Kajári és Fia Csomagolóanyag Gyártó Korlátolt Felelősségű Társaság

Informatikai Üzemeltetési Szabályzat

A szabályzatot kidolgozta: Lajos János
mérnök tanácsadó

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

A szabályzat 19 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 Üzemeltetési Szabályzat célja

A 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 a közelmúltban alakította ki és vezette be Informatikai Biztonsági Szabályzatát.

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.
A fentieket követve kidolgoztuk és bevezettük a működtetés feltételeit, az üzemeltetés szabályait rögzítő Információ Üzemeltetési Szabályzat (továbbiakban: IÜSZ) előírásait.
Az IÜSZ alapvető célja, hogy a Társaságunknál az elérhető informatikai szolgáltatások használata, alkalmazása során az informatikai és infokommunikációs eszközök előírásoknak megfelelő és biztonságos használatát elősegítse, az adott üzemeltetésre vonatkozóan útmutatást nyújtson, a szükséges felhasználói-, üzemeltetői-, vezetői teendők és felelősségi körök meghatározásával biztosítsa az informatikai rendszerek folyamatos és rendeltetésszerű működését.
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 IÜSZ célja továbbá:

- az informatikai eszközök helyes használatával 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 IÜSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

2. Az Informatikai Üzemeltetési Szabályzat hatálya

2.1. Személyi hatálya

A szabályzat szervezeti hatálya kiterjed:

- a Társaság minden munkatársára,
- a Társasággal szerződéses viszonyban tevékenykedő partnerekre,
- a Társaság tulajdonában lévő informatikai eszközök felhasználóira

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

Társaságunk tekintetében az Informatikai Üzemeltetési Szabályzat hatálya alá tartoznak, következésképpen

- az informatikai infrastruktúra eszközei és a hozzátartozó építmények, helyisége,
- számítógéptermek és a hozzájuk kapcsolódó helyiségek,
- a Társaságnál munkavégzés céljából saját tulajdonú informatikai eszközök

az informatikai üzemeltetési szabályzatban meghatározott feltételek teljesítése esetén használhatók.
Az IÜSZ tárgyi hatálya kiterjed a Társasági birtokában és tulajdonában lévő összes informatikai vagyontárgyra, szerződés alapján üzembehelyezett, nem a Társasági tulajdon részét képező eszközökre (vezérlő eszközök, szerverek, munkaállomások stb.), illetve munkatársak saját tulajdonában lévő eszközeire, amelyek a Társaság informatikai rendszerével kapcsolatba kerülnek, ezen belül eszköztípusonként:

- a számítógép-hálózatok aktív és passzív elemeire,
- szerverekre és hálózati szolgáltatást nyújtó berendezésekre,
- valamennyi munkaállomásra, nyomtatóra,
- perifériákra és tartozékaira,
- hordozható számítógépekre,
- adathordozókra,
- valamennyi szoftverre.

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 üzemeltetés 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.

Funkcionalitás: az informatikai rendszer megfelelő tervezésének és üzemeltetésének köszönhetően az adat tartalmi és formai használhatóságának biztosítása.

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.

Illegális szoftverhasználat: az illegális szoftverhasználat azt jelenti, hogy valaki egy számítógépes programot jogosulatlanul másol le és használ, ezzel megsértve a szerzői jogi törvényt, valamint a szerzőnek a szoftver licenc szerződésben leírt feltételeit.

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.

Informatikai biztonság: az informatikai biztonság az az állapot, amikor az informatikai rendszer által kezelt adatok védelme – bizalmasság, hitelesség, sértetlenség, rendelkezésre állás és funkcionalitás szempontjából – zárt, teljes körű, a kockázatokkal arányos és folyamatos.

Informatikai biztonságpolitika: a Társaság minden munkatársa és az informatikai rendszer minden felhasználója számára meghatározza, hogy melyek az informatikai rendszerek által kezelt adatok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásnak és funkcionalitásának megőrzésével kapcsolatos biztonsági elvek, szabályok és előírások.

