INFORMATIKAI BIZTONSÁGI SZABÁLYZAT 2020.

Szervezet neve: **Székesfehérvár Városgondnoksága Kft.**

Címe: 8000 Székesfehérvár, Szent Vendel u. 17/a.

Adószáma: 14823495-2-07

Képviseletre jogosult személy neve: Bozai István ügyvezető

Jelen szabályzatban nem szabályozott kérdésekben az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény és a kapcsolódó jogszabályok vonatkozó előírásai szerint kell eljárni. Felülvizsgálata és karbantartása a jogszabályi változások függvényében.

Hatályba lépett: 2020.04.01

Egyidejűleg hatályát veszti: Informatikai Biztonsági Szabályzat 2019.

Bozai István
ügyvezető

1. Az Informatikai Biztonsági Szabályzat célja

Az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) alapvető célja, hogy a Székesfehérvár Városgondnoksága Kft.-nél (továbbiakban: Kft., vagy: munkáltató) az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, és megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

A szabályzatban rögzített intézkedések célja, hogy a Kft. informatikai rendszereinek és az azok által kezelt adatok biztonságának megfelelően eredményes és hatékony működést biztosítson.

A Kft.-nél található informatikai rendszerek, a számítástechnikai infrastruktúra létének elsődleges célja a munkavégzés biztosítása. A számítástechnikai eszközök, a rajtuk zajló folyamatok, a felhasználó által kifejtett aktivitás és a tárolt adatok az informatikai rendszerek biztonsága érdekében a munkáltató által ellenőrizhetők és rögzíthetők. Az informatikai és alkalmazói rendszerekkel, szolgáltatásokkal való szándékos visszaélések megelőzése és utólagos felderítése érdekében az informatikai és alkalmazói rendszerek, szolgáltatások használatát a munkáltató jogosult rögzíteni (naplózni) és ellenőrizni.

Az IBSZ célja továbbá:

- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használatának biztosítása,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése,
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság, valamint az archiválás feltételeinek megteremtése.

2. Az Informatikai Biztonsági Szabályzat hatálya

2.1. Személyi hatálya

Az IBSZ személyi hatálya kiterjed a Székesfehérvár Városgondnoksága Kft. minden munkavállalójára, minden olyan személyre, aki a Székesfehérvár Városgondnoksága Kft. tulajdonában lévő informatikai eszközöket vagy informatikai szolgáltatásokat használja, valamint az informatikai rendszerrel kapcsolatba kerülő, de nem a Kft. alkalmazásában álló jogi- és természetes személyekre.

2.2. Tárgyi hatálya

Az IBSZ-ben foglaltakat alkalmazni kell a Kft. valamennyi informatikai rendszerére, amely tárolja, kezeli, feldolgozza, ellenőrzi vagy továbbítja a Kft. kezelésében vagy tulajdonában álló adatokat, információkat.

2.3. Területi hatálya

Az IBSZ-ben foglaltakat alkalmazni kell a Kft. összes telephelyén, valamint minden egyéb helyszínen, ahol a Kft. tulajdonában lévő informatikai eszközt alkalmaznak.

3. Az adatkezelés során használt fontosabb fogalmak

Adathordozó: olyan eszközök összessége, amelyek alkalmasak az adatok tárolására, megőrzésére.

Informatikai eszközök: olyan hardvereket, szoftvereket, hálózatokat és szolgáltatásokat jelent (eszközök), amelyek információk rögzítésével, kezelésével, rendszerezésével, továbbításával foglalkoznak.

Adatkezelés: az adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

Adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza (ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja).

Adatfeldolgozás: az adatkezelő nevében végzett adatkezelés, köztük például adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adaton végzik.

Adattovábbítás: ha az adatot meghatározott harmadik fél számára hozzáférhetővé teszik.

Harmadik fél: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.

Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel

Adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Nyilvánosságra hozatal*:* ha az adatot bárki számára hozzáférhetővé teszik.

4. Védelmet igénylő, az informatikai rendszerre ható elemek

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.
Az informatikai rendszerre az alábbi tényezők hatnak:

- a környezeti infrastruktúra,
- a hardver elemek,
- az adathordozók,
- a dokumentumok,

- a szoftver elemek,
- az adatok,
- a rendszerelemekkel kapcsolatba kerülő személyek.

A védelmi intézkedések kiterjednek:

- az alkalmazott hardver eszközökre és azok működési biztonságára,
- az informatikai eszközök üzemeltetéséhez szükséges dokumentációkra,
- az adatokra és adathordozókra a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára.
- informatikai hálózatok elemeinek felügyeletére, szükséges esetekben a hálózati kapcsolatok, vagy egyes veszélyesnek minősített weboldalak és szolgáltatások elérésének korlátozására.

A mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

5. A védelem felelősei

Az informatikai védelem felelőse a mindenkori informatikai vezető és az informatikusok.

A felelősök feladatai:

a) Informatikai vezető feladatai:

- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására,
- amennyiben szükséges, meghatározza a védett adatok körét,
- ellátja az adatkezelés és adatfeldolgozás informatikai felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- az adatvédelmi feladatok ismertetése,
- ellenőri tevékenységének adminisztrációja,

b) Informatikus feladatai:

- Jogosultságok kezelése: az informatikus feladata a munkavállaló vezetője által adott utasítás alapján a számítástechnikai jogosultságok kiosztása, kezelése és karbantartása.
- Vírusvédelem: a vírusvédelmi rendszer működőképességének folyamatos vizsgálata, illetve biztosítása, az esetleges vírusvédelmi riasztások tanulmányozása és a teljes körű védelem érdekében szükséges intézkedések megtétele.
- Hozzáférés védelem: az informatikus köteles a Kft. területén elérhető vezeték nélküli internet hálózatot (wifi) jelszóval ellátni. Továbbá feladata a vezeték nélküli hálózat használatára szoruló, jogos igényt felmutató felhasználók tájékoztatása, a hozzáférés biztosítása, active directory.
- Az informatikus köteles a központi szerveren kialakított „közös” meghajtók, mappák hozzáférését központilag szabályozni.
- Hibaelhárítás: az informatikus köteles a lehető legrövidebb időn belül elhárítani az informatikai rendszerhez kapcsolódó hibákat.

