MNF Magyar Nemzeti Filharmonikus Zenekar,
Énekkar és Kottatár Nonprofit Kft.
Alapítva: 1923

Informatikai Biztonsági Szabályzat

Hatályos: 2019. május 1.

Herboly Domonkos Zoltán
főigazgató
2019.04.15.

MNF NONPROFIT KFT. 1.

1095 Budapest, Komor Marcell utca 1. (MÜPA Üzemeltető Kft.)
Telefon: 411-6600 Fax: 411-6699 E-mail: info@filharmonikusok.hu Honlap: www.filharmonikusok.hu

Tartalom

1 Általános Rendelkezések

1.1 Az IBSZ célja

A jelen Informatikai Biztonsági Szabályzat (a továbbiakban IBSZ) célja, hogy az MNF Magyar Nemzeti Filharmonikus Zenekar, Énekkar és Kottatár Nonprofit Kft., (a továbbiakban Társaság) által használt informatikai rendszerre vonatkozóan a biztonsági intézkedéseket szabályozza, meghatározza a számítástechnikai eszközök beszerzésének és használatának, a szoftverkészítés és alkalmazás, az adatkezelés folyamatának biztonsági szabályait, továbbá az informatikai szerepköröket, és előírja az egyes szereplők informatikai biztonságot érintő feladatait.

Az IBSZ által szabályozható:

- A titok-, vagyon- és tűzvédelemre vonatkozó előírások betartása.
- Az adatvédelmi és személyiségi jogok kellő védelme (tekintettel a külön Adatvédelmi Szabályzat betartására).
- Az üzemeltetett számítástechnikai eszközök, hardverek, szoftverek, hálózatok, stb. rendeltetésszerű használata és megfelelő üzemvitele.
- Az üzembiztonságot szolgáló műszaki fenntartási és karbantartási teendők elvégzése.
- A számítógépes feldolgozások és az eredményadatok további hasznosítása során az illetéktelen hozzáférésből és felhasználásból eredő károk megelőzése, illetve minimális mértékűre való csökkentése.
- Az adatállományok formai és tartalmi helyességének és épségének megőrzése.
- Az alkalmazott szoftverek sértetlenségének, megbízható működésének biztosítása.
- Az adatállományok biztonságos mentése.
- A felhasznált és keletkezett írásos dokumentumok megfelelő kezelésének biztosítása.
- Annak rögzítése, hogy mi a Társaság vezető beosztású és az informatikai feladatokat irányító dolgozóinak a feladata, felelőssége és a jogköre az informatikai biztonság tekintetében.
- A jogosultság és a hozzáférés rendszerének dokumentált kialakítása.
- A célok elérése érdekében a védelemnek működnie kell az egyes rendszerelemek fennállásának teljes ciklusa alatt – a megtervezéstől az alkalmazáson (üzemeltetésen) keresztül a felszámolásukig, és azt követően az elévülés, illetve a selejtezhetőség időtartama alatt.

1.2 Alapul vett irányelvek, követendő szabványok, ajánlások, szabályzatok

Az IBSZ mint az információvédelem szabályozásának elsődleges eszköze, a vállalat működési területén szükségszerűen a hatályos jogszabályok, szabványok, ajánlások előírásain alapul. Ezek jellemzően a következők:

1995. évi LXV. törvény. az államtitokról és a szolgálati titokról,

79/1995. (VI. 30.) Korm. rendelet a minősített adat kezelésének rendjéről,

233/2001. (XII.10.) Korm. rendelet a közszolgálati jogviszonnyal összefüggő adatkezelésre és közszolgálati nyilvántartásra vonatkozó szabályokról,

7/2002. (III. 12.) BM rendelet a közszolgálati nyilvántartás egyes kérdéseiről,

1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről.

A Társaság **belső Adatvédelmi Szabályzata**, annak mellékletei, a (1/2018 - 10/2018-ig számozott) belső adatvédelmi utasítások, valamint **külső**, - a honlapon (http://www.filharmonikusok.hu/adatvedelem/) nyilvánossá tett- **Adatvédelmi Szabályzata**, illetve **Adatvédelmi Incidens Kezelési Szabályzata**.

Tűzvédelmi Szabályzat,

A vagyonvédelemmel kapcsolatos rendelkezések,

Az informatikai rendszerekre vonatkozó szabványok, ajánlások (elsősorban a MeH ITB 12. ajánlása),

A Társaság tevékenységét a rá vonatkozó Szervezeti és Működési Szabályzat (a továbbiakban SZMSZ), valamint az ebből, a szakági utasításokból és a magasabb jogszabályokból levezetett ügyrendek, eljárásrendek és belső szabályzatok szabályozzák.

1.3 A szabályzat felülvizsgálatának rendje, hatálya

A felülvizsgálatot évente, vagy ha a működés rendjében változás történik, alkalmanként a Gazdasági Igazgatóság végzi el, és a felülvizsgálat tényét ellenőrzési lapon dokumentálja, melyet irattárba helyez.

Felülvizsgálat szükséges jogszabályváltozások esetén is, a jogszabályokban jelzett határidőig.

A szabályzatot és módosításait a Társaság nevében eljárni jogosult személy hagyja jóvá.

1.4 Az IBSZ hatálya

1.4.1 Az IBSZ területi hatálya

Az IBSZ rendelkezéseinek teljes körű és értelemszerű alkalmazása a Társaságnak a 1095 Budapest, Komor Marcell u. 1. (MÜPA) épületében elhelyezett valamennyi Társasági egységére nézve kötelező.

1.4.2 Az IBSZ személyi hatálya

Az IBSZ személyi hatálya kiterjed a Társaság minden alkalmazottjára, felhasználójára. A Társasággal nem jogviszonyban állók esetében gondoskodni kell arról a szerződéskötőnek, foglalkoztatónak, illetékes főosztályvezetőnek stb., hogy a szerződésekben az IBSZ megfelelő előírásai kötelezettségként megjelenjenek.

1.4.3 Az IBSZ tárgyi hatálya

Az IBSZ tárgyi hatálya kiterjed a Társaság valamennyi telephelyén lévő, különböző Társasági egységei által használt, vagy általuk tárolt valamennyi informatikai berendezésre, beleértve a berendezések műszaki dokumentációját is;

rendszerprogramokra és a felhasználói programokra;

védelmet élvező adatok teljes körére, keletkezésük és felhasználásuk, valamint feldolgozásuk helyétől, továbbá a megjelenési formájuktól függetlenül;

adathordozókra, azok tárolására és felhasználására, beleértve a feldolgozásra beérkezés és a felhasználókhoz történő eljuttatás folyamatait is;

az informatikai folyamatban szereplő valamennyi dokumentációra.

Az IBSZ területi, személyi és tárgyi hatálya kiterjed különösképpen a Társaság Gazdasági Igazgatóságára, a Társasággal szerződéses viszonyban és nem munkajogi kapcsolatban állók esetében a szerződéskötőnek gondoskodnia kell arról, hogy a szerződésekben az IBSZ megfelelő előírásai kötelezettségként megjelenjenek.

A felhasználók számára az IBSZ megismertetésére - hasonlóan az Adatvédelmi Szabályzathoz – kiadott ismertető, tájékoztató dokumentum hivatott.

Az IBSZ rendelkezéseit minden újonnan üzembe helyezett informatikai rendszer esetében teljes körűen alkalmazni kell. A szabályozás hatályba lépésének időpontjában már üzemeltetett rendszer esetében egyedi eltérés az informatikai biztonsági felügyelő jóváhagyásával meghatározott, átmeneti időszakra megengedhető.

2 Alapfogalmak

A jelen Szabályzatban, és annak mellékleteiben használt alapfogalmak meghatározásait két témakörben alkalmazzuk: általánosságban, illetve a kockázatviselés tekintetében. Az IBSZ tekintetében általános fogalmak:

Rendelkezésre állás - Olyan tulajdonság, amely lehetővé teszi, hogy az adott objektum, feljogosított entitás által támasztott igény alapján hozzáférhető és igénybe vehető legyen.

Bizalmasság, titkosság - Olyan tulajdonság, amely biztosítja, hogy az információt jogosulatlan egyének, entitások vagy folyamatok számára nem teszik hozzáférhetővé, és nem hozzák azok tudomására.

Információbiztonság - Az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá, egyéb tulajdonságok, mint a hitelesség, a számon kérhetőség, a letagadhatatlanság és a megbízhatóság, szintén ide tartozhatnak.

Információbiztonsági esemény - Valamely rendszer, szolgáltatás, illetve hálózat meghatározott állapotának előfordulása, amely az információbiztonsági szabályzat lehetséges megsértésére, vagy a biztonsági ellenintézkedések hiányára, vagy a biztonsággal esetleg összefüggő, korábban nem ismert helyzetre utal.

Információbiztonsági incidens - Nem kívánt, illetve nem várt egyedi vagy sorozatos információbiztonsági események, amelyek nagy valószínűséggel veszélyeztetik a működési tevékenységet és fenyegetik az információk biztonságát. [ISO 27001 / 3.6]

Sértetlenség - A vagyontárgyak pontosságának és teljességének védelmét biztosító tulajdonság.

Azonosító - Minden egyes felhasználónak saját személyes és kizárólagos használatára szóló egyedi azonosítóval (felhasználó ID) kell rendelkeznie.

