INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

Verzió 1:0

Cégnév: Kartonpack Dobozipari Nyilvánosan Működő Részvénytársaság
Rövidített név: Kartonpack Nyrt.
Adószám: 10547009-2-41
Nemzetközi adószám: HU10547009
Székhely címe: 1024 Budapest Ady Endre utca 19/A

Hatályba lépés: 2021.01.28.
Érvényességi ideje: határozatlan
Belső használatú!

	Információbiztonsági Szabályzat
Jóváhagyó	dr. Uszkay-Boiskó Sándor elnök-vezérigazgató
Készítette	4iG Nyrt.
Kabinet vélemény: jóváhagyásra benyújtható	Szabolcs Márta kontrolling és beszerzési igazgató
Kabinet vélemény: jóváhagyásra benyújtható	Szalona Péter számviteli igazgató
Időbeli hatály	**2022. január 28.**-től visszavonásig
Személyi hatály	A Társaság valamennyi fő- és részfoglalkozású munkavállalója, aki az IBSZ tárgyi hatályát érintő vagyonelemek kezelésében részt vesz.
Tárgyi hatály	A védelmet élvező adatok és eszközök teljes körére
Hatályon kívül helyezi	

Dokumentumtörténet

Verzió	Dátum	Változás	Szerző
0v1	2022. 01. 13.	Struktúra kidolgozása, alapvető rendelkezések.	Szalmási Erik (4iG Nyrt.)
0v2	2022. 01. 17.	Egyéb kiegészítések.	Tóth László (4iG Nyrt.)
1v0	2022. 01. 28.	Véglegesítés, garanciális javítások.	Szalmási Erik (4iG Nyrt.)

TARTALOMJEGYZÉK

ÁBRAJEGYZÉK

1 BEVEZETŐ RENDELKEZÉSEK

1.1 AZ INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT CÉLJA

Az Információbiztonsági szabályzat (a továbbiakban: IBSZ) célja a Kartonpack Nyrt. (a továbbiakban: Társaság) stratégiai céljait és üzleti tevékenységét támogató információ-feldolgozó rendszerek, valamint az e rendszerek által kezelt, feldolgozott, továbbított adatok bizalmasságát, sértetlenségét, rendelkezésre-állását fenyegető veszélyek megelőzésére, felderítésére, elhárítására, enyhítésére vonatkozó általános védelmi feladatok meghatározása.

Az Információbiztonsági szabályzat 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.

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

Jelen Információbiztonsági szabályzat az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

1.2 ALKALMAZÁSI TERÜLET

Az MSZ ISO/IEC 27001:2014 nemzetközi információbiztonsági szabvány követelményeit a Társaság iránymutatásként kívánja figyelembe venni jelen szabályzat kialakításához, információbiztonság irányítási rendszerének fejlesztéséhez, illetve informatikai szolgáltatásaira.

1.3 AZ IBSZ HATÁLYA

Az IBSZ végrehajtását a hatályba lépésnek megfelelően, kihirdetéstől kezdődően meg kell kezdeni. Az IBSZ a biztonságos információellátás érdekében utasításokat tartalmaz, amelyek hatálya kiterjed a Társaság informatikai rendszereinek teljes életciklusára (tervezés, fejlesztés, beszerzés, bevezetés, üzemeltetés, kivonás).

Az IBSZ személyi-szervezeti, tárgyi, területi és egyéb hatályát a következők határozzák meg:

1.3.1 SZEMÉLYI-SZERVEZETI HATÁLY

A személyi hatály az IBSZ tárgyi hatályát érintő vagyonelemek kezelésében részt vevő fő- és részfoglalkozású munkavállalókra, illetve az informatikai folyamatokban résztvevő más szervezetek dolgozóira egyaránt kiterjed.

1.3.2 TÁRGYI HATÁLY

Az IBSZ tárgyi hatálya kiterjed:

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

1.3.3 TERÜLETI HATÁLY

Az IBSZ területi hatálya kiterjed mindazon területekre, ahol a Társaság az informatika használatával a tevékenységét kifejti, függetlenül geográfiai elhelyezkedésétől.

1.3.4 AZ IBSZ TOVÁBBI HATÁLYA

Az IBSZ hatálya kiterjed:

- A védelem körébe vont adatok és információk teljes körére, felmerülésüktől, feldolgozási helyüktől és az adatok fizikai megjelenési formájától függetlenül.

1.4 VONATKOZÓ JOGSZABÁLYOK, AJÁNLÁSOK, BELSŐ UTASÍTÁSOK ÉS DOKUMENTUMOK

1.4.1 JOGSZABÁLYOK

- 2013. évi V. törvény a Polgári Törvénykönyvről
- 2012. évi I. törvény a munka törvénykönyvéről
- 2000. évi C. tv. a számvitelről
- 2017. évi CL. törvény az adózás rendjéről
- 2007. évi CXXVII. törvény az általános forgalmi adóról
- 1996. évi LXXXI. törvény a társasági adóról és az osztalékadóról
- 2018. évi LII. törvény a szociális hozzájárulási adóról
- 2019. évi LXXX. törvény a szakképzésről
- 2011. évi CXCI. törvény a megváltozott munkaképességű személyek ellátásairól és egyes törvények módosításáról

- 2019. évi CXXII. törvény a társadalombiztosítás ellátásaira jogosultakról, valamint ezen ellátások fedezetéről
- 2011. évi LXXXV. törvény a környezetvédelmi termékdíjról
- 2001. évi CXX. törvény a tőkepiacról
- 24/2008. (VIII. 15.) PM rendelet a nyilvánosan forgalomba hozott értékpapírokkal kapcsolatos tájékoztatási kötelezettség részletes szabályairól
- 1990. évi C. törvény a helyi adókról

1.4.2 SZABVÁNYOK ÉS AJÁNLÁSOK

- MSZ ISO/IEC 27001:2014: Informatika, az információbiztonság irányítási rendszerei és követelményei.

1.4.3 BELSŐ UTASÍTÁSOK ÉS DOKUMENTUMOK

Az Információbiztonsági szabályzatot az alábbiakban felsorolt szabályzatokkal és eljárásokkal összhangban kell alkalmazni:

- Iratkezelési szabályzat;
- Leltározási szabályzat, amely szabályzat a selejtezési eljárást is szabályozza;
- Folyamatba épített előzetes és utólagos vezetői ellenőrzés rendszere, amely több szabályzatban leírt eljárások összessége.

A Társaság belső utasításainak és dokumentumainak pontos listáját a *„Mellékletek”* fejezet tartalmazza.

1.5 AZ IBSZ MINŐSÍTÉSE

A Társaság Információbiztonsági Szabályzata egy **belső használatú dokumentum**. Így jelen belső használatú dokumentumot a Társaság vezetősége és informatikai területen, vagy informatikai rendszerekkel és alkalmazásokkal dolgozó munkatársai és szerződéses felei megismerhetik és birtokolhatják, de illetéktelenek részére nem adhatják tovább.

