Dél-Kom
Dél-Dunántúli Kommunális Szolgáltató Nonprofit Kft.

DK-27-11-4-10/B-1/2018. Ikt. szám

# SZ-16

# INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

# (IBSZ)

# TARTALOMJEGYZÉK

# 1. Általános rendelkezések

## 1.1. Az IBSZ kiadásának célja

Ezen szabályzat célja, hogy a Dél-Kom Nonprofit Kft. (továbbiakban **Társaság**) információs rendszerei és az azok által tárolt, feldolgozott és alkalmazott információk/adatok megfelelő védelméhez szükséges előírásokat egységbe foglalja, és az alapvető, általános „minimálisan" betartandó előírásokat meghatározza. Az ezektől való eltérést, – amely minden esetben csak szigorítás és / vagy kiegészítés lehet, – az adott informatikai / információs rendszer, részterület rendszer-specifikus utasításai tartalmazzák.

Az információbiztonság a Társaság működésének meghatározó feltétele. Az üzletmenet folytatásához/fenntartásához szükség van az üzleti és a megrendelői információk védelmére, amelynek sikerességétől minden munkatárs munkahelye függhet.

A szabályzat feladata a Társaságnál meghatározni:

- a minősített elektronikusan és más módon tárolt adatok,
- minősített adatok tárolására, feldolgozására, továbbítására, archiválására szolgáló információs rendszerek, rendszerelemek, és adathordozók,
- ezen informatikai rendszerek biztonságát, ill. folyamatos működését biztosító rendszereke és segédberendezések,

védelmét.

A védelmen kívül, – mely az adatok által hordozott információk sértetlenségének, hitelességének és bizalmasságának elvesztését hivatott megakadályozni, – feladata még a szabályzatnak az információs rendszer megbízható működésének, azaz az adatok rendelkezésre állásának és a hozzájuk kapcsolódó alkalmazói rendszerek funkcionalitásának a biztosítása.

## 1.2. Az IBSZ hatálya, érvényessége

***Személyi hatálya***

Az IBSZ hatálya kiterjed a Társaság minden alkalmazottjára, beosztástól és állampolgárságtól függetlenül, valamint, a Társasággal szerződéses, vagy más módon kapcsolatba kerülő természetes vagy jogi személyekre, gazdasági társaságokra a velük kötött megállapodás, és/vagy titoktartási nyilatkozatok alapján, melyek a szerződésekben, vagy annak mellékletként megtalálhatók, továbbá a Társaság irodájában (telephelyén) tartózkodás idejére minden külső személyre.

***Tárgyi hatálya***

Az IBSZ hatálya kiterjed a Társaság:

- Székhelyére, telephelyeire, amely címeken az informatikai rendszerek is megtalálhatók,
- Fióktelepeire: hulladékudvarok, ügyfélszolgálatok és ügyfélképviseletek
- a védelmet élvező adatai teljes körére, (feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül),

- a Társaság irodáján (telephelyén) belül és azon kívül a tulajdonában, ill. a használatában lévő informatikai rendszerekre, berendezésekre, adathordozókra, rendszer, hálózati és felhasználói programjaira, valamint azok dokumentációira,
- a Társaság ügyfélszolgálati, pénzügyi, személyügyi és rendszerüzemeltetési dokumentációira.

Az IBSZ hatálya nem terjed ki a Társaság telephelyén és fióktelepein kívül üzemeltetett olyan informatikai eszközökre és rendszerekre melyek nincsenek a Társaság tulajdonában, és üzemeltetésére ill. felügyeletére szerződés nem kötelezi.

# 2. *Az információbiztonság szervezete*

A Társaság minden informatikai / információs rendszere számára kijelöltük az üzemeltetésért és biztonságáért felelős szervezetet, személyt, vagy személyek csoportját, akiknek kötelessége e szabályzat előírásait a rendszer felhasználóival megismertetni és betartatni. A Társaságnál nem létezhet olyan informatikai / információs rendszer, vagy akár önálló számítógép, ill. egyéb adathordozó, amelyhez ne tartozna felelős személy, és annak elérhetetlensége esetére, kijelölt helyettese.

A Társaság informatikai / információs rendszerének biztonságáért felelős személyek, jogaik és kötelességeik alapján különböző funkcionális szintekhez tartoznak, amelyek szigorú hierarchiát alkotnak.

Az információbiztonságban érintett személyek / csoportok:

- a Társaság ügyvezetői,
- a Társaság cégvezetője,
- információbiztonsági megbízottja,
- rendszergazda (BIOKOM Nonprofit Kft. alkalmazásában),
- informatikus (BIOKOM Nonprofit Kft alkalmazásában),
- a felhasználók.

## *2.1. Ügyvezető*

***Feladata***: A Társaság informatikai / információs rendszerével és működtetésével kapcsolatos elvárások megfogalmazása, jóváhagyása, az információbiztonsági irányítási rendszer felelősének kinevezése, egyéb (kapcsolódó) felelősök kijelölése, és a szükséges erőforrások biztosítása.

***Helyettesítése***: Ügyvezető

***Dokumentumok,*** melyekkel rendelkeznie kell:

- a menedzsment rendszer kézikönyve és eljárásai,
- Információbiztonsági Szabályzat (IBSZ),
- Üzletmenet-folytonossági és katasztrófa-elhárítási terv.

## 2.2. *Információbiztonsági megbízott*

Felelős a Társaság vezetőségén belül az MR információbiztonsági (IBIR) részének működtetéséért és fejlesztéséért.

***Feladatai:***

- az IBIR működtetési feltételeinek biztosítása, működtetésének felügyelete, működtetése hatékonyságának figyelemmel kísérése, információbiztonsági incidensek esetén a szükséges lépések elrendelése, valamint az IBIR fejlesztésének – új vagy módosított biztonsági eljárások bevezetésének – elrendelése,
- a Társaság informatikai / információs rendszerének felügyelete, az IBIR koordinálása és működtetése, az információvédelmi szervezet munkatársai tevékenységének irányítása és ellenőrzése, a szükséges jelentéstételi rendszer kialakítása,
- a Társaság informatikai / információs rendszerére vonatkozó fejlesztési igények meghatározása, és ezek alapján a fejlesztés megtervezése a cégvezetővel, a Társaság vezetőségével és a rendszergazdával egyeztetve. A fejlesztési igények során figyelembe kell venni a kockázatértékelés által levezetett védelmi követelményeket, valamint az aktuális állapotra és a tervezett jövőbeli állapotra vonatkozó működési követelményeket és Társaság lehetőségeit. A fejlesztési igényeket előterjeszti az ügyvezetőnek,
- feladata az informatikai / információs rendszert használó munkatársakkal (felhasználókkal) e szabályzat és a rájuk vonatkozó kiegészítések tartalmának megismertetése (oktatás), és velük a tudomásulvételi nyilatkozatot aláírattatása,
- megismerteti és betartatja az IBSZ előírásait a szervezetben. A munkatársakat vezetői példamutatással és rendszeres biztonsági ellenőrzésekkel az IBSZ előírásainak betartására ösztönzi,
- meghatározza, hogy a szervezetben milyen adatbázist / információhalmazt kell létrehozni és működtetni, valamint hogy kik és milyen jogosultságokkal férhetnek hozzá az adatokhoz (írás / olvasás / létrehozás / listázás / törlés / stb.) – *ez jelenti az adott adatok és adatbázisok adatgazdai feladatait.*

***Helyettesítése***: Informatikus

***Dokumentumok,*** melyekkel rendelkeznie kell:

- Menedzsment rendszer kézikönyve és folyamatok leírásai;
- Információbiztonsági Szabályzat (IBSZ);
- Üzletmenet-folytonossági és katasztrófa-elhárítási terv.

## 2.3. *Rendszergazda*

A rendszergazda olyan munkatárs, aki munkakörénél fogva rendszer-adminisztrátorként hozzáférhet a Társaság minden bizalmas és szigorúan bizalmas információjához. Az általa működtetett informatikai rendszer folyamatos, megfelelő és biztonságos működése alapvető fontosságú, sőt kritikus jelentőségű is lehet a Társaság számára. Ezért a munka- vagy megbízási szerződése különleges kritériumokat tartalmaz a titoktartásra, bizalmas információk kezelésére, a rendszeradminisztrátori jelszavak kezelésére, valamint egyéb biztonsági követelményekre tekintettel.