Jelszó - „Valami, amit tudunk" Egy olyan egyedi karaktersorozat, amely az adott azonosítóval párosítva egyértelműen alkalmas a felhasználó azonosítására, és megfelel a jelszóval szemben támasztott követelményeknek.

Kulcs alapú azonosító - „Valami, amit birtoklunk" Egy a felhasználó birtokában lévő tárggyal azonosítjuk magunkat, ez lehet mechanikus kulcs, elektronikus kulcs, vagy intelligens kulcs.

Központi felhasználó menedzsment rendszer - A központi felhasználó menedzsment rendszer megoldást nyújt egy informatikai rendszer felhasználóinak mindenféle a rendszerrel kapcsolatos jogosultságainak kezelésére, a felhasználók Társaságba történő belépésétől a Társaságban történő tényked esein keresztül a Társaságból történő kilépésükig, és kiterjed más informatikai erőforrások, alkalmazások rendszerbe illesztése, módosítása, eltávolítása esetén szükséges felhasználói jogosultságok beállítására is. [Központi jogosultság és felhasználó menedzsment rendszerek fontossága az E-világban /2.2]

2.1 Kockázatkezelési alapfogalmak

Az ISO2700 szabványban nagy szerepet kapnak a kockázatkezelés egyes szakkifejezései, a következőkben az ISO Guide 73:2002-ben szereplő többi, kockázatkezeléssel kapcsolatos szakkifejezés és meghatározása található:

Esemény/ incidens - A körülmények egy adott összességének bekövetkezése.

Valószínűség - Annak a mértéke, hogy egy esemény milyen eséllyel következik be.

Következmény - Egy esemény eredménye.

Mérséklés - Egy adott esemény negatív következményének korlátozása.

Kockázat - Egy esemény valószínűségének és következményének kombinációja.

Kockázati forrás - Dolog vagy tevékenység, amely valamilyen következményt idézhet elő.

Kockázati szempontok - Hivatkozási alap, amely szerint a kockázat jelentőségének felmérése történik.

Érintett - Tetszőleges egyén, csoport vagy Társaság, amely befolyással lehet egy adott kockázatra, illetőleg amelyet e kockázat befolyásolhat, esetleg úgy érzékeli, hogy befolyásolhatja őt.

Érdekelt fél - Személy vagy csoport, amelynek érdeke fűződik egy Társaság teljesítményéhez vagy sikeréhez.

Kockázatkezelési rendszer - Egy Társaság irányítási rendszerének azon elemei, amelyek a kockázat kezelésével foglalkoznak.

Kockázatérzékelés - Az, ahogy egy érintett egy adott kockázatot felfog bizonyos értékekből és szempontokból kiindulva.

Kockázatismertetés - Kockázatra vonatkozó információ cseréje vagy megosztása a döntéshozó és más érintettek között.

Kockázatazonosítás - A kockázat egyes elemeinek megtalálása, összegyűjtése és jellemzése.

Forrásazonosítás - A kockázati források megtalálása, összegyűjtése és jellemzése.

Kockázatbecslés - Folyamat, amelynek segítségével értékeket rendelnek a kockázat valószínűségéhez és következményeihez.

Kockázatfelügyelet - A kockázatkezelés döntéseit megvalósító tevékenységek.

Kockázatoptimalizálás - Folyamat, amely. egy kockázathoz kapcsolódóan. minimalizálja annak negatív és maximalizálja annak pozitív következményeit, valamint ezek vonatkozó valószínűségeit.

Kockázatcsökkentés - Intézkedések, amelyeket egy kockázattal kapcsolatos valószínűség vagy a negatív következmények (vagy mindkettő) enyhítésére hoztak.

Kockázatelkerülés - Döntés bizonyos kockázati helyzetbe jutás megakadályozásáról, illetve intézkedés az ilyen helyzetből való kijutás érdekében.

Kockázatáthárítás - Egy adott kockázatból származó kár terhének, vagy hasznának másik féllel történő megosztása.

Kockázatvállalás - Egy adott kockázatból származó kár terhének, vagy hasznának tudomásul vétele.

Kockázatfinanszírozás - Pénzügyi támogatás biztosítása a kockázatfejlesztés megvalósításának költségeire és más kapcsolódó költségekre.

2.2 Egyéb alapfogalmak

Az ISO27001-ban előfordulnak olyan további szakkifejezések is, amelyek nem szerepelnek a szabvány szakkifejezései és meghatározásaik között, azonban a magyar megfelelőjének helyes értelmezéséhez további magyarázatra lehet szükség. A legfontosabb ilyen szakkifejezések meghatározása a következőkben található:

Érzékeny rendszer - Érzékeny információkat kezelő és feldolgozó rendszer. Az információ akkor tekinthető érzékenynek, ha az információhoz való jogosulatlan hozzáférés súlyos következményekkel járhat az érdekelt felek számára (pl. tulajdonos, üzemeltető, felhasználó).

Beültetett kód - Olyan rosszindulatú programkód, amely nem közvetlenül, illetve azonnal, hanem közvetetten és áttételeken keresztül, rendszerint időben jóval a beültetés (tulajdonképpen a szoftver megrontása) után fejti ki nem kívánt hatását.

Bevált gyakorlat - Olyan rutinszerűen végzett tevékenység, amely széles körű tapasztalatokon alapul, és több, különböző szervezetben is eredményesnek bizonyult. Megjegyzés: Gyakran félrevezetően "legjobb gyakorlat"-nak nevezik. Azonban semmilyen "adott körben és időszakban" bevált gyakorlat sem ad garanciát arra, hogy nem létezhet nála jobb gyakorlat.

Továbbvitel - Egy incidensre, problémára vagy változtatásra vonatkozó információ továbbadása nagyobb befolyással rendelkező személynek vagy más, nagyobb szakértelemmel rendelkező szakértőnek, és/vagy intézkedés kérése tőlük.

Helyreállítás - Egy szolgáltatás akkor tekinthető helyreállítottnak, ha a felhasználó újra képes az általa végzett tevékenység keretében feladatot végrehajtani, azaz a

rendszer és a rendelkezésre álló adatok visszaállítása megtörtént, a szükséges teszteket elvégezték, a felhasználót tájékoztatták, és minden elveszett munkát újra elvégeztek.

Meghibásodás - Akkor következik be, amikor valamilyen funkcionális egység (pl. berendezés, szoftver) alkalmatlanná válik rendeltetése betöltésére.

Megoldás - Az a tevékenység, amely egy incidenst követően újra lehetővé teszi a felhasználók számára feladataik végzését. Ez lehet akár ideiglenes megkerülő megoldás, akár a hibás részegység végleges megjavítása vagy cseréje.

Változásfelügyelet - Azok az eljárások, amelyek biztosítják, hogy minden változtatás ellenőrzött legyen, beleértve annak kérelmezését, rögzítését, elemzését, a vonatkozó döntés meghozását, jóváhagyását, kivitelezését és a változtatás megvalósítás utáni áttekintését is.

Vagyontárgy - Bármi, ami a Társaság számára érték, az infrastruktúra, eszközpark részét képező dolog.

3 Szabályozási elemek

A Társaság vezetése a szervezeti egységek vezetőinek közvetlen irányításával és a szervezeti egységek vezetői által a beosztott Munkatársak felé tett utasításokkal, eljárásrendek kialakításával közvetett módon köteles a Szabályzat elvárásainak megfelelő célok teljesülése érdekében irányítani a teljes Társaság információvédelmi működését.

3.1 Vezetőkre vonatkozó szabályok

A szervezeti egységvezető felelős jelen Szabályzat, és az Adatvédelmi Szabályzat szerinti működés betartásáért és beosztott Munkatársakkal történő betartatásáért, ellenőrzéséért és szükséges esetben az előírások megszegéséből eredő károk rendezéséért, szankcionálásáért, felelősségre vonásért.

A szervezeti egységvezető felelős a Szabályzat megismertetése érdekében információs anyagok kiadásáért, oktatás szervezésének elrendeléséért, a Munkatársak tájékoztatásáért.

A fentieken túl mindegyik szervezeti egységvezető köteles jelen Szabályzat, és az adatvédelemmel kapcsolatos Szabályzat előírásait megismerni és betartani.

