Kajári és Fia Csomagolóanyag Gyártó Korlátolt Felelősségű Társaság

Informatikai Biztonsági Szabályzat

A szabályzatot kidolgozta: Lajos János
mérnök tanácsadó

A szabályzat alkalmazását 2025. február 04.-i hatállyal elrendelte: Kajári Ferenc
ügyvezető igazgató

A szabályzat 21 számozott oldalt tartalmaz!

A szabályzat felelőse az informatikai felelős!

Székhely és Telephely: 6230. Soltvadkert, Szarvaskút dűlő 13/1
Telefon/Telefax: 78/481-194
E-mail: kajarikft@kajarikft.hu Honlap: www.kajarikft.hu

1. Az Informatikai Biztonsági Szabályzat célja

Az Kajári és Fia Csomagolóanyag Gyártó Korlátolt Felelősségű Társaság (továbbiakban: Társaság) a belső szabályozások megfelelő szintű kezelése, a hazai és nemzetközi irányítási sztenderdeknek és jogszabályoknak való megfelelés, valamint a tevékenységek átlátható kezelése érdekében alakította ki Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) kidolgozása és hatályba léptetése mellett döntött.
Az informatikai eszközök egyre szélesebb körű felhasználása változó és mindig megújuló kockázatot is jelent számunkra ezért jelen szabályzat célja egységes keretszabályokat, értelmezéseket, iránymutatást adni az adatgazdák, az informatikai eszközök üzemeltetői, fejlesztői, felhasználói számára, rögzítve azokat a szabályokat, melyeket a munkakörükhöz rendelt adatok kezelése során követniük kell.

Az IBSZ alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az IBSZ célja továbbá:

- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- 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 feltételeinek megteremtése,
- az adatbiztonsággal kapcsolatok szerepek, felelősségi és jogkörök rögzítése,
- a számítástechnikai alkalmazási rendszerek, berendezések, hálózati eszközök biztonságának elősegítése.

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzembehelyezésen keresztül az üzemeltetésig.
A jelen IBSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

2. Az Informatikai Biztonsági Szabályzat hatálya

2.1. Személyi hatálya

A szabályzat szervezeti hatálya kiterjed:

- a Társaság minden munkatársára,
- a Társasággal szerződéses viszonyban tevékenykedő partnerekre.

2.2. Tárgyi hatálya

- kiterjed a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed a vállalkozás tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre,
- valamint az informatikai eszközök műszaki dokumentációira,
- kiterjed az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- kiterjed a rendszer- és felhasználói programokra,
- kiterjed az adatok felhasználására vonatkozó utasításokra,
- kiterjed az adathordozók tárolására, felhasználására.

2.3. Területi hatálya

- kiterjed a Társaság telephelyén üzemeltetett informatikai erőforrások üzemelési helyszíneire.

2.4. Időbeli hatálya

A jelen szabályzat a jóváhagyás napján lép hatályba, a szabályzatban foglalt feladatok és szabályok ezen időponttól alkalmazandók. A szabályzat visszavonásig érvényes.

3. A szabályzat minősítése

A jelen szabályozás belső nyilvános dokumentum, amelyet a szabályzat személyi hatálya alá nem tartozó harmadik személy csak és kizárólag az ügyvezető igazgató előzetes írásos engedélye alapján ismerhet meg. Jelen szabályzat személyi hatálya alá tartozóknak a szabályzat előírásait kötelezően ismerniük és követniük kell, azonban harmadik személynek a szabályzatból információkat nem adhatnak ki.

4. Az adatkezelés során használt fontosabb fogalmak

Adatkezelés: az alkalmazott eljárástól függetlenül az adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is;

Adatfeldolgozás: az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

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

Adatkezelő*:* az a természetes vagy jogi személy, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bízhat meg.

Adatfeldolgozó: az a természetes vagy jogi személy, aki vagy amely az adatkezelő megbízásából adatok feldolgozását végzi.

Adatbiztonság: az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

Adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítás többé nem lehetséges.

Adatmegjelölés: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából.

Adatzárolás: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából.

Adatmegsemmisítés: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése.

Adatállomány: az egy nyilvántartásban kezelt adatok összessége.

Adatvédelmi incidens: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

Biztonsági esemény: minden esemény, amelynek káros hatása lehet az informatikai eszköz vagy azon tárolt adatok bizalmasságára, sértetlenségére illetve rendelkezésre állására.

Felhasználó: az a személy, aki a Társaság valamely szolgáltatását igénybe veszi. Belső felhasználó a Társasággal munkaviszonyban álló személy, külső felhasználó a társasággal jogviszonyban nem álló személy. Külső felhasználók a Társaság publikus szolgáltatásait vehetik igénybe , egyéb szolgáltatások igénybevételére csak az üzemeltető határozott időre szóló engedélyével jogosultak.

