgató	(BIG) Biztonsági Igazgató	(DIG) Digitalizációs Igaz-	(DAIG) Data and Analy-	Ügyvezető	Számítástechnikai főmun-	Információbiztonsági fele-				
MGEP-SZ2021/79-D-01	Döntés a társaságok nyilvántartásba vételi kérelmük hatóság felé történő benyújtásáról.		D			E	I	I		-	KIE-17-4-D-01	KIE-17
MGEP-SZ2021/79-D-02	Döntés a társasági ügyviteli informatikai rendszerre vonatkozó üzleti igény felhő alapú megoldásának engedélyezéséről.		D			I				-	KIE-17-4-D-02	KIE-17
MGEP-SZ2021/79-D-03	Döntés a társasági üzemviteli informatikai igény felhő alapú megoldásának engedélyezéséről.		D			I				-	KIE-17-4-D-03	KIE-17
MGEP-SZ2021/79-D-04	Döntés a társaságok ügyviteli informatikai rendszerének sérülékenységi vizsgálatáról.		D			I				-	KIE-17-4-D-04	KIE-17

Azonosító	Döntési hatáskör meghatározása	MVM Zrt.				MVM Mátra Gép Kft.				Megjegyzés	Kapcsolódó központi DHL sor azonosítója	Kapcsolódó központi szabályozó azonosítója
		(VIG) Vezérigazgató	(BIG) Biztonsági Igazgató	(DIG) Digitalizációs Igaz-	(DAIG) Data and Analy-	Ügyvezető	Számítástechnikai főmun-	Információbiztonsági fele-				
MGEP-SZ2021/79-D-05	Döntés a társaságok üzemviteli rendszereinek sérülékenységi vizsgálat engedélyezéséről.		D			I				-	KIE-17-4-D-05	KIE-17
MGEP-SZ2021/79-D-06	Döntés a társaság és az ICT belső technológiai szolgáltató közötti üzleti IT szolgáltatásokkal, valamint csoporton belüli ügyviteli elektronikus hírközlési szolgáltatásokkal kapcsolatos viták rendezése ügyében.			D		E	I			-	KIE-20-5-D-01	KIE-20
MGEP-SZ2021/79-D-07	Döntés a társasági üzleti IT fejlesztési igények, valamint a csoporton belüli ügyviteli elektronikus hírközlési fejlesztési portfolió tervbe történő felvételéről, a portfolió terv módosításairól.			D		E	I			-	KIE-20-5-D-02	KIE-20

Azonosító	Döntési hatáskör meghatározása	MVM Zrt.				MVM Mátra Gép Kft.				Megjegyzés	Kapcsolódó központi DHL sor azonosítója	Kapcsolódó központi szabályozó azonosítója
		(VIG) Vezérigazgató	(BIG) Biztonsági Igazgató	(DIG) Digitalizációs Igaz-	(DAIG) Data and Analy-	Ügyvezető	Számítástechnikai főmun-	Információbiztonsági fele-				
MGEP-SZ2021/79-D-08	Döntés a társasági üzleti IT fejlesztési projektek, valamint a csoporton belüli ügyviteli elektronikus hírközlési projektek indítása ügyében a projektek kezelésére vonatkozó központi szabályozóban meghatározott értékhatárok figyelembevételével.			D		E	I			-	KIE-20-5-D-03	KIE-20
MGEP-SZ2021/79-D-09	Döntés a társaság által a csoport szinten alkalmazott ügyviteli rendszert támogató BI technológiáktól való eltérésről				D	E				-	KIE-20-5-D-04	KIE-20
MGEP-SZ2021/79-D-10	Döntés a társaság által használt üzemviteli rendszert támogató BI megoldások és termékek bevezetéséről és felelősségviseléséről				D	I	I			-	KIE-20-5-D-05	KIE-20