***Feladatai:***

A feladatkörébe tartozó, valamint a helyettesítés során gondjaira bízott informatikai rendszer(ek) meghatározott követelmények alapján történő üzemeltetése. Ez a következő tevékenységeket jelenti:

- a beszerzésre került, javításból visszaérkezett, rendszerbe állítandó informatikai eszközök, szoftverek ellenőrzése és telepítése,
- az érdekeltségi körébe tartozó informatikai rendszer(ek) elemeinek azonosító címkékkel való ellátása,
- az érdekeltségi körbe tartozó informatikai rendszer hardver és szoftver eszközeiről nyilvántartás vezetése. Ebbe beleértendők külön is a felelősségi körébe tartozó, hálózatba nem kapcsolt egyedi gépek és laptopok is,
- gondoskodás arról, hogy az általa karbantartott adatbázis / információhalmaz logikailag és fizikailag rendelkezésre álljon,
- a tervszerű hardver és szoftver karbantartások előre jelzése az ügyvezetőnek és a felhasználóknak, majd azok elvégzése,
- az adatok tervszerű mentésének végrehajtása,
- a vírusvédelmi szoftver rendszeres, előírt időben történő frissítése,
- vírusfertőzés vagy annak gyanúja esetén a „*Teendők vírus észlelése esetén*” pontban leírtak alapján kell eljárni,
- nyilvántartás vezetése a számítástechnikai eszközök üzembe helyezéséről, javításáról és cseréjéről,
- a felhasználók által használt szolgáltatások, kialakítása, aktualizálása,
- az érintett informatikai rendszer felhasználói számára a személyesen használható tárterület megjelölése, a rendelkezésre álló tárterület nagyságának figyelemmel kísérése. Még mielőtt a szabad tárterület elérné a kritikus alsó határt, karbantartás végzése, és az adatgazda / felhasználó engedélyével a felesleges, elavult információk törlése, és ez által tárterületek felszabadítása. Amennyiben ez nem megvalósítható, kérje az Ügyvezető segítségét,
- nyilvántartás vezetése - az illetékességi körében - a meghatározott hozzáférési jogosultságokról, és az azokra vonatkozó beállítási és változtatási igényekről. (Legyen nyomon követhető, hogy milyen igény vagy igényváltozás miatt jöttek létre

az aktuális hozzáférési jogosultságok, továbbá rendszer visszaállítás esetén minden érvényes hozzáférési konfiguráció legyen a követelményeknek – igényeknek megfelelően visszaállítható),

- a felhasználók tájékoztatása az informatikai változásokról (pl.: újonnan beszerzett szoftver, új szolgáltatás stb.),
- bármilyen – az IBSZ előírásával kapcsolatos – visszaélés, szabálysértés (incidens) felfedezése vagy észrevétele esetén azt azonnal jelenteni kell az Információbiztonsági megbízottnak,
- eseménynapló vezetése. Ide fel kell jegyezni minden bekövetkezett, – az informatikai rendszerrel kapcsolatos – információvédelmi incidenst, annak időpontját, leírását, meghatározott okát (amennyiben lehetséges), következményét és a helyreállítás időpontját és módját,
- a vezetett nyilvántartásoknak a Társaságon belül az Információbiztonsági megbízott számára, betekintésre, folyamatos rendelkezésre állásának biztosítása,
- javaslatok tétele az Információbiztonsági megbízott felé, az illetékességi körébe tartozó informatikai rendszerek üzemeltetésével kapcsolatos észrevételeiről, és közreműködés az adott informatikai rendszereket érintő, rendszer-specifikus rendszabályok kidolgozásában.

***Helyettesítése***: Informatikus

***Dokumentumok,*** melyekkel rendelkeznie kell:

- Menedzsment rendszer kézikönyve és folyamatok leírásai,
- a DÉL-KOM Nonprofit Kft. Információbiztonsági Szabályzata (IBSZ),
- a BIOKOM Nonprofit Kft. Informatikai biztonsági Szabályzata,
- Üzletmenet-folytonossági és katasztrófa-elhárítási tervek,
- informatikai rendszer elemeinek műszaki leírása, dokumentációja,
- rendszerek üzemeltetési kézikönyve,

***Dokumentumok,*** amelyeket vezetnie kell:

- nyilvántartás a felelősségi körébe tartozó informatikai rendszer összes hardver és szoftver eleméről,
- nyilvántartás a hálózatba nem kapcsolt és speciális hordozható berendezésekről,
- számítástechnikai eszközök üzembe helyezése, javítása és cseréje,
- tervszerű karbantartások naplója,
- adatmentési terv és napló,
- rendszer-hozzáférési nyilvántartás: az érdekeltségi körébe tartozó felhasználók hozzáférési jogosultságai, és azok beállításaira vonatkozó igények,
- számítástechnikai eseménynapló,
- egyéb informatikai naplók.

## 2.4. *Felhasználók*

A munkavégzéshez szükséges informatikai rendszerhez megfelelő jogosultságokkal rendelkező személyek.

***Kötelességei:***

- a rendszerbe történő első belépése előtt, ezen szabályzat és a rá vonatkozó kiegészítések elolvasása, és erről tudomásulvételi nyilatkozatot aláírása,
- a jelen szabályzat és a rá vonatkozó kiegészítések pontjaiban foglaltak betartása,
- az észlelt hálózati és a munkahelye számítástechnikai berendezései rendellenességeiről, információbiztonsági incidensekről (pl. vírusfertőzés, betörés észlelés) a Rendszergazda és / vagy az Információbiztonsági megbízott értesítése,
- részvétel a témában tartott képzéseken.

***Helyettesítés***: A Társaságnál minden felhasználóhoz/funkcióhoz is helyettest jelölünk ki, aki a munkatárs elérhetetlensége esetén, annak munkáját – a hozzáférési jogok ideiglenes módosításával – képes rövid idő alatt átvenni. Ezt a helyettesítési rendszert az érintett szervezeti egységek vezetői tartják nyilván.

# 3. *Az infrastruktúrához kapcsolódó védelmi intézkedések*

## 3.1. *Biztonsági területek*

***Biztonsági területek meghatározása***

A Társaság a nem engedélyezett, illetéktelen hozzáféréseket, behatolást, szándékos károkozást, az ebből következő károkat a különböző funkciójú területek fizikai elkülönítésével is korlátozza.

A Társaság a következő funkciójú területeket határozza meg a pécsi telephelyeken:

- Szerverszoba,
- Iroda helyiségek,
- Folyosó/ közlekedő,

A fióktelepeken:

- Iroda helyiségek
- Hulladékkezelők
- Hulladéklerakók
- Hulladékudvarok

***Biztonsági területek védelme***

A Társaság a belépésekkel kapcsolatosan a következő szabályokat hozza a telephelyekkel kapcsolatban:

- Minden munkatárs engedélyezetten rendelkezik az iroda nyitásához és zárásához szükséges eszközökkel (bejárati ajtókulcs)
- Minden munkatársnak távozáskor meg kell győződnie, hogy nem utolsónak hagyja el az épületet, és távozási szándékát jelezni kell a még maradó kollegájának.
- Az épület és az irodák területén a vendégek csak kísérővel közlekedhetnek.

Munkaidőn kívül a szerződött szolgáltatóhoz központilag bekötött riasztó jelzi az épületbe történő illetéktelen behatolást. A meghatározott értesítési szabályoknak megfelelően a szolgáltató azonnal riadóztatja az ügyvezetőt, illetve szükség esetén az egyéb funkciójú munkatársakat.

A fióktelepeken:

- Iroda helyiségek riasztóval és biztonsági zárral rendelkeznek
- Kökény RHK területén 24 órás őrzés
- Barcs RHK területén a munkaidőn kívül őrzés-védés
- Hulladéklerakón 24 órás őrzés
- Hulladékudvarok kamerával felszereltek
- Átrakóállomásokon a nyitvatartási időn kívül őrzés-védés

***Berendezések védelme***

A Társaság az informatikai rendszer elemeit úgy helyezi el, hogy azok folyamatos üzemét a külső és környezeti hatások lehetőleg ne akadályozzák.

Az épület villám- és tűzvédelmét előírás szerinti időszakos felülvizsgálatok biztosítják. Elemi károkra a Társaság megfelelő biztosítási szerződéssel rendelkezik.

Megfelelő tűzoltó készülékek állnak rendelkezésre az irodában a Tűzvédelmi tervben meghatározott helyeken.

A szerverszoba túlmelegedés elleni védelmét klíma biztosítja. Az áramkimaradás és túláram esetére a szervereket szünetmentes tápegységek védik, a szerverek ilyen esetben is adminisztrálhatóak (leállíthatóak) távolról. Ezen berendezések akkumulátorainak teszteléséről, kapacitásának ellenőrzéséről az informatikai rendszert üzemeltető **BIOKOM Nonprofit Kft.** gondoskodik.

A Társaság az elektromos-, hálózati adat- és távközlési kábeleket védi a károsodás és a zavarások ellen. Az energiaellátó tápkábeleket a kommunikációs és adatkábelektől szeparáltan helyezi el. A Társaság a számítógép hálózati kábelrendszeréhez való illetéktelen hozzáférés vagy rongálás megakadályozására az irodába való belépést ellenőrzi, fizikai védelmét azok részben rejtett elhelyezésével is biztosítja.