Az informatikus a saját feladatkörébe tartozó rendszert felügyeli, illetve

- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újraindításhoz

szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének folyamatos ellenőrzése,
- felelős a vállalkozás informatikai rendszer hardver eszközeinek karbantartásáért,
- gondoskodik a folyamatos vírusvédelemről,
- vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működése és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a szoftverek használatának jogszerűségét.
- ellenőrzi a rendszer adminisztrációját.

c) A hálózati infrastruktúra:
A hálózati infrastruktúrát és szervereket az Önkormányzati Informatikai Központ Kft üzemelteti. Az ÖIK feladatait az érintett felek által megkötött karbantartási, üzemeltetési és adatfeldolgozási szerződés tartalmazza részletesen.

6. A Felhasználó és az informatikai biztonság:

A Kft. valamennyi munkavállalójának, mint felhasználónak kötelezettsége az információvédelem területén az adott helyzetben elvárható magatartást tanúsítani és tartózkodni minden károkozó tevékenységtől. A felhasználónak a tőle elvárható módon gondoskodnia kell az adatok és információk biztonságáról.

Minden munkavállaló munkaviszonya létesítésekor köteles a jelen szabályzat 1. számú mellékletét képező „Nyilatkozat informatikai eszköz használatának szabályairól" című nyomtatványban foglaltakat értelmezni és azokat aláírásával tudomásul venni.

Rögzíteni kell, hogy a munkavállaló által átvett informatikai eszközök a Székesfehérvár Városgondnoksága Kft. tulajdonában vannak, azok a munkaköri feladatok ellátását hivatottak szolgálni. Az informatikai rendszerek biztonsága érdekében a munkavállalókat tájékoztatni kell arról, hogy az internet és e-mail eléréseket a munkáltató szűri és az informatikai- és alkalmazói rendszerekkel, szolgáltatásokkal való szándékos visszaélések megelőzése és utólagos felderítése érdekében az informatikai alkalmazói rendszerek, szolgáltatások használatát rögzítheti (naplózhatja) és ellenőrizheti.

A munkáltató jelen szabályzat megismerésével felhívja a munkavállalók figyelmét arra, hogy informatikai eszköz/ök visszaadásakor a munkavállalónak törölnie kell a magánjellegű fájlokat.

6.1. Általános rendelkezések:

Minden felhasználó kötelessége a hozzá rendelt informatikai eszközök rendeltetésszerű használata, a Kft. alkalmazói rendszereinek, felhasználói leírásainak megismerése, és az alkalmazások használatakor az őt érintő előírások maradéktalan betartása.

A felhasználónak a következő fizikai biztonsági előírásokat kell betartani:

- Az informatikai eszközökhöz és adatokhoz történő illetéktelen vagy jogosulatlan hozzáférés megelőzése érdekében a felhasználónak a felügyelet nélkül hagyott munkaállomást zárolnia kell, vagy jelszavas védelemmel ellátott képernyővédőt kell alkalmaznia. A felhasználó köteles gondoskodni az általa használt informatikai eszközök biztonságos, lehetőleg zárt helyen történő tárolásáról.
- A felhasználónak ügyelnie kell arra, hogy monitorja kijelzőjét munka közben illetéktelen személy ne láthassa, arról adatokat ne gyűjthessen.

- Tilos az informatikai eszköz közelében külső harmadik személyt felügyelet nélkül hagyni.
- Az informatikai eszköz munkahelyről történő elvitele/kivitele esetén a felhasználónak be kell tartania a Kft. vagyonvédelemre, illetve iratkezelésre/adatkezelésre vonatkozó szabályait.
- A felhasználó köteles a részére előírt informatikai oktatáson részt venni, az oktatási anyagot elsajátítani és legjobb tudása szerint alkalmazni.

6.2. A felhasználói hozzáférési jogosultságok meghatározása:

A felhasználói hozzáférési jogosultságok engedélyezése, módosítása és visszavonása felhasználó közvetlen vezetőjének feladata.

A felhasználói jogosultságok meghatározása egyedileg, a munkavállaló munkakörének, feladatainak és a munkavégzés helyének figyelembevételével az adott szervezeti egység vezetőjének írásbeli kezdeményezése alapján jelen szabályzat 2. számú melléklete szerinti „Informatikai jogosultságkezelő lap" kitöltésével történik. A felhasználói jogosultságok meghatározásakor figyelembe kell venni a munkaköri feladatok végrehajtásához minimálisan szükséges jogosultság-engedélyezés elvét. A felhasználói jogosultságokat a munkavállaló közvetlen felettesének időközönként, de legalább évente ellenőriznie kell. A felhasználó munkakörének változása esetén minden esetben ellenőrizni kell a felhasználói jogosultságok körét.

Munkakör váltásakor, vagy a munkaviszony megszűnésekor a jogosultságok a munkában/munkakörben töltött utolsó munkanapon megszüntetésre kerülnek.

A jogosultságigénylés alapján az informatikus feladata a megfelelő beállítások rögzítése, azok ellenőrzése, valamint a munkaviszony megszűnésekor/munkakör váltásakor - Humán csoport jelzése alapján - a jogosultságok megszüntetése.

A Kft. tulajdonában lévő informatikai eszköz csak úgy értékesíthető munkavállaló számára, ha az értékesítést megelőzően az informatikus, a jelen szabályzat 3. sz. mellékletét képező adatlapot kitöltötte, és aláírásával igazolta, hogy az eszközről minden adat és program, törlésre került.