Információvédelem: az informatikai rendszerek által kezelt adatok által hordozott információk védelme a bizalmasság, a hitelesség és a sértetlenség sérülése, elvesztése ellen, mint az információvédelem az informatikai biztonság egyik alapterülete.

Informatikai szolgáltatás: a Társaság által használt, vagyis információs technológiai/informatikai rendszerrel nyújtott szolgáltatás.

Jogosulatlan másolás: a szoftver licenc szerződés, amennyiben eltérően nem rendelkezik, a vevőnek csak egyetlen „biztonsági" másolat készítését engedélyezi, arra az esetre, ha az eredeti szoftver lemeze megsérülne, vagy megsemmisülne, az eredetiszoftver bármely további másolata jogosulatlan másolásnak minősül.

Kockázat: a szoftver licenc szerződés, amennyiben eltérően nem rendelkezik, a vevőnek csak egyetlen „biztonsági" másolat készítését engedélyezi, arra az esetre, ha az eredeti szoftver lemeze megsérülne, vagy megsemmisülne, az eredetiszoftver bármely további másolata jogosulatlan másolásnak minősül.

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.

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.

Nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik.

Probléma: a probléma egy állapot, mely gyakran több hasonló tünetet produkáló incidens alapján ismerhető fel, a probléma azonosítható lehet egyetlen jelentős incidens alapján is, mely valamilyen hibára utal, melynek oka nem ismert, de hatása jelentős.

Szellemi tulajdon: a törvény szerint az eredeti számítógépes program az azt létrehozó személy vagy vállalat szellemi tulajdona.

Szoftver: a számítógépes programalkotás és a hozzá tartozó dokumentáció akár forráskódban, akár tárgykódban vagy bármilyen más formában rögzített minden fajtája.

Szoftver licenc szerződés: egy adott szoftver esetében a licenc szerződés határozza meg a szerzői jog tulajdonosa által megengedett szoftverhasználat feltételeit, amelynek során utalás történik a szoftver dokumentációjában, vagy a program indításakor megjelenő képernyőn is.

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. A Társaság informatikai működése

5.1. Az informatikai rendszer működtetésének végrehajtói

Az informatikai rendszer működésében valamennyi az IBSZ által meghatározott vezető és munkatárs a szabályzat előírásai szerinti mértékben, felelősséggel és hatáskörrel működteti az informatikai rendszert.

5.2. Szolgáltatási időszak, elérhetőségek

A Társaság minden munkatársa és szerződéses partnere az informatikai szolgáltatás egész évben folyamatos (7x24 óra) működésben biztosítandók.

5.3. Informatikai szolgáltatások

A Társaság felhasználói számára folyamatosan biztosítja (munkaidőben, illetve munkaidőn kívül készenléti ügyelettel támogatja) az informatikai rendszerek működését és a következő alapszolgáltatásokat

- vezetékes és WIFI hálózatok, stb.
- levelezőrendszer működés, integrált metodika elérés rendszer
- internet és intranet elérés, web szerver funkciók, fájlszerver-funkciók
- vírusvédelem, automatikus vírusadatbázis-frissítés
- készenlét, sürgős hibák elhárítása
- központi tűzfal konfigurálási és DNS szolgáltatások
- munkaállomások és perifériák installálása
- felhasználók közötti gépátadások bonyolítása, követése
- üzem közben észlelt hardver, szoftverhibák elhárítása
- adat visszatöltés a munkaállomásra
- jogosultsági rendszer menedzselése

- a hálózati forgalmi adatok elemzése, közlése
- infrastuktúra fejlesztésében történő közreműködés
- eseti szolgáltatások

5.4. Tervezett rendszerkarbantartás, leállás

A tervezett rendszerkarbantartásokról és leállásokról, áramszünetről legalább kettő munkanappal korábban írásban értesíteni kell a felhasználói kört.

5.5. Informatikai rendszerek

Az egyes informatikai rendszerek működésének és üzemeltetésének rendjét a konkrét rendszerek egységes elvek és tartalom szerint kötelezően elkészített, üzemeltetési dokumentumai tartalmazzák.