Folyamatos védelem: folyamatos a védelem, ha az időben változó körülmények és viszonyok ellenére is megszakítás nélkül valósul meg.

Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely, nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval.

Hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat- teljeskörű vagy egyes műveletekre kiterjedő- kezeléséhez.

Incidens: minden esemény, amelynek káros hatása van az informatikai eszköz vagy azon tárolt adatok bizalmasságára, sértetlenségére illetve rendelkezésre állására.

Információ védelem: az informatikai rendszerek által kezelt adatok által hordozott információk védelme a bizalmasság, a hitelesség és a sértetlenség sérülése, elvesztése ellen, Az információ védelem az informatikai biztonság egyik alapterülete.

Kockázattal arányos védelem: kockázattal arányos a védelem, ha kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékek összegével és megvalósított védelmi intézkedések következtében a kockázatok elviselhető mértékűre mérséklődtek.

Nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik;

Megbízható működés: az informatikai rendszerek által kezelt adatok által hordozott információk védelme a rendelkezésre állás, és a funkcionalitás sérülése, elvesztése ellen. A megbízható működés az informatikai biztonság másik alapterülete.

Személyes adat: bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha öt-közvetlenül vagy közvetve-név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.

Teljeskörű védelem: teljeskörű a védelem, ha a védelmi intézkedések az informatikai rendszer összes elemére, és az összes rétegére kiterjednek.

Tiltakozás: az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri.

Zárt védelem: zárt a védelem, ha az összes releváns fenyegetés figyelembe lett véve a védelmi intézkedések megtervezésénél és megvalósításánál.

5. Az IBSZ szervezete

5.1. A vezetés elkötelezettsége

Az Információ Biztonsági Politika és a jelen IBSZ által meghatározott követelményrendszeren keresztül testesül meg azon vezetői akarat és elkötelezettség, amely meghatározza minden érintett személy viszonyát az informatikai rendszer által kezelt adatok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzéséhez.

Rögzíti mindazokat az informatikai biztonság területén alkalmazandó védelmi alapelveket, amelyek a teljeskörűségre, a zártságra, a kockázatarányosságra, a védelem szintjének folytonos biztosítására, a szabályozás zárt folyamatára és az informatikai rendszer teljes életciklusára vonatkoznak.

Biztosítja, hogy a rendszerek védelme a jogszabályi előírásoknak eleget tegyen, valamint a védelem hiányából eredő kockázatokkal legyen arányos.

5.2. Az információbiztonság koordinálása

Az információbiztonsági tevékenységek koordinálására a Társaság ügyvezető igazgatója Információ Biztonsági Felelőst nevezett ki.
Hatásköre alá tartoznak az informatikai biztonsági eljárások betartásának ellenőrzése, továbbá az eljárásokkal kapcsolatos folyamatok felügyelete, az IBSZ kidolgozásának, rendszeres aktualizálásának és a benne foglaltak érvényre juttatásának elsődleges felelőse. Jelentési kötelezettséggel tartozik az ügyvezető igazgató felé, aki elbírálja a felé intézett igényeket és azokat jóváhagyja, illetve elutasítja.

5.3. Az információbiztonsági feladatok, felelősségi körök és hatáskörök

A jelen szabályzatban rögzített, az információbiztonsággal kapcsolatban rögzített feladatok végrehajtásában érintettek feladata, felelőssége és hatásköre:

Ügyvezető igazgató feladatai
– az IBSZ működtetéséhez szükséges személyi és tárgyi feltételek megteremtése,
– az IBSZ jóváhagyása és hatálybaléptetése,
– az IBSZ rendszeres felülvizsgálatát követő jelentés értékelése, jóváhagyása,
– az IBSZ működésével kapcsolatos intézkedések elrendelése
– az IBSZ működésével kapcsolatos külső, független ellenőrzés elrendelése
Ügyvezető igazgató felelőssége kiterjed
– a tevékenység működtetéséhez szükséges személyi és tárgyi feltételek megteremtésére,
– a szabályzat hatálybaléptetésért, felülvizsgálatát követő jelentés jóváhagyására,
– a szabályzat működésével kapcsolatos intézkedések elrendelésére,
Ügyvezető igazgató hatáskörébe tartozik
– a szükséges személyi és tárgyi feltételek megteremtése,
– a szabályzat jóváhagyása és hatálybaléptetése,
– a szabályzat rendszeres felülvizsgálatát követő jelentések értékelése, jóváhagyása,
– a szabályzat működésével kapcsolatos intézkedések elrendelése