Előzetes engedély nélkül tilos a Társaság területéről berendezéseket, információkat, szoftvereket kivinni, vagy oda bevinni.

A Társaság a telephelyén/fióktelepein kívül használt berendezések esetén is a jelen eljárásban és a hozzá kapcsolódó szabályozásokban előírt információvédelmi intézkedéseket

valósítja meg. A telephelyen kívüli távmunka engedélyezésekor figyelembe veszi az ezzel járó kockázatot. A kiadott berendezések fizikai védelméért, megóvásáért, az általános információbiztonsági szabályok betartásáért a felhasználó felelős.

A Társaság az informatikai rendszerében üzemelő szervereit legalább félévi rendszerességgel felülvizsgálja és karbantartja.

## 3.2. *Hálózatszervezési és tervezési elvek*

***A BIOKOM Nonprofit Kft. pécsi épületében***

A Társaság információs rendszere a BIOKOM Nonprofit Kft. hálózatával egy egységet képez. A hálózati munkaállomások internetre való kijutása csak biztonságos hálózati eszközökön lehetséges. A belső hálózathoz az interneten keresztüli hozzáférés tűzfalon keresztül vagy azonosítással biztosított VPN kapcsolattal biztosított.

A **BIOKOM Nonprofit Kft.** informatikai hálózatának, szerver infrastruktúrájának és a kapcsolódó szolgáltatásainak aktuális és részletes leírását a BIOKOM Nonprofit Kft. informatikai biztonsági szabályzata tartalmazza.

***A fióktelepeken***

- egyedi munkaállomás
- egyedi védelem
- internet hozzáférés

## 3.3. *Szerverszoba biztonsága*

Szerver szoba a BIOKOM Nonprofit Kft. pécsi irodaházában és a Kökényi RHK irodaházaiban is van.

Az adatbázis és fájl szervereket csak a szerverszobában lehet elhelyezni. A szerver üzembiztos működése érdekében az informatikai rendszert üzemeltető **BIOKOM Nonprofit Kft.** szünetmentes tápellátást (UPS), a szabványoknak és igényeknek megfelelő kábelezést, és megfelelő klimatizálást alkalmaz.

A szerverszoba kiemelt biztonságú terület, oda a bejutás az ügyvezető vagy a rendszergazda engedélyezésével lehetséges. A helyiségbe csak az arra illetékesek léphetnek be a munkavégzés idejére.

A Társaság a szerverszoba hőmérsékletét klimatizálással tartja folyamatosan a megfelelő határértékeken belül.

A szerverszobában a szerverek zárható „rack" szekrényben kerültek elhelyezésre.

## 3.4. *Számítógépes munkahelyek biztonsága*

Azon személyek, akik nem rendelkeznek jogosultsággal a Társaság informatikai rendszeréhez, de szolgálati okokból belépnek olyan helyiségbe, ahol hálózatra kapcsolt vagy

egyedi munkaállomás van, csak a jogosult felhasználó kíséretében tartózkodhatnak ott. Ebben az esetben a kísérő felelős a személy mindennemű tevékenységéért.

A számítógépes munkahely elhagyásakor a munkaállomást zárolni kell, illetve aktiválni kell a jelszóval védett képernyővédőt. Így csak jelszó ismeretében lehet a munkaállomáshoz és az azon tárolt adatokhoz hozzáférni.

Amennyiben előreláthatólag 60 percnél hosszabb időre távozik a felhasználó, a gépet lehetőség szerint vagy hibernálja vagy kapcsolja ki.

Munkavégzés után az adatállományokat hálózati szerverre mentjük, a berendezéseket áramtalanítjuk (amennyiben ennek ellenkezőjéről külön rendszabály nem rendelkezik).

A munkahelyeken való munkavégzés során betartjuk a „tiszta asztal – tiszta képernyő politikát": Ez a következőket jelenti:

- Az íróasztalon mindig csak az aktuális munkavégzés dokumentumai vannak elöl. Hosszabb idejű eltávozáskor, illetve minden munkanap végén az elöl levő dokumentumokat, és feljegyzéseket elpakoljuk a helyére.
- A számítógépeken való munkavégzéskor betartjuk a „tiszta képernyő elvét", azaz betartjuk a következő irányelvet: az egyszerre mindig csak szükséges minimális, az adott munkavégzéshez szükséges alkalmazást tartjuk megnyitva, valamint hosszabb idejű eltávozáskor, illetve minden munkanap végén bezárjuk a nyitott alkalmazásokat.

## *3.5. Tűzvédelmi előírások*

A továbbiakban az **irodákra** vonatkozó általános tűzvédelmi előírások:

- Az irodák "D" tűzveszélyességi osztályba tartoznak.
- Elektromos hősugárzót, villanyfőzőt, üzemeltetni, csak az Ügyvezető által engedélyezett helyeken, tűzálló anyagból készült hőszigetelő lapra helyezve szabad.
- Elektromos világítótestekre és azoktól 30 cm-re éghető anyagot elhelyezni tilos!
- A fűtőtestektől 30 cm-es távolságon belül éghető anyagot elhelyezni nem szabad.
- A helyiségben tűzveszélyes folyadékot, robbanásveszélyes és gyulladásra hajlamos anyagot bevinni vagy tárolni tilos!
- A helyiség kijáratát leszűkíteni, eltorlaszolni még ideiglenesen sem szabad.
- A telefonkészülékek mellé a tűzoltóság hívószámát el kell helyezni (105).
- A napi munka befejeztével az eltávozók kötelesek a helyiséget tűzvédelmileg átvizsgálni (pl. áramtalanítás, stb.) és az esetleges szabálytalanságot megszüntetni.

Továbbá a **dohányzásra kijelölt helyiségekre** vonatkozó külön előírások:

- A Társaság dohányzás céljára kellő számú, nem éghető anyagból készült (fém, üveg, kerámia) hamutartót biztosít.
- A hamutartó tartalmát (csikk, gyufa) a papírkosárba önteni tilos. Erre a célra csak nem éghető anyagból készült gyűjtő használható.

### 3.6. *Dohányzás, táplálkozás*

A számítógépes munkahelyeken tilos a dohányzás és táplálkozás, mivel ezek károsíthatják a hardver eszközöket. Táplálkozásra külön konyha áll rendelkezésre.

Az ennél részletesebb előírásokat lásd a Tűzvédelmi szabályzatban.

## 4. *Hardverekhez kapcsolódó védelmi intézkedések*

### 4.1. *Szerverekre vonatkozó előírások*

A **BIOKOM Nonprofit Kft.** a szervereket az erre a célra kialakított szerverszobában, illetve rack- szekrénybe telepíti és üzemelteti. A szerverek folyamatos üzeműek, azokat leállítani, illetve azok házát, kábelezését megbontani és azokhoz egyéb eszközt csatlakoztatni csak a rendszergazda, illetve az általa megbízott személy jogosult.
A **BIOKOM Nonprofit Kft.** a szerverszobában elhelyezett eszközök működésének biztonságát kiemelt figyelemmel kezeli:

- A **BIOKOM Nonprofit Kft.** kiemelt feladatokat ellátó szervereit redundáns módon alakítja ki, és a merevlemezek RAID tömbjeivel biztosítja azok folyamatos, biztonságos üzemét.
- Áramszünet idején a szünetmentes áramforrások (UPS) automatikus bekapcsolásával biztosítják az áramellátás zavartalanságát. Hosszabb idejű áramkimaradás esetén a rendszergazda (helyszínen vagy távoli eléréssel) gondoskodik a szerverek biztonságos leállásáról.
- A szerverek hozzáférését a **BIOKOM Nonprofit Kft.** korlátozza, a jogosultságokat a rendszergazda tartja nyilván.
- Rendszeres (a rendszergazdánál elérhető Mentési tervben részletezett) mentésekkel biztosítjuk az esetleges meghibásodások miatt kieső hardvereken tárolt adatok gyors és tervszerű visszaállítását.
- A szerverszoba füstjelzővel van ellátva, az esetleges tűzesetek időbeni jelzésére, a károk mérséklése érdekében.
- Tűz esetén a szerverszobában az ott elhelyezett tűzoltó készüléket szabad használni, vagy azzal megegyező halónnal oltó használható. A szerverszobában vízzel oltani tilos!

### 4.2. *Felhasználói munkaállomásokra vonatkozó előírások*

A vállalati munkaállomások, laptopok megbontása, szétszerelése tilos! Erre csak a rendszergazda vagy az általa megbízott személyek jogosultak.

A munkaállomásokhoz új hardver eszközt csak a rendszergazda csatlakoztathat, vagy a rendszergazda felügyeletével, engedélyével szabad.

A vállalati munkaállomásokon, laptopokon csak a rendszergazda által feltelepített, beállított és nyilvántartott programok futhatnak, a rendszergazda által feltelepített installációs

beállításokkal. Azokat megváltoztatni, vagy más programokat feltelepíteni a felhasználóknak tilos! *(Összhangban a 7. pontban kirészletezett, a szoftverek használatára vonatkozó irányelvekkel és szabályokkal.)*

A munkaállomásokon és laptopokon is kötelező a jelszavas képernyővédő beállítása. Ezeket a beállításokat a rendszergazda bármikor ellenőrizheti.