6.3 Távoli munkavégzés VPN kapcsolaton keresztül

A vezetői jóváhagyást követően az informatikusok lehetővé teszi a kijelölt felhasználók részére a Kft. által üzemeltetett hálózat bizonyos részeinek távoli, otthoni elérését. Az otthoni, távoli munkavégzés során is be kell tartani jelen IBSZ által előírt biztonsági rendszabályokat, különös tekintettel az illetéktelen hozzáférés megakadályozására és a belső hálózat munkavégzés céljára vonatkozó kizárólagos használatát. A távoli hozzáférés esetében minimális biztonsági követelmény, hogy a hitelesítés során használt jelszó a hálózaton titkosított formában halad, valamint az adatforgalom is titkosított.

Az Kft. hálózatára a távoli munkavégzés során VPN segítségével csatlakoztatott eszközök fokozott védelme, karbantartása, vírusvédelme, az illetéktelen hozzáférés megakadályozása a felhasználó kötelessége. A VPN kapcsolat használata esetén tilos külső adathordozót csatlakoztatni és magánjellegű internet tevékenységet folytatni.

6.4. A felhasználó kötelezettségei:

A felhasználó köteles rendeltetésszerűen használni a Kft. tulajdonában lévő hardvereket és szoftvereket. A nem rendeltetésszerű használatból eredő károkat köteles megtéríteni.

A felhasználó: köteles a munkavégzése során keletkező és a munkavégzéshez kapcsolódó elektronikus dokumentumokat a számítógépe azon meghajtóján tárolni, amelyről az automatikus mentés a központi szerverre megoldott. A „H" betűvel jelzett meghajtón tárolt adatokhoz kizárólag a számítógép felhasználójának van hozzáférése, csak ő szerkesztheti, az adatok naponta többször automatikusan mentésre kerülnek a központi szerverre.

A felhasználó felelősséggel tartozik azokért a munkavégzéshez szükséges adatokért, amelyeket (bármilyen oknál fogva) a számítógép háttértárára (ide tartozik az „asztal" is) ment.

A felhasználó köteles a munkavégzése szempontjából fontosnak tekintett e-mail üzenetek megőrzéséről gondoskodni.

A felhasználó köteles az általa tapasztalt rendellenes eseményeket az informatikai szervezeti egység munkatársaival haladéktalanul közölni.

A felhasználó tudomásul veszi, hogy nem jogosult önállóan, az informatikusokkal való egyeztetés nélkül szoftvert telepíteni, törölni, vagy annak beállításait módosítani az általa használt informatikai eszközre vonatkozóan.

6.5. A felhasználót terhelő további, kiemelt tilalmak:

Tilos az informatikai rendszer bármely elemének eredeti felhasználási céljától eltérő használata vagy az erre irányuló próbálkozás.

Tilos olyan információ, adattartalom továbbítása, letöltése vagy közzététele az interneten, amely jogszabályba ütközik.

Tilos a Kft. szoftvereit másolni vagy más informatikai eszközre telepíteni.

6.6. Külső adathordozók kezelése:

A Kft. tulajdonában lévő, cserélhető- és mobil adathordozókon kizárólag külön engedély alapján lehet személyes adatokat tárolni (pl. pendrive, mobil HDD, vagy SSD) Az ilyen adathordozókat jelszavas védelemben kell részesíteni.

Az engedélyben meg kell határozni az ilyen adatok adathordozón való tárolásának célját és időtartamát. Az ilyen adatok tartós, vagy rendszeres felhasználása esetében az engedély visszavonásig is kiadható.

A Kft. tulajdonában lévő külső adathordozókról az adatvédelmi tisztviselő nyilvántartást vezet, ezért használatukat be kell jelenteni az adatvedelem@varosgondnoksag.hu címre.

A nem a Kft. tulajdonában lévő, harmadik személytől származó cserélhető- és mobil adathordozó informatikai eszközhöz való csatlakoztatáskor a felhasználó köteles a számítógépén található vírusvédelmi programmal ellenőrizni az eszközt vagy az informatikussal vírusvédelmi szempontból ellenőriztetni. A felhasználó a magántulajdonában álló számítástechnikai, telekommunikációs eszközt a Kft. rendszeréhez kizárólag vezetői engedéllyel, az informatikus által elvégzett vírusvédelmi ellenőrzés után csatlakoztathatja.

A felhasználó felelős a kezelésében lévő külső adathordozók körültekintő használatáért, az azon tárolt dokumentumok illetéktelenektől való megóvásáért.

6.7. A felhasználói jelszókezelés:

A jelszó az informatikai rendszerhez való hozzáférés alapvető eszköze.

Az informatikai rendszer védelme érdekében az informatikai eszköz használójának felelőssége, hogy megfelelő biztonsági szintű jelszót válasszon, hogy azt mások előtt titokban tartsa, azt ne jegyezze fel, vagy amennyiben feljegyzi, azt elzártan tartsa, illetve a jelszó ne legyen illetéktelen személy által hozzáférhető.

A jelszóválasztás követelményei:

- a jelszónak legalább 6 karakter hosszúságúnak kell lennie és tartalmaznia kell kis- és nagybetűt is,
- kerülni kell a felhasználó nevét, beosztását tartalmazó szó használatát,
- a jelszó nem lehet azonos a felhasználói azonosítóval.

A jelszógondozás szabályai:

- az informatikai eszköz első használatakor az informatika által kiadott kezdeti Windows, e-mail és minden egyéb jelszót meg kell változtatni;
- a felhasználói jelszavakat legalább évente meg kell változtatni;
- a Kft. informatikai rendszerében használt jelszót tilos külső rendszerekben használni.

A jelszóváltoztatás és jelszógondozás követelményeinek betartását az informatikusok szúrópróbaszerűen is ellenőrizni kötelesek.