Információbiztonsági felelős feladatai
– az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
– javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására,
– meghatározza a védett adatok körét,
– ellátja az adatkezelés és adatfeldolgozás felügyeletét,
– ellenőrzi a védelmi előírások betartását,
– az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
– az adatvédelmi feladatok ismertetése,
– ellenőri tevékenységét adminisztrálja,
– ellenőrzi a szoftverek használatának jogszerűségét

Információbiztonsági felelőssége kiterjed

– a szabályzat kezelésére, naprakészen tartására, módosítások átvezetésére,
– a védett adatok körének meghatározására,
– a védelmi előírások betartásának ellenőrzésére,
– az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítására,
– az adatvédelmi feladatok ismertetésére,
– a szoftverek használata jogszerűségének ellenőrzésére

Információbiztonsági felelős hatáskörébe tartozik

– javaslat készítése a rendszer szűk keresztmetszeteinek felszámolására,
– a védett adatok körének meghatározása
– az adatkezelés és adatfeldolgozás felügyelete,
– a védelmi előírások betartása,
– az adatvédelmi feladatok ismertetése,

A rendszergazda feladatai

– a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli,
– felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
– gondoskodik a rendszer kritikus részeinek újra indíthatóságáról,
– gondoskodik az újra indításához szükséges paraméterek reprodukálhatóságáról,
– feladata a védelmi eszközök működésének folyamatos ellenőrzése,
– felelős a vállalkozás informatikai rendszer hardver eszközeinek karbantartásáért,
– nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
– gondoskodik a folyamatos vírusvédelemről
– a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
– figyelemmel kíséri a rendszer működése szempontjából a lényeges paraméterek alakulását,
– évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását,
– rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
– előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat részét.

A rendszergazda felelőssége kiterjed

– felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
– a rendszer kritikus részeinek újra indíthatóságára,
– a védelmi eszközök működésének folyamatos ellenőrzésére,
– felelős a vállalkozás informatikai rendszer hardver eszközeinek karbantartásáért,
– nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
– a folyamatos vírusvédelemre
– a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
– a rendszer működése szempontjából a lényeges paraméterek alakulására,

A rendszergazda hatáskörébe tartozik

– a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli,
– az informatikai rendszerek üzembiztonságának, szerverek adatairól biztonsági másolatok készítésének és karbantartásának végrehajtása,
– a védelmi eszközök működésének folyamatos ellenőrzése,

– a beszerzett, illetve üzemeltetett hardver és szoftver eszközök nyilvántartására,
– a folyamatos vírusvédelemre
– a vírusfertőzés gyanúja esetén felelős a fertőzött rendszerek vírusmentesítéséért,
– évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását,
– a védelmi eszközökkel való ellátottság rendszeres ellenőrzésére,
– bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét,
– a szabályzat előírásai ellen vétőkkel szemben felelősségre vonást kezdeményezhet,
– valamennyi iratba, ami informatikai feldolgozásokkal kapcsolatos betekinthet,
– javasolhat védelmi eszközök beszerzését, véleményezheti az informatikai beruházásokat

5.4 Titoktartási megállapodások

A Társaság minden munkatársa és szerződéses partnere csak előzetes titoktartási nyilatkozat megtételét követően férhet hozzá a munkakörének, megbízásának megfelelő jogosultságokkal bíró informatikai rendszereihez és az ahhoz kapcsolódó adatokhoz.

5.5. Az információbiztonság független átvizsgálása

A rendszeres információbiztonsági felülvizsgálatok célja a kialakított védelmi rendszer működési hatékonyságának mérése az egyenszilárdságot veszélyeztető hiányosságok és sebezhetőségek feltárása, a szükséges helyesbítő védelmi intézkedések kidolgozása, és előterjesztések készítése az ügyvezető igazgató részére.

Az ügyvezető igazgató feladata az információbiztonsági kockázatok független szakértővel történő felülvizsgálata legalább kétévente.
A felülvizsgálatnak az alábbi területekre kell kiterjednie:

- adminisztratív biztonság
- személyi biztonság
- fizikai és környezet biztonság
- hozzáférés védelem
- informatikai rendszer biztonság
- fejlesztés biztonság
- üzemeltetés biztonság

6. Külső ügyfelek és partnerek

6.1. A külső partnerekkel összefüggő informatikai biztonsági kockázatok azonosítása

Társaságunk külső partnere lehet:

- kiszervezett tevékenységet ellátó, adatfeldolgozó
- egyéb szerződéses partner

A kiszervezett tevékenységet végzővel szemben támasztott információbiztonsági követelmények nem lehetnek enyhébbek, mint a Társasággal szemben támasztott jogszabályi követelmények.