3.2 Felhasználókra vonatkozó szabályok

Alábbiak tekintetében minden Munkatárs köteles a legnagyobb gondossággal eljárni:

Számítástechnikai eszközökkel kapcsolatos szabályok

- Az eszközök főigazgatói vagy gazdasági igazgatói döntés szerint a következők lehetnek: asztali számítógép (munkaállomás), hordozható számítógép, tablet, nyomtató, szkenner, FAX, fénymásoló, GPS és/vagy egyéb informatikai eszköz.
- A Felhasználó az eszközöket kizárólag a munkaköri feladatainak ellátása érdekében használhatja.
- A MÜPA Üzemeltető Kft. LAN hálózatához kizárólag nem hálózati (azaz nem router, switch, hub, wifi) saját eszköz csatlakoztatása lehetséges, ezt a rendszergazdával előzetesen egyeztetni szükséges.
- A Felhasználóknak biztosított eszközök és azok tartozékai, valamint az eszközökön telepített szoftverek licencei a Társaság vagy a MÜPA Üzemeltető Kft. tulajdonát képezik, azt a felhasználó másra át nem ruházhatja.
- Amennyiben a felhasználó bármilyen biztonsági problémát vagy hibát észlel azonnal köteles értesíteni az infrastruktúra szolgáltatást nyújtó (MÜPA Üzemeltető Kft.) üzemeltetésével kapcsolattartásra jogosult személyt, az informatikus rendszergazdát, vagy a biztonsági személyzetet.
- Tilos a számítástechnikai eszközöket és azok részeit áthelyezni, burkolatukat, csatlakozásaikat megbontani.
- Tilos a számítástechnikai eszközök közelében enni, inni, dohányozni.
- Tilos bármely hiba elhárítását jogosulatlanul megkezdeni. Meghibásodás esetén a Felhasználó köteles a rendszergazdát haladéktalanul értesíteni, a rendszergazda jogosult a hibák kijavításáról gondoskodni főigazgatói vagy gazdasági igazgatói engedély alapján.
- Tilos az irodai munkaállomásokon és a hordozható számítógépeken található rendszergazdai (admin) fiók törlése és a rendszergazdai fiók jelszavának megváltoztatása.

Jelszókezeléssel kapcsolatos szabályok

- A felhasználó 3 havonta (illetve meghatározott időnként) köteles jelszavait lecserélni.
- A megfelelő jelszó javasolt, hogy minimum 8 karakter hosszú legyen, (kicsi és nagy) betűket és számokat is kell tartalmaznia.
- A jelszó nem írható le semmilyen jól látható, vagy könnyen hozzáférhető helyre.
- Tilos a névre szóló jelszó kiadása más felhasználók számára.

Szoftverekkel kapcsolatos szabályok

- Az Társaság kizárólag jogtiszta szoftverekkel dolgozik. A jogtisztaság biztosítása a Társaság számára az infrastruktúra rendelkezésre állását biztosító MÜPA Üzemeltető Kft. feladata.
- Bármely más felhasználónak bármilyen terjesztési engedéllyel (freeware, shareware, stb.) rendelkező szoftvert, a cég tulajdonát képező számítógépre feltelepíteni nem megengedett. Egyéb szoftver igényt a főigazgatónak, gazdasági igazgatónak, vagy a rendszergazdának kell jelezni.
- Szoftverek telepítését/törlését csak az informatikus rendszergazda végezheti el. Ez alól kivételt képeznek a víruskeresők, melyek fertőzés esetén jogosultak a számítógépről fájlokat törölni.
- A szoftver licencek és telepítő lemezek a rendszergazda irodájában kerülnek tárolásra.

Adatvédelmi szabályok

- A munkahely elhagyása esetén a számítógépet zárolni kell a "Windows" + "L" billentyűk egyidejű lenyomásával, illetve olyan képernyővédőt kell beállítani, melyek jelszóval engedik csak a gép feloldását.
- A személyes, munkához közvetlenül nem kapcsolódó állományok tárolása mind a munkaállomásokon, mind a szervereken nem engedélyezett.
- A vállalati megosztott tárhelyekre (Google Drive, K meghajtó, Dropbox stb.) való feltöltéskor a Felhasználó felelőssége arról gondoskodni, hogy kizárólag illetékesek férhessenek hozzá az állományokhoz.
- Amennyiben a feltöltött állományok személyes adatokat tartalmaznak, Felhasználó köteles tájékoztatni a rendszergazdát, akinek kötelessége ellenőrizni, hogy az állományhoz kizárólag az illetékes Felhasználók férhetnek hozzá.
- A rendszergazda által minden számítógépen létrehozott osztott (Shared) mappa használata kizárólag arra az esetre vonatkozik, amikor a számítástechnikai eszközök között - üzleti céllal - adatállomány-mozgatás történik, illetve azokhoz feladatai során több Munkatárs hozzáférése is szükségszerű. Ezen mappákban tilos magánjellegű állományokat tárolni! Gondoskodni kell minden felhasználónak arról, hogy a munkájához kapcsolódó adatállományok adat-és titokvédelmi eljárásoknak megfelelően kerüljenek ezekbe a mappákba, a jogosulatlan munkatársak számára nem hozzáférhető

módon, az Adatvédelmi Szabályzattal összhangban védett módon sor kerülhessen az adatmentésre.

- Az eszközökön létrehozott és tárolt adatok (beleértve szöveges és képi állományokat és e-maileket is) a Társaság tulajdonát képezik és a Társaság ekként is kezeli, amíg ennek ellenkezőjéről megfelelő bírósági határozat nem születik. Amennyiben a Felhasználó mégis személyes adatot tárol a számítógépén, tudomásul veszi, hogy arról rendszeres biztonsági másolat készül.

- A felhasználónak a saját maga által kezelt (akár papíralapú, akár digitális formában elérhető) adatok tekintetében gondoskodnia köteles azok védelméről, közvetlen felügyeletéről, illetve őrizetlenül hagyása esetén elérhetetlenségéről (pl: zárt fiókban tárolás).

Internethasználattal kapcsolatos szabályok

- Tilos a munkahelyen minden valós idejű kommunikációs program használata (ide tartozik az facebook, skype és egyéb hasonló üzenetküldő használata), amennyiben nem a Munkatárs feladata a közösségi oldalak kezelése. Tilos, illetve engedélyhez kötött továbbá web- felületen keresztül elérhető valós idejű üzenetküldő úgynevezett "chat" program (pl: google hangouts program). A vezető jóváhagyása után használata megengedhető. Indokolt esetben a rendszergazda jogosult központilag tiltani ezen alkalmazásokhoz szükséges feltételeket.

- Tilos a munkahelyi internet kapcsolaton keresztül minden olyan program és egyéb fájl letöltése, ami nem a munkavégzéshez szükséges.

- Nem üzleti célú levelezés nem engedélyezett munkaidőn belül a munkahelyi számítógépeken.

- Mindenféle fájlmegosztó alkalmazás használata a Társaság számítástechnikai eszközein tiltott, a közös tárterületek használata biztosítja a csoportmunkát.

Vírusvédelmi szabályok

- A számítógépen vírusellenőrző program fut, mely a gép működése közben automatikusan figyeli a rendszert. A vírusellenőrző programot leállítani és annak működésébe beavatkozni szigorúan tilos.

- Minden fájlművelet előtt ez a program ellenőrzi a megnyitott fájlokat. Bármilyen, adatbiztonságot veszélyeztető esemény figyelmeztetése jelenik meg a felhasználó monitorán, azonnal értesítenie kell a rendszergazdát, hogy a megfelelő lépésekkel megakadályozhassák a kártékony programok további

fertőzéseit. Ugyanerről az eseményről a vírusirtó program elektronikus üzenetet küld rendszergazdák számára.

- Vírustalálat esetében a munkát azonnali hatállyal fel kell függeszteni, a számítógépet az adathálózatról le kell választani és megkezdeni az okok feltárását és a helyreállítást.

Eljárásrenddel kapcsolatos szabályok

- Az eszközök és szoftverek beszerzésére a Felhasználó javaslatot tehet a rendszergazdánál. A beszerzésről a végső döntést a főigazgató vagy gazdasági igazgató hozza meg a rendszergazda javaslata alapján.
- Az eszközöket főigazgatói vagy gazdasági igazgatói utasításra a rendszergazda szerzi be a következő szempontok együttes figyelembevételével: ár, szerviz szolgáltatás, a szállítás várható ideje, a szállító megbízhatósága.
- Átadás előtt a rendszergazda felelőssége az eszközök megfelelő üzembe helyezése, a szoftverek telepítése, majd a Felhasználó szükséges tájékoztatása a megfelelő használatról.
- A Felhasználó az informatikai eszközök átvételét és a használathoz szükséges tájékoztatást az aláírásával igazolja.
- Az eszközök állagának és üzemképességének megőrzéséről a Felhasználó köteles gondoskodni. Az eszköz elvesztéséből, megrongálásából, illetve nem megfelelő használatából eredő rendkívüli költségeket főigazgatói vagy gazdasági igazgatói döntés alapján a Társaság levonhatja a Felhasználó munkabéréből. Ehhez nyilatkozat aláírásával járul hozzá.
- Az eszköz átadására és használatára kizárólag az előzőekben említett nyilatkozat aláírásával egyidejűleg vagy azt követően kerülhet sor.
- Az informatikai eszközök visszavétele főigazgatói vagy gazdasági igazgatói utasításra jegyzőkönyv alapján történik a rendszergazdánál.
- A Felhasználó a munkafolyamatok megfelelő szabályozása és szervezése útján gondoskodni köteles arról, hogy jelen Szabályzat, valamint az Adatvédelmi Szabályzat előírásai maradéktalanul betarthatóak legyenek.

3.3 Külső felhasználókra vonatkozó szabályok

Külső felhasználók közvetlenül nem érik el, és nem használják a Társaság erőforrásait, alkalmazásait.

Minden külső felhasználóval történő kapcsolattartás (pl: a jegyrendelés, koncertszervezés, kottakölcsönzés) külön rendszerben működő alkalmazásokon keresztül történik (pl a ticket rendszeren keresztül), illetve a megfelelő Munkatárssal

történő kommunikáció alapján, meghatározott eljárásrend során benyújtott igények kezelésével.