2 INFORMÁCIÓBIZTONSÁGI SZABÁLYOK

2.1 AZ INFORMÁCIÓBIZTONSÁG VEZETŐI IRÁNYÍTÁSA

2.1.1 INFORMÁCIÓBIZTONSÁGI SZABÁLYOK

Információbiztonsági szabályokat kell meghatározni, a vezetés által jóváhagyni, közzétenni, valamint a munkatársak és a fontos, külső érdekelt felek felé kommunikálni.

Az IBSZ-be foglalt információbiztonsági szabályokat az **Elnök-Vezérigazgatónak** jóvá kell hagyni és támogatni. A munkatársak, valamint a külső érdekelt felek számára közzé kell tenni az IBSZ-t.

2.1.2 AZ INFORMÁCIÓBIZTONSÁGI SZABÁLYOK ÁTVIZSGÁLÁSA

Az információbiztonsági szabályokat tervezett időközönként vagy jelentős változások esetén át kell vizsgálni, hogy a folyamatos alkalmasságuk, megfelelőségük és eredményességük biztosítva legyen.

Az információbiztonsági szabályokat évente, vagy jelentős változások esetén a változást követő lehető legrövidebb határidőn belül év közben is teljes egészében felül kell vizsgálni.

Az IBSZ legalább részleges, a megváltozott körülményeket érintő felülvizsgálatát el kell végezni az alábbi események bármelyikének bekövetkezésekor:

- Az Információbiztonsági politika és célok (IPC) módosítása,
- az információbiztonságot is érintő jogszabályváltozás, amennyiben annak hatálya a Társaságra és annak működésére is kiterjed,
- az információkezelést és -feldolgozást végző vagy támogató folyamatokban, illetve a kezelt adatok körében beállt lényeges változás,
- a Társaság tulajdonában vagy használatában lévő információs rendszerekben, illetve azok fizikai környezetében beálló lényeges változás.

Az IBSZ karbantartása, felülvizsgálata az **Információbiztonsági felelős** feladata.

2.1.3 A VEZETÉS ELKÖTELEZETTSÉGE AZ INFORMÁCIÓBIZTONSÁG MELLETT

A vezetői elkötelezettség kinyilvánításának a Társaság Információbiztonsági politika és célok (IPC) felel meg.

2.2 KOCKÁZATOK FELMÉRÉSE, KEZELÉSE

A kockázatmenedzsment folyamat az információbiztonság irányításának kulcsfolyamata.

Az információbiztonsági kockázatok felmérése és kezelése érdekében *Kockázatelemzési és kockázat kezelési módszertan* dokumentációt kell kialakítani.

A *Kockázatelemzési és kockázat kezelési módszertan* alapján biztosítani kell, hogy Társaságunk kockázatelemzése és kockázatkezelése tervszerű, jól követhető, megismételhető és ellenőrizhető legyen.

A kockázataránYos védelem érdekében rendszeres időközönként kockázatelemzést kell lefolytatni és a feltárt kockázatokra kockázatkezelési tervet kell meghatározni.

A kockázatmenedzsment folyamatainak végrehajtása, illetve koordinálása, valamint szükség esetén a *Kockázatelemzési és kockázat kezelési módszertan* felülvizsgálata az **Információbiztossági felelős** feladata.

3 AZ INFORMÁCIÓBIZTONSÁG SZERVEZETE

3.1 BELSŐ SZERVEZET

3.1.1 AZ INFORMÁCIÓBIZTONSÁG KOORDINÁLÁSA

A Társaság információbiztonságának koordinálásért az **Információbiztonsági felelős** felel.

Információbiztonsági felelős: A Társasággal információbiztonságra vonatkozóan szerződésben álló 4iG Nyrt. által kijelölt személy.

Munkáját az egyes szakterületi vezetők támogatják.

3.1.2 INFORMÁCIÓBIZTONSÁGGAL FOGLALKOZÓ VEZETŐI FÓRUM

A vezetőségnek Információbiztonsági Fórumot kell létrehoznia, melynek éves rendszerességgel kell vezetői ülést tartania. A Fórum feladata az információbiztonsági stratégiai kérdések áttekintése, az információbiztonságot érintő fejlesztések előre haladásának mérése, szükséges döntések meghozatala és az erőforrások biztosítása, valamint intézkedések meghozatala, az **Információbiztonsági felelős** javaslatai alapján.

Az Információbiztonsági Fórum tagjai:

- **Elnök-Vezérigazgató**
- **Információbiztonsági felelős**
- **Kontrolling és beszerzési igazgató**
- **Rendszerkoordinátor**
- **Szakterületi vezetők** (eseti jelleggel)

Az Információbiztonsági Fórumnak a Társaságnál esetlegesen bekövetkező kiemelt információbiztonsági incidensek esetén rendkívüli ülést kell tartania. Ennek célja a biztonsági incidens kiderítésére vonatkozó vizsgálatok azonnali elrendelése és kiértékelése, szükség esetén szankcionálási módok meghatározása.

3.1.3 INFORMÁCIÓBIZTONSÁGI SZEREPEK ÉS FELELŐSSÉGEK

Minden információbiztonsággal kapcsolatos felelősséget meg kell adni, és ki kell osztani.

Az információbiztonság a Társaság teljes állományának felelőssége.

A személyi kockázatok csökkentése érdekében:

- Meg kell határozni a felhasználók rendszeres információbiztonsági oktatását, tudatosítását.
- Minden munkatársnak aláírásával el kell fogadnia a szerepkörének megfelelő munkaköri leírást.
- Minden munkatársnak aláírásával el kell fogadnia az Alkalmazotti nyilatkozatot, mely tartalmazza az adott munkaterületre vonatkozó információbiztonsági követelményeket.

- Meg kell határozni az alkalmazottak információbiztonsággal kapcsolatos feladatait, felelősségeit.
- Meg kell határozni a biztonsági szabályok megsértésével járó szankciókat, és azokat következetesen alkalmazni kell.

A Társaságnál az információbiztonságot tekintve az alábbi szerepköröket kell megkülönböztetni:

Felhasználó

A felhasználók információbiztonsági feladatait és felelősségeit az *Alkalmazotti nyilatkozat* tartalmazza.