A kiszervezési szerződésnek tartalmaznia kell a törvényben megfogalmazott általános elemeket. A szerződés megkötését párhuzamosan kísérnie kell egy intézkedési tervnek, amelyben az

adatkezelés, az adatfeldolgozás vagy az adattárolás folyamatosságának biztosításához szükséges személyi, tárgyi és biztonsági követelmények érvényesülésére tett feladatokat kell megjeleníteni az üzletmenet folytonosságának biztosítása érdekében.

6.2. Az információbiztonság az ügyfelekkel való foglalkozás során

Társaságunk ügyfelei számára többféle módon biztosítja a kapcsolattartás lehetőségét (személyes, papír alapú levelezés, elektronikus levelezés, internet stb.).
Az ügyfél adatainak megfelelő kezelését minden esetben biztosítani kell. Az internet felöl érkező, ügyfelek által küldött adatok megfelelő védelmét biztosítani kell, amelyeket illetéktelen személyektől elrejtve (titkosított csatornán) kell szállítani.

6.3. A biztonság kérdésének kezelése harmadik féllel kötött megállapodásokban

Társaságunk szerződéseiben rögzíteni kell azokat a feltételeket, amelyek alapján a szerződő partner magára nézve kötelezőnek ismeri el a Társaságunkra vonatkozó jogszabályi követelmény-rendszert, továbbá a jelen szabályzatban előírtakat.

7. Kapcsolódó szabályozások

Az IBSZ előírásai összhangban vannak:
- Leltározási és értékelési szabályzattal,
- Számviteli politikával,
- Más irányítási rendszerekkel (pl. minőség és környezetirányítás)

8. 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.

8.1. A védelem tárgya

A védelmi intézkedések kiterjednek:
- az alkalmazott hardver eszközökre és azok működési biztonságára,
- az informatikai eszközök üzemeltetéséhez szükséges okmányokra és 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,

8.2. A védelem eszközei

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.

9. Az információ biztonság emberi erőforrásai

9.1. Feladat-és felelősség, alkalmazási feltételek

A Társaság az alkalmazottakkal, a kiszervezet tevékenységet ellátó felekkel, egyéb szerződéses partnerekkel és harmadik felekkel szemben támasztott követelményei a következők:

- szakmai képesítések és az azokat igazoló bizonyítványok megléte,
- indokolt esetben ellenőrizhető referenciák.

Munkavállaló alkalmazását megelőzően javasolt a jelentkező referenciáit ellenőrizni, szerződéses partner esetében rögzíteni kell a partner munkatársaival szemben támasztott követelményeket.
A munkáltatói jogokat gyakorló, vagy nevében eljáró kötelessége, hogy a Társaságnál felvételre kerülő személy részére a munkaszerződésben, a kinevezési okiratban, vagy a munkaköri leírásban rögzítse az információbiztonsági kötelezettségeket, megszegésük esetére pedig hívja fel a figyelmet a fegyelmi, kártérítési és büntetőjogi következményekre.
A Társaság minden munkatársa, szerződéses partnere csak előzetes titoktartási nyilatkozat megtételét követően férhet hozzá a munkakörének, megbízásának megfelelő jogosultságokkal a Társaság informatikai rendszereihez és adataihoz. A munkáltatói jogokat gyakorló, vagy nevében eljáró köteles az információbiztonsággal kapcsolatos szerepeket ellátó minden egyes munkavállaló munkaköri leírásában rögzíteni az információbiztonsággal kapcsolatos kötelezettségeket.

9.2. Oktatásokkal és képzésekkel kapcsolatos alapelvek

A Társaság működése szempontjából kiemelt fontosságú a munkatársak szakmai képességének színvonala, ebből következően kiemelt cél a Társaság működtetéséhez szükséges képességek fenntartása és bővítése, a Társaság alapvető érdeke az emberi erőforrások minősége, azaz munkatársainak tudása, elkötelezettsége, hatékonysága.
Munkatársak új felvételekor kiemelt szempont a lehető legmegfelelőbb és legnagyobb szaktudással és szakmai tapasztalattal rendelkező személyek felvétele. A meglévő szakember gárda szakmai tudásának fenntartására és tudásszintjének emelése a vezetés kiemelt szempontja, és ezért a vezetés elkötelezett a rendszeres szakmai oktatás biztosításában, következésképpen az éves költségek tervezésekor gondoskodik a képzésre és oktatásra szánt erőforrások rendelkezésre állásáról. Minden évben oktatási tervet kell készíteni, gondoskodni kell annak megvalósulásáról.
Minden új munkatárs belépésekor részletes tájékoztatást kap a belső működésről, a szervezet felépítéséről, a belső szabályozásokról és az információ biztonsági szabályzásokban leírtakról,

valamint a munkavállalói jogokról és kötelezettségről. Minden új belépő oktatásban részesül az alábbi témakörökben, úgymint:

- tűzvédelem,
- munkavédelem,
- irányítási rendszerek,
- informatikai rendszerek használata, jogok jogosultságok,
- nyomtatás, másolás.