Az adatkezelés, kapcsolattartás szabályozására az Adatvédelmi Szabályzat hivatott, annak megfelelő jogosultságok gyakorlása annak mellékletében rögzített módon történhet.

A Társaság üzemeltetése alatt álló weboldalon keresztül sem közvetlen (rendszer-alkalmazás-) elérés valósul meg, így csak az általános adatkezelési szabályok vonatkoztathatóak ezen felhasználókra.

4 Szerepkörök és felelősségek kialakítása

Szükségszerű meghatározni a munkafolyamatok, a Társaság működéséhez kellő kulcsfontosságú tevékenységek és végtermékei, adatai, dokumentumai, vagyontárgyai védelmében végzendő feladatokat. Egyértelmű szerepköröket és felelősségeket kell kijelölni, azokat az IBSZ hatékony végrehajtása, valamint az informatikai biztonságot megsértő események nyomán keletkező károk felmérése, szankciók meghatározása érdekében meghatározni.

Az informatikai munkatársak és a végfelhasználók szerepköreit és felelősségeit oly módon kell kialakítani, és ismertetni, hogy az informatikai munkatársak és a felhasználók között el legyen különítve a hatáskör, a felelősségek és a Társaság igényeinek kielégítéséért való felelősség tekintetében.

Megfelelő eljárásokat kell megvalósítani a felügyeletre vonatkozóan az informatikai funkción belül annak biztosítása érdekében, hogy a szerepköröket és felelősségeket szabályosan gyakorolják, valamint annak felmérése érdekében, hogy az összes munkatárs rendelkezik-e a szerepeik és felelősségi köreik teljesítéséhez szükséges megfelelő hatáskörrel és erőforrásokkal, valamint általában a Társaság informatikai biztonságának szemmel tartása végett.

A szerepköröket és felelősségeket oly módon kell megosztani, amely csökkenti annak lehetőségét, hogy egyetlen egy ne veszélyeztethessen egy teljes, kritikus fontosságú folyamatot.

Gondoskodni kell arról, hogy a munkatársak csak a munkakörüknek és beosztásuknak megfelelő, engedélyezett feladatokat hajtsanak végre.

4.1 Rendszergazda

Az infrastruktúrát a MÜPA Üzemeltető Kft. biztosítja a Társaság számára. A rendszergazda számára megfelelő infrastruktúra áll rendelkezésére, amely segíti a biztonság folyamatos szinten tartásában, a gyanús programok megkeresésében, vírusvédelemben stb.

A rendszergazda szerepkörben megbízott személy jogosult a megfelelő intézkedések megtételére – amelynek természetesen összhangban kell lenniük a biztonsági politikával –, valamint a MÜPA Üzemeltető Kft. üzemeltetésével kapcsolattartásra.

4.1.1 A rendszergazda/informatikus/ adatbázis adminisztrátor feladatai, felelőssége

A vírusellenőrző programok működésének beállítása a rendszergazda feladata és felelőssége, és a felhasználó nemhogy engedélyt, de lehetőséget sem kaphat a vírusvédelmi beállítások bármilyen módosítására.

A rendszer biztonságát közvetlenül vagy potenciálisan veszélyeztető helyzetben (pl: vírus- vagy beépített kódú támadás) a rendszergazdának joga van (és kötelessége) a hálózatról leválasztani és elérhetetlenné tenni bármely eszközt.

A rendszergazda által megszerezhető, a tevékenységek számítógépes naplózásával, a forgalom ellenőrzésével, továbbá más számítástechnikai eszközökkel gyűjtött információk csak a hálózat működésének javítására, a rendellenes használat kiszűrésére, illetve szabálysértő magatartás felderítésére használhatók.

Folyamatosan figyelemmel kíséri a Társaság infrastruktúrájának működését, rendelkezésre állását, az informatikai biztonságot sértő események előfordulását, az esetleges – legális felhasználók által – elkövetett tevékenységeket, amelyek a rendszer biztonságát veszélyeztetik.

Az üzletmenet szempontjából alapvető fontosságú informatikai rendszerek adatait tervezett módon, rendszeresen olyan biztonsági adathordozókra kell mentenie, amelyekről egy esetleges üzemzavar esetén egy utolsó, működőképes állapotot vissza lehet állítani. A biztonság érdekében a mentések egyik példányát az informatikai központtól távol kell elhelyezni. A biztonsági másolatok olyan készletét kell ilyen módon tárolni, amelyből újraindíthatók a számítógépes rendszerek, pótolhatóak a sérült adatbázisok, illetve biztosított az adatbázis teljes körű, naprakész adatainak kinyerése.

A Társaság domainjének, szervereinek, hálózati tárolóinak, Google szolgáltatásainak működéséről, valamint a szerverek és irodai munkaállomásokról készülő mentések ütemezett elvégzése, biztonságos tárolása a rendszergazda feladata, felelőssége. A szerverekről és az irodai gépekről rendszerszintű (image) és adatállomány szintű biztonsági mentéseket készít.

A rendszergazda tesz javaslatot arra, hogy mely rendszerek adatait, milyen gyakorisággal kell menteni és ehhez milyen eszközökre van szükség. A javaslatot a Gazdasági Igazgató hagyja jóvá.

A biztonsági mentések tartalmához kizárólag a rendszergazda férhet hozzá, kizárólag a következő esetekben:

a. hardverhiba, vírus-, beépített kód- és egyéb szoftveres támadás vagy eszköz meghibásodás következtében a munkaállomást és/vagy szervert újra kell telepíteni a biztonsági mentések felhasználásával, vagy

b. főigazgatói vagy gazdasági igazgatói utasítás esetén.

A rendszergazda kötelessége a saját felügyelet alatt használt szerverek karbantartása, adatainak biztonságos mentése, és kezelése, különös tekintettel a (fizikailag nem elkülönülő) munkaügyi szerverre is. A szerverterem biztonságosságát megvédi, a védelmi rendszereket rendeltetésszerűen, és kellő gondossággal, körültekintéssel használja (ajtózárral védett bejutás, tűzoltásra szolgáló készülékek, stb).

Az informatikai infrastruktúra bővítéséről, szoftverfrissítéséről és bármilyen fejlesztés elvégzéséről a rendszergazda gondoskodik, minden esetben a főigazgató vagy gazdasági igazgató írásos elrendelésével és engedélyével.

4.1.1.1 Feladatai az informatikai biztonság területén

Felméri és elemzi a működésből eredő, az adat- és az információvédelemmel összefüggő veszélyforrásokat.

Ellenőrzi az informatikai biztonság kialakítására, a megfelelő informatikai biztonság elérésére, illetve fenntartására vonatkozó szabályok, utasítások, előírások végrehajtását.

Szakmai szempontból, közvetlenül irányítja a használt informatikai rendszerek információvédelmét.

Szakmai szempontból irányítja az Informatikai biztonságra vonatkozó oktatást, a Szabályzat ismertetését.

Elemzéseket végez, szükség esetén javaslatokat tesz a megfelelő adat- és információvédelmi intézkedésekre, valamint a biztonságos működéssel összefüggő szabályok megváltoztatására.

Végzi az informatikai rendszerek információvédelmében vállalkozóként résztvevő gazdasági társaságok szakmai irányítását, ellenőrzi tevékenységüket.

Jogosult:

A vizsgálati tevékenysége során, a használatban lévő bármilyen iratba, dokumentumba, okmányba, adatbázisba, számítógépes vagy más adathordozó tartalmába való betekintésre.

A kezelésben, vagy használatban levő helyiségekben a berendezések, különösen az informatikai eszközök vizsgálatára.

Részt vesz:

- a rendkívüli események kezelésére szolgáló tervek elkészítésében, azok naprakészen tartásában;
- az Informatikai biztonság szempontjából fontosnak minősített munkakörök betöltési szabályainak, feltételeinek meghatározásában;
- a biztonsági követelmények és az előírások betartásának ellenőrzésében.
- A rendszergazda felelőssége, hogy
- tájékoztassa a Társaság új alkalmazottját a Társaság biztonsági rendjéről, a jelszavak használatáról,
- az új alkalmazottnak azonnal meg kelljen változtatnia a kiosztott jelszót (domain fiók és vállalati Google fiók megfelelő beállításával),
- tájékoztassa a Társaság új alkalmazottját a közös hálózati meghajtók (belső meghajtók és vállalati Google Drive) használati rendjéről, valamint az e-mail listák használatáról,
- egyeztessen a Társaság új alkalmazottjával a szükség szerint kijelölt mappák (pl. Dokumentumok, Asztal) rendszeres és automatikus biztonsági mentéséről,
- felmérje a Társaság új alkalmazottjának egyéb informatikai igényeit.

4.2 Társaság alkalmazottja, felhasználó

Köteles megismerni, munkavégzése során betartani ezen Szabályzat előírásait, valamint a külön szabályozott Adatvédelmi előírásokat.

Gondoskodni köteles különösen a 7. pontban meghatározott informatikai eszközök biztonsága érdekében hozott intézkedések betartásáról, valamint a 3.2 pontban meghatározott szabályok betartásáról.