6.8. Az elektronikus levelezés használatára vonatkozó szabályok:

A felhasználó a munkavállalói e-mail címét kizárólag munkavégzés céljából használhatja. A munkavállalói e-mail cím nem adható meg munkavégzésen kívüli tevékenységhez értesítési, vagy kapcsolattartási címként, illetve tilos a levelezést nem Városgondnokságos e-mail címre irányítani.
Az elektronikusan bonyolított levelezések központi szerverre történő mentése napi rendszerességgel történik. A napi mentések során a tárolt adatok az e-mail fiók adott napi állapotát tükrözik.
Az elektronikus levelek küldése és fogadása, kezelése a felhasználó feladata. Az archiválást a felhasználó az adott e-mail archiv@varosgondnoksag.hu e-mail címre történő elküldésével teheti meg.

A munkaviszony megszűnésekor a munkában töltött utolsó munkanaptól a munkavállaló e-mail címe nem használható, az más munkavállalónak át nem adható, nem átirányítható. Az utolsó munkában töltött napon a munkavállaló e-mail címét 30 napra passziválni kell, a passzív e-mail címről üzenet nem küldhető.

6.9 Az e-hatósági eljárások szabályai

Az elektronikus felületeken végzett hatósági eljárások esetében, használatuk feltételeit jogszabályok és az azokon alapuló Felhasználói kézikönyvek, Általános Szerződési Feltételek, stb. szabályozzák. A használatukhoz általában Ügyfélkapus azonosítás, vagy fokozott biztonságú elektronikus aláírás szükséges.

A Kft. nevében ügyfélkapuval/cégkapuval, illetve egyéb elektronikus eljárásban, e-kapcsolattartásban belépési jogosultsággal rendelkező munkavállaló felelős azért, hogy az azonosítóhoz tartozó felhasználó nevét, jelszavát mások előtt titokban tartsa, azt ne jegyezze fel, vagy amennyiben feljegyzi, azt elzártan tartsa, illetve, hogy a jelszó és felhasználónév ne legyen illetéktelen személy által hozzáférhető.

Az elektronikus eljárás során az e-ügyre irányadó eljárási szabályokat be kell tartani.

Az eljárással kapcsolatosan keletkezett elektronikus, vagy papír alapú dokumentumokat az általános iratkezelési szabályozásoknak megfelelően kell iktatni és tárolni. A dolgozó, akadályoztatása, vagy munkaviszonyának megszűnése esetén köteles gondoskodni arról, hogy az általa megindított hatósági eljárást a helyettesítésére kijelölt személy folytatni tudja.

6.10. Az internethasználatra vonatkozó szabályok:

- A web használatának elsődleges célja a munkavégzés, ebből adódóan a felhasználó munkaidőben munkavégzés céljára, munkája segítésére használhatja az internetet. Csak a munkavégzéshez, szakmai tájékozottság bővítéséhez szükséges, vagy általános tájékozottságot biztosító információt, segítséget nyújtó oldalak látogathatók.

- Az internetről csak a munkavégzéshez szükséges adatállományok, táblázatok tölthetők le, alkalmazások, programok telepítését csak az informatikai csoport munkatársai végezhetik.

- A munkavállalót tájékoztatni kell arról, hogy a web magáncélú használatából eredő károkért felelősség terheli, illetve, hogy a munkáltató az internet eléréseket szűrheti, egyes weboldalak és szolgáltatások elérését korlátozhatja, az informatikai alkalmazói rendszerek, szolgáltatások használatát rögzítheti (naplózhatja) és ellenőrizheti.

- A látogatott oldal nem szokványos működése (pl. folyamatos újratöltődés, kilépés megtagadása, ismeretlen oldalak látogatására történő átirányítás, ismeretlen program futásának észlelése stb.) esetén azonnal közvetlen technikai támogató segítségét kell kérni.

A munkavállalók az internethasználat során kötelesek a Munka Törvénykönyvéről szóló 2012. évi I. törvény 8. §-ának rendelkezéseire is fokozottan figyelemmel lenni. A törvény 8. §-a szerint a munkavállaló a munkaviszony fennállása alatt - kivéve, ha erre jogszabály feljogosítja – nem tanúsíthat olyan magatartást, amellyel munkáltatója jogos gazdasági érdekeit veszélyeztetné. A munkavállaló munkaidején kívül sem tanúsíthat olyan magatartást, amely - különösen a munkavállaló munkakörének jellege, a munkáltató szervezetében elfoglalt helye alapján - közvetlenül és ténylegesen alkalmas munkáltatója jó hírnevének, jogos gazdasági érdekének vagy a munkaviszony céljának veszélyeztetésére. A munkavállaló véleménynyilvánításhoz való jogát a munkáltató jó hírnevét, jogos gazdasági és szervezeti érdekeit súlyosan sértő vagy veszélyeztető módon nem gyakorolhatja. A munkavállaló köteles a munkája során tudomására jutott üzleti titkot megőrizni. Ezen túlmenően sem közölhet illetéktelen személlyel olyan adatot, amely munkaköre betöltésével összefüggésben jutott a tudomására, és amelynek közlése a munkáltatóra vagy más személyre hátrányos következménnyel járhat. A titoktartás nem terjed ki a közérdekű adatok nyilvánosságára és a közérdekből nyilvános adatra vonatkozó, törvényben meghatározott adatszolgáltatási és tájékoztatási kötelezettségre.
E szabályozást alapul véve a Kft. munkavállalói az interneten - különös tekintettel a közösségi oldalakra, fórumokra, chat oldalakra, illetve bármilyen más személy által is megtekinthető oldalakra - történő megjelenése, véleményformálása, bármilyen közlése során köteles az alábbiakat betartani:

- tilos bármilyen személy, közösség becsmérlése, azok elleni izgatás, különösen azok faji, vallási, nemi, szexuális hovatartozását illetően;
- tilos a jóízlést, közerkölcsöt sértő, rasszista, uszító és más, a véleménynyilvánítás kereteit meghaladó oldalak szándékos látogatása, online játékok, fogadási oldalak felkeresése, bármely tartalommal kapcsolatos magánvélemény nyilvánítása (privát blogolás).