Azonosító	Döntési hatáskör meghatározása	MVM Zrt.				MVM Mátra Gép Kft.				Megjegyzés	Kapcsolódó központi DHL sor azonosítója	Kapcsolódó központi szabályozó azonosítója
		(VIG) Vezérigazgató	(BIG) Biztonsági Igazgató	(DIG) Digitalizációs Igaz-	(DAIG) Data and Analy-	Ügyvezető	Számítástechnikai főmun-	Információbiztonsági fele-				
MGEP-SZ2021/79-D-11	Döntés a társaság által használt BI termék hitelességi besorolásáról				D	I	I			-	KIE-20-5-D-06	KIE-20
MGEP-SZ2021/79-D-12	Döntés a Csoportszintű IT Szolgáltatási Keretszerződés standardtól eltérő megállapodásokról			D		E	I			-	KIE-20-5-D-07	KIE-20
MGEP-SZ2021/79-D-13	Döntés az SAP rendszerekben felmerülő fejlesztési igények megvalósításáról VK Bizottság javaslata alapján			D		E	I			-	KIE-20-5-D-08	KIE-20
MGEP-SZ2021/79-D-14	Döntés a nettó 100 MFt-ot meghaladó üzleti informatikai OPEX és CAPEX jellegű külső kötelezettségvállalásról.			D		E	I			-	KIE-20-5-D-09	KIE-20

Azonosító	Döntési hatáskör meghatározása	MVM Zrt.				MVM Mátra Gép Kft.				Megjegyzés	Kapcsolódó központi DHL sor azonosítója	Kapcsolódó központi szabályozó azonosítója
		(VIG) Vezérigazgató	(BIG) Biztonsági Igazgató	(DIG) Digitalizációs Igaz-	(DAIG) Data and Analy-	Ügyvezető	Számítástechnikai főmun-	Információbiztonsági fele-				
MGEP-SZ2021/79-D-15	Döntés a tervezett konkrét AI megoldás felhasználásáról/ felhasználhatóságáról			D		E	I			-	KIE-20-5-D-10	KIE-20

Rövidítés: Á – Állást foglal D – Dönt E – ElőterjesztEJ – Előzetesen jóváhagy I – Információt kap

Társasági besoroló kérdőív információbiztonsági kategóriákba

A TÁRSASÁG ALAPADATAI	
Társaság neve	
Információbiztonsági felelős neve	
Információbiztonsági felelős beosztása, szervezeti egysége	

BESOROLÁSI SZEMPONTOK	
Hány munkavállalója van a Társaságnak?	Jelöljön ki egy elemet.
A Társaság telephelye hol helyezkedik el?	Jelöljön ki egy elemet.
Az ügyviteli rendszerek mellett technológiai/üzemviteli rendszert alkalmaz-e a Társaság?	Jelöljön ki egy elemet.
A Társaság ISO 27001 szabvány szerinti tanúsítása megtörtént-e?	Jelöljön ki egy elemet.
A Társaság számlázási rendszer audit kötelezett-e?	Jelöljön ki egy elemet.
Az MVM Csoporton belül szolgáltató szerepet tölt be a Társaság?	Jelöljön ki egy elemet.
Vonatkoznak-e a Társaságra nukleáris biztonsági vagy egyéb speciális biztonsági követelmények?	Jelöljön ki egy elemet.

TÁRSASÁGI MEGJEGYZÉSEK

KÉRDŐÍV JÓVÁHAGYÁSA			
Jóváhagyó	Beosztás/ Szerepkör	Dátum	Aláírás

MVM
Mátra Gép

Törzspéldány megőrzési helye:	Ügyvezetést támogató iroda
megőrzési ideje:	5 év
Irattári tételszám:	
Nyilvántartási szám:	

NYILATKOZAT

Alulírott <név, állandó belépőkártya száma>, az MVM Mátra Gép Kft. munkavállalója kijelentem, hogy