A munkaállomásokról az adatokat alapvetően a hálózati meghajtóra mentjük, mert a munkaállomások üzemét szünetmentes tápegység nem biztosítja. Munkavégzés idején kívül a beépített merevlemezeken vállalati, munka adatokat tárolni tilos!

### *4.3. Speciális hordozható berendezésekre vonatkozó előírások*

A Társaság minden hordozható számítógépének felhasználója ismert. Azokon csak olyan vállalati adatok, információk lehetnek, amelyek a fájl szerveren is mentésre kerültek.

A Társaság a hordozható számítógépeinek adatait az operációs rendszer által biztosított titkosítással védi, hogy eltulajdonítás esetén az esetleg érzékeny vállalati adatokat ne használhassák föl illetéktelenek a társaság érdekeivel ellentétesen. Az ehhez szükséges beállításokat a rendszergazda végzik és egyezteti az illetékes vezetőkkel.

Ezen szabályok betartásáért minden hordozható eszköz használója személyesen felelős.

## *5. Adathordozókhoz kapcsolódó védelmi intézkedések*

### *5.1. Optikai, elektronikus adathordozók kezelésének szabályai*

Ide a következő eszközök tartoznak, pl.:

- *Optikai adathordozók*: CD, DVD, stb.
- *Elektronikus adathordozók*: USB key, Flash memory, Smartcard., Memory Stick, stb.

Nem a Társaság tulajdonát képező optikai adathordozót tartalmazó számítástechnikai eszközt (számítógépet, laptopot, stb.) a Társaság területére behozni, és onnan kivinni csak külön ügyvezetői engedéllyel szabad.

A munkaállomásokba – minősített adat kivétele céljából – csak nyilvántartott, optikai és elektronikai adathordozókat szabad behelyezni. Minden minősített optikai és elektronikai adathordozó elszámolás köteles, függetlenül a tartalmától és a minősítés („FOKOZOTT", „KIEMELT") fokától.

Nyilvántartott adathordozót csak zárt, illetéktelen személyek számára nem hozzáférhető helyen szabad tárolni (pl. biztonsági zárral ellátott zárható szekrény, páncélszekrény).

Csak olyan optikai adathordozó kerülhet a munkaállomások meghajtóiba (elsősorban az "ellenőrzött adat be- és kiviteli helyen"), melyet a felhasználó előzetesen vírus és egyéb rosszindulatú programok szempontjából ellenőrzött vagy a rendszergazdával ellenőriztetett.

Az adathordozókat óvni kell a mechanikai, hő- és mágneses hatásoktól. Szállításuk csak megfelelő biztonságot nyújtó dobozban történhet.

Csak ellenőrzött optikai adathordozóról, illetve adathordozóra másolható adat. Minősített adat mentése csak ugyanolyan vagy magasabb minősítésű adathordozóra történhet.

### *5.2. Adathordozók másolásának rendje*

***Jogvédelem alá tartozó adathordozók másolása*** csak az ügyvezető előzetes engedélyével történhet. (*A másolásból eredő jogvita esetén a vállalat első vezetőjét terheli a felelősség.*)

***Minősített adathordozók másolása*** esetén a biztonsági másolatokat a rendszergazda köteles az eredetivel azonos szilárdságú védelemmel rendelkező, de attól távoli (legalább másik épület), ilyen célra alkalmas, tűzálló helyen biztonságba helyezni, a minősítés feltüntetésével megjelölni, naplózni és elzárni.

### *5.3. Adathordozók raktározási, hozzájutási, selejtezési és nyilvántartási rendje*

Az adathordozók beszerzésénél előnyben részesítjük a Társaság által megbízhatónak tartott termékeket.

Minősített adatokat tartalmazó számítástechnikai eszköz garanciális időn belüli javítását kizárólag a helyszínen, folyamatos felügyelet mellett lehet végeztetni.

Minősített adatokat tartalmazó merevlemezt, meghibásodása esetén külső vállalatnak javításra átadni tilos, az adathordozót meg kell semmisíteni. Ettől eltérni csak különleges esetekben (pl. nem készült mentés a merevlemezről) lehetséges, az ügyvezető igazgató külön írásos engedélyével.

Az olvashatatlan adathordozók javítása bármilyen segédprogrammal csak a rendszergazda számára engedélyezett.

A Társaságnál a minősített („ALAP", „FOKOZOTT", „KIEMELT") adatokat tartalmazó, sérült adathordozót mindenki a rendszergazdához köteles eljuttatni, ahol gondoskodnak a szakszerű megsemmisítésről.

## *6. Dokumentumokhoz kapcsolódó védelmi intézkedések*

### *6.1. Elektronikus dokumentumok védelme*

***Elektronikus dokumentumok tárolásának és kezelésének a rendje***

A Társaságnál minden munka dokumentumot (specifikációk, tervek, forráskódok, stb.) a fájlszerveren szabad csak tárolni. A Társaság által fejlesztett/létrehozott valamennyi forrást és dokumentumot kizárólag az aktuális rendszerben a fájlszerveren tároljuk, ezzel biztosítva a rendszerek egyes verzióinak konzisztens állapotainak összeállíthatóságát és egy korábbi konzisztens verzió visszaállíthatóságát.

Minősített adat, illetve másolatának továbbítása a hálózaton másolással, ill. a belső levelező rendszeren keresztül, valamint azok tárolása a lokális meghajtókon a felhasználó

egyéni felelőssége. A felhasználó minősített adatokat kizárólag olyan személynek továbbíthat, akinek az arra a konkrét minősített adatra vonatkozó betekintési jogosultsága megegyezik az adat minősítésével, vagy meghaladja azt, valamint olyan adathordozóra másolhatja azokat, amelynek minősítése megegyezik, vagy meghaladja a másolt adatok minősítését.

A rendszergazda a Társaság fájlszerverén az igényeknek megfelelő és a dokumentumok kezelési előírásait figyelembe vevő könyvtárszerkezetet hoz létre, ahova a felhasználók kötelesek a dokumentumaikat elhelyezni.

A rendszergazda állítja be a fájlszerveren a megfelelő jogosultságokat. Az elektronikus jogosultságok beállítását külön dokumentumban feljegyzi.

### *Elektronikus dokumentumok nyomtatása*

A **Társaságnál** a minősített dokumentumok nyomtatása csak a dedikált nyomtatókon engedélyezett. Ezen eszközök meghibásodása esetén sem megengedett a többi (hálózati) nyomtató használata. Ilyen esetben a feladatra, ideiglenesen belső cserével biztosítjuk a tartaléknyomtatót.

### *Biztonsági másolatok készítésének és tárolásának rendje*

A Társaság szerverén tárolt adatokról és adatbázisokról biztonsági másolatot napi illetve a „Mentési terv"-ben előírt rendszerességgel a rendszergazda köteles készíteni. A mentések elvégzését a rendszergazda az ún. „Mentési logfile-ban naplózza.

### *Az elektronikus levelezés (e-mail) biztonsági rendszabályai*

A Társaság az elektronikus levelezés biztonsági kockázatának csökkentését a kialakított információbiztonsági és informatikai rendszerrel, annak oktatásával, és az *Adatvédelmi szabályzattal* védi. A rendszergazda gondoskodik a vírusvédelemnek a levelező szolgáltatásokra történő kiterjesztéséről, ezen belül a központi vírusadatbázis letöltéséről, és a munkaállomások közötti (automatikus) szétosztásáról.

A Társaság a levelező rendszerében spam szűrőt használ a kéretlen levelek számának csökkentésére.

Tilos a levelező rendszeren nagyméretű állományokat továbbítani, helyette az állományokra mutató linket, vagy az állomány helyét kell elküldeni.

Tilos ismeretlen feladótól származó e-mailt megnyitni, tárolni, továbbítani.

Minden munkatárs köteles e-mail címét bizalmasan kezelni. Tilos a munkatársak saját és más munkatársak e-mail címét nem megbízható személynek kiadni, a munkával nem összefüggő területeken felhasználni.

Tilos a levelező rendszerben küldő címét figyelmen kívül hagyó, olyan szabályt beállítani, amely minden a kapott levélben szereplő címre választ küld.

A Társaság a munkatársak távozásakor a munkatárs e-mail címét megszünteti.