6. Szolgáltatás támogatás

6.1. Felhasználói hozzáférés, támogatás

A Társaság információbiztonsági felelőse biztosítja a kapcsolatot az informatikai szolgáltatások és a felhasználók között.
Az operációs rendszerekhez való hozzáférést biztonságos bejelentkezési eljárásokkal kell ellenőrzés alatt tartani, a felhasználói bejelentkezésnek felhasználónévvel és egyedi jelszóval kell történnie.

A jelszavak használatánál és kezelésénél az alábbi szabályokat minden esetben be kell tartani, úgymint

- a jelszavakat minden esetben titokban kell tartani
- tilos közös jelszavakat használni
- a jelszót nem szabad leírni és elérhető helyen tárolni
- a jelszót tilos számítógépes rendszeren titkosítás nélkül tárolni
- a jelszót tilos telefonon vagy e-mail-ben továbbítani, más személynek átadni, más jelszavával belépni
- ne utaljunk a jelszó tartalmára
- tilos a programok jelszó megjegyző funkcióját használni, a jelszót kérdőívekbe, űrlapokba írni
- ha a jelszó kompromittálódott, vagy erre utaló jeleket lehet észlelni, azonnal meg kell változtatni és értesíteni az információbiztonsági felelőst
- a jelszavakat rendszeresen és időszakosan cserélni kell
- az induló jelszót az első bejelentkezéskor meg kell változtatni
- sikertelen próbálkozás után a felhasználói fiók 15 percre zárolandó

Minden felhasználó személyesen felel a saját azonosítójával végrehajtott tevékenységekért, a jelszót harmadik személynek, munkatársnak nem adhatja át, a jelszóval történő visszaélés esetén egyetemleges felelősséget válla a visszaélő személlyel.
A jelszóvédelemnek biztosítani kell

a felhasználók számára, hogy a jelszavakat megváltoztassák

a jelszavak bonyolultságával kapcsolatos követelmények kikényszerítését
az azonosítás protokollja a lehallgatás, ismétléses támadás elleni védelmet
jelszavak rejtjelezett tárolását
sikeres és sikertelen bejelentkezések, jelszóváltoztatások naplózását
a hozzáférés korlátozását meghatározott időszakokra (pl. munkaidőre)
hogy a hozzáférési adatok törlése oly módon történjel, hogy a jelszó adatbázis esetleges visszaállítása esetén se legyen mód a törölt felhasználói jogosultságok visszaállítására

A felhasználó és a rendszer között kialakított kapcsolatot minden esetben titkosítani szükséges, a rendszer működésének felügyelet és a jelen előírások a betartása, betartatása az információbiztonsági felelős feladata.

6.2. Rendszerek felhasználóinak kezelése

Az új felhasználók felvételét, a meglévő jogosultságok törlését az információbiztonsági felelős kezdeményezése alapján az ügyvezető igazgató engedélyezi.
Kilépett munkatársak az információbiztonsági felelős gondoskodik, a kilépett munkatársak leveleinek időleges kezelést, átirányítását, mentését ugyancsak elvégzi.

6.3. Munkaállomások

Munkaállomások kezelőit illetően a munkáltató jogokat gyakorló, vagy nevében eljáró kötelessége, hogy a felvételre kerülő személy számára a munkaszerződésben, a kinevezési okiratban, vagy munkaköri leírásban rögzítse az információbiztonsági kötelezettségeket, megszegésük esetén pedig hívja fel a figyelmet a fegyelmi, kártérítési és büntetőjogi következményekre.
A Társaságnál munkaállomást kezelő valamennyi munkatárs csak előzetes titoktartási nyilatkozat megtételét követően férhet hozzá a munkakörének, megbízásának megfelelő jogosultságokkal az informatikai rendszerhez és annak adataihoz.