- tilos a társaság, valamint a tulajdonos negatív színben történő feltüntetése, jó hírnevének megsértése;
- tilos a társaságra vonatkozó adatok közzététele, kivéve a munkavégzésből adódó közzétételt;
- tilos a társaság bármely telephelyének, gépének, berendezésének képpel, videóval történő megjelenítése, kivéve a munkavégzésből adódó megjelenítést;
- a dolgozó képpel, videóval történő megjelenítése amennyiben azon megjelenik a társaság bármelyik munka- vagy védőruházata, jelképe, megnevezése, a munkavégzés helye, csak felettesének engedélye alapján történhet, kivéve a munkavégzésből adódó megjelenítést.

Ezen előírások megsértése a munkavállaló azonnali fegyelmi felelősségre vonását vonja maga után.

A Kft. területén elérhető vezeték nélküli internet hálózatot (wifi) a külső, illetéktelen felektől elzártan, jelszóval védetten kell működtetni. Ezen biztonsági intézkedés folyamatos betartásáért, ellenőrzéséért az informatikusok felelősek.

A Kft. egyes telephelyein jelszóval védett, publikus wifi hálózatot üzemeltet. Amennyiben a munkavállaló nem munkavégzési céllal használja az internetet, az elkülönített wifi hálózatra kell csatlakoznia.

6.11. A mobiltelefonok és táblagépek használatára vonatkozó szabályok:

A Kft. a munkavállalóknak a mobiltelefont és táblagépet, vagy USB mobilinternet sticket (továbbiakban: mobileszköz) biztosíthat munkájuk ellátása érdekében, azzal, hogy a mobiltelefonok használata során a munkavállalók nem léphetik túl az előre meghatározott havi forgalmi keretüket. A mobileszköz havi díjas előfizetéssel rendelkezik, és a Kft. tulajdonában lévő valamennyi mobileszköz díjmentesen tud egymás között kommunikálni. Az eszköz használata során, a Kft. csak indokolt és szükséges esetben engedélyezi az emelt díjas sms, internet böngészés, e-mail és egyéb fel nem sorolt, az általános mértékűhöz képest magas díjú forgalmi módokat.

A Kft. a mobileszközök használata során csoportonként forgalmi kereteket határoz meg. A forgalmi keretek csoportonkénti meghatározását és mértékét ügyvezetői utasítás tartalmazza. Az egyes munkatársak keretbesorolását a gazdasági vezető határozza meg. Amennyiben a mobileszközzel rendelkező munkavállaló a részére meghatározott forgalmi keretet túllépi az adott hónapban, úgy a forgalmi kerete és a tényleges forgalmi érték közti különbözetét köteles megtéríteni a Kft. részére. Amennyiben a munkavállaló a forgalmi keretét igazoltan a Kft. érdekében végzett munkavégzése során lépte túl, úgy a megtérítési kötelezettsége nem áll fenn. A havi forgalmak vizsgálata a gazdasági vezető felelőssége, ő gondoskodik a forgalmi túllépések indokainak megvizsgálásáról és a megtérítési kötelezettségek behajtásáról is.

A Kft. tulajdonában lévő mobileszközökről a vagyonnyilvántartó, a hozzá kiadott SIM kártyákról a kontrolling csoport nyilvántartást vezet. A nem használt mobileszközöket és SIM kártyákat az informatikusok az erre kijelölt zárt szekrényben kötelesek tárolni.

A munkavállaló kötelezettsége, hogy a részére átadott mobileszközt rendeltetésszerűen használja, azt az azon tárolt adatok védelme érdekében képernyőzárral lássa el.

Amennyiben a mobileszköz SIM kártyájához internet-előfizetés is tartozik, úgy a munkavállalóknak a telefon, tablet használata során az internethasználatra és az elektronikus levelezésre vonatkozó szabályokat is be kell tartani.

A Kft. nem zárja ki a mobiltelefonok, tabletek korlátozott mértékű magánhasználatát, ezért a készülékek karbantartásra, javításra történő átadásakor, illetve a munkaviszony megszűnésekor a munkavállalót tájékoztatni kell arról, hogy a készülék leadásakor, visszaadásakor a dolgozónak törölnie kell a

magánjellegű fájlokat.

Amennyiben a Kft. tulajdonában lévő mobiltelefon vagy táblagép elvész, a munkavállaló köteles az informatikust minél rövidebb időn belül tájékoztatni.

7. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését a munkavállalók részére a vezetők és az informatikusok oktatás formájában is biztosítják, melyről nyilvántartást kötelesek vezetni. Az IBSZ-t hozzáférhetővé kell tenni a „közös" meghajtón, illetve a Kft. Iránytű rendszerében is.

Az IBSZ-t évente aktualizálni kell. Az IBSZ folyamatos karbantartása a mindenkori informatikai vezető feladata.

8. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök elhelyezésekor különös figyelemmel kell lenni a fizikai károsodást okozó veszélyforrásokra.

8.1. Környezeti infrastruktúra okozta ártalmak különösen:

- vis maior,
- légszennyezettség,
- nagy teljesítményű elektromágneses térerő,
- elektrosztatikus feltöltődés,
- a levegő nedvességtartalmának felszökése vagy leesése,
- szennyeződés (pl. por),
- közüzemi szolgáltatásban bekövetkező zavarok:
- feszültség-kimaradás,
- feszültségingadozás,
- elektromos zárlat.

8.2. Emberi tényezőre visszavezethető veszélyek:

Szándékos károkozás:

- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a megváltozott körülmények figyelmen kívül hagyása,
- vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,

- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

9. Az informatikai eszközök környezetének védelme, fizikai biztonsága:

9.1. Gépterem:

A Kft. gépterme a Székesfehérvár, Szent Vendel u. 17/a szám alatti székhely épület 1. emeletén található szerverszoba.