- az MVM Mátra Gép Kft. **MGEP-SZ2021/79 Információbiztonsági és infokommunikációs szabályzatának tartalmát megismertem és tudomásul vettem.** Köteles vagyok a Szabályzatban részletezett informatikai biztonsági előírásoknak eleget tenni, melynek megszegése munkaviszonyból származó vétkes kötelezettségszegésnek minősül, és kártérítési jogi, büntető jogi, és a munkaviszonyból származó vétkes kötelezettségszegésért járó jogkövetkezményeket vonhat maga után.
- köteles vagyok a munkavégzés során tudomására jutott üzleti titkot, vállalati adatot, valamint a megbízóra, illetve a tevékenységére vonatkozó alapvető fontosságú információkat megőrizni. Az előbbiekben kifejtetteken túlmenően sem közölhetek illetéktelen személlyel olyan adatot, amely munkafeladatom ellátásával összefüggésben jutott a tudomásomra, és amelynek harmadik személlyel történő közlése az MVM Mátra Gép Kft.-re vagy más személyre hátrányos következménnyel járna. Köteles vagyok az MVM Mátra Gép Kft. megbízásából, az MVM Mátra Gép Kft. munkavállalójaként végzett tevékenységem keretében megismert információkat titokként kezelni, és azokat harmadik személy részére nem adhatom ki.

A titoktartási kötelezettség megszegéséből eredő kárért anyagi felelősséggel tartozok.

.....

< név >

MVM Mátra Gép Kft. munkavállaló

Kelt: Visonta, ...

Mátra Gép

Törzspéldány megőrzési helye:	Ügyvezetést támogató iroda
megőrzési ideje:	5 év
Irattári tételszám:	
Nyilvántartási szám:	

NYILATKOZAT

Alulírott <név, állandó belépőkártya száma>, a < cégnév, székhely > és az MVM Mátra Gép Kft. között fennálló < szerződés száma > számú szerződés alapján az MVM Mátra Gép Kft. területén / megbízásából tevékenységet végző külső partner kijelentem, hogy

az MVM Mátra Gép Kft. MGEP-SZ2021/79 Információbiztonsági és infokommunikációs szabályzatának tartalmát megismertem és tudomásul vettem.

Az MGEP-SZ2021/79 Információbiztonsági és infokommunikációs szabályzat 6.11.1. pontja alapján alulírott köteles:

a munkavégzés során tudomására jutott üzleti titkot, vállalati adatot, valamint a megbízóra, illetve a tevékenységére vonatkozó alapvető fontosságú információkat megőrizni. Az előbbiekben kifejtetteken túlmenően sem közölhet illetéktelen személlyel olyan adatot, amely feladata ellátásával összefüggésben jutott a tudomására, és amelynek harmadik személlyel történő közlése az MVM Mátra Gép Kft.-re vagy más személyre hátrányos következménnyel járna. Köteles az MVM Mátra Gép Kft. megbízásából végzett tevékenysége keretében megismert információkat titokként kezelni, és azokat harmadik személy részére nem adhatja ki.

A titoktartási kötelezettség megszegéséből eredő kárért anyagi felelősséggel tartozik.

.....

< név >

külső partner

Kelt: Visonta, ...

Mátra Gép

Törzspéldány megőrzési helye:	Ügyvezetést támogató iroda
megőrzési ideje:	5 év
Irattári tételszám:	
Nyilv ántartási szám:	

NYILATKOZAT

……. (törzsszáma:……) az MVM Mátra Gép Kft. **MGEP-SZ2021/79 Információbiztonsági és infokommunikációs szabályzatának** mobiltelefonok használatáról szóló előírásait megismertem és magamra nézve kötelező érvényűnek tekintem. A számomra biztosított mobiltelefont, mobilinternetet rendeltetésszerűen használom, azon a biztonsági megoldásokat nem kerülöm meg. Vállalom, hogy a készülék elvesztése vagy eltulajdonítása esetén a rajta tárolt adatok törléséről haladéktalanul gondoskodom az ún. OWA rendszeren keresztül a mellékelt használati útmutató alapján (ehhez szükség esetén munkaidőben segítséget nyújt az MVMI Helpdesk). Tudomásul veszem, hogy a mobiltelefon használati jogosultságom megszűntével köteles vagyok az addig el nem számolt, a munkáltató által nem engedélyezett magánjellegű mobil szolgáltatás igénybevétele miatt felmerült költségeit megtéríteni.

.....

< név >

MVM Mátra Gép Kft. munkavállaló

Kelt: Visonta, ...