Munkaállomások esetén az üzleti titkot, személyes adatokat tartalmazó információkat, dokumentumokat munkaidőn túl nem szabad az asztalon tárolni, azokat csak a munkavégzés idejére szabad elővenni, érvényesíteni kell minden esetben a „tiszta asztal” politikát.
Új munkaállomás telepítését az információbiztonsági felelős kezdeményezi, annak jóváhagyása az ügyvezető igazgató hatásköre. Az információbiztonsági felelős telepíti az operációs rendszert és a szükséges alkalmazásokat, átvezeti a személyes beállításokat, valamint intézi a szükséges központi alkalmazásokhoz szükséges jogosultságok beállítását, majd ezt követően a munkaállomást átadja a felhasználónak.

Hardver konfigurációjának változtatása a fentiekben leírt folyamat végrehajtásaként történik. A munkaállomás konfigurációjának módosítását is át kell vezetni az eszközök nyilvántartásán, melyet ugyancsak az információbiztonsági felelős végez.

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.

6.4. Szoftvertelepítés

A központilag beszerzett szoftver licenceket az információbiztonsági felelős kezeli, kontrollálja, licencek nyilvántartása, a jogszerű használat biztosítása mellett.
A szerzői jogvédelem által védett számítógépes szoftverek illegális használata és másolása törvénybe ütköző cselekedet, amely egyben ellentétes Társaságunk belső irányelveivel, az IBSZ előírásaival, adatvédelmi és információbiztonsági előírásaival.

Minden szoftvervásárlásnál, telepítésnél és változásnál biztosítani kell a szoftverek jogtisztaságára vonatkozó elvek betartását.

Szabad, ingyenes programok telepítése is kizárólag megfelelő szakmai indoklással lehetséges és csak azok a felhasználók rendelkeznek szoftvertelepítési jogosultsággal, akiknek a munkavégzéshez az feltétlenül szüksége.
A szoftverekhez tartozó végfelhasználói licencszerződések tartalmáról a szoftvereket felhasználók számára minden esetben az információbiztonsági felelős ad tájékoztatást, gondoskodik ezen szoftverek nyilvántartásba vételéről.
Egyéb, licenccel nem rendelkező szoftvert telepíteni tilos.

6.5. Problémamegelőzés

Az egyes szolgáltatások üzemeltetői reaktív és preventív intézkedéseket tegyenek a szolgáltatás zavartalansága érdekében. Ezek az intézkedések lehetnek általános és az adott szolgáltatásra speciálisan jellemző feladatok, így különösen

- igény szerinti újraindítás, alapállapotba hozás
- javítócsomagok, patchek telepítése
- jelszavak és hozzáférési kódok rendszeres cseréje
- naplóállományok rendszeres kiértékelése
- a vírusvédelem működésének ellenőrzése

6.6. Incidenskezelés

Az informatikai leállását eredményező incidenskezelés elsődleges célja az érintett szolgáltatás mielőbbi visszaállítása. Az incidenskezelés felelőse az informatikai szolgáltatást nyújtó szervezet az incidens teljes életciklusa alatt.

A Társaság minden alkalmazottjának és partnereinek kötelessége az általa tapasztalt biztonsági eseményt vagy az általa feltért biztonsági sebezhetőséget haladéktalanul jelenteni az információbiztonsági felelősnek.

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 incidens megoldása történhet úgyis, hogy a szolgáltatás biztosítása csökkentett szinten valósul meg.
Az ismerté vált gyengeség, sebezhetőség kezelését a lehető legrövidebb időn belül, de legkésőbb az ismerté válást követő kettő munkanapon belül meg kell kezdeni.

A probléma végleges megoldása után a szolgáltatás működőképességének, vagy eredeti színvonalának visszaállítása az információbiztonsági felelős feladata. Az incidens lezárása minden esetben az érinett felhasználók értesítése után történhet.
Személyes adatot érintő incidensről az adatvédelmi munkatársat haladéktalanul értesíteni kell és az elhárítást vele együttműködve szükséges biztosítani.

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.