4.3 Az informatikai biztonsági vezető /felelős kinevezett személy

Az informatikai biztonsági vezető (illetve a kinevezett felelős személy) általános feladata a MÜPA Üzemeltető Kft. által üzemeltetett és biztosított informatikai és távközlési rendszerek információvédelmével összefüggő tevékenységek jogszabályokkal való összhangjának megteremtése és fenntartása, ennek országos hatáskörű és Társasági szintű tervezése, szervezése, irányítása, koordinálása és ellenőrzése.

A felelősként kijelölt személy az informatikai rendszergazda személye, feladatait az Informatikai infrastruktúrát biztosító Társaság (MÜPA Üzemeltető Kft.) eszközeivel látja el.

4.4 Védelmi előírások

A felhasználó erőforrás, vagy szolgáltatás használatakor ne legyen jogosulatlanul azonosítható, azaz biztosítani szükséges a megfelelő azonosítást.

Az adat felhasználás tényének, módjának számon kérhetőségét biztosítani kell.

A felhasználás tényének védelme, mely szerint ne lehessen erőforrás, vagy szolgáltatás felhasználásairól jogosulatlanul adatokat gyűjteni.

A Társaság fentiekről a jogosultságkezelés, vírusvédelem, valamint az adatvédelem eljárásrendjei használatával gondoskodik.

5 Biztonsági szabályzás

Ezen szabályozás az információbiztonság tekintetében a működés követelményeinek, valamint a vonatkozó törvényeknek és szabályozásnak megfelelően lép érvényre.

A Társaság a korábban elkészült Adatvédelmi Szabályzat 0. fejezetében leírtak szerint gondoskodik az adatbiztonság, a személyes adatok tárolása, az információbiztonság érdekében vállalt intézkedésekről, biztosítja azok feltételeit.

5.1 Informatikai biztonsági rendelkezések, szabályozandó kérdések, eljárásrendek

A Társaság által megalkotott szabályzatokban nem kezelt eljárásrendek a kialakított gyakorlat során felülvizsgálatra kell kerüljenek, annak érdekében, hogy jelen Szabályzatnak és az Adatvédelmi Szabályozásnak megfeleljenek, valamint elkerülhetőek legyenek további információvédelmi kockázatokkal járó incidensek, események.

5.2 A kommunikáció és az üzemeltetés irányítása

A MÜPA Üzemeltető Kft. által biztosított informatikai és távközlési rendszerek üzemeltetetésével megbízott személyekkel való kapcsolattartásra az informatikus rendszergazda jogosult.

5.3 Jogosultságkezelés

5.3.1 Jogosultságkezelés célja

A jogosultságkezelés célja annak szabályozása, hogy csak azok férjenek hozzá az informatikai rendszerben tárolt adatokhoz és szolgáltatásokhoz, akiknek azokhoz szükséges hozzáférniük, valamint természetesen, akiknek mi előzetesen felhatalmazást adtunk erre.

5.3.2 Jogosultságkezelés során felhasznált eszközök

A Társaságnál minden felhasználó azonosítása megtörténik, (domain-szerveren keresztül) ám nem alkalmaznak kulcs alapú azonosítást egyetlen rendszer/alkalmazás eléréséhez sem, csak jelszavas azonosítással védett alkalmazásokat használnak.

5.3.3 Jogosultságkezelés folyamat lépései

Hozzáférés ellenőrzés - Hozzáférés-ellenőrzési szabályzat: Dokumentált hozzáférés-ellenőrzési szabályzatot kell kialakítani és azt a hozzáférésre vonatkozó, működési és biztonsági követelmények alapján felül kell vizsgálni.

Felhasználói hozzáférés irányítása - Az első lépés mindig a felhasználó regisztrálása. Minden információs rendszerhez és azokon belül minden szolgáltatáshoz egy hivatalos regisztrálási eljárást kell kezdeményezni. Amennyiben a felhasználó regisztrálása megtörténik, úgynevezett előjogokat és jelszavakat kell kiosztani a felhasználó számára, később a jogosultságokat időnként hivatalosan át kell vizsgálni. Amennyiben az alkalmazottnak megszűnik az alkalmazása, úgy a hozzáférésének jogosultságát meg kell szüntetni, változás esetén természetesen csak módosítani kell.

Felhasználói felelősségek - Azon túl, hogy szabályozzuk a felhasználók jogosultságait, minden a rendszerben regisztrált felhasználó felelősséggel tartozik a jelszavának védelméért, a jelszóválasztásnál figyelembe kell venni, az azzal kapcsolatos alapvető biztonsági elvárásokat.

A felhasználóktól meg kell követelni, hogy a jelszavak kiválasztásában és használatában a jó biztonság gyakorlatot kövessék. Védeni kell az őrizetlenül hagyott berendezéseket. A felhasználóknak biztosítaniuk kell az őrizetlenül hagyott berendezések megfelelő védelmét. Az úgynevezett „Tiszta asztal, tiszta képernyő" szabályzatot kell alkalmazni. Az iratok és eltávolítható adathordozók tekintetében a „tiszta asztal", míg az információ-feldolgozó eszközök tekintetében a „tiszta képernyő" szabályzatát kell alkalmazni.

5.4 Jelszókezelés követelményei

- A kezdetben generált jelszót az első bejelentkezés alkalmával kötelezően meg kell változtatni.
- A jelszónak minden felhasználó számára bármikor szabadon megváltoztathatónak kell lennie.
- A választott jelszó összefüggő szövegként soha ne legyen olvasható.
- A jelszó és a hozzátartozó azonosító soha nem kerülhet egy postai küldeménybe, még elektronikus levelezés során sem.
- A jelszó minimális hossza felhasználók esetében minimum 8 karakter, kiemeltebb jogosultság esetén 12 karakter hosszúnak kell lennie.
- A biztonságos jelszó kialakításánál, a kisbetűk, nagybetűk, számok és speciális karakterek csoportok közül legalább 3 fajta típust tartalmaznia kell a választott jelszónak.
- További feltétel, hogy nem tartalmazhatja a felhasználó nevét még részleteiben sem.
- A jelszó maximális élettartama felhasználók esetén 90 nap, míg adminisztrátorok esetén 30 nap.

- Amennyiben a felhasználó azt gyanítja, hogy jelszavát valaki megismerte azonnal le kell azt cserélnie.
- A jelszó ne legyen kívülálló számára kitalálható, ne tartalmazzon a felhasználó személyére utaló információkat.
- A jelszavakat nem szabad felírni, papíron tárolni, amennyiben az elkerülhetetlen (kezdetben generált jelszó esetén) gondoskodni kell a jelszó biztonságos helyen zárt borítékban történő tárolásáról.
- Amennyiben a felhasználó multiplatformos környezetet vagy több hitelesítés igénylő alkalmazást használ, lehetőség van a felhasználó számára egyetlen kellő hosszúságú és bonyolultságú jelszó alkalmazására.

A biztonságos jelszóhasználatot minden felhasználó számára oktatni kell. A felhasználókkal tudatosítani kell, hogy mindazon műveleteket, melyeket az ő azonosítójával és jelszavával mások hajtanak végre, az informatikai rendszer az ő „terhére" könyveli el, és azokért személyesen felel.

A személyes jelszóhoz a rendszergazda soha semmilyen formában nem fér hozzá, azonban megváltoztathatja, kizárólag a következő esetekben:

a. a Felhasználó saját kérésére,
b. az informatikai rendszer biztonságát veszélyeztető helyzetben (pl. vírustámadás),
c. ha a Felhasználó munkaviszonya megszűnik, vagy
d. főigazgatói vagy gazdasági igazgatói utasításra.

A rendszergazda, magasabb szintű biztonsági fiókkal hozzáférhet a Felhasználó adataihoz, kizárólag a következő esetekben:

e. a Felhasználó saját kérésére, vagy
f. főigazgatói vagy gazdasági igazgatói utasításra.

6 Kockázatkezelés /Kockázat felügyelet

A kockázatkezelés célja a kritikus rendszerek meghatározása, a folyamatos működésüket lassító vagy megszüntető veszélyforrások meghatározása, azok bekövetkezési valószínűségének vizsgálata és az általuk okozott kár felbecsülése. A megállapított kockázatok elkerülésére, észlelésére és/vagy elhárítására védelmi politikák kidolgozása.

Kockázatbecslés az a folyamat, amelynek segítségével értékeket rendelnek a kockázat valószínűségéhez és következményeihez.

Kockázatbecslés főbb lépései:

- Meghatározni a vállalat működése szempontjából kritikus rendszereket.
- Ezen rendszerek működését lassító vagy megakasztó veszélyforrásokat azonosítani.
- Szükségszerű elemezni a veszélyforrások bekövetkezési valószínűségét.
- Szükségszerű elemezni a veszélyforrások által okozott kárt.
- Szükségszerű a kockázatok kategorizálása.

A Társaság nem használ külön Kockázatfelügyeleti rendszert, nem végzett kockázatelemzést, kockázatbecslést, kockázatoptimalizálást, mivel nem használ kritikus vagy érzékeny rendszert. A kockázatok ésszerű mérséklésére törekszik, a kockázatelkerülés érdekében megelőző intézkedéseket tesz.