A gépteremre vonatkozó előírások:

- a szerverszobát biztonsági zárral kell felszerelni
- a szerverszoba kulcsából az informatikusoknál és a portaszolgálaton egy-egy másolatot kell elhelyezni zárható kulcsdobozban,
- a gépterembe csak az informatikusok léphetnek be önállóan,
- a belépési jogosultsággal nem rendelkezők csak az arra jogosultak felügyelete mellett léphetnek be, tartózkodhatnak a szobában,
- a gépterembe történő illetéktelen behatolás tényét haladéktalanul jelenteni kell az informatikai vezetőnek,
- a gépteremben irodai tevékenység nem végezhető,
- a géptermet klímaberendezéssel kell ellátni, melyet úgy kell beállítani, hogy az biztosítsa az eszközök optimális működését.

A gépterem tűzvédelme:

- a gépterem, illetve kiszolgáló helyiség az "AK" kockázati osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent,
- a gépteremben tilos dohányozni, tűz- és robbanásveszélyes anyagot tárolni,
- a menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell,
- a gépterembe minimum 1 db porral oltó készüléket kell elhelyezni.
- a gépteremben elektromos vagy más munkát csak a tűzvédelmi referens tudtával, ill. engedélyével szabad végezni.

9.2. A számítógépek és szerverek védelme

Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- menteni a még használható információkat,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása.

9.3. Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell.
A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.
Az üzemeltetést, karbantartást és szervizelést az informatikusok végzik.
A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlatait,
- a tapasztalatokat.

Alapgép megbontását (kivéve a garanciális gépeket) csak informatikus végezheti el.

A harmadik személyek által végzett karbantartási- és javítási eljárások során biztosítani kell, hogy a Kft. adatainak bizalmassága, titkossága ne sérülhessen. A javítást- és karbantartást végző személyekkel a jelen szabályzat 4. számú melléklete szerinti „Titoktartási nyilatkozatot" kell aláíratni. A nyilatkozat aláíratásáért az informatikus felel.

10. Az informatikai feldolgozás folyamatának védelme

10.1. Az adatrögzítés védelme érdekében a következőket kell betartani:

- adatbevitel hibátlan műszaki állapotú berendezésen történhet,
- tesztelt adathordozóra lehet csak adatállományt rögzíteni,
- az adatrögzítő szoftver védelme érdekében olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is.
- hozzáférési lehetőség:
    - a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (alapelv: a tárolt adatokhoz csak az illetékes személyek férjenek hozzá),
    - az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
    - A szerverek jelszavát az informatikusok kezelik.

10.2. Az adathordozók nyilvántartása

Az adathordozókról nyilvántartást kell vezetni. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval (sorszámmal) kell ellátni.
A nyilvántartás vezetése, annak naprakészen tartása a leltárfelelős feladata.

10.3. Adathordozók tárolása

Az adathordozókat a műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelően kell tárolni.

10.4. Selejtezés, sokszorosítás, másolás

A selejtezést a Kft. Selejtezési Szabályzata alapján kell lefolytatni.
Sokszorosítást, másolást csak az érvényben és hatályban lévő Iratkezelési Szabályzat szerint szabad végezni, azzal, hogy a biztonsági, illetve archív adatállomány előállítása is másolásnak számít.

10.5. Leltározás

A szoftvereket és adathordozókat a Leltározási szabályzatban foglaltaknak megfelelően kell leltározni.

10.6. Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését.
A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó felhasználók feladata.
A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban az informatikusok segítséget nyújtanak**.**
A szervereken tárolt adatokról a mentést rendszeresen el kell végezni.

11. Szoftver védelem

11.1. Rendszerszoftver védelem

Az informatikusnak biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak hozzáférhetők legyenek a felhasználók számára.

11.2. Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem
A használat folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.
Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

11.3. Programok megőrzése, nyilvántartása

A programokról a leltárfelelősnek naprakész nyilvántartást kell vezetni.
A számvitelről szóló többször módosított 2000. évi C. törvény értelmében a Kft.-nek az üzleti évről készített beszámolót, valamint az azt alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá más, a számviteli törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 10 évig meg kell őrizni. A bizonylat elektronikus formában is megőrizhető, ha az alkalmazott módszer biztosítja az eredeti bizonylat összes adatának késedelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az utólagos módosítás lehetőségét.

12. A szervergép és a hálózat munkaállomásainak működésbiztonsága

12.1. Szervergépek

Szünetmentes áramforrást kell használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.
A központi gépek háttértárairól biztonsági mentést kell készíteni.
Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.

12.2. Munkaállomások

Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.
A Kft. informatikai eszközeiről programot, illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.
A hálózati vezeték és egyéb csatlakozó elemeit mindennemű sérüléstől meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.
A mobileszközök kivételével informatikai eszközt és tartozékait a helyéről áthelyezni csak az eszköz leltárfelelőse engedélyével szabad.

13. Információbiztonsági incidensek kezelése

13.1. INFORMÁCIÓBIZTONSÁGI ESEMÉNYEK ÉS GYENGESÉGEK JELENTÉSE

A Kft. mindenkor hatályos Adatvédelmi és adatkezelési szabályzata tartalmazza és rendezi az adatvédelmi incidens esetén alkalmazandó szabályokat és eljárásrendet. A szabályzat szerint „az adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen

vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményez."

Jelen informatikai biztonsági szabályzat kifejezetten az informatikai rendszer érő külső vagy jogosulatlan belső sérülés, támadás és sebezhetőségek kivédése érdekében tartalmaz szabályokat és eljárási rendet. Azonban ha az információbiztonsági incidens személyes adatokat is érint, azaz az az információbiztonsági incidens egyben adatvédelmi incidens is, akkor a jelen informatikai biztonsági szabályzatban előírtak mellett az Adatvédelmi és adatkezelési szabályzat előírásait is alkalmazni kell.

Az információbiztonsági incidensek súlyos következményekkel járhatnak, így ha megelőzni nem is sikerül ezeket, fontos, hogy nagyon rövid határidőn belül intézkedések történjenek az incidensek következményeinek az elhárítása érdekében.