Minden olyan beosztást, amelyhez valamilyen ismeretanyag elsajátítására van szükség, és ahol ennek az ismeretanyagnak a hiánya problémát okozna a tevékenység, szolgáltatás minőségébe vagy a biztonsági rendszer működésében, ott a képzést az érintett terület vezetője folyamatosan és igény szerint kell, hogy megoldja.
A Társaság üzleti tevékenységének támogatásához használt üzlet/alkalmazói rendszerek ismerete az egyes munkaörök betöltése esetén nem alapfeltétel, de a próbaidő időtartama alatt a szakterületi vezetőnek gondoskodnia kell a megfelelő ismeretanyag elsajátításához szükséges feltételek biztosítására, és a munkaszerződés véglegesítésének feltétele a munkavállaló által használt üzleti/alkalmazói rendszerek ismerete.

9.3. Az információ biztonság tudatosítása, oktatás és képzés

A Társaság az informatikai rendszer valamennyi felhasználóját információbiztonsági oktatásban részesíti, a Társaság vezetése gondoskodik az oktatások lefolytatásának feltételeiről.
Az információbiztonsági felelős kötelessége a felhasználói biztonság tudatosság építő oktatást megtervezni és megszervezni, a biztonsági oktatások megtörténtét dokumentálni köteles. Az oktatáson való részvételt a felhasználó aláírásával az oktatásról készült jegyzőkönyvön hitelesíti. A jegyzőkönyvnek tartalmaznia kell a következő mondatot: „Alulírott, felelősségem teljes tudatában kijelentem, hogy az információbiztonsági oktatáson részt vettem, az azon elhangzottakat megértettem tudomásul vettem”
Az információbiztonsággal kapcsolatos kockázatot csökkenti, ha a Társaság munkavállalói tisztában vannak a munkafolyamataikat támogató informatikai rendszerekkel, következésképpen a dolgozók kötelesek a hatályos IBSZ-t megismerni, az abban foglaltakat betartani és betartatni, valamint az oktatáson rész venni. Oktatást kell tartani az érintett munkavállalóknak hardver- és szoftver eszközök, valamint a használatukat szabályozó eljárások jelentős változásakor. A szükséges oktatásokat elektronikus rendszerben is el lehet végezni, ebben az esetben az elektronikus oktatási rendszerben rögzített részvétel a jelenléti ív aláírásának felel meg.

9.4. Fegyelmi eljárás, alkalmazható szankciók

Az információbiztonsági felelős a felhasználó súlyos mulasztását, az információ gondatlan veszélyeztetését köteles írásba foglalni és jelentést készíteni az ügyvezető igazgató számára.

A jelentésnek tartalmaznia kell:

- a biztonság sértés időpontját,
- a vétkes nevét és beosztását,
- a tevékenység által közvetlenül okozott kárt,
- a tevékenységgel közvetve okozott kár mértékét,
- a javasolt intézkedéseket.

A biztonsági esemény kivizsgálása során az eseménnyel kapcsolatban érintett munkatársaknak együttműködési kötelezettségük van, azok nem akadályozhatják a vizsgálat lefolytatását.

10. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére a vezetők és a rendszergazdák oktatás formájában biztosítják. Erről nyilvántartást kötelesek vezetni.
Az Informatikai Biztonsági Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

10.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában - valamint a vállalkozásnál - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. Az IBSZ folyamatos karbantartása az informatikai vezető feladata.

11. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:
– közlésre szánt, bárki által megismerhető adatok,
– minősített, titkos adatok.
Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik.
Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot. A kijelölt dolgozók előtt az adatvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.
Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.
Az információhoz való hozzáférést lehetőség szerint a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység – adatbázisokhoz való hozzáférés, a fájlba vagy mágneslemezre történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető.
A naplófájlokat rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét a vállalkozás vezetőjének jelenteni kell.
A naplófájlok áttekintéséért, értékeléséért az informatikai vezető és a rendszergazdák a felelősek.
Az adatok védelmét, a feldolgozás – az adattovábbítás, a tárolás - során az operációs rendszerben és a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver adatvédelem).