6.7. Hibakezelés

A felhasználók az informatikai jellegű hibákat (helyi hálózat, helyi szerver, munkaállomások, nyomtatók stb.) az információbiztonsági felelősnek kötelesek bejelenteni. Amennyiben az információbiztonsági felelős nem tudja a hibát elhárítani, azt jelzi az informatikai szolgáltatást nyújtó szervezet felé.

6.8. Konfigurációkezelés

A konfigurációkezelés célja az informatikai infrastruktúra komponenseinek azonosítása, adatainak követése, segítve ezzel az incidens-, probléma- és változáskezelést, biztosítva a gazdaságos üzemeltetés lehetőségét.

6.8. Katasztrófa-elhárítás

Katasztrófahelyzet bekövetkezhet elháríthatatlan ok, szándékos károkozás következtében is. A katasztrófa bekövetkezte után az informatikai szervezetnek képesnek kell lennie a szolgáltatás helyreállítására.

Ennek érdekében katasztrófaelhárítási terveket kell kidolgozni minden olyan területre, amelyek a Társaság főbb funkcióinak ellátásában, végzésében nélkülözhetetlenek.
A katasztrófa-elhárítási tervek az egyes rendszerek üzemeltetési szabályzatának részei.

7. Kapcsolódó szabályozások

Az IÜSZ előírásai összhangban vannak:
- Leltározási és értékelési szabályzattal,
- Számviteli politikával,
- Más irányítási rendszerekkel (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.

Jelen szabályozás keretei között rögzítettük a védelem tárgyaival és a védelem eszközeivel kapcsolatos magatartási és intézkedési szabályokat.

8.1. A védelem tárgya

A hálózatokat a fenyegetésektől való megóvásuk, a hálózatot használó rendszerek és alkalmazások – beleértve az átvitel alatti információt – biztonságának fenntartása érdekében megfelelő irányítás és ellenőrzés alatt kell tartani.

A tűzfalakra vonatkozó intézkedéseket az információbiztonsági felelős hajtja végre, ő működteti a rendszert és dokumentálja a rendszerdokumentációban.
A tűzfal üzemeltetésére vonatkozó eljárások, a tűzfal konfigurációs beállításai kiemelt üzleti titkot képeznek.
A rendszerdokumentációnak a következőket kell tartalmaznia:

- a tűzfalak konfigurációjának, ellenőrzésének módját
- a statisztikai adatgyűjtést, ezen adatok feldolgozását, a jelentések tartalmát
- a riasztási és a mentési rendszer specifikációját és működését
- a jelentési kötelezettségeket
- a rendszergazdák jogait és kötelezettségeit

A belső hálózatot tűzfalaknak kell védenie, amelyekre a következő előírások vonatkoznak, úgymint

- biztosítson lehetőséget a gyanús tevékenység észlelésére, valamint az azonalli beavatkozásra, riasztásra
- kezelése, üzemeltetése legyen egyszerű és könnyen elsajátítható
- architektúrája legyen nyitott, biztosítson lehetőséget olyan kiegészítésekre, fejlesztésekre, amelyek a mindenkori igények kielégítésére szolgálnak

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.
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,

8.3. A biztonsági mentés

A Társaság egyik legfőbb értékét a számítógépeken tárolt adatok jelentik. Ezek védelmében meghatározó jelentőségű a biztonsági másolatok készítése.
A mentés célja egyrészt a ritkán használt adatok, illetve kulcsfontosságú adatok (pl. adatbázis) rendszeresített, biztonságos és visszakeresésre alkalmas tárolása, másrészt, hogy előre nem látott adatsérülés, vagy adatvesztés esetén a sérült adatok a korábban, szabályozott módon eltárolt mentésekből hiánytalanul visszaállíthatók legyenek.
Mentés során mind az egyes rendszerek adatait, mind az operációs rendszer, adatbázis rendszer és szoftverkörnyezet beállításait is tárolni kell.
A működési rendszernek, illetve a termékforgalmazásnak számítógépeken készített és tárolt adatai elvesztésének megelőzése alapvető érdekünk biztonságos működésünk szempontjából.