Rendszerkoordinátor

Feladatai és felelősségei:

- ellátja az adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- ellátja az informatikai titokvédelmi munka szervezését és felügyeletét,
- kialakítja a védelmi eszközök alkalmazására vonatkozó döntés elkészítése érdekében a szakterületek bevonásával a biztonságot növelő intézkedéseket,
- felelős az informatikai rendszerek üzembiztonságáért, biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indítás-hoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének, szerviz ellátás biztosításának folyamatos ellenőrzése,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- informatikai adatvédelmi feladatok ismertetése
- a védelmi rendszer érvényesülésének ellenőrzése,
- felelős a Társaság informatikai rendszere hardver eszközeinek karbantartásáért, és időszakos hardver tesztjeiért,
- ellenőrzi a vásárolt szoftverek helyes működését, vírusmentességét, a használat jog-szerűségét,
- a vírusvédelemmel foglalkozó szervezetekkel kapcsolatot tart,
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek izolálásáról,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működése és biztonsága szempontjából a lényeges paraméterek alakulását,
- tevékenységéről rendszeresen beszámol a Társaság vezetőjének,
- évente egy alkalommal ellenőrzi az IBSZ előírásainak betartását,
- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
- előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

Jogai:

- Az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a Társaság erre jogosult vezetőjénél,
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,
- betekinthet valamennyi iratba, ami az informatikai feldolgozásokkal kapcsolatos,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére, illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

A **Rendszerkoordinátor** személyének az alábbi követelményeknek kell megfelelnie:

- Összeférhetetlenség – a **Rendszerkoordinátori** adatvédelmi felelős funkció összeférhetetlen minden olyan vezetői munkakörrel, amelyben adatvédelmi kérdésekben a napi munka szintjén dönteni, intézkedni kell,
- az informatikai hardver eszközök és a védelmi technikai berendezések ismerete,
- üzemeltetésben jártasság,
- szervezőkészség,
- a szakterületre vonatkozó jogi szabályozás ismerete.

A **Rendszerkoordinátor** megbízatása:

- A **Rendszerkoordinátort** az **Elnök-Vezérigazgató** bízza meg, aki jogosult ellátni a hatáskörébe tartozó feladatokat.
- A **Rendszerkoordinátor** feladatait a **Kontrolling és beszerzési igazgató** felügyelete mellett látja el.

Adatkezelő

Adatkezelőnek a Társaság vezetője az **Elnök-Vezérigazgató** minősül. Az Elnök-Vezérigazgató **Adatkezelői** szerepkörben végrehajtandó feladatát delegálja a **Szakterületi vezetők** felé, akik a saját üzleti folyamataik által keletkeztetett adatok kezeléséért felelősek.

Adatgazda:

Az adatok osztályozását (bizalmasság, sértetlenség, és rendelkezésre állás) az **Adatgazdá**k végzik az erre a célra kialakított *Adatvagyon nyilvántartásban*. Az **Adatgazdai** szerepkört minden adatkörhöz/adatcsoporthoz ki kell jelölni, ennek szabályai külön eljárásrendben kerülnek megfogalmazásra.

Adatgazdának az **Elnök-Vezérigazgató** és a **Szakterületi vezetők** minősülhetnek, akik – a hatáskörükbe utalt adatkör és rendszer vonatkozásában – felelnek a következők meghatározásáért:

- Az adatkezelés kapcsán érintett folyamatok,
- az adatkezelés célja,
- az adatok tartalma és struktúrája;
- az adatot kezelő rendszer funkcionalitása;
- az adatok rögzítésének, módosításnak, feldolgozásának és törlésének szabályai;
- az adathelyességi, adatminőségi elvárások; valamint

- az adatokhoz való hozzáférésre, az adatok felhasználására jogosultak köre.

A Társaság egyes **Adatgazdái** jogosultság menedzsment szabályoknak megfelelően döntenek a hozzájuk rendelt rendszerek és adatok vonatkozásában a hozzáférésekről (igénylés, módosítás, visszavonás).

Az **Adatgazdák** további feladatai és felelősségei a Kontrolling és beszerzési igazgató felügyelete és irányítása mellett:

- A jogosultságok évenkénti felülvizsgálata a Rendszerkoordinátorral közreműködve,
- a hozzáférésekben történő bármilyen változtatási igény azonnali, dokumentált formában történő közlése a Rendszerkoordinátor felé, és a változtatás végrehajtásának ellenőrzése.

Információbiztonsági felelős

Feladatai és felelősségei:

- Az Információbiztonsági feladatok (az információbiztonsági rendszer ellenőrzése, felülvizsgálata, fejlesztése) koordinálása, vagy végrehajtása.
- az informatikai rendszereket fenyegető veszélyforrások azonosítása, illetve a fellépő kockázatok meghatározása és a kockázatcsökkentő intézkedésekben javaslattétel,
- az informatikai beszerzések, informatikai fejlesztések során a biztonsági követelmények érvényre juttatása,
- a Társaság információbiztonsági dokumentációs rendszerének (Információbiztonsági Politika és Célok, Információbiztonsági szabályzat és az abban hivatkozott dokumentumok) rendszeres karbantartása,
- az információbiztonsági szabályzatokban deklarált követelmények betartatásának ellenőrzése,
- annak biztosítása, hogy megtörténjen:
    - az információbiztonsági incidensek kivizsgálása,
    - az incidensek nyilvántartása,
    - az incidensek kezelése,
    - és az incidensek kapcsán felmerült problémák elhárítása,
- az információ-, informatikai biztonság tudatosságának növelése – oktatás lefolytatása.

Jogai a kötelezettségek teljesítése érdekében:

- Jogosult külön engedély nélkül a Társaság bármely helyiségébe belépni, amennyiben ott az információbiztonságot érintő munkavégzés folyik,
- az információbiztonsági incidensek kivizsgálása során a szükséges információkat minden munkavállaló köteles a rendelkezésére bocsájtani,
- jogosult minden értekezleten részt venni, észrevételeit és javaslatait megtenni, amelynek számítástechnikai, illetve információbiztonsági vonatkozása van, és ez az értekezlet összehívásakor ismert,
- jogosult a vezetői fórumnak információbiztonsággal kapcsolatos kérdésekben javaslatokat tenni,
- jogosult az információbiztonsággal kapcsolatos riportok készítésére.

Elnök-Vezérigazgató

Feladatai és felelősségei:

- Az információbiztonsági rendszer működéséhez szükséges erőforrások biztosítása,
- gondoskodik arról, hogy az információbiztonsági feladatok és követelmények beépüljenek a Társaság működési folyamataiba,
- részt vesz az információbiztonsággal kapcsolatos incidensek kivizsgálásában, az esetleges felelősök felelősségre vonásában, mint a munkáltatói jogkör gyakorlója döntést hoz,
- a papír alapon keletkezett információk (számlák, szerződések, titoktartási nyilatkozatok) az Iratkezelési szabályzatban meghatározott módon történő biztonságos kezelésének kialakításáért és működtetéséért felel.
- évente a Kontrolling és beszerzési igazgató vagy általa ezzel megbízott **Rendszerkoordinátor** által készített riportok alapján felülvizsgálni a szerepkörökbe történő besorolást és az egyes szerepkörökhöz tartozó jogosultságokat,
- információbiztonsági vonzatkozásban felelős a szállítókkal történő megállapodásokért, azok nyomon követéséért és az üzleti érdekek képviseléséért,
- az új munkatárs regisztrálásának (felhasználó létrehozásának) jóváhagyása,
- munkakör megváltozás esetén a jogosultságok felülvizsgálata,
- fegyelmi eljárás esetén feladata a szankciók meghatározása.