11.1 Osztályozási elvek

A Társaság teljes feldolgozási, végrehajtási munkafolyamataira biztosítani kell a három alapfenyegetettség bekövetkezési valószínűségének csökkentését, vagyis az adatok, információk és az azokat kezelő rendszerek

- bizalmasságát,
- sértetlenségét,
- rendelkezésre állását

Minden számítógépes rendszernél alapvető szempont az adatok biztonsága. A bekövetkezendő adat-és információ vesztésekből adódó károk minimalizálásának leghatékonyabb eszköze a helyesen megtervezett és következetesen végrehajtott adatkezelési, mentési és helyreállítási rendszer, valamint a hatályban lévő biztonsági szabályozások betartásának rendszeres ellenőrzése. A vonatkozó törvényi előírások szerint mindenkor rendelkezésre kell állnia az informatikai rendszer elemeinek a társaság által meghatározott biztonsági osztályokba sorolási rendszerének. Az erre vonatkozó felügyeleti ajánlás alapján a Társaság kialakította az informatikai eszközök rendelkezésre állási követelményi szerinti biztonsági osztályba sorolási rendszerét, valamint adatainak bizalmasság szerinti biztonsági osztályokba sorolási rendszerét.

11.2 Informatikai eszközök biztonsági besorolása

A Társaság egyes informatikai eszközei valamint a rajtuk futtatott alkalmazásai különböző jelentőséggel bírnak a Társaság biztonságos működésének szempontjából. A tevékenységek biztonsági kockázatának figyelembevételével a következő szinteket kell kialakítani.

Kiemelt (High):
Ebbe a szintbe tartoznak alapfunkciók működtetése és biztonsága szempontjából legfontosabb adatok, alkalmazások, rendszerszoftverek, eszközök, berendezések és a környezeti infrastruktúra idetartozó elemei. közös jellemzőjük, hogy még rövid időre történő működéskiesésük sem viselhető el a rendszer számára, illetve hiányuk és rajtuk tárolt adatok bizalmasságának, sértetlenségének, hitelességének elvesztése olyan biztonsági problémát okoz, amelynek kockázata nem vállalható. Ide tartoznak azok a szerverek, alkalmazások és adatbázisok, amelyek a Társaság létfontosságú feladatait, üzletvitelét hivatottak szolgálni, valamint a hálózati eszközpark azon aktív elemei, amelyek nélkül a hálózatnak olyan szegmensei válnának kommunikáció képtelenné, amelyek a működés szempontjából létfontosságúak illetve azok a speciális informatikai eszközök, amelyek a Társaság, mint szervezet biztonságos működését és védelmét hívatottak szavatolni.

Fokozott (Medium):
Az ide tartozó informatikai eszközök, alkalmazások működésének viszonylag rövid ideig (24-48 óra) tartó kiesése elviselhető terheket ró a Társaságra, mind a tevékenység ellátása, mind a biztonság szempontjából. Enne a szintbe tartoznak azok a szerverek, amelyek működésének kiesése ideiglenesen elviselhető kockázatot jelent valamint a hálózati eszközpark azon aktív elemei, amelyek nem sorolhatók a kiemelt szintbe, illetve azok a személyi számítógépek, amelyek kiemelt fontosságú adatokat tartalmaznak, vagy kiemelt fontosságú hálózati kapcsolattal rendelkeznek.

Alap (Low):
A harmadik szintbe tartozó informatikai eszközök, alkalmazások még hosszabb ideig (1 hét) tartó megszűnése sem befolyásolja jelentős mértékben a társaság működését.
Ide tartoznak az egyéb, a kiemelt és fokozott szintbe be nem sorolt informatikai eszközök, amelyeken nem tárolnak kiemelt jelentőségű adatokat, illetve amelyek működésének kiesése a feladat ellátás szempontjából nem meghatározó valamint azok a munkaállomások és hordozható számítógépek.

Az informatikai vagyon minden elemét be kell sorolni valamelyik szintre, annak megfelelően, hogy működésének megszűnése hogyan hat a Társaság egészének funkcionalitására.
Az adatgazdák feladata adatvagyon besorolása, ezt követően az informatikai alkalmazások és eszközök besorolása.
A három kategóriába tartozó eszközökre csoportonként és eszköz típusonként más-más biztonsági előírások vonatkoznak.

11.3 Az adatok és információk osztályozása

A Társaságnál keletkező és ott kezelt adatokat, információkat biztonsági osztályokba kell sorolni az alábbi szempontok figyelembevételével:

- az adatok nyilvánosságra kerülésének kockázata és lehetséges következményei,
- vonatkozó törvényi és szabályozói rendelkezések (a jogszabály által előírt védelmi szint az osztályozással nem csökkenhet),
- az adatok bizalmasságára és pontosságára/helyességére vonatkozó követelmények.

A Társaság módszertanával összhangban az alábbi négy osztály valamelyikébe kell sorolni az adatokat.