## 6.2. *Papíralapú dokumentumok védelme*

***Dokumentumok, iratok kategorizálása***

A dokumentumok bizalmasságuk alapján a következő kategóriákba sorolandók be:

- „**Nyilvános**": Nyilvános iratok nem tartalmaznak semmilyen olyan információt, amelynek nyilvánosságra kerülése a Társaság működésében fennakadásokat, presztízsveszteséget okozhat. Ezek az iratok rendszerint célzottan külső fél számára készülnek.
- „**Belső használatra**": A belső használatra minősített iratok alapvetően a Társaság munkavállalóira tartozó információkat tartalmaznak, és ezek a munka végzéséhez, a Társaság működéséhez szükségesek. Azonban ezek az információk illetéktelen kezekbe kerülve nem jelentenek veszélyt a Társaság működésére, legfeljebb enyhébb presztízsveszteséget okozhatnak. Kiadásuk külső fél részére lehetséges, de csak ügyvezetői engedéllyel, és ellenőrzött tartalommal.
- „**Bizalmas**": A Társaság bizalmas iratai olyan belső feljegyzések és dokumentumok, amelyek a Társaság számára fontos belső üzleti információkat tartalmaznak (pl. személyzeti adatok). Ezek általában csak a Társaság meghatározott vezetői szintjére, valamint bizonyos folyamatok üzemeltetőire tartoznak, és ezek illetéktelen kezekbe jutása a Társaság számára üzleti hátrányt, veszteséget és / vagy presztízsveszteséget jelenthet. A „**Bizalmas**" iratokhoz való hozzáférés a Társaságon belül szabályozott, és csak a jogosultak számára engedélyezett.
- „**Szigorúan bizalmas**" vagy „**Titkos**". A Társaság szigorúan bizalmas iratai olyan stratégiai, üzleti, személyi vagy egyéb titkot képező iratok, amelyek illetéktelen kezekbe kerülése valamely törvényt sértene, vagy a Társaság számára súlyos károkat okozhatna (pl. pályázati anyagok, pénzügyi adatok). A szigorúan bizalmas iratokhoz való hozzáférés a Társaságon belül szabályozott, és csak a jogosultak, és bizonyos folyamatokhoz kapcsolt, meghatározott személyek számára engedélyezett.

A dokumentumok bizalmasságának besorolása egyaránt érvényes, mind a papíralapú, mind az elektronikus dokumentumokra, iratokra, feljegyzésekre.

***Iratok minősítése***

A Társaságnál a Feljegyzések információs mátrixa (Bizonylati Album) tartalmazza az egyes iratok fajtái (kategóriái) minősítésének besorolását. Általánosan a következő besorolási alapelvek érvényesek:

- „**Nyilvános**" minősítésű iratok, pl. általában a marketing és PR anyagok, külső kommunikációk, valamint a külső dokumentumok, mint törvények, jogszabályok, engedélyek, stb.
- „**Belső használatra**": minősítésű iratok általában a Társaság belső működési szabályzatai, előírásai, az ezekhez illetve a mindennapi munkához kapcsolódó feljegyzések
- „**Bizalmas**" minősítésű iratok általában a Társaság ajánlatai, szerződései, megbízásai, bizonyos üzleti iratai, és az ezekkel kapcsolatos feljegyzések, továbbá az ügyfelekkel,

partnerekkel kapcsolatos feljegyzések. Bizalmas iratnak minősülnek továbbá a Társaság számviteli bizonylatai is. (Pl. beszállítók szerződései, ügyféllel kapcsolatos adatok és levelezések, könyvelési bizonylatok, számlák, személyi állomány bizonylatai, munkabér kifizetési lista, stb.)

- „**Szigorúan bizalmas**" minősítésű iratok általában a Társaság ***üzleti titkot*** tartalmazó iratai (Pl. szerződések, üzleti tervek, tenderek ajánlati dokumentumai és feljegyzései a készítés és beadás időszakában, pályázatok, stb.)

***Minősített iratok kezelése***

A Társaságnál a minőségirányítási rendszer és az információbiztonsági irányítási rendszer által szabályozott belső és külső dokumentumok kezelési módját a kézikönyv szabályozza

A „**Nyilvános**", a „**Belső használatra**" és a „**Bizalmas**" minősítésű dokumentumok, iratok besorolása a Feljegyzések információs mátrixa, illetve az ügyfél/törvényi előírások szerint történik. Az egyes iratokon nem kötelező az iratok minősítésének külön feltüntetése, mivel az adott irat fajtája / kategóriája alapján egyértelműen meghatározott, és az iratkezelés is ennek megfelelően történik.

A „**Bizalmas**" és a „**Szigorúan bizalmas**" (vagy „**Titkos**") iratok (nem „**Nyilvános**" iratok) nyomtatására dedikált eszközöket állítunk rendszerbe, illetve jelölünk ki, melyek fizikai elhelyezése (pl. a könyvelés és bérszámfejtésen, ügyvezető) és a hálózati konfigurációikból adódó exkluzív használata zárja ki az illetéktelen hozzáféréseket. E célra más nyomtatók használata nem megengedett. A dedikált nyomtatók használatát a többi nyomtatóhoz hasonló módon naplózzuk.

A „**Bizalmas**" iratokat zárható szekrényben, a „**Szigorúan bizalmas**" iratokat páncélszekrényben kell tárolni, és csak a használat idejére – folyamatos személyes jelenlét esetén – lehet a tárolási helyéről kivenni.

A „**Szigorúan bizalmas**" (vagy „**Titkos**") minősítésű dokumentum minősítését a dokumentumon és annak tárolási helyén is fel kell tüntetni.

## *7. Szoftverekhez kapcsolódó védelmi intézkedések*

A Társaság valamennyi számítógépén telepített szoftvert a rendszergazda a **Szoftverleltár**ban tartja nyilván, melyek csak érvényes licensszel rendelkező, vagy „freeware" szoftverek lehetnek.

Ez a nyilvántartás a viszonyítási alapja a szúrópróbaszerű ellenőrzéseknek és tartalmazza a szoftverkomponensek nevét, verzióját, licensz számát, illetve a hardver eszköz azonosítóját, amelyre telepítették.

A Társaság betartja és betartatja a szellemi tulajdonjogokra vonatkozó törvényi, jogszabályi előírásokat. A szoftvertermékek használatára vonatkozó korlátozást, az illegális szoftverek használatának megakadályozását biztosítja. A licensz gazdálkodást a rendszergazda szúrópróbaszerűen ellenőrzi.

### *7.1. Rendszerprogramok telepítésének, használatának rendje*

A Társaságnál a rendszerprogramok telepítését és azok konfigurációs komponenseinek beállításait kizárólag a rendszergazda, vagy az általa megbízott személyek végezhetik.

A Társaság többi munkatársainak tilos a rendszerprogramokat, vagy azok beállításait módosítani, másolni, törölni. A munkatársak e-mailben jelezzék a rendszergazdának, ha az operációs rendszerrel, hálózattal, vagy annak beállításaival kapcsolatban problémájuk van.

A hálózati- és rendszerprogramok vagy azok konfigurációs elemeinek minden sérülését, vagy váratlan módosulását a rendszergazda kivizsgálja, és mint biztonsági incidenst naplózza.

A hálózati- és rendszerprogramok legfrissebb, biztonsági hibáktól mentes verzióinak automatikus frissítését a rendszergazda biztosítja.

### *7.2. Alkalmazói programok telepítésének és használatának a rendje*

A munkaállomásokra, laptopokra telepített szoftvereken és azok beállításain változtatni tilos.

Az illegális és/vagy kártékony szoftverek telepítésének megakadályozására és a Társaság informatikai rendszerének biztonsága garantálására, a munkaállomásokra a munkatársak alap esetben nem telepíthetnek szoftvereket. Ettől eltérni csak az Ügyvezető vagy az Információbiztonsági megbízott írásos engedélyével lehet. A munkatársak adminisztrátori jogosultságot a munkaállomásokra indokolt esetekben, a fenti vezetők írásos engedélyével kaphatnak.

A szoftvertelepítés kizárólag a rendszergazda feladata és felelőssége.

### *7.3. Az internet-használat biztonsági követelményei*

Az internet használata alapvetően a szoftverfejlesztésekhez és a könyvelési/bérszámfejtési szolgáltatásokhoz szükséges mértékben megengedett, de az elfogadható hálózati terhelés fenntartása érdekében a Társaság a munkatársak önkorlátozását várja el. Az internet forgalmat a Társaság ellenőrzi és naplózza, a sávszélességet korlátozza, és bizonyos, a törvényi rendelkezésekbe ütköző oldalak látogatását tiltja. Az indokolatlanul nagy felhasználókkal szemben megfelelő intézkedéseket hoz, ha azok, az üzleti érdekeit sértő mértékben korlátoznák.

## *8. Adatokhoz kapcsolódó védelmi intézkedések*

### *8.1. Az adatkezelés általános szabályai a Társaságnál*

A Társaság informatikai rendszerében tárolt és feldolgozott adatok vonatkozásában gondoskodik arról, hogy az adatok sértetlensége és hitelessége az adatkezelés során megőrződjön, és azok rendelkezésre állása folyamatosan biztosítható legyen.