Szakterületi vezető

Feladatai és felelősségei:

- Közreműködés az adatok védelmi szintjének meghatározásában,
- „korlátozott használatú” besorolással ellátott adatok esetén az adatmegosztás szolgálati útjainak meghatározása,
- egyedi hozzáférési igény vagy módosítás esetén a kérés kezdeményezése,
- egyedi hozzáférések megszüntetésének jóváhagyása,
- egy munkatárs elbocsájtása esetén feladata elsősorban a **Kontrolling és beszerzési igazgató** vagy tartós akadályoztatása esetén a **Rendszerkoordinátor** értesítése a kilépésről, a jogosultságok felülvizsgálata, az érintett külső felek értesítése. Továbbá engedélyezheti a magántitok és a személyhez köthető információk elvitelét.

3.2 KÜLSŐ FELEK

Az informatikai rendszerrel kapcsolatba kerülő, vagy az információbiztonságra hatást gyakorló külső személyekkel vagy cégekkel olyan írásbeli szerződést kell kötni, melyben ki kell térni az információbiztonsági szabályokra, követelményekre, továbbá tartalmaznia kell egy titoktartási nyilatkozat pontot. A szerződés szakmai felülvizsgálatáért a Kontrolling és beszerzési igazgató és az általa adott ügybe bevonásra kerülő **Információbiztonsági felelős** felel.

A Társaság külső érdekelt ügyfeleit az *Érdekelt felek listája* táblázat tartalmazza.

3.2.1 FELADATKÖRÖK SZÉTVÁLASZTÁSA

Az egymással ütköző kötelességeket és felelősségi területeket szét kell választani annak érdekében, hogy csökkenjen a lehetősége a szervezeti vagyonelemek jogosulatlan vagy nem szándékos módosításának, illetve az azokkal történő visszaélésnek.

Külső felek esetén biztosítani kell, hogy a kereskedelmi/gazdasági és szakmai kapcsolatot külön munkatárs biztosítsa, ez alól csak a Társaság vezetősége adhat felmentést.

3.2.2 KAPCSOLAT A HATÓSÁGOKKAL

- Cégbíróság
  - Kapcsolattartó: Rátky és Társa Ügyvédi Iroda
  - Szervezeti egység: külsős
- Nemzeti Adó- és Vámhivatal (NAV)
  - Kapcsolattartó: főkönyvelő
  - Szervezeti egység: számviteli igazgatóság
- Központi Statisztikai Hivatal (KSH)
  - Kapcsolattartó: főkönyvelő
  - Szervezeti egység: számviteli igazgatóság

3.2.3 KAPCSOLAT SZAKMAI CSOPORTOKKAL

Megfelelő kapcsolatot kell fenntartani szakmai csoportokkal vagy más specializálódott biztonsági fórumokkal és szakmai egyesületekkel.

- A Társaság az üzleti tevékenységeivel kapcsolatban számos gyártóval áll partneri viszonyban. A partnerségi kapcsolatokból adódóan magas kompetenciákkal rendelkezik az alábbi területeken:
- Határvédelem
- Hálózat védelem
- Sérülékenység menedzsment
- Kártékony kódok elleni védelem (vírusvédelem)

A partnerségből adódó előnyöket a Társaság információbiztonsági folyamataiban is hasznosítani kell a tudásmenedzsment keretében.

3.3 MOBIL ESZKÖZÖK ÉS TÁVMUNKA

3.3.1 SZABÁLY MOBIL ESZKÖZÖKRE

Szabályt és azt támogató biztonsági intézkedéseket kell bevezetni a mobil eszközök használatával járó kockázatok kezelésére. A mobil eszközökön (laptop, tablet, mobiltelefon) tárolt adatok mobilitásuknál fogva fokozott veszélynek vannak kitéve, ezért a kezelésükre nézve a következő előírásokat kell betartani:

- Minden alkalmazottra nézve kötelező, a munkavégzés céljából átadott mobil eszközöket rendeltetésszerűen használni, és a biztonságos használathoz szükséges beállításokat elvégezni.

- szervezeti eszközön magánjellegű levelező rendszert kezelni tilos,
- magántulajdonú mobil eszközzel a felhasználó belső hálózatra nem csatlakozhat,
- a szervezeti e-mail fiók kezelése magántulajdonú mobil eszközökön nem engedélyezett,
- mobiltelefonok esetében kötelező a képernyőfeloldó kód, valamint a PIN kód, tabletek esetében a képernyőfeloldó kód, laptopok esetében felhasználói jelszó alkalmazása,
- az eszköz esetleges fizikai vagy szoftveres sérülését, illetve az eszköz elvesztését a felhasználó köteles a lehető leghamarabb jelezni a közvetlen vezetőjének, illetve az információbiztonsági felelősnek.

A mobil eszközöket tilos kitenni:

- Erős fizikai behatásnak,
- sugárzó hőnek,
- erős mágneses, vagy elektromágneses térnek,
- nedves vagy poros környezetnek.

A Társaság tulajdonát képező tablet és mobiltelefon készülékek biztonságos használatához a következő beállítások és szabályok betartása kötelező:

- SIM kártya zárolása PIN kóddal,
- legalább 4 karakterből álló jelkód beállítása,
- a jelkód kiegészíthető egyéb azonosítási módszerekkel, pl.: mintázattal vagy biometrikus azonosítással (ujjlenyomat, arcfelismerés, íriszszkenner),
    - mintázattal történő azonosítás esetén legalább 4 pontból álló mintázat összeállítása szükséges,
- automatikus lezárás funkció beállítása,
- eszköz keresése funkció beállítása lehetőség szerint,
- az eszköz szoftveres feltörése tilos,
- a támogatott mobil eszközök szoftverfrissítése.

A Társaság tulajdonát képező laptopok biztonságos használatához a következő beállítások és szabályok betartása kötelező:

- A Társaság jelszóházirendjének megfelelő jelszó alkalmazása,
- a Társaság vírusvédelmi szoftver folyamatos rendelkezésre állásának biztosítása és frissítése,
- merevlemez titkosítás beállítása,
- eszköz keresése funkció beállítása lehetőség szerint,
- vendég felhasználó tiltása.

3.3.2 TÁVMUNKA

Szabályt és azt támogató biztonsági intézkedéseket kell megvalósítani a távmunkahelyeken hozzáférhető, feldolgozott és tárolt információk védelme érdekében.

A távoli munkavégzést a Társaság vállalati tűzfala mögött végződtetett, titkosított csatornán keresztül kell megvalósítani.

- Távoli munkavégzés csak a *VPN engedélyezési listában* szereplő személyek számára engedélyezett.

Ezen személyek számára az alábbi biztonsági pontok betartása kötelező:

- Távoli elérés csak működő személyi tűzfal, illetve vírusvédelmi szoftver mellett kezdeményezhető,
- a távoli elérés alatt tilos más, nem az aktuális munkával kapcsolatos tevékenységek folytatása,
- a távoli elérés alatt használt erőforrásokat csak a szükséges időtartamra szabad foglalni, a nem használt hozzáféréseket be kell zárni,
- távoli elérés csak a mindennapi munkavégzés céljából rendelkezésre bocsátott mobil eszközökről kezdeményezhető.