- Nyilvános: olyan adatok és információk, amelyek a Társaságon belül és kívül szabadon terjeszthetők.
- Belső használatra: olyan adatok és információk, amelyek a Társaságon belül szabadon terjeszthetők. Alapértelmezés szerint ebbe a csoportba tartozik minden, másképpen nem osztályozott adat, továbbá az olyan harmadik félhez tartozó adatok, melyek nem képezik titoktartási megállapodás tárgyát.
- Bizalmas: olyan adatok és információk, melyek nyilvánosságra kerülése anyagi, vagy jogi kárt okozhat a Társaságnak. Bizalmas adatokhoz csak azok férhetnek hozzá, akiknek a munkájához szükséges a hozzáférés és/vagy rendszergazda engedélyezte számukra a hozzáférést. Alapértelmezés szerint ebbe a kőrbe tartoznak a személyes adatok, üzleti titkok és a banktitkok.
- Szigorúan bizalmas: olyan adatok és információk, amelyek nyilvánosságra kerülése jelentős anyagi vagy jogi kárt okozhat a Társaságnak. Az ebbe az osztályba sorolt adatokhoz csak az rendszergazda által erre külön felhatalmazottak férhetnek hozzá. Az adatok kezelése ebben a kategóriában fokozott körültekintést igényel.

Az adatkör végleges biztonsági osztályát az alapkövetelmények általi besorolásból a legmagasabb minősítésű adja meg.

11.4 Az adatkezelés szabályai osztályok szerint

Miután az adatok osztályozása megtörtént, azokat a dokumentum minden oldalán jelezni kell. Ezen túlmenően az adatokat a következő szabályok szerint kell kezelni, figyelemmel a hatályos jogszabályi előírásokra is:

Nyilvános adatok:

- elektronikus formában
  - szabadon tárolhatók
  - szabadon másolhatók
  - szabadon megoszthatók
  - szabadon törölhetők, ha törvény, szabályozás másképp nem rendeli

- papír formában
  - szabadon tárolhatók
  - szabadon másolhatók
  - szabadon megoszthatók
  - szabadon selejtezhetők, ha törvény, szabályozás másképp nem rendeli

Belső használatra rendelt adatok:

- elektronikus formában
  - olyan formában tárolhatók, hogy csak a terjesztési körön belül lévők férhetnek hozzá
  - terjesztési körön belül másolhatók
  - terjesztési körön belül megoszthatók
  - szabadon törölhetők, ha törvény, szabályozás másképp nem rendeli
- papír formában
  - olyan formában tárolhatók, hogy csak a terjesztési körön belül lévők férhetnek hozzá
  - terjesztési körön belül másolhatók
  - terjesztési körön belül megoszthatók
  - a selejtezés során az adatokat meg kell semmisíteni

Bizalmas adatok:

- elektronikus formában
  - olyan formában tárolhatók, hogy csak az erre felhatalmazott felhasználók férhetnek hozzá
  - a hozzájuk kapcsolódó feladatok végrehajtásához szükséges mértékben másolhatók
  - harmadik féllel történő megosztásukkor gondoskodni kell az adatok védelméről
  - törlésük során helyreállíthatatlan formában meg kell semmisíteni az adatokat
- papír formában
  - csak zárt helyiségben vagy helyen tárolhatók
  - a hozzájuk kapcsolódó feladatok végrehajtásához szükséges mértékben másolhatók
  - csak zárt, nem átlátszó borítékban továbbíthatók
  - a selejtezés során az adatokat meg kell semmisíteni

12. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

12.1. Környezeti infrastruktúra okozta ártalmak

- elemi csapás:
- földrengés,
- árvíz,
- tűz,

- villámcsapás, stb.
- környezeti kár:
- légszennyezettség,
- nagy teljesítményű elektromágneses térerő,
- elektrosztatikus feltöltődés,
- a levegő nedvességtartalmának felszökése vagy leesése,
- piszkolódás (pl. por).
- közüzemi szolgáltatásba bekövetkező zavarok:
- feszültség-kimaradás,
- feszültségingadozás,
- elektromos zárlat,
- csőtörés.

12.2. 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.

A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

13. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

13.1. Tervezés és előkészítés során előforduló veszélyforrások

– a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
– hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

13.2. A rendszerek megvalósítása során előforduló veszélyforrások

– hibás adatállomány működése,
– helytelen adatkezelés,
– programtesztelés elhagyása.

13.3. A működés és fejlesztés során előforduló veszélyforrások

– emberi gondatlanság,
– szervezetlenség,
– képzetlenség,
– szándékosan elkövetett illetéktelen beavatkozás,
– illetéktelen hozzáférés,
– üzemeltetési dokumentáció hiánya.

14. Az informatikai eszközök környezetének védelme

14.1. Vagyonvédelmi előírások

– a géptermek külső és belső helyiségeit biztonsági zárakkal kell felszerelni,
– a gépterembe való be- és kilépés rendjét szabályozni kell,
– a gépterembe, szerverterembe történő illetéktelen behatolás tényét a vállalkozás vezetőjének azonnal jelenteni kell,
– az informatikai eszközöket csak a vállalkozás arra felhatalmazott alkalmazottai használhatják,
– az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

14.2. Adathordozók

– könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
– az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni,
– a használni kívánt adathordozót (floppy, CD) a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni,
– a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,
– adathordozót másnak átadni csak engedéllyel szabad,
– a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

14.3. Tűzvédelem

A gépterem illetve kiszolgáló helyiség a „D” tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.
A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.