Az adatvesztés, károsodás megelőzése érdekében valamennyi számítógépen készült és tárolt adatokat gondosan kezeljük, azokról minden esetben biztonsági másolatot kell készíteni és egy fizikailag a számítógépektől elhatárolt helyiségben

- külső merevlemezen, külső szerveren: napi teljes mentés NAS-ra, megőrzési idő 7 nap NAS elkülönített épületben
- felhőszolgáltatás igénybevételével: heti mentés teljes, napi növekményes mentés, megőrzési idő 2 hét

tároljuk, nevezetesen heti mentésekkel biztosítjuk adataink megőrzését.

A biztonsági mentéseket legalább heti gyakorisággal kell végezni, ezért előzetesen be kell állítani az e célra rendszeresített emlékeztetőt.

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 alkalmazottaival 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.

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.

10. 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.

10.1. 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.

10.2. 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.

11. A szoftverhasználat rendje

11.1. A szoftverhasználattal kapcsolatos szabályok

A szoftverek beszerzése és használata során figyelembe kell venni a szerzői jogra vonatkozó rendelkezéseket és szoftvert kisérő licencszerződés feltételeit.
A licencszerződés megsértésével törvénysértést követ el, aki

- a szoftvert, vagy annak dokumentációját, beleértve a programokat, alkalmazásokat, adatokat, kódokat és kézikönyveket a szerzői jog tulajdonosának engedélye nélkül lemásolja vagy terjeszti
- szerzői jog által védett szoftvert egyidejűleg két vagy több gépen futtat, hacsak ezt a szoftver licenc szerződése külön nem engedélyezi
- tudatosan vagy akaratlanul munkatársait arra ösztönzi, kötelezi, vagy számukra megengedi, hogy illegális szoftvermásolatot készítsenek, használjanak, vagy terjesszenek
- az illegális szoftvermásolást tiltó törvényt megsérti azért, mert valaki erre kéri vagy kényszeríti
- szoftvert kölcsön ad úgy, hogy arról másolatot lehessen készíteni, vagy aki aki a kölcsönkért szoftver lemásolja
- olyan eszközöket készít, importál, vagy birtokol, amelyek lehetővé teszik a szoftver védelmét szolgáló műszaki eszközök eltávolítását, vagy ilyen eszközzel kereskedik

12. Az informatikai eszközök környezetének védelme

12.1. Védett helyiségek

Védett helyiségnek kell tekinteni azokat a helységeket, ahol adatok feldolgozására, tárolására alkalmazott informatikai erőforrások találhatók. A védett területek zárt területnek minősülnek, ezért védelmükről ennek megfelelően kell gondoskodni. Társaságunk esetén védett területnek minősül

- a szerverhelyiség, aktív hálózati elemek elhelyezésére szolgáló helyiségek
- valamennyi számítástechnikai eszközzel felszerelt iroda.

12.2. Vagyonvédelmi előírások

Vagyonvédelmi eszközök védelmét illetően a következő szabályozás érvényesítése minden esetben szükséges, úgymint

- a szerverhelyiségeket és a rendező szekrényeket biztonsági zárokkal kell felszerelni
- a szerverhelyiségekbe és az aktív hálózati elemek elhelyezésére szolgáló helyiségekbe való be- és kilépés rendjét szabályozni kell
- a fentvédett területekre történő illetéktelen behatolás tényét az információbiztonsági felelősnek azonnal jelenteni kell

- az informatikai eszközöket csak a megfelelő jogosultságokkal rendelkező felhasználók használhatják, azok rendeltetésszerű használatáért a felhasználó a felelős

12.3. Tűzvédelmi előírások

Az informatikai eszközök tűzvédelmét illetően a következő előírásokat kell a eszközök felhasználása során érvényesíteni