4 AZ EMBERI ERŐFORRÁS BIZTONSÁGA

4.1 A MUNKAVISZONY KEZDETE ELŐTT

4.1.1 ÁTVILÁGÍTÁS

A munkaviszonyra jelölteknek olyan háttérellenőrzését kell elvégezni, amely megfelel a vonatkozó törvényeknek, szabályozásoknak és etikai elvárásoknak, valamint arányos az üzleti követelményekkel, az elérendő információk besorolásával és a feltételezett kockázatokkal.

A Társaság a pályázati felhívásra beérkező önéletrajzok alapján kompetencia szintű ellenőrzést végez és kiszűri azokat a jelentkezőket, akik nem felelnek meg a felhívás alap követelményeinek (iskolai végzettség, tapasztalat stb.).

Az érintett **Szakterületi vezetőnek** minden esetben meg kell győződnie a munkavállaló szakmai tudásáról és referenciáiról még a munkába lépés előtt, mely jelenti a szakmai minősítések meglétének ellenőrzését is. Ezt követően a munkavállalónak szűrési kérdésekre kell válaszolnia.

4.1.2 A MUNKAVISZONNYAL KAPCSOLATOS FELTÉTELEK ÉS KIKÖTÉSEK

A titoktartási nyilatkozattétel az alkalmazotti munkaszerződés része. Az alkalmazottakkal és a szerződéses munkavállalókkal kötendő szerződéses megállapodásoknak meg kell adniuk az információbiztonságra vonatkozó felelősségeket mind a munkavállalók, mind a szervezet oldaláról.

Új belépő esetén az *Alkalmazotti nyilatkozat* aláírása a munkáltatói szerződés alapfeltétele.

4.2 A MUNKAVISZONY FENNÁLLÁSA SORÁN

4.2.1 VEZETŐI FELELŐSSÉGEK

A vezetésnek meg kell követelnie, hogy minden alkalmazott és szerződéses munkavállaló a bevezetett szervezeti szabályok és eljárások szerint járjon el az információbiztonsági kérdésekben.

Minden alkalmazottra nézve kötelező az információbiztonságot érintő szabályzatok megismerése és betartása. Az információbiztonsági szabályzatok megismerésére a munkába lépést követően 3 munkanap áll rendelkezésre. Az új munkavállaló által megismerendő információbiztonsági szabályokat az *Alkalmazotti nyilatkozat* dokumentum tartalmazza.

4.2.2 AZ INFORMÁCIÓBIZTONSÁG TUDATOSÍTÁSA, OKTATÁSA ÉS KÉPZÉSE

A szervezet minden alkalmazottjának és - ahol szükséges - a szerződéses munkavállalóknak megfelelő tudatosító oktatásban és képzésben kell részesülniük, illetve a munkakörükhöz kapcsolódó szervezeti szabályok és eljárások terén rendszeresen frissíteni kell ismereteiket.

A munkavégzéshez szükséges és az információbiztonsággal kapcsolatos ismeretek megszerzése után az új munkatársnak aláírásával kell igazolnia, hogy az *Alkalmazotti nyilatkozatot* önmagára nézve kötelező érvényűnek tekinti.

A munkavégzés céljából átvett eszközök birtokbavételéről *Átadás-átvételi jegyzőkönyvet* kell kitölteni. Az átvevő köteles az *Átadás-átvételi jegyzőkönyvet*, az átadás teljesítését követően aláírásával igazolni, valamint aláírásával el kell fogadnia, hogy az átvett eszközt csak üzleti célra használja fel.

4.2.3 FEGYELMI ELJÁRÁS

Léteznie kell egy formális és kommunikált fegyelmi eljárásnak, hogy fel lehessen lépni az olyan alkalmazottakkal szemben, akik információbiztonsági szabálysértést követtek el.

Minden információbiztonsági incidensről tájékoztatni kell az adott incidens kezeléséért felelős személyt, akinek az incidens részleteit fel kell vinnie az *Információbiztonsági incidens nyilvántartás* táblázatba. A kitöltött táblázat alapján az érintett **Szakterületi vezetőnek** meg kell határoznia a megfelelő szankciót a szabálysértő alkalmazottra nézve. Ezután az **Információbiztonsági felelős** feladata ismertetni a szabálysértő alkalmazottal az érintett szabályzatot vagy eljárást.

A Társaság információbiztonsági politikáját durván sértő szabálysértés esetén fegyelmi eljárást kell kezdeményezni a szabálysértővel szemben. A fegyelmi eljárásban résztvevő személyek:

- **Elnök-Vezérigazgató**
- **Érintett Szakterületi vezető**
- **Kontrolling és beszerzési igazgató**
- **Információbiztonsági felelős** (az **Elnök-Vezérigazgató** döntésétől függően az információbiztonsági incidens szakmai véleményezésében, külső szakértőként vehet részt)

A fegyelmi eljárás során vizsgálni kell

- a szabálysértés
  - elkövetési magatartását (szándékos vagy vétlen)
  - mértékét és lehetséges következményeit
- a szabálysértő
  - súlyosbító és felmentő körülményeit

A fegyelmi eljárás során a szabálysértőnek lehetőséget kell biztosítani, hogy saját maga védelmében átadjon információkat a fegyelmi eljárás résztvevőinek.

4.3 A MUNKAVISZONY MEGSZŰNÉSE ÉS MEGVÁLTOZÁSA

4.3.1 A MUNKAVISZONY MEGSZÜNTETÉSÉHEZ VAGY MEGVÁLTOZTATÁSÁHOZ KAPCSOLÓDÓ FELELŐSSÉGEK

A munkaviszony megszűnése vagy megváltozása után is érvényben maradó információbiztonsági felelősségeket és kötelességeket meg kell határozni, közölni kell az alkalmazott vagy a szerződéses munkatárs felé, és ezeket érvényesíteni kell.

Munkaviszony megszüntetésekor, azonnali felmondás esetén a munkavállaló már nem veheti igénybe a Társaság erőforrásait. Ebben az esetben a felmondást megelőzően valamennyi jogosultságát vissza kell vonni. A felmondást követően kísérőt kell biztosítani, hogy a munkavállaló

magához vegye személyes dolgait és a legrövidebb idő alatt biztosítani kell, hogy elhagyhassa a Társaság területét.

Felmondás esetén, az adott személyhez köthető jogosultságokat az érintett **Szakterületi vezetőnek** felül kell vizsgálni. Kilépéskor az adott személyhez köthető jogosultságokat, jelszavakat az IT Szolgáltatónak vissza kell vonnia, a felhasználó által ismerteket meg kell változtatni. A gyártói és egyéb partneri eléréseket vissza kell szolgáltatni, továbbá a Kontrolling és beszerzési igazgatót az **Elnök-Vezérigazgatót, valamint az érintett üzletfeleket** tájékoztatni kell a kilépésről, mely a közvetlen vezető feladata. A kilépő személy köteles, a munkavégzése során a részére kiadott eszközökkel, feladatokkal maradéktalanul elszámolni, azok teljesítését követően azt az Elszámolási lapon aláírásával igazolni. A kilépő személy részére átadott munkaeszközök és feladatok elszámolásáról az *„A vagyonelemekért viselt felelősség”* fejezetben foglaltak mérvadóak a *„Vagyonelemek visszaszolgáltatása”* bekezdés alapján.