A Társaság nem használ külön Központi felhasználó menedzsment rendszert sem, a felhasználókról a rendszergazda naprakész dokumentációt tart fenn, mely lezárt borítékban megtalálható a titkárságvezető páncélszekrényében arra az esetre, ha a Társaság működését veszélyeztető informatikai probléma állna elő és a rendszergazda nem elérhető.

Információbiztonsági esemény / incidens előfordulásakor törekszik a károk, sérülések elhárítására, kezelésére, illetve további kockázatok elkerülésére.

6.1 Megelőző intézkedések

A Társaság érvényes, időszerűen naprakészen tartott Szabályzatokban gondoskodik a megelőző intézkedések alkalmazásáról.

A Társaság az infrastruktúrát biztosító MÜPA Üzemeltető Kft. Üzemeltetésével együttműködve gondoskodik a megfelelő eszközökről, munkakörülmények biztosításáról.

A számítástechnikai eszközök, géppark frissítése, selejtezés elrendelése a MÜPA Üzemeltető Kft., illetve a Társaság vezetése által automatikusan, (kb. 5 éventi rendszerességgel) történik.

Cél: Valamennyi olyan berendezést, amely tárolóeszközt foglal magában, ellenőrizni kell annak biztosítása érdekében, hogy az érzékeny adatok és engedélyezett szoftverek a selejtezést megelőzően eltávolításra, illetve biztonságos felülírásra kerüljenek.

Fenti cél teljesülése érdekében az informatikus rendszergazda gondoskodik az adatok végleges megsemmisítéséről.

6.2 Működési-folytonossági és katasztrófa-elhárítási intézkedések

A MÜPA Üzemeltető Kft. által biztosított épület, infrastruktúra része a megfelelő biztonsági intézkedések során elrendelt tűz-és vagyonvédelmi eljárás.

6.3 Mérés / monitorozás, annak ellenőrzése

A Társaságnál nem történik külön alkalmazással mérés, illetve monitorozás. Az alapvetően logolási eljárásokkal tárolt információk rögzítése történik automatikusan.

A MÜPA Üzemeltető Kft. által biztosított infrastruktúra része a megfelelő biztonsági intézkedések során a kamerafelvételek rögzítése, ki-be léptetés ellenőrzése, mágneskártyás beléptetések, ajtózárás / portai pótkulcs megfelelő kezelése.

7 Az informatikai eszközök biztonsága

A Társaság számára külső üzemeltető (MÜPA Üzemeltető Kft.) biztosítja az infrastruktúrát, ám szükségszerű hogy „jó gazdamódjára" megvédjük ezeket az eszközöket külső vagy belső támadásoktól esetleg a felhasználók tapasztalatlanságától. Az informatikai eszközök biztonságába egyaránt beleértendők a hardver és a szoftver összetevők védelme. Alábbi területeken a MÜPA Üzemeltető Kft. üzemeltetése biztosítja a feltételeket, a felhasználók a rendeltetésszerű használatot kötelesek megvalósítani.

7.1 Fizikai védelem és a környezet védelme

A fizikai védelmi intézkedések az információ feldolgozását kiszolgáló berendezések, helyiségek és az alkalmazottak védelmét szolgálják. Ilyenek például a vagyonvédelmi, a tűzjelző-, a beléptető- és a videó megfigyelőrendszerek vagy akár a szünetmentes áramforrások, védett kábelrendezők, klíma berendezések. Mindezeket a MÜPA Üzemeltető Kft. üzemeltetése biztosítja a Társaság számára.

7.2 Berendezések védelme

Cél: A vagyontárgyak elvesztésének, károsodásának, eltulajdonításának, illetve megrongálásának, valamint a Társasági működés fennakadásának megelőzése.

A berendezéseket úgy kell elhelyezni, illetve védeni, hogy csökkenjen a környezeti fenyegetésekből és veszélyekből eredő kockázat, valamint a jogosulatlan hozzáférés lehetősége. A berendezéseket védeni kell a közüzemi létesítményekben bekövetkező meghibásodások okozta áramkimaradásoktól és más kiesésektől, lehetőség szerint szünetmentes áramforrás használatával.

7.3 Kábelbiztonság

Az adatátvitelt bonyolító, illetve az információszolgáltatásokat támogató elektromos energiaátviteli és távközlési kábelhálózatot védeni kell a lehallgatástól és a károsodástól.

7.4 Berendezések karbantartása

A berendezéseket előírásszerűen karban kell tartani folyamatos rendelkezésre állásuk és sértetlenségük biztosítása érdekében.

A telephelyen kívüli berendezések biztonságot nyújtsanak, figyelembe véve a Társaság telephelyein kívül történő munkavégzésből eredő különböző kockázatokat.

Valamennyi olyan berendezést, amely tárolóeszközt foglal magában, ellenőrizni kell annak biztosítása érdekében, hogy az érzékeny adatok és engedélyezett szoftverek a selejtezést megelőzően eltávolításra, illetve biztonságos felülírásra kerüljenek.

7.5 Vagyontárgyak eltávolítása

Számítástechnikai berendezések, információk, illetve szoftverek előzetes engedély nélkül nem vihetők ki a telephelyről.

7.6 Logikai védelem és hozzáférés-ellenőrzés

A logikai védelmi intézkedések, megoldások az adatok bizalmas kezelését, sértetlenségének megőrzését, és folyamatos rendelkezésre állását biztosítják. Néhány példa a teljesség igénye nélkül: vírusvédelem, tűzfalak, behatolás-érzékelő rendszerek, autentikációs rendszerek, nyilvános kulcsú infrastruktúra a digitális aláírás és titkosítás megvalósítására, tartalomszűrés, stb.

7.7 Hozzáférés-ellenőrzési szabályzat

Dokumentált hozzáférés-ellenőrzési eljárást kell kialakítani és azt a hozzáférésre vonatkozó, működési és biztonsági követelmények alapján felül kell vizsgálni.

7.8 Felhasználói hozzáférés irányítása (lásd jogosultságkezelés)

Az információs rendszerekhez való jogosult hozzáférés biztosítása, illetve a jogosulatlan hozzáférés megakadályozása.

7.9 Felhasználók (pl: kölcsönzők, vevők) regisztrálása

Valamennyi információs rendszerhez és szolgáltatáshoz való hozzáférés megadására és visszavonására hivatalos felhasználó regisztrálási és regisztráció megszüntetési eljárást kell alkalmazni. A Társaság számára „külső" felhasználók regisztrálása a megfelelő szakterületi rendszerekben, alkalmazásokban történik, az infrastruktúrát üzemeltető (MÜPA Üzemeltető Kft.) hatáskörén túl.

7.10 Felhasználói jelszavak kezelése

A jelszavak kiosztását hivatalos kezelési folyamattal kell ellenőrizni, amit a Windows-os rendszerek alapján biztosított lehetőség használatával valósítható meg. Ez a Társaság hatáskörében történik, az infrastruktúrát üzemeltető (MÜPA Üzemeltető Kft.) feladatait nem képezi.

7.11 Felhasználói felelősségek

A MÜPA Üzemeltető Kft. által biztosított infrastruktúra használata során a jogosulatlan felhasználói hozzáférés, valamint az információk és információ-feldolgozó eszközök megrongálásának, illetve eltulajdonításának megelőzése.

7.12 Jelszóhasználat

A felhasználóktól meg kell követelni, hogy a jelszavak kiválasztásában és használatában a jó biztonság gyakorlatot kövessék, valamint ezen Szabályzat vonatkozó előírásait betartsák, alkalmazzák.

7.13 Őrizetlenül hagyott felhasználói berendezések

A MÜPA Üzemeltető Kft. üzemeltetésének biztosítania kell az őrizetlenül hagyott berendezések munkaidőn túli megfelelő védelmét, mindazonáltal a felhasználóknak szükséges gondoskodni a munkaidőben az őrizetlenül hagyott berendezések biztonságosságára.

7.14 A "Tiszta asztal, tiszta képernyő" szabályzata

Az iratok és eltávolítható adathordozók tekintetében a "tiszta asztal", míg az információ-feldolgozó eszközök tekintetében a "tiszta képernyő" szabályzatát kell alkalmazni. A felhasználónak gondoskodnia kell a felelőssége alá tartozó iratok, eszközök felügyeletlenül hagyásának elkerülésére mind a munkaasztaluk és számítógépük képernyője tekintetében.

8 Hálózati szintű hozzáférés ellenőrzés (külső szolgáltató végzi a hálózat üzemeltetését)

A Társaság számára külső üzemeltető (MÜPA Üzemeltető Kft.) biztosítja az infrastruktúrát, az alábbi területeken ezen cég üzemeltetése biztosítja a feltételeket az alábbi célok elérése érdekében. A felhasználók a rendeltetésszerű használatot kötelesek megvalósítani.

8.1 Hálózati szolgáltatások használatára vonatkozó szabályok

Cél: A hálózatos szolgáltatásokhoz való jogosulatlan hozzáférés megakadályozása

8.2 Felhasználó hitelesítése külső csatlakozások esetén

Cél: A felhasználók csak azokhoz a szolgáltatásokhoz kaphassanak hozzáférést, amelyek használatára kifejezett jogosultságuk van.

8.3 Berendezések azonosítása a hálózatokban

Cél: Az automatikus berendezés azonosítást úgy kell tekinteni, mint a speciális helyekről és elrendezésekről megvalósuló összeköttetések hitelesítési módját.