*Adatgazdák*

Az „adatgazda" fogalmi alkalmazásának célja a Társaság adatvagyona számára a megfelelő működési és biztonsági követelmények meghatározása azáltal, hogy az adatok kezelésének szabályaival kapcsolatos felelősségek az adatokat ténylegesen használó szervezeti egységekre hárulnak.

Az egyes adatfajták, adattípusok, adatbázisok működésének és működtetésének szabályait és biztonsági követelményeit meghatározó felelős munkatársakat nevezzük az adott adatok / adatbázisok adatgazdáinak. Az adatgazdák határozzák meg – többek között – az adott adatfajták, adattípusok, adatbázisok működtetési folyamatait, az adatokhoz hozzáféréssel rendelkező személyek körét és jogosultságait.

*Adatok értékének súlya*

A **Társaság** Informatikai rendszerében feldolgozott, továbbított, tárolt adatok kockázatarányos védelmének biztosítása érdekében az adatokat formálisan azonosítjuk, és soroljuk be azokat prioritásuk szerint.

Az informatikai rendszerben elektronikusan tárolt adatok esetén az adatok azon halmaza, amelyekre a tárolás számítástechnikai körülményeiből adódóan jellemzően azonos védettség valósítható meg (közös adatbázis, azonos könyvtár), ugyanabba az információvédelmi osztályba sorolandó, mégpedig oly módon, hogy a halmaz egészére ki kell terjeszteni a halmaz legérzékenyebb elemének besorolását.

Az adatosztályozás során az adatokat bizalmasságuk, sértetlenségük és a rendelkezésre állásuk elveszítéséből eredő vagyoni és nem vagyoni kár nagyságától függően „információvédelmi osztályokba" soroljuk.

Az adatgazdák az adatok osztályozását évente legalább egy alkalommal felülvizsgálják, és a besorolást megváltoztatják, vagy jóváhagyják, ha

- az információ kezelését és feldolgozását végző vagy támogató folyamatokban, illetve a kezelt adatok körében lényeges változás áll be;
- a Társaság tulajdonában vagy használatában lévő informatikai rendszerekben lényeges változás áll be.

Az IBSZ, és a Társaság bármely egyéb szabályzata a különböző információvédelmi osztályokra, illetve az azokba besorolt adatok kezelésére, tárolására, megtekintésére, feldolgozására, nyomtatására, törlésére (selejtezésére), vonatkozóan további különös, szigorító szabályokat állapíthat meg.

*Információvédelmi osztályok*

A **Társaság** három információvédelmi osztályt különböztet meg:

- „**ALAP**" védelmi osztály (dokumentumként „**Belső használatra**" jelölés)
- „**FOKOZOTT**" védelmi osztály (dokumentumként „**Bizalmas**" jelölés)
- „**KIEMELT**" védelmi osztály (dokumentumként „**Szigorúan bizalmas**" vagy „**Titkos**" jelölés)

A besorolás különös szempontjai (összhangban az iratok minősítésének irányelveivel 6.2.2 fejezetben) :

Az információvédelmi „**ALAP**" biztonsági osztályba soroljuk az olyan adatokat, dokumentumokat, melyek a **Társaság** működése szempontjából nem lényegesek, és amelyeknek nyilvánosságra kerülése nem okoz sem jelentős anyagi, sem erkölcsi és/vagy szellemi kárt a Társaságnak.

Az információvédelmi „**ALAP**" biztonsági osztály csak az általános hálózati hozzáféréssel védett, hozzá további biztonsági eljárások (mentés, naplózás) nem, vagy csak korlátozottan kapcsolódnak. Kezelésére különös szabályok nem vonatkoznak.

Az „**ALAP**" biztonsági osztály az alapértelmezés, azaz minden, be nem sorolt adatot „**ALAP**" biztonsági osztályba soroltnak kell tekinteni a tényleges besorolás megtörténtéig. (Amennyiben ettől eltérés szükséges, ott az adott Adatgazda feladata és felelőssége az eltérő besorolás előre jelzése.)

A "**FOKOZOTT**" vagy „**KIEMELT**" védelmi osztályba sorolt adat, dokumentum, információ akár a jog által védelemben részesített is lehet, így azok védelmére büntetőjogi, polgári jogi és munkajogi szabályok is vonatkozhatnak.

Legalább információvédelmi „**FOKOZOTT**" biztonsági osztályba kell sorolni:

- személyes adatokat,
- közérdekű, illetve közérdekből nyilvános adatokat,
- magántitkokat, így különösen, de nem kizárólagosan a levéltitkot,
- a Társaság egyéb belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) adatokat.

Információvédelmi „**KIEMELT**" biztonsági osztályba kell sorolni azon belső dokumentumokat, adatokat, amelyek a nem kívánt nyilvánosságra kerülése a Társaság üzleti érdekeinek és céljainak nagy kárt okozhat. Ezen adatok bizalmasságának, sértetlenségének és rendelkezésre állásának elvesztése a Társaság súlyos érdekeit sértené. Ilyen minősített adatok lehetnek:

- üzleti titoknak minősülő adatok,
- vállalati, technológiai stratégiák,
- a Társaság tervezett bevételeiről ill. kiadásairól szóló jelentések,
- gazdasági tervek, fejlesztések adatai.

### *Adatok osztályozása*

Az adatgazdák feladata, hogy a felelősségi körükbe tartozó adatok besorolását elvégezzék, és felelősek az adatok osztályozásáért:

a) az egyes informatikai alkalmazásokért, továbbá az elektronikus levelezésben és a szervezeti egységük által kezelt adataiért
b) a fájlszervereknek a szervezeti egységük számára elkülönített területén tárolt minden adatért,

mindkét esetben különös tekintettel az adatok nyomtatott formában való megjelentetéseire, a kinyomtatott dokumentumokra, táblázatokra, jelentésekre, riportokra.

Az adatgazdák minden adatot illetve adatfajtát, annak megjelenési formájától függetlenül, információvédelmi osztályba sorolnak. Az információvédelmi besorolást az kezdeményezi, akinél a feladata végrehajtása során az adat keletkezik, illetve az, aki beosztásánál fogva olyan munkamegbízást ad valamely dolgozónak, melynek során adatok, dokumentumok keletkeznek, vagy keletkezhetnek.

Az adatok osztályozását kezdeményezni kell:

a) új informatikai alkalmazás fejlesztésekor az alkalmazás által kezelt adatok körében,
b) informatikai alkalmazás módosítása esetén, amennyiben a módosítás a kezelt adatok körére is kiterjed,
c) az ügyviteli folyamatokban beállt olyan változás esetén, amely az adott ügyviteli folyamat által kezelt adatok körére is kiterjed.

Az adatgazda a besorolás különös szempontjait figyelembe véve dönt az adott adat, dokumentum besorolásáról. Az adatgazda a besorolásról tájékoztatja a rendszergazdát. A rendszergazda a besorolást átvezetik az általuk vezetett „Adatosztályozási séma" nyilvántartásban, továbbá – amennyiben szükséges – kezdeményezik a besorolásnak megfelelő jelzés feltüntetését az adat nyomtatott megjelenési formáin.

## *8.2. Jelszavak kezelésének és használatának a rendje*

***Felhasználói hálózati és alkalmazás jelszók és kezelésének szabályai:***

A Társaságnál jogosultsági rendszert alakítottunk ki a szervereken tárolt adatokhoz történő szabályozott hozzáférések biztosítása érdekében, melyet igény szerint módosítunk és rendszeresen ellenőrzünk.

A munkaállomások indításakor, a hálózatra, illetve a használt egyes alkalmazásokra történő bejelentkezéshez minden felhasználónak a felhasználói nevét és jelszavát kéri a rendszer, amely biztosítja, hogy illetéktelen felhasználók mások nevében ne tevékenykedhessenek. Ugyanezen okokból a felhasználó, amikor elhagyja a számítógépet, jelentkezzen ki, zárolja a munkaállomást, vagy aktiválja a jelszóval védett képernyővédőt!

- A felhasználói név és jelszó azonosítja és hitelesíti a felhasználót a hálózaton, és ezzel az azonosítással használhatja a személyéhez hozzákapcsolt engedélyeket mind a hálózaton, mind a levelezésben valamint a különböző, a munkája végzéséhez szükséges fájlszervereken és az általa használt alkalmazásokban.
- A jelszó nehezen kitalálható, de könnyen begépelhető, könnyen megjegyezhető, de minimum 6 karakter hosszú, kis-, nagybetűt és számot is tartalmazó legyen. A követelménynek való megfelelést az operációs rendszer ellenőrzi. Az operációsrendszer beállítása a rendszergazda felelőssége.
- A jelszavát mindenki köteles titokban tartani, senki sem adhatja át másnak, vagy nem teheti lehetővé más általi megismerését sem.
- Hosszabb hiányzás, betegség esetén a hálózati jelszó nem adható át más személynek. A helyettesítést a hozzáférési jogosultságok ideiglenes megváltoztatásával biztosítjuk. A hozzáférések változtatási igényét időben, a rendszergazdának kell eljuttatni.