Munkakör megváltoztatása során az adott személyhez köthető jogosultságokat és munkaeszközöket az érintett **Szakterületi vezetőnek** a Kontrolling és beszerzési igazgatóval együttműködve felül kell vizsgálni.

5 VAGYONELEMEK KEZELÉSE

5.1 A VAGYONELEMEKÉRT VISELT FELELŐSSÉG

5.1.1 VAGYONLELTÁR

Az információs vagyonelemeket és az információ-feldolgozó eszközöket azonosítani kell, ezeknek a vagyonelemeknek egy leltárát kell kialakítani, és azt karban kell tartani.

A Társaság minden vagyonelemét, mely a normál üzletmenet-folytonossághoz szükséges, nyilvántartásba kell venni, a felsorolt vagyonelemekhez felelősöket kell rendelni. Az így kialakított felelősségeket az *Információs vagyonleltár* nyilvántartás tartalmazza.

5.1.2 A VAGYONELEMEK FELELŐSEI

A vagyonleltárban szereplő vagyonelemek esetében be kell tölteni a gazdaszerepet.

A Társaság központi infrastruktúra elemek, az alkalmazottaknak munkavégzés céljából átadott informatikai eszközök és egyéb irodai berendezések a Társaság tulajdonát képezik.

A vagyonelemeket minden esetben felelőshöz kell kötni, amelynek rendje az alábbi:

- Az egyéni felhasználású vagyonelemek átvételét az egyéni felhasználók aláírásukkal igazolják.
- A közös felhasználású vagyonelemekért az anyagnem felelősök felelnek:
    - IT eszközök és anyagok: **Kontrolling és beszerzési igazgató**
    - Bútorok és berendezési tárgyak: **Elnök-Vezérigazgató**
    - Kulcsos autó(k) kulcshozzáférése: **Kontrolling és beszerzési igazgatót**

A felelősök feladatai az alábbiak:

- Vagyonelemek megőrzése, rendeltetésszerű használatának biztosítása
- Vagyonelemek karbantartása
- Vagyonelemek leltárkori elszámolása

5.1.3 A VAGYONELEMEK ELFOGADHATÓ HASZNÁLATA

Az információk, valamint az információkkal és információ-feldolgozó eszközökkel kapcsolatos vagyonelemek elfogadható használatára vonatkozó szabályokat azonosítani kell, dokumentálni kell és be kell vezetni.

A Társaság tulajdonát képező eszközök rendeltetésszerű és a gyártói ajánlásoknak megfelelő használatáért a Társaság teljes állománya felel. Az eszközök esetleges elvesztéséről, vagy azok bármilyen károsodásáról a **Kontrolling és beszerzési igazgató** vagy az **Elnök-Vezérigazgatót** tájékoztatni kell.

Az egyes vagyonelemek használatára vonatkozó speciális szabályokat a *„Berendezés”* fejezet tartalmazza.

Az IT infrastruktúra elemeket fix helyen kell tárolni, melyről csak szervizelés esetén szabad az eszközöket elmozdítani.

Az adathordozó eszközök használatával az *„Adathordozók kezelése”* fejezet foglalkozik.

A munkaállomások és mobil eszközök használatával a *„Mobil eszközök és távmunka”* fejezet foglalkozik.

5.1.4 A VAGYONELEMEK VISSZASZOLGÁLTATÁSA

Minden alkalmazottnak és a külső felek felhasználóinak vissza kell szolgáltatniuk a birtokukban lévő, összes szervezeti vagyonelemet, ha megszűnik a munkaviszonyuk, szerződésük vagy megállapodásuk.

A munkaviszony vagy egyéb szerződéses viszony megszűnésekor a vagyonelemeket vissza kell szolgáltatni a Társaság részére.

A Társaság tulajdonát képező vagyonelemeket a vagyonelemért felelős munkatársnak kell átvennie „*A vagyonelemek felelősei”* fejezet alapján.

A visszaadott munkaállomásokon maradt szervezeti adatok törlése tilos, azokat minimálisan 10 napig meg kell őrizni, hogy a folyamatban lévő tevékenységek kapcsán a **Szakterületi vezetők** a szükséges dokumentumokhoz még hozzá tudjanak férni. A 10 munkanap letelte után az adott szakterület vezetője rendelheti el a munkaállomások háttértárolójának törlését. A kilépő személy levelezési postafiókjához hozzáférést kell biztosítani az érintett **Szakterületi vezető** számára. A kilépő személy felhasználói fiók jelszavát a **Kontrolling és beszerzési igazgatónak** vagy az ő döntése alapján a **Rendszerkoordinátornak** meg kell változtatni.

A Társaság tulajdonát képező tabletek és mobiltelefonok leadásakor gyári visszaállítást kell végrehajtani, a hozzájuk tartozó SIM kártyák PIN kódját a gyári értékre kell beállítani, melyet a **Kontrolling és beszerzési igazgatónak** vagy az ő döntése alapján a **Rendszerkoordinátornak** kell ellenőrizni.

5.2 INFORMÁCIÓOSZTÁLYOZÁS

5.2.1 AZ INFORMÁCIÓK OSZTÁLYOZÁSA

Az információkat osztályozni kell a jogi követelmények, az értékük, a kritikusságuk, valamint a jogosulatlan nyilvánosságra hozásra és módosításra való érzékenységük szerint.

Az információosztályozás célja, hogy a különböző osztályozási kategóriába sorolt adatokhoz, illetve a kezelésüket megvalósító eszközökhöz különböző szintű, kockázatarányos védelmi intézkedéseket, eljárásokat lehessen meghatározni.

Az információosztályozást az Adatgazdák éves rendszerességgel elvégzik, illetve felülvizsgálják az Információbiztonsági felelős közreműködése és iránymutatása alapján.

Az információkat bizalmasság, sértetlenség és rendelkezésre állás szerint osztályozni kell, amelyet az alábbi négy szinten kell megvalósítani.

Osztályozási szintek	Bizalmasság (B)	Sértetlenség (S)	Rendelkezésre állás (R)
1	Nyilvános	Nem védett	Általános
2	Belső használatú	Védett	Fontos
3	Bizalmas	Fokozottan védett	Kiemelten fontos
4	Szigorúan bizalmas	Kiemelten védett	Kritikus

1. Információbiztonsági osztályok

Az adat keletkezésekor, vagy beérkezésekor a felhasználónak meg kell határozni, hogy melyik adatkörbe sorolható, amelynek adatosztályozását az **Adatkezelő** elvégezte. Amennyiben a keletkezett, vagy beérkezett adat egyetlen adatkörbe se sorolható, értesíteni kell az **Információbiztonsági felelőst**, aki gondoskodik annak adatosztályozásáról.