8.4 Távdiagnosztikai és konfigurációs portok védelme

Cél: Az automatikus berendezés azonosítást úgy kell tekinteni, mint a speciális helyekről és elrendezésekről megvalósuló összeköttetések hitelesítési módját.

8.5 Elkülönítés a hálózatokban

Cél: Az automatikus berendezés azonosítást úgy kell tekinteni, mint a speciális helyekről és elrendezésekről megvalósuló összeköttetések hitelesítési módját.

8.6 Hálózathoz való csatlakozás ellenőrzése

Cél: Az automatikus berendezés azonosítást úgy kell tekinteni, mint a speciális helyekről és elrendezésekről megvalósuló összeköttetések hitelesítési módját.

8.7 Hálózati útvonal ellenőrzése

Cél: A hálózatokban az útvonal ellenőrzést kell bevezetni annak biztosítására, hogy a számítógépes összeköttetések és az információáramlás ne sértsék a működési alkalmazásokra vonatkozó hozzáférés-ellenőrzési szabályzatot.

8.8 Operációs rendszer szintű hozzáférés-ellenőrzés

Cél: Az operációs rendszerekhez való jogosulatlan hozzáférés megelőzése

8.9 Biztonságos bejelentkezési eljárások

Cél: Az operációs rendszerekhez való hozzáférést biztonságos bejelentkezési eljárásokkal kell ellenőrzés alatt tartani.

8.10 Felhasználó azonosítása és hitelesítése

Cél: Minden egyes felhasználónak saját személyes és kizárólagos használatára szóló egyedi azonosítóval (felhasználó ID) kell rendelkeznie, és alkalmas hitelesítési technikát kell választani a felhasználó állítólagos azonosságának igazolására.

8.11 Jelszókezelő rendszer

Cél: A jelszavak kezelésére szolgáló rendszereknek interaktív rendszereknek kell lenniük és jó minőségű jelszavakat kell biztosítaniuk.

A Társaság nem alkalmaz jelszókezelő rendszert, az informatikus rendszergazda által megadott első jelszó azonnali (felhasználó általi) megváltoztatásával biztosított annak ismeretlensége, titkossága.

8.12 Rendszer-segédprogramok használata

Cél: Korlátozni és szigorúan ellenőrizni kell a rendszer segédprogramjainak használatát, amelyek alkalmasak lehetnek a rendszer- és alkalmazásellenőrzés megkerülésére.

8.13 Kapcsolati idő túllépése

Cél: Az inaktív összeköttetéseket meghatározott időtartamú inaktivitás után bontani kell.

8.14 Az összeköttetés idejének korlátozása

Cél: A magas kockázatú alkalmazások kiegészítő biztonsága érdekében korlátozni kell az összeköttetés idejét.

9 Alkalmazás és információ szintű hozzáférés-ellenőrzés

Az alkalmazási rendszerekben tárolt információhoz való jogosulatlan hozzáférés megelőzése céljából eljárásrendet kell kidolgozni az alábbiakra tekintettel:

9.1 Információ hozzáférés korlátozása

Az információkhoz és az alkalmazási rendszerek funkcióihoz való felhasználói és támogatószemélyzeti hozzáférést a kialakított hozzáférés-ellenőrzési szabályzattal összhangban korlátozni kell.

9.2 Érzékeny rendszerek elkülönítése

Az érzékeny rendszereknek egy erre a célra létesített (elkülönített) számítógépes környezettel kell rendelkezniük. (A Társaság nem használ érzékeny/kritikus rendszert, csak a vállalati felépítés szerint elkülönített munkaügyi / gazdasági rendszereket)

9.3 Mobil számítógép használata és távmunka

Az információbiztonság megőrzése mobil számítógép használatra és távmunka végzésére szolgáló berendezések használata esetén is biztosítva legyen. Azon felhasználóknak, akiknek a távmunka engedélyezett különös tekintettel kell lenniük eszközeit védelmére.

Hordozható számítógépeken a Felhasználó rendszergazdai jogokkal rendelkezik, ezért Felhasználó fokozott elővigyázatossággal köteles az eszköz működőképességéről gondoskodni.

Felhasználó kötelessége, hogy a hordozható eszközökön tárolt kritikus fontosságú állományokról másolatot tartson fenn az irodai munkaállomásokon vagy bármely rendelkezésre álló, a Társaság tulajdonában lévő megosztott tárhelyen, ahonnan ezek az állományok automatikusan biztonsági mentésre kerülnek.

A hordozható számítógépekre a rendszergazda saját, rendszergazdai (admin) fiókot is létrehoz, mely a Felhasználótól független elérhetőséget biztosít az eszközhöz.

9.4 Mozgatható perifériák és adathordozók kezelése, engedélyezése

Vagyontárgyak illetéktelen kiadásának, módosításának, eltávolításának, vagy tönkretételének, valamint a működési tevékenységek megszakadásának megelőzése érdekében az engedélyezés menete eljárásrenddel szabályozott kell legyen.

9.5 Összegző megállapítások / Eljárásrendek kialakítása

Szükségszerű eljárásrendek kialakítása, dokumentálása a mobil eszközök engedélyezése, a kockázatkezelés, incidenskezelés és a felhasználói felelősségek ezen Szabályzat által nem részletezett pontjainak tekintetében.

Az Adatvédelmi Szabályzat, annak betartása szerves egységét képezi jelen Szabályzatnak is, betartása és ellenőrzése a Társaság hatásköre, felelőssége.

9.6 Drótnélküli eszközök használatának szabályai

A drótnélküli eszközöket működését tekintve több kategóriába soroljuk, melyek Infravörös vagy Rádióhullámon működhetnek. A szabályzat használat közbeni célja, az ilyen eszközökön lévő információk megóvása, és az azt támogató infrastruktúra védelme.

A biztonsági jellemzőket, a szolgáltatási szinteket és a valamennyi hálózati szolgáltatásra vonatkozó irányítási követelményeket azonosítani és hálózati szolgáltatási megállapodásban rögzíteni kell, legyenek ezek akár belső, akár külső szolgáltatásként nyújtottak.

Az infrastruktúra szolgáltatást nyújtó (MÜPA Üzemeltető Kft.) cég hatáskörébe tartozó feladat ennek biztosítása.

9.7 Asztali telefon, mobil eszköz használat

Engedélyezési eljárás után használhatóak a mobil eszközök, felhasználójuk köteles fokozott elővigyázatossággal használni, védeni mobil eszközeit.

Az asztali telefon használatához kötött korlátozás érinti a külföldi távbeszélés tiltását.

9.8 Incidenskezelés

9.8.1 Az incidens megfogalmazása

Nem kívánt, illetve nem várt egyedi vagy sorozatos információbiztonsági események, amelyek nagy valószínűséggel veszélyeztetik a működési tevékenységet és fenyegetik az információk biztonságát. Ennek megtörténtekor – például egy vállalat levelezése támadás vagy vírus következtében megbénul – fontos, hogy legyen egy olyan csoport, akik az incidenst lekezelik és a bekövetkezett problémát megoldás céljából a megfelelő helyre eszkalálják. A rendkívüli eseményt (incidenst) érzékelő személy (felhasználó) köteles jelezni az intézkedésre jogosult személy felé. Az informatikai problémákat az informatikus, rendszergazda felé, aki adott esetben a MÜPA Üzemeltető Kft. üzemeltetésével kapcsolattartóként eljárhat.

9.8.2 Az incidens megoldása

A rendszergazda/ infrastruktúra üzemeltető az incidenst követően újra lehetővé teszi a felhasználók számára feladataik végzését. Ez lehet akár ideiglenes megkerülő megoldás, akár a hibás részegység végleges megjavítása vagy cseréje, illetve egyéb megoldás.

9.8.3 Információbiztonsági incidensek kezelése

Szükséges annak biztosítása, hogy az információs rendszerekkel összefüggő információbiztonsági események és gyengeségek kommunikálása olyan módon történjék, ami időben lehetővé teszi a szükséges helyesbítő intézkedések megtételét.

9.9 Információbiztonsági események és gyengeségek jelentése

Az információk biztonságát érintő eseményeket megfelelő Társasági csatornákon keresztül a lehető leggyorsabban jelenteni kell.

Az események jelentésére külön eljárást van érvényben (értesítendő az informatikus rendszergazda), amelyet minden szerződő és használó harmadik félnek ismernie és használnia kell.

Az információs rendszereket és szolgáltatásokat használó valamennyi alkalmazottól, szerződő vállalkozótól és harmadik féltől meg kell követelni, hogy jegyezze fel és jelentse a rendszerekben, illetve szolgáltatásokban észlelt, vagy feltételezett bármiféle gyenge pontot.

A felhasználók a felfedezett gyenge pontokról és rendellenességekről – annak súlyosságától és sürgősségétől függően – e-mailben és/vagy telefonon haladéktalanul értesíti a rendszergazdát. A jelentést elkészítő személyt okvetlenül tájékoztatni kell arról, hogy a sejtett biztonsági gyengeséget ne ellenőrizze: a rendszerben kárt okozhatnak, vagy információkkal élhetnek vissza, ami jogi következményekkel járhat a vizsgálatot végző személynek.