- a szerverhelyiség a „D" mérsékelt tűzveszélyességi osztályba tartozik
- a menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell
- a szerverhelyiségben biztosítani kell a megfelelő tűzoltókészüléket
- a nagy fontosságú, pl. törzsadat-állományokat két példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni, ezen adatállományok kijelölése az ügyvezető igazgató feladata

12.4. Intézkedés elemi csapás esetén

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

- menteni a még használható anyagokat
- biztosítási mentésekről, háttértárakról a megsérült adatok visszaállítása
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást

12.5. Hardvervédelem

Hardver eszközök védelmét illetően a következő szabályozás érvényesítése minden esetben szükséges, úgymint

- a berendezések hibátlan és üzemszerű működését biztosítani kell
- a működési biztonság megóvását jelenti a szükséges alkatrészek időben történő beszerzése
- az üzemeltetést, karbantartást és szervizelést szerződött az informatikai szolgáltatást nyújtó partnerünk végzi, az szolgáltatását igényeljük

12.6. Gyártói előírások

Az informatikai eszközöket illetően messzemenően érvényesíteni kell az egyes berendezésekre vonatkozó, gépkönyvekben rögzített gyártói előírásokat

12.7. Az adatrögzítés védelme

Az adatrögzítés védelme érdekében szükséges intézkedések

- az 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
- hozzáférési lehetőségek
  - a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz

- az adatok bevitele során az alapelv, hogy azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti

12.8. Adathordozók védelme

Adathordozók védelmét illetően a következő szabályozás érvényesítése minden esetben szükséges, úgymint

- az adathordozókat a tűz- és vagyonvédelmi előírásokat betartva oly módon kell elhelyezni, hogy tárolás közben ne sérüljenek vagy károsodjanak
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről az egységek nyilvántartást vezetnek
- a használni kívánt adathordozót a tárolásra kijelölt helyről kell kivenni, és használat után oda kell visszahelyezni
- a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek
- adathordozót másnak átadni csak engedéllyel szabad

12.9. Adathordozók megőrzése, másolása, leltározása

Adathordozók megőrzése, másolása, leltározása során a következő szabályozás érvényesítése minden esetben szükséges, úgymint

- az adathordozók megőrzését a jogszabályi előírások szerint kell végezni
- sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni, biztonsági illetve archív adatállomány előállítása másolásnak minősül
- a szoftvereket és adathordozókat a leltározási szabályzatban foglaltaknak megfelelően kell leltározni

12.10. Mentések, fájlok védelme

Mentések, fájlok védelme tekintetében a következő szabályozást kell érvényesíteni

- adatfeldolgozás után biztosítani kell az adatok mentését
- a munkák során létrehozott általános dokumentumok mentése és az azt létrehozó felhasználók feladata
- a felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie, az archiválásban az információbiztonsági felelősnek kell segítséget nyújtani
- a szervereken tárolt adatokról a mentést rendszeresen el kell végezni, a mentésért a rendszergazdák a felelősek

12.11. Programokhoz való hozzáférés, programvédelem

Programokhoz való hozzáférés, programvédelem tekintetében a következő szabályozásban rögzített eljárást kell követni

- a Társaság biztosítja, hogy a rendszerszoftverek naprakész állapotban legyenek és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára

- 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

12.12. Központi gépek, szerverek védelme

A központi gépek, szerverek védelme során a következő biztonsági intézkedések végrehajtása szükséges, úgymint

- szünetmentes áramforrást kel használni, amely megvédi a berendezést a feszültségingadozástól, áramkimaradás esetén az 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

12.13. Munkaállomások védelme

Munkaállomsok védelme tekintetében a következő szabályozás előírásai a követendők, úgymint

- külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal
- vírusfertőzés gyanúja esetén a rendszergazdát azonnal értesíteni kell
- a Társaság informatikai eszközeiről programokat illetve adatállományt másolni a jogos belső felhasználói igények kielégítésén kívül nem szabad
- új rendszereket használatbavételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket
- az informatikai eszközt és tartozékait helyéről elvinni csak az eszköz leltárfelelőse tudtával és engedélyével szabad