5.2.2 BIZALMASSÁGI SZINTEK KÖVETELMÉNYEI

Kategória	Definíció	Követelmények
B-1	**Nyilvános** adat, melynek társadalmi nyilvánosságra kerülése elhanyagolható, a Társaság érdekeit semmilyen módon nem sérti.	Nincs meghatározott követelmény.
B-2	**Belső használatú** adat, melynek társadalmi nyilvánosságra kerülése legalább jelentős kár és szervezeten belüli nyilvánosságra kerülése elhanyagolható, tartalmát kizárólag a Társaság munkavállalói ismerhetik meg.	Csak a Társaság felhasználója kaphat hozzáférést az adathoz. Felhasználó hitelesítés szükséges.
B-3	**Bizalmas adat**, melynek szervezeten belüli nyilvánosságra kerülése legalább jelentős kár, tartalmát kizárólag adott szakterületek ismerhetik meg (pl. HR adatok, partnerek adatai stb.).	A B-2 követelményeken felül csoport szintű jogosultságokkal szükséges biztosítani a védendő adatok bizalmasságát.

Kategória	Definíció	Követelmények
B-4	**Szigorúan bizalmas** minden olyan fontos tény, információ, adat és megoldás, amelynek titokban maradásához a Társaságnak és partnereinek méltányolható érdeke fűződik, és amelyet üzleti titokká minősített. Hozzáférés kizárólag a felső szintű vezetők (Elnök-Vezérigazgató, Tulajdonosok) engedélyével történhet.	A B-3 követelményeken felül titkosítási megoldást kell alkalmazni az adatok tárolása, illetve továbbítása során.

2. Bizalmassági szintek követelményei

5.2.3 SÉRTETLENSÉGI SZINTEK KÖVETELMÉNYEI

Kategória	Definíció	Követelmények
S-1	**Nem védett** adat, mely hitelességének sérülése elhanyagolható kár.	Nincs meghatározott követelmény.
S-2	**Védett** adat, melynek illetéktelen törlése legalább jelentős kár.	Felhasználó hitelesítés szükséges.
S-3	**Fokozottan védett** adat, melynek illetéktelen módosítása legalább jelentős kár.	Az S-2 követelményeken felül csoport szintű jogosultságokkal szükséges biztosítani a védendő adatok bizalmasságát, továbbá az adatok nem kívánt módosítása érdekében az adathoz való írási jogot csak korlátozott számú felhasználó kaphat.
S-4	**Kiemelten védett** adat, melynek illetéktelen törlése vagy módosítása legalább súlyos kár.	Az S-3 követelményeken felül az **Elnök-Vezérigazgató** szintje alatt alkalmazni kell a négy-szem elvet az adatok módosítása során.

3. Sértetlenségi szintek követelményei

5.2.4 RENDELKEZÉSRE ÁLLÁSI SZINTEK KÖVETELMÉNYEI

Kategória	Rendelkezésre állási követelmények		Maximális adatvesztési követelmények
	Min. éves rendelkezésre állás	Max. kiesési idő	
R-1	95%	1 hét	Nincs meghatározott követelmény
R-2	97,5%	1 nap	1 hét
R-3	99%	0,5 nap	1 nap
R-4	99,5%	2 óra	0,5 nap

4. Rendelkezésre állási szintek követelményei

Az osztályozási szinteknek megfelelően besorolt adatokat „*A vagyonelemek kezelése”* alfejezetben szereplő táblázat szerint kell kezelni.

5.2.5 AZ INFORMÁCIÓK MEGJELÖLÉSE

Megfelelő eljárásokat kell kialakítani és bevezetni az információk megjelölésére a szervezet által elfogadott információosztályozási módszerrel összhangban.

Az információk megjelölését az alábbi eljárásoknak megfelelően el kell végezni:

- Elektronikus dokumentumok esetén a fejlécbe jelezni kell annak bizalmassági szintjét.
- Az ügyfélnek készített dokumentumokra az ügyfél szerinti adat kategóriát kell jelölni, amennyiben az magasabb, mint a Társaság belső kategória.
- Papír alapú dokumentációnál a legalább B3 adatbiztonsági kategória esetén rá kell pecsételni a dokumentum első oldalára a „bizalmas” feliratot.

5.2.6 A VAGYONELEMEK KEZELÉSE

A vagyonelemek kezelésére eljárásokat kell kialakítani és bevezetni a szervezet által elfogadott információosztályozási módszerrel összhangban.

	Nyilvános vagy Nem védett	Belső használatú vagy Védett	Korlátozott használatra vagy Fokozottan védett	Üzleti titok vagy Kiemelten védett
Tárolás	Nincs követelmény.	Csak a Társaság által hozzáférhető tárhelyeken kell tárolni.	Személyes, vagy korlátozott hozzáférésű mappában kell tárolni	Titkosított mappában kell tárolni.
Adatátvitel	Nincs követelmény.	A Társaságon kívülre jelszóvédett állományban kell küldeni.	A Társaságon kívülre jelszóvédett állományban kell küldeni.	A fájl titkosításával kell küldeni.
Adatmegosztás	Nincs követelmény.	A Társaság központi tároló helyén nyilvános mappában is megosztható.	Az adott szakterület vezetője által jóváhagyott jogosultsági rend szerint osztható meg.	Nem megosztható
Megsemmisítés, törlés	Nincs követelmény.	Csak az **Adatkezelő** engedélyével törölhető, vagy iratmegsemmisítővel semmisíthető meg.	Csak az **Adatkezelő** engedélyével törölhető, vagy iratmegsemmisítővel semmisíthető meg.	Csak az **Adatkezelő** engedélyével törölhető, vagy iratmegsemmisítővel semmisíthető meg.
Felülvizsgálat	Nincs követelmény.	Minimálisan évente a törvényi előírások figyelembevételével.	Minimálisan évente a törvényi előírások figyelembevételével.	Minimálisan évente a törvényi előírások figyelembevételével.
Szállítás	Nincs követelmény.	Nem látható helyen, gépjármű csomagtartójában. Amennyiben harmadik fél által történik a szállítás, akkor csakis zárt borítékban kerülhet átadásra.	Nem látható helyen, gépjármű csomagtartójában. Amennyiben harmadik fél által történik a szállítás, akkor csakis zárt borítékban kerülhet átadásra.	Az **Elnök-Vezérigazgató** engedélyével lehetséges. Nem látható helyen, gépjármű csomagtartójában.

5. *A vagyonelemek adatosztályok szerinti kezelése (bizalmasság és sértetlenség)*

	R1	R2	R3	R4
Hibatűrés	Nincs	Nincs	Nincs	Eszköz szintű (pl. klaszter)
Szünetmentes tápellátás	Nincs	Nincs	Nincs	UPS 20 perc áthidalással
Adatmentés gyakorisága	Nincs	1 nap	1 nap	online szinkron

6. A vagyonelemek adatosztályok szerinti kezelése (rendelkezésre állás)

5.3 ADATHORDOZÓK KEZELÉSE

5.3.1 A PAPÍR ALAPÚ ADATHORDOZÓK KEZELÉSE

A papír alapú adathordozók kezelésére vonatkozó követelményeket a Társaság *Iratkezelési szabályzata tartalmazza,* melyet az *„Információosztályozás”* fejezettel összhangban kell tartani.