9.10 Tanulságok levonása az információbiztonsági incidensekből

A Társaság számára cél annak biztosítása, hogy az információbiztonsággal összefüggő incidenseket következetes és hatékony megközelítéssel kezeljék, esetleges előfordulás után a kiváltó okok ismétlődésének elkerülésére eljárásrend módosítását szükséges eszközölni. (Pl: a telefonközpont hackelése után a kimenő külföldi hívások tiltása).

Az információbiztonsági incidensekre történő gyors, hatékony és szabályszerű válasz biztosítása érdekében rögzíteni kell a vezetői felelősségeket és eljárásokat.

A rendszert és a rendszert érintő riasztásokat és sérülékenységeket folyamatosan figyelemmel kell kísérni az információbiztonsági incidensek felfedésére.

Az információbiztonsági incidensek kezelésének célját egyeztetni kell a vezetőséggel, és biztosítani kell, hogy a Társaság elsőbbséget élvezzen.

9.11 Monitorozás és naplózás

A rendszergazda incidens esetén a domain-szerver információból, logok alapján tud monitorozást végezni, más, külön célú monitorozás és naplózás nem történik a Társaságnál.

9.12 Vírusvédelem

Az infrastruktúra részeként a MÜPA Üzemeltető Kft. biztosítja, a hálózati tűzfal és szoftveres megoldások által.

9.13 Segédeszközök

Tömeges fájl-műveleteket blokkoló alkalmazás bevezetése, alkalmazása biztosítja még a védelmet.

9.14 Informatikai üzemeltetés

Az alábbi használati előírások betartásáról az informatikus, rendszergazda gondoskodik (az infrastruktúrát biztosító (MÜPA Üzemeltető Kft.) eszközein:

A vírusvédelmi szoftvereket naprakészen tartása, mindig az elérhető legújabb stabil verziót kell feltelepíteni a felhasználók gépeire.

A vírusvédelmi szoftver kikapcsolását sosem szabad engedélyezni.

Minden fájlt ellenőrizni kell a használata előtt, amelyet elektronikus vagy optikai adathordozóról szeretnénk használni vagy a hálózaton keresztül szereztünk be.

Ellenőrizni kell az e-mail csatolmányait és a letöltött állományokat mielőtt használnánk azokat.

Ellenőrizni kell a weboldalakat kártevő kódok ellen.

Az üzletmenet-folytonosság érdekében rendszeresen mentenünk kell a fájlokat, hogy azok visszaállíthatóak legyenek a kártevő kódok támadása után is.

10 Használati előírások

10.1 Levelezés (Elektronikus üzenetek küldése/fogadása)

A 2./2018. sz., és a 4./2018 sz. belső adatvédelmi utasításokban meghatározott szabályok betartása kötelező.

10.2 Az IBSZ figyelemmel kisérése és átvizsgálása

A felülvizsgálatot évente, vagy ha a működés rendjében változás történik, alkalmanként a Gazdasági Igazgatóság hatáskörében eljáró személy végzi el, és dokumentálja, esetleg jelen szabályzat rendelkezéseinek módosításával.

10.3 Használati előírások

Az IBSZ használatára vonatkozó nyilatkozat, az utasítás tudomásul vételének igazolása

- Minden jelen utasítás hatálya alá tartozó személy jogállásától, jogviszonyától függetlenül köteles a szolgálati út betartásával a jelen utasításra vonatkozó megismerési nyilatkozatot saját kezűleg aláírni.

10.4 Képzés, tudatosság és felkészültség

A Szabályzat ismeretéről, betartásáról, módosításáról, illetve a Szabályzathoz kapcsolódó képzésről, valamint az ezekhez kapcsolódó információs anyagokról a Társaság gondoskodik a felhasználói felé.

10.5 Internet használat

Az infrastruktúrát biztosító (MÜPA Üzemeltető Kft.) tartalomszűrő rendszerén keresztül engedélyezett.

10.6 Segédeszközök

A Társaság által készített dokumentumok (pl „Munkatársi adatvédelmi kisokos") segítik a Szabályzatok ismertetését.

10.7 Külső ügyfelek, partner kezelés

A biztonság kérdésének kezelése harmadik féllel kötött megállapodásokban: A harmadik felekkel kötött megállapodásoknak, beleértve a Társaság információihoz, illetve információ-feldolgozó eszközeihez való hozzáférést, azok feldolgozását, kommunikálását, illetve kezelését, valamint termékeknek, illetve szolgáltatásoknak az információ-feldolgozó eszközökhöz való hozzáadását, valamennyi vonatkozó biztonsági követelményt tartalmazniuk kell.

Valamennyi alkalmazottnak, a szerződőknek és a felhasználó harmadik félnek vissza kell szolgáltatnia a Társaság valamennyi birtokukban lévő vagyontárgyát, amikor alkalmazásuk, szerződésük, illetve megállapodásuk lejár, illetve megszűnik.

A külső partnerek adatait, szerződéseit a megfelelő feladatra, kapcsolattartásra jogosult alkalmazott kezeli, a Társaság Adatvédelmi Szabályzatának megfelelően.

10.8 Szolgáltatásnyújtás (pl: kottatár/ kölcsönzés) szabályai

Biztosítani kell a harmadik felekkel szolgáltatásnyújtására kötött megállapodásokban foglalt biztonsági intézkedések, szolgáltatás meghatározások és szolgáltatásnyújtási szintek harmadik felek általi megvalósítását, működtetését és fenntartását.

10.9 Harmadik felek szolgáltatásainak figyelemmel kisérése és átvizsgálása

A harmadik felek által nyújtott szolgáltatásokat, jelentéseket és feljegyzéseket rendszeresen figyelemmel kell kísérni és át kell vizsgálni.

Pl: A gazdálkodási rendszer könyvelését külső szolgáltató végzi, a megfelelő felhasználó rendelkezzen csak hozzáféréssel a kliens gépen futó alkalmazáshoz.

10.10 Adathordozók kezelése

Vagyontárgyaknak minősülő adathordozók illetéktelen kiadásának, módosításának, eltávolításának, vagy tönkretételének, valamint a működési tevékenységek megszakadásának megelőzése céljából kialakítandó megfelelő eljárásrend.

10.11 Információcserére vonatkozó szabályzatok és eljárások

Az 1./2018. sz., 4.62018. sz., 8./2018. sz., valamint a 10./2018 számú belső adatvédelmi utasítás szabályai alkalmazandóak.

10.12 Fizikai adathordozók szállítása

A felhasználók fokozott figyelmű, biztonságra való törekedés mellett engedélyezett

11 Az információbiztonsági oktatás rendje, célja

A rendszergazdai, felhasználói tájékoztatáson kívül, amint szükségességét érzi, a Társaság dönt az oktatás lebonyolításáról.

12 Intézkedések:

12.1 Társasági feljegyzések védelme / adatvédelem

A törvényben meghatározott, szabályozási, szerződéses és működési követelményekkel összhangban a fontos feljegyzéseket meg kell óvni az elvesztéstől, a megsemmisüléstől és a meghamisítástól.

A felhasználó, mint a Társaság alkalmazottja köteles védeni a Társasági feljegyzések mind papíralapú, mind elektronikus változatát.

A Társaság nem rendelkezik a különös tekintettel a szerződések tárolására nagyobb biztonságot nyújtó szoftveres védelemmel, az adatok tárolására csak mint a windows-os rendszerek alapvető alkalmazásai (pl: excel) használtak.

12.2 Adatvédelem és a személyes adatok titkossága

Külső és belső Adatvédelmi Szabályzat elkészítése, bevezetése korábban megtörtént.

https://drive.google.com/drive/folders/1TwSuidRRmOjq-4Z9JHTOrdYxPna_MJ6_

12.3 Információ-feldolgozó berendezésekkel való visszaélések megelőzése

Az információ-feldolgozó eszközök előírásszerű és biztonságos üzemeltetésének biztosítása érdekében

- Dokumentált üzemeltetési eljárások: Az üzemeltetési eljárásokat dokumentálni szükséges, és azokat karban kell tartani, illetve minden olyan felhasználó számára hozzáférhetővé kell tenni, akiknek arra szükségük van.

- Változáskezelés: Az információ-feldolgozó eszközök és rendszerek változtatásait szabályozni kell.

- Feladatkörök, kötelezettségek elhatárolása: A feladatköröket és felelősségi területeket szét kell választani a Társaság vagyontárgyai jogosulatlan, illetve nem szándékolt módosítása, illetve az azokkal való visszaélés lehetőségeinek csökkentése érdekében

- Jogosultsági engedélyezési folyamat az információ-feldolgozó eszközökre vonatkozóan: Folyamatot kell kialakítani és bevezetni az új információ-feldolgozó eszközökkel kapcsolatos jogosultságok vezetőségi engedélyezésére.

12.4 Titkosítási eljárások szabályozása

A Társaság nem rendelkezik Titkosítási, Titkosított iratok Ügykezelésével foglalkozó szabályzattal, nem is kezel ebbe a kategóriába tartozó iratokat, információkat.

13 Záró rendelkezés

Jelen szabályzat 2019. május 1. napján, lép hatályba, és a hatályos Adatvédelmi Szabályzattal együtt érvényes.