A vállalkozás géptermeibe, szerverszobáiba minimum 1-1 db tűzoltó készüléket kell elhelyezni.
A vállalkozás géptermeiben, szerverszobáiban elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.

A nagy fontosságú, pl. törzsadat-állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni. (Ezen adatállományok kijelölése az informatikai vezető feladata.)

15. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

15.1. 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 anyagot,
– biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
– archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

15.2. 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.

15.3. Az informatikai feldolgozás folyamatának védelme

15.3.1. Az adatrögzítés védelme

– adatbevitel hibátlan műszaki állapotú berendezésen történjen,
– tesztelt adathordozóra lehet adatállományt rögzíteni,
– a bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
– az adatrögzítő szoftver védelme. Lehetőség szerint 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 rendszergazda jelszavát az informatikai vezető kezeli.

Az adatrögzítés folyamatához kapcsolódó dokumentációk:

- adatrögzítési utasítások,
- ellenőrző rögzítési utasítások,
- tesztelő és törlő programok kezelési utasításai,
- megőrzési utasítások,
- gépkezelési leírások.

15.3.2. Az adathordozók nyilvántartása

Az adathordozókról az egységeknek nyilvántartást kell vezetni. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval (sorszámmal) kell ellátni.

15.3.3. Adathordozók tárolása

Az adathordozók tárolására műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

15.3.5. Az adathordozók megőrzése

Az adathordozók megőrzési idejét a törvényekben meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani

15.3.6. Selejtezés, sokszorosítás, másolás

A selejtezést a vállalkozás selejtezésének szabályzata és jelen szabályozás figyelembevételéve alapján kell lefolytatni.
Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni. Biztonsági illetve archív adatállomány előállítása másolásnak számít.

15.3.8. Leltározás

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

15.3.9. 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 munkatársak (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. A mentésért az informatikai vezető illetve a rendszergazdák a felelősek.

15.4. Szoftver védelem

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

15.4.1. Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem
A kezelés 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.

Programok megőrzése, nyilvántartása

A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni. A számvitelről szóló többször módosított 2000. évi C. törvény értelmében a vállalkozásoknak 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.
A programok nyilvántartásáért és működőképes állapotban való tartásáért a vezetők a felelősek.

16. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

16.1. Központi gépek

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

16.2. Munkaállomások

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal. Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell. Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket. A vállalkozás informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.
A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.
Az informatikai eszközt és tartozékait helyéről elvinni csak az eszköz leltárfelelőse tudtával és engedélyével szabad.

17. Események, gyengeségek kiértékelése, incidensek kezelése

A biztonsági események kiértékelése, incidensek kezelése elsődlegesen az információbiztonsági felelős feladata, mely tevékenységbe a rendszergazdát is be kell vonnia. A biztonsági események kezelésekor az információbiztonsági felelősnek, mint szakértőnek be kell tartania a jelen IBSZ előírásait. Ugyancsak ezen szabályzat előírása szerint kötelessége a bejelentés dokumentálása, valamint a kiértékelés elvégzése és átadása az ügyvezető igazgató részére. Az ismerté vált gyengeség, sebezhetőség kezelését a lehető legrövidebb időn belül, de legkésőbb az ismerté válást követő kettő munkanapon belül meg kell kezdeni. Az incidensek kezelését a bejelentést, ismerté válást követően haladéktalanul meg kell kezdeni.
A biztonsági esemény kiértékelése az információbiztonsági felelős 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, vagy pontatlanságával,
  - vagy biztonság sértéssel kapcsolatos.
- meg kell határoznia a biztonsági esemény okát
- meg kell határoznia a javító intézkedést az adatok felhasználásával
- értesíteni kell az ügyvezető igazgatót a foganatosított intézkedésekről
- ha az intézkedés hasonló biztonsági esemény kizárását célozza, akkor jeleznie kell az ügyvezető igazgató felé a hiányosságokat
- meg kell határoznia a biztonsági esemény elhárításának végső határidejét.

Az információbiztonsági felelős köteles negyedévente

- a beérkező biztonsági eseményekről statisztikát készíteni
- a biztonsági eseményekből közvetlenül származtatott kárt megbecsülni
- a jellemző információbiztonsági sérüléseket azonosítani, dokumentálni
- a felülvizsgálatokkal összhangban, védelmi intézkedéseket előterjeszteni.