***Rendszergazdai jelszó és kezelésének szabályai:***

- A Társaság által üzemeltetett szerver és egyéb fontos adminisztratív jelszavakat a páncélszekrényben tárolja (és megfelelően titkosított fájlban is).
- A rendszergazdai jelszó minimum 8 karakter hosszú „erős jelszó" legyen, tartalmazzon betűket, számokat és írásjel karaktereket.
- Új jelszó megadásánál a jelszó nem lehet azonos az 5 legutóbb megadott jelszóval.
- A beállított jelszót másnak kiadni, illetve látható helyre felírni, rögzíteni tilos!

## *8.3. Adatok bevitele, feldolgozása és kiadása*

***Az (éles)adatbázisok működtetése és karbantartása***

Éles adatbázisok alatt értjük a produktív, illetve a rendszer-/integrációs-/regressziós teszt-adatbázisokat is.

Az adatgazdák felügyeletével a rendszergazda feladata és felelőssége.

**Adatok bevitele:**

Az adatok beviteli módjának meghatározása és ellenőrzésének végrehajtása az adatgazda felelőssége. Az adatok bevitele az ügyviteli rendszerek felületein keresztül és ellenőrzésével történhet. Az adatgazda engedélyezése nélkül a rendszergazda közvetlen nem hajthat végre adatváltoztatásokat az adatbázisokban.

**Adatok feldolgozása:**

Az adatok feldolgozását alapvetően az ügyviteli rendszerek végzik. Rendszergazdai beavatkozásra csak adatgazdai vagy ügyvezetői engedély szükséges.

**Jogosultságok kezelése:**

Az adatgazda határozza meg a rendszergazda számára az ügyvezető jóváhagyásával.

**Adatok kivétele:**

Az adatok kivétele szintén alapvetően az ügyviteli rendszerek meghatározott interfészeivel lehetséges. Közvetlenül az adatbázisból adatgazdai vagy ügyvezetői engedély szükséges.

**Adatbázisok mentése:**

Az adatbázis állományokat a rendszergazda a Mentési Tervnek megfelelően menti és tárolja.

## *8.4. A (Éles)rendszerek/alkalmazások karbantartása*

A rendszerek frissítéseinek telepítését a rendszergazda végzi. Az éles rendszerek frissítéseinek installálását lehetőleg munkaidő után végezzük. Ha sürgős biztonsági vagy egyéb frissítést kell telepíteni, akkor erről a munkatársakat e-mailben, az aktualizálás időpontjának, tartalmának és idejének egyidejű közlésével előre értesítjük.

## 8.5. *Egyéb (elektronikus) üzleti adatok biztonsága*

A Társaság szervezeti egységei a náluk keletkező egyéb tervezési, üzleti, gazdasági stb. adataikat a központi fájlszerveren erre a célra létrehozott, megfelelő hozzáférési jogosultságokkal elérhető könyvtárakban kötelesek tárolni, hogy a mentési rendszer által biztosított védelem ezen adatokra is érvényesüljön.

## 8.6. *Mentési rendszer*

A Társaság az adatbázisok, és fájlszerver(ek) adattartalmát rendszeres biztonsági mentésekkel védi. A munkaállomásokon ezért munkaidő után csak olyan társasági adatok tárolhatók, melyeket a szerveren is mentettek.

***Az adatbázis szerver(ek) mentése***

Az adatbázis állományokat a rendszergazda a Mentési tervnek megfelelően mentik és tárolják. A mentések megtörténtét Mentési logfile-ban vezetjük.

A biztonsági másolatok visszaállítási tesztelésével a rendszergazda köteles rendszeres időközönként meggyőződni a mentések visszaállíthatóságáról. Ezen a tesztelések eredményeit a Mentési logfile-ban kell rögzíteni és megőrizni.

***A fájl- és nyomtatószerver(ek) mentése***

A kijelölt könyvtárstruktúrákat és nyomtatószerver naplókat a rendszergazda a Mentési tervnek megfelelően menti és tárolja. A mentések megtörténtét Mentési logfile-ban vezetjük.

A biztonsági másolatok visszaállítási tesztelésével a rendszergazda köteles rendszeres időközönként meggyőződni a mentések visszaállíthatóságáról. Ezen a tesztelések eredményeit a Mentési logfile-ban kell rögzíteni és megőrizni.

# 9. *Személyekhez kapcsolódó védelmi intézkedések*

## 9.1. *Biztonsági ellenőrzés*

A Társaság informatikai rendszereihez csak olyan munkatársak kaphatnak hozzáférést (felhasználói név / jelszó) akik:

- Sikeresen átestek a személyzeti felvételi folyamat biztonsági megfelelőségi ellenőrzésén;
- Munkaszerződésüket, az abban szereplő általános információbiztonsági és titoktartási kötelezettségeikkel együtt, aláírásukkal fogadták el;
- Jelen szabályzat és a Társaság minőségügyi és információvédelmi politikájának tartalmát képzés keretében megismerték;

A Társaság a dolgozók információbiztonsági képzését, az informatikai rendszerben történt jelentős változásokhoz kapcsolódva, aktualizáló tudatosító képzés keretében, de legalább évi egy alkalommal, ismétlődő oktatással rendszeresen biztosítja.

A Társaság által üzemeltetett adatbázisokat csak a megrendelő által elfogadott és ellenőrzött felhasználók használhatják a megfelelő biztonságot nyújtó biztonságos internetkapcsolaton keresztül.

A Társaság hálózatához, az azokon tárolt adatokhoz vagy adatbázisokhoz, illetve azok bizonyos részeihez biztonságos vonalon távoli hozzáféréssel csak olyan alkalmazottak vagy szerződéses partnerek férhetnek hozzá, akiknek a szerződéses feltételek alapján ehhez jogosultságuk van. A hozzáférések minden esetben csak a szerződés szerinti adatokra, információkra korlátozódnak.

## *9.2. Kilépés vagy átlépés adminisztrálása*

Ha egy alkalmazott munkaviszonya megszűnik, a rendszergazda adminisztrálja, hogy:

- a felhasználó összes user neve (felhasználói neve) és jelszava törlésre, ill. az új beosztásnak megfelelően módosításra került,
- továbbá a rendelkezésére bocsátott vállalati informatikai vagyontárgyakat sértetlenül visszaszolgáltatta. Ezeket a hozzárendeléseket az erre szolgáló nyilvántartásokból törölte ill. a változásoknak megfelelően módosította.

Ez biztosítja, hogy a felhasználó minden időpontban az őt aktuálisan megillető jogosultságokkal rendelkezzen. A visszavonásnak a (régi) beosztás megszűnésekor kell megtörténnie, aminek megtörténtét az *Elszámoló lapon* a Vezető rendszergazda aláírásával igazolja. Az új jogosultságok kiosztása mindig csak az új beosztásba helyezés után történhet meg. Ez biztosítja az esetleges szándékos, vagy vétlen károkozás elkerülését a védett információs vagyontárgyakban, vagy a jogosulatlan hozzáférésekből fakadó, esetleges jogi eljárásokat.

## *9.3. Titoktartás*

A Társaság minden alkalmazottja köteles a munkaviszonya során tudomására jutott bizalmas információkat és adatokat üzleti titokként kezelni, és azokat a munkaviszony fennállása alatt valamint annak megszűnését követően megőrizni, és semmilyen harmadik félnek ki nem adni.

A Társasággal szerződéses kapcsolatban álló partnereket és alvállalkozókat is Titoktartási kötelezettség terheli, amelyeket a velük kötött szerződésekben, azok mellékleteként és a vállalati szerződésmintákban is érvényesítünk.

A titoktartási kötelezettség megszegése esetén a munkaköri leírás titokvédelmi kitétele, illetve külső felek esetén az együttműködési megállapodás titokvédelemre vonatkozó része képezi a felelősségre vonhatóság alapját.

# 10. Információs rendszerek működésének biztonsági ellenőrzései

## 10.1. Információs rendszerek felülvizsgálata

A Társaságnál az információs rendszerek felülvizsgálatának a célja, hogy teljes körűen meggyőződjön arról, hogy:

- az információs rendszer biztonsága megfelel-e a Társaság vezetősége által elfogadott / elvárt biztonsági követelményeknek,
- érvényesülnek-e az Információbiztonsági Politikában, az IBSZ-ben és a Menedzsmentrendszer Kézikönyvében foglaltak,
- történnek-e az információs rendszerek illetve az általuk nyújtott szolgáltatások biztonságát sértő események (incidensek), illetve mekkora ezek bekövetkezési valószínűsége.

Ennek érdekében minimum éves rendszerességgel az egész információbiztonsági irányítási rendszer (IBIR) működésére teljes körű felülvizsgálatokat – belső auditokat – tartunk. Ennek szabályozását a Menedzsmentrendszer Kézikönyve tartalmazza.