A Kft. információbiztonsági incidensnek tekint minden, az informatikával kapcsolatba hozható rendellenes működést, fenyegetést, amely az adatok bizalmasságát, sértetlenségét, vagy rendelkezésre állását veszélyezteti.

Információbiztonsági incidensnek minősülnek különösen – de nem kizárólagosan – az alábbiak:
- a Kft. adatait tároló szerver feltörése,
- a Kft. valamely informatikai eszközének megsérülése, megsemmisülése,
- valamely informatikai rendszer vírusfertőzése,
- ha a Kft. valamely adathordozó eszköze (pendrive, mobiltelefon, tablet, notebook…stb.) kikerül a munkavállaló felügyelete alól (elveszti, nem tudja megmondani, hogy hová tette), vagy az illetéktelen, jogosulatlan személy kezébe kerül (ellopták).

A Kft. minden informatikai eszközt kezelő munkavállalójának kötelessége az általa felhasználóként tapasztalt biztonsági sérülést, támadást, vagy általa feltárt biztonsági sebezhetőséget haladéktalanul – a megtapasztalással egyidejűleg azonnal - jelenteni az informatikai vezetőnek. (Ennek elmulasztása vagy a gyengeség kihasználása önmagában is biztonsági eseménynek minősül.)

A felhasználó által jelentendő biztonsági sérülésnek, támadásnak, biztonsági sebezhetőségnek tekintendők különösen – de nem kizárólagosan – az alábbi események:
- a felhasználói azonosítóval való visszaélés,
- illetéktelen rendszer- vagy adathozzáférés, bármely, a felhasználó által használt szolgáltatás, rendszer, infokommunikációs eszköz tekintetében (pl. elektronikus levelezés
- adathalász tevékenység, amely a felhasználó adatainak vagy hozzáféréseinek, illetve a Kft.-t érintő – nem publikus – információk megszerzésére irányul (pl. adathalász oldalak, kéretlen levelek vagy közvetlen telefonhívások, amelyek személyes vagy munkahelyi információk megszerzésére irányulnak),
- rosszindulatú szoftverek (vírusok, trójai programok stb.) jelenléte a felhasználó által használt rendszeren, infokommunikációs eszközön,
- adatszivárgás észlelése, ami megvalósulhat a Kft. adatvagyonát képező nem közérdekű adatok szándékos vagy véletlen továbbításával, kiszivárogtatásával azok megismerésére nem jogosult szervezetek, személyek vagy az adatok bizalmasságának megőrzése szempontjából megbízhatatlan rendszerek felé,
- felhasználó használatában lévő informatikai eszköz megbontására utaló jelek.

A Kft. minden informatikus munkavállalójának külön kötelessége a hozzá bejelentett, vagy általa észlelt incidenst jelenteni az informatikai vezetőnek attól függetlenül, hogy a bejelentő esetleg az informatikai vezetőt is értesítette már.

Az informatikai vezető a hozzá érkezett bejelentést köteles azonnal megvizsgálni, és amennyiben az incidens személyes adatot is érint, azaz az információbiztonsági incidens egyben adatvédelmi incidensnek is minősül, a vizsgálat megkezdésével egyidejűleg köteles az adatvédelmi tisztviselőt értesíteni.

A vizsgálat során az informatikai vezető – adatvédelmi incidens esetén az adatvédelmi tisztviselővel együtt eljárva, - az incidens bejelentőjétől további adatszolgáltatást kérhet, amelyet a bejelentő köteles haladéktalanul, de legkésőbb 1 munkanapon belül teljesíteni. Az adatszolgáltatásnak tartalmaznia kell legalább a következőket:

- az incidens bekövetkezésének időpontját és helyét,
- az incidens leírását, körülményeit, hatásait,
- az incidens során kompromittálódott adatok körét, számosságát,
- amennyiben az incidens személyes adatokat is érint, akkor a kompromittálódott adatokkal érintett személyek körét,
- az incidens elhárítása érdekében tett intézkedések leírását,
- a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

A bejelentés megvizsgálását, illetve az adatszolgáltatás beérkezését követően az informatikai vezető – adatvédelmi incidens esetén az adatvédelmi tisztviselővel együtt eljárva, - köteles haladéktalanul megkezdeni az események értékelését, az incidens kezelését.

13.2. ESEMÉNYEK, GYENGESÉGEK KIÉRTÉKELÉSE, INCIDENSEK KEZELÉSE

A biztonsági események kiértékelése, incidensek kezelése elsődlegesen az informatikai vezető feladata, azonban ezen tevékenységbe az informatikusokat is be kell vonnia. Sürgős intézkedést igénylő esetben, az informatikai vezető akadályoztatása, elérhetetlensége esetén az informatikusoknak önállóan is meg kell kezdeniük az incidensek kezelését.

Az incidens kezelésének megkezdésekor informatikai vezetőnek az incidenst minősíteni, rangsorolni kell. A minősítésekor meg kell állapítani, hogy az eseményben érintett alkalmazások, eszközök, illetve szolgáltatások mennyire fontosak, fennáll-e szolgáltatás-kiesés. Ha van szolgáltatás-kiesés, az mekkora anyagi vagy egyéb kárt okoz, illetve fel kell mérni az érintett felhasználók számát, körét, összetételét.

Az információbiztonsági esemény minősítését, rangsorolását a következő tényezők összességének figyelembe vételével kell elvégezni:

- alkalmazás kritikussága
- az érintett felhasználók száma
- alkalmazás(ok)ban a hiba által érintett funkciók jellege
- érintett alkalmazások száma.

A minősítés, rangsorolás alapján az informatikai vezető az informatikusok bevonásával köteles meghozni az incidens elhárításához szükséges döntéseket és rövid - a biztonsági esemény súlya alapján maximum 15 napos határidő tűzésével intézkedik a szükséges intézkedések elvégzéséről. Az olyan incidens esetén, ami kritikus súlyozású, az informatikai vezető indokolatlan késedelem nélkül köteles intézkedni a biztonsági esemény, adatszivárgás, leállás megszüntetése érdekében.