## 10.2. Informatikai rendszer működésének naplózása

A Társaság az informatikai rendszerében történt eseményeket, állapotváltozásokat a szervereken beállított naplófájlokban tartja nyilván. A naplófájlok biztosítják az esetleges biztonsági incidensek bizonyítékait, ezért azokat és a beállításokkal, különös gondossággal kell kezelni és védeni.

Rendszeresen naplózzuk a következő eseményeket:

- Hálózati forgalom (külső: internet),
- E-mail forgalom naplózása,
- Illetéktelen hozzáférési kísérletek (! Sikeres / sikertelen),

A naplófájlokat a rendszergazda heti rendszerességgel ellenőrzi, illetéktelen hozzáférések és egyéb tiltott, nemkívánatos események után kutatva.

## 10.3. Vírusok elleni védelem

Minden önálló és hálózati munkaállomásra, szerverre automatikus vírusellenőrző szoftvert telepítünk.

A rendszer nem csak a fájlokat, hanem a levelezést is ellenőrzi. A telepítésért és a rendszer működéséért, a vírus információk napra készségéért a rendszergazda felelős.

A szerveren futó vírusellenőrző szoftver telepítése a rendszergazda feladata. A víruskereső beállításait (mikor lépjen működésbe, mit ellenőrizzen, és mit tegyen, ha vírust talál) a rendszergazda állítja be.

A vírusirtó szervizeit leállítani, komponenseit törölni, automatikus indítási módjukat, prioritásukat megváltoztatni tilos.

A felhasználó értesítse a számítógép szokatlan működéséről a rendszergazdát. Vírus-gyanús esetben kellő körültekintéssel a hálózatról le kell kapcsolni, és az esetet a rendszergazda vizsgálja ki!

Teendők vírus észlelése esetén:

- A munkaállomáson vírus felfedezése esetén tovább dolgozni tilos.
- Ha a munkaállomás hálózati kapcsolatban van, csatlakoztassuk le, a gépet kapcsoljuk ki és jól láthatóan, írjuk ki, hogy tilos rajta dolgozni.
- Haladéktalanul értesítsük a rendszergazdát.
- Az Információbiztonsági megbízott feladata annak dokumentálása, hogy ki által, mi módon került a vírus a rendszerbe (amennyiben ez kideríthető), ennek jelentése a Társaság vezetése felé. A megfelelő következtetések levonása, illetve bizonyítható szándékosság esetén a fegyelmi eljárást (vagy megfelelő szankció) kezdeményezése a Társaság vezetőségének a feladata.

A vírusellenőrző által nem ismert vírus felfedezése esetén azt csak a rendszergazda irthatja le. A rendszergazda feladata és felelőssége továbbá annak megvizsgálása, hogy milyen további károkat okozott / okozhatott-e a vírus, és annak megfelelően a szükséges intézkedések megtétele.

Vírusok előállítása/terjesztése szigorúan tilos. Számítógépes vírusok birtoklása (minták, gyűjtemények) csak Ügyvezetői engedéllyel az arra fölhatalmazott rendszergazda esetében lehetséges.

Tilos az ismeretlen eredetű, nem beazonosítható feladótól származó levelek ill. azok csatolmányainak (fájlok, linkek) megnyitása. Ezeket megnyitás nélkül törölni kell.

Riasztásokat, figyelmeztetéseket csak a rendszergazda adhat ki. Álhíreket, vírusokról hibás információkat, láncleveleket előállítani, terjeszteni tilos.

## *10.4. Informatikai események, incidensek kezelése*

Információbiztonsági eseménynek minősülnek:

- Minősített adatok szóbeli megosztása illetéktelennel vagy azok nyilvánosságra hozása.
- Minősített adatok dokumentumban, adathordozón vagy informatikai rendszeren (pl. levelezéssel) történő illegális továbbítása.
- Illetéktelen hozzáférés a számítógépes rendszerhez (jelenlegi, vagy volt alkalmazott vétlen, vagy tudatos közreműködése által, vagy biztonsági gyengeség kihasználásával).
- Valamely adatbázis részének vagy egészének, vagy egyéb minősített adatok sérülése vagy elvesztése oly módon, hogy a mentésből a sérült vagy elveszett adatok nem visszaállíthatóak.
- Az IT rendszer részének vagy egészének használhatatlanná válása vírus, egyéb rosszindulatú szoftver által vagy egyéb módon.

Információbiztonsági incidenst (eseményt) észlelő személy köteles azonnal tájékoztatni közvetlen munkahelyi vezetőjét, aki haladéktalanul tájékoztatja az Információbiztonsági Megbízottat.

Az eset kivizsgálásának meg kell állapítani:

- milyen események történtek,
- történt-e bűncselekmény,
- az események milyen és mekkora kárt okoztak, illetve okozhattak,
- milyen intézkedések szükségesek a kárelhárításhoz, illetve mérsékléséhez,
- az események kiváltó okait, előzményeit,
- az eseményekért közvetlenül és közvetve felelős személyeket és a felelősség mértéket.

Amennyiben bűncselekmény történt, haladéktalanul megtesszük az illetékes hatóságoknál a feljelentést. Bűnügyi eljárás esetén a nyomozó hatósággal együttműködve folytatjuk le a további vizsgálatot. Amennyiben ilyen esetben konkrét gyanú merül fel, úgy az illetőt az ügy kivizsgálásának befejezéséig munkaköréből felfüggesztjük.

A kivizsgálás eredményéről az Ügyvezető igazgatót írásban kell tájékoztatni, amely tartalmazzon javaslatot:

- a felelős személyekre,
- a felelősségre vonás mértékére,
- a szükséges új intézkedések bevezetésére vonatkozólag,

amelyekkel további hasonló események, incidensek, biztonságsértések elkerülhetők.

A jelen IBSZ-ben foglalt biztonsági szabályok megsértése munkaügyi vagy komolyabb esetben büntetőjogi felelősségre vonást vonhat maga után.

# *11. Az IBSZ felülvizsgálata és frissítése*

Az IBSZ -t rendszeresen, évente legalább egy alkalommal felülvizsgáljuk. Az IBSZ felülvizsgálatát köteles kezdeményezni az Ügyvezető, az Információbiztonsági megbízott, ill. a Társaság valamennyi vezetője, amennyiben az információbiztonságot érintő változtatás történik a Társaság egyéb szabályzataiban vagy a hatályos törvényekben, jogszabályokban. A módosítások átvezetéséért az információbiztonsági megbízott, a jóváhagyásért az Ügyvezető felelős. A változtatások érintettek általi megismertetéséért minden szervezeti egység vezetője a felelős.

# *12. Hivatkozások*

## *12.1. Rövidítések*

IBSZ..... Információbiztonsági Szabályzat
IBIR..... **Információbiztonsági Irányítási Rendszer**
IBMB ..... **Információbiztonsági Megbízott**

## *12.2. Fogalmak és meghatározások*

***Az információ biztonsága*** = az információ rendelkezésre állása + az információ sértetlensége + az információ bizalmassága.

***Rendelkezésre állás***: az információ az arra jogosult személyek illetve folyamatok számára mindig hozzáférhetően, a szükséges módon legyen elérhető, felhasználható.

***Sértetlenség***: az adathordozó, az azon levő információ és a tárolására, feldolgozására, továbbítására szolgáló informatikai rendszer az eredeti állapotának megfelelő, ép és teljes.

***Bizalmasság***: az információhoz és a tárolására, feldolgozására, továbbítására szolgáló informatikai rendszerekhez és adathordozóihoz csak korlátozott számú, és az arra jogosult személyek férhetnek hozzá.

***Hitelesség***: az információ forrása a megjelölt, tartalma eredeti.

## *12.3. Hatályos információbiztonsági jogszabályok, előírások*

***Jogszabályok, törvények, rendeletek:***

2011. éci CXII. tv. az információs önrendelkezési jogról és az információszabadságról
2009. évi CLV. törvény a minősített adat védelméről
1996. LVII tv. a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról;
2012. évi C. törvény a Büntető Törvénykönyvről
XLIII. fejezet: Tiltott adatszerzés és az információs rendszer elleni bűncselekmények (422-424 §)
*Biztonságtechnikai, tűzvédelmi szabványok, előírások:*
MI-02-102-79 Számítóközpontok tűzvédelme (műszaki irányelvek);
MSZ EN 50173-1, MSZ EN 50174-1,2 és 3 Információtechnikai kábeltelepítés;
MSZ EN 50310 A potenciál-kiegyenlítés;

# *13. Mellékletek*

IIR Kézikönyve

A Társaság vállalati politikája

Adatvédelmi és adatbiztonsági szabályzat 2018.

**Érvényes: 2018. május 1. napjától.**

Jóváhagyta:

Biró Péter
ügyvezető