13.3. INCIDENSEK KIÉRTÉKELÉSE

A biztonsági esemény kiértékelése az informatikai vezető feladata, melyet az alábbi szabályok szerint kell elvégeznie:

- meg kell határoznia, hogy a biztonsági esemény:

  - az informatikai rendszer kiesésével, vagy meghibásodásával;
  - a szolgáltatás megtagadásával;
  - az adatok megsérülésével, pontatlanságával;
  - biztonságsértéssel kapcsolatos;
- meg kell határoznia a biztonsági esemény okát;
- meg kell határoznia a javító intézkedést az előzetesen gyűjtött adatok felhasználásával;
- értesítenie kell az Ügyvezetőt a foganatosított intézkedésekről;
- meg kell határoznia a biztonsági esemény elhárításának végső határidejét.

13.4. INCIDENSEK ÖSSZEGZÉSE

Az informatikai vezető köteles évente:

- a beérkező biztonsági eseményekről nyilvántartást vezetni és statisztikát készíteni,
- a biztonsági eseményekből közvetlenül származtatott kárt megbecsülni,
- a jellemző információbiztonsági sérüléseket azonosítani, dokumentálni
- a felülvizsgálatokkal összhangban, a védelmi intézkedésekkel együtt előterjesztést készíteni a vezetői értekezlet elé.

Az incidensek elemzéséből, összegzéséből és megoldásából szerzett ismereteket fel kell használni arra, hogy csökkenjen a jövőbeni incidensek bekövetkezésének valószínűsége és hatása, illetve, hogy növekedjen az incidenskezelési rendszer hatékonysága.

14. Záró rendelkezések

Az Informatikai Biztonsági Szabályzatban előírt feladatokat a feladattal érintett munkavállalók munkaköri leírásába be kell építeni.

1.

1. számú melléklet

NYILATKOZAT
informatikai eszköz használatának szabályairól

Alulírott …….

kötelezettséget vállalok arra, hogy az informatikai rendszerekben az azonosításomra szolgáló információk (felhasználói név, jelszó) titkosságát megőrzöm, azokat mások tudomására nem hozom és leírva mások által hozzáférhető helyen nem tartom.

Tudomásul veszem, hogy az általam átvett informatikai eszközök a Székesfehérvár Városgondnoksága Kft. tulajdonában vannak, azok a munkaköri feladataim ellátását hivatottak szolgálni.

Tudomásul veszem, hogy az informatikai rendszerek biztonsága érdekében az internet és e-mail elérésemet ellenőrzik, szűrik.

Tudomásul veszem, hogy az informatikai és alkalmazói rendszerekkel, szolgáltatásokkal való szándékos visszaélések megelőzése és utólagos felderítése érdekében az informatikai alkalmazói rendszerek, szolgáltatások használatát rögzítik (naplózzák) és ellenőrzik.

Tudomásul veszem, hogy az internet-szolgáltatás és az elektronikus levelezőrendszer a munkaköri feladataim ellátását hivatott támogatni, amelyek magáncélú használatából eredő károkért kártérítési felelősséggel tartozom.

Tudomásul veszem, hogy kötelességem az általam tapasztalt informatikai biztonsági eseményt (incidenst) vagy általam feltárt biztonsági sebezhetőséget haladéktalanul jelenteni az informatikai vezetőnek és az informatikusoknak. Informatikai biztonsági incidensnek minősül például a mobil adathordozó (pendrive) elvesztése vagy eltulajdonítása továbbá minden egyéb informatikai eszköz és jogosultság illetéktelen személy általi hozzáférhetősége is.

Kijelentem, hogy az általam átvett informatikai eszköz hardver- és szoftverintegritását megőrzöm, azokon jogosulatlanul programokat nem telepítek, alkatrészt nem cserélek.

Kijelentem, hogy munkakörömből adódóan megismert, tudomásomra jutott személyes adatokat megőrzöm, azokról másolatot engedély nélkül nem készítek, az adatok kezelésére vonatkozó szabályokat betartom.

Székesfehérvár, 20… ……

…….
munkavállaló

2. számú melléklet

Informatikai jogosultságkezelő lap

Munkavállaló neve:

Beosztása:

Szervezeti egység:

ID azonosító:

Jogosultság:	**Engedélyezés:**	**Módosítás:**	**Tiltás**
VMA rendszer			
VPN kapcsolat * *(külön indoklással!)*			

*VPN kapcsolat szükségessége:

……

……

A jogosultságokat a fentiek alapján engedélyezem.

Székesfehérvár, 20……

.....
vezető

3. számú melléklet

Adatlap informatikai eszköz értékesítéséhez

Alulírott …….. igazolom, hogy a mai napon átadott …… azonosító (gyári szám, IMEI, stb.) számú …….. készülékről minden adat és program törlésre került.

Székesfehérvár, 20……. ……

……

4. számú melléklet

Titoktartási nyilatkozat

Alulírott …….. tudomásul veszem, hogy a Székesfehérvár Városgondnoksága Kft.-nél végzett tevékenységem során, minden tudomásomra jutott és kapott, mind papíralapú, mind elektronikus informatikai-, pénzügyi-, műszaki-, szervezeti információt, adatbázist, személyes adatot illetve bármely egyéb dokumentumot, valamint a fentiekkel kapcsolatos információt bizalmasan kezelem, azt más, arra nem jogosult harmadik személynek nem juttathatom tudomására, illetve nem adhatom birtokába, azt saját célra sem használom fel. Mindezek mellett vállalom, hogy ezen kötelezettségeimnek az információ tudomásomra jutásától számított 5 évig eleget teszek.

Tudomásul veszem azt, hogy köteles vagyok megtéríteni, a jelen nyilatkozatban vállaltak szándékos vagy gondatlan megszegéséből eredő károkat.

Székesfehérvár, 20…. ……

……