5.3.2 A CSERÉLHETŐ ADATHORDOZÓK KEZELÉSE

Eljárásokat kell megvalósítani a cserélhető adathordozók kezelésére a szervezet által elfogadott információosztályozási módszerrel összhangban.

A cserélhető adathordozók tárolására nézve be kell tartani a gyártó által meghatározott, a környezeti paraméterekre és tárolási feltételekre vonatkozó ajánlásokat.

Az adatok biztonsága érdekében a cserélhető adathordozókon a legalább B-2 és S-2 adatbiztonsági kategóriába sorolt adatokat csak a szükséges időtartamra szabad tárolni, amennyiben szükségtelenné válnak, törölni kell őket. Továbbá be kell tartani az *„Információosztályozás”* fejezetben leírtakat, különös tekintettel a tárolás, a szállítás és a megosztás részekre.

5.3.3 ADATHORDOZÓK ELTÁVOLÍTÁSA

Formális eljárások alkalmazásával kell az adathordozókat biztonságosan eltávolítani, ha többé már nincs szükség rájuk.

Olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért selejtezni kell:

- A fizikailag sérült, javíthatatlan, a gyári, raktározási hibából követően felhasználásra alkalmatlan (deformálódott) adathordozót
- véglegesen elhasználódott anyagot.

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni.

Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adathordozókról, törlő programokkal kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

A selejtezésről (3 példányban) jegyzőkönyvet kell készíteni, melynek az alábbi adatokat kell tartalmaznia:

- A selejtezendő adathordozók tulajdonosának megnevezését,
- a selejtezés időpontját,
- milyen adathordozók, és azok mely adatai kerülnek selejtezésre,
- a selejtezést végzők aláírását.
- A selejtezési jegyzőkönyvek nem selejtezhetőek.

Titkos adatokat tartalmazó adathordozókat selejtezni nem lehet, ezen adatokat tartalmazó adathordozókat külön utasítás szerint kell kezelni.

Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni. (Az üzemi másolás nem minősül másolásnak.)

A biztonsági, illetve az archív adatállomány előállítása másolásnak számít.

5.3.4 FIZIKAI ADATHORDOZÓK SZÁLLÍTÁSA

Az információkat tartalmazó adathordozókat védeni kell a jogosulatlan hozzáféréstől, visszaéléstől vagy megrongálódástól a szállítás során.

A legalább B-2 és S-2 adatbiztonsági kategóriába sorolt információkat tároló adathordozók szállítását úgy kell megoldani, hogy azok felügyelet nélkül soha nem maradhatnak.

Az adathordozó szállítása közben is biztosítani kell az adathordozó gyártója által meghatározott környezeti paramétereket. Általában az adathordozókat magas hőnek, fröccsenő víznek, fizikai behatásnak, mágneses adathordozó esetén elektrosztatikus, és mágneses térnek kitenni is tilos.

Az adathordozó eszközöket tilos a gépjárműben látható helyen szállítani, helyette csomagtartóba kell elhelyezni.

A fizikai adathordozók szállítására az *„Információosztályozás”* fejezet *Vagyonelemek kezelésére* vonatkozó táblázatban szereplő követelmények betartása kötelező.

5.3.5 FIZIKAI ADATHORDOZÓK LELTÁROZÁSA

Az adathordozókat a Leltározási szabályzatban foglaltaknak megfelelően kell leltározni.

A beszerzett, illetve üzemeltetett hardver és szoftver eszközök leltározása a Kontrolling és beszerzési Igazgatóság feladata.

6 HOZZÁFÉRÉS-FELÜGYELET

6.1 A HOZZÁFÉRÉS-FELÜGYELETTEL KAPCSOLATOS ÜZLETI KÖVETELMÉNYEK

6.1.1 SZABÁLY A HOZZÁFÉRÉS-FELÜGYELETRE

Hozzáférés-felügyeleti szabályt kell létrehozni, dokumentálni és megvizsgálni az üzleti és az információbiztonsági követelmények alapján.

A központi fájlmegosztásról külön szerepkör alapú jogosultság hozzáférési szabályozást kell kialakítani.

A szerepkörökbe történő besorolásról és jogosultságokról a **Kontrolling és beszerzési igazgatónak** vagy az ő döntése alapján a **Rendszerkoordinátornak** kell évente riportot készíteni az egyes szakterületi vezetők számára, akiknek ez alapján felül kell vizsgálni az adott szerepkörbe tartozó személyek körét és jogosultságaikat. Amennyiben a **Szakterületi vezető** döntése alapján a jogosultsági besorolásról és a személyekhez köthető szerepkörökben változást kezdeményez, arról a **Kontrolling és beszerzési igazgatót** értesíteni kell. Ezekről a döntésekről minden esetben a **Kontrolling és beszerzési igazgató** belátása szerint értesíti a **Rendszerkoordinátort, illetve az Információbiztonsági felelőst.**

A többi rendszer esetén a **Kontrolling és beszerzési igazgatónak** vagy az ő döntése alapján a **Rendszerkoordinátornak** kell évente riportot készíteni az **Információbiztonsági felelős** számára, akinek ez alapján felül kell vizsgálni a felhasználói és kiemelt jogosultságokat.

Hozzáférés hálózatokhoz és hálózati szolgáltatásokhoz

A felhasználókat csak olyan hálózatokhoz és hálózati szolgáltatásokhoz való hozzáféréssel szabad ellátni, amelyek használatára kifejezetten fel lettek jogosítva.

A Társaságnál a hozzáférési jogosultságok kialakítását szabályozó követelmények a következők:

- A hozzáférési jogosultságokat az adatok osztályozásával összhangban kell megállapítani. Az adatok besorolási eljárásáról az *„Információosztályozás”* fejezet a mérvadó.
- A hozzáférési jogosultságok kiadását és visszavonását minden esetben csoporttagságok alapján kell végrehajtani.
- Az optimális hozzáférési rendszer kialakításához minél kevesebb, a feladathoz kapcsolódóan minimális jogokkal rendelkező felhasználói csoport kialakítása szükséges. A csoportok kialakítását a Társaság szervezeti felépítéshez igazodva kell elvégezni.
- A felhasználói csoportok jogosultsági körét az általuk végzett feladatokhoz képest úgy kell minimalizálni, hogy a felhasználónak csak a munkaköri feladataik elvégzéséhez szükséges minimális hozzáférési jogok álljanak rendelkezésre.
- A felhasználókat valamennyi általuk használt rendszerben egyedileg azonosítani kell.
- A felhasználók azonosítását egy egyedi, titkos információval kell hitelesíteni (legalább jelszó). Ez alól csak a csoportos azonosítású hozzáférések a kivételek, melyekre az *„A felhasználói hozzáférések kezelése”* fejezet a mérvadó.

- A jogosultsági rendszer kialakításánál figyelembe kell venni a védelemre vonatkozó szerződésszerű kötelezettségeket, melyben az adatokhoz, vagy alkalmazásukhoz való hozzáférésről esik szó.
- Egyedi, személyre szabott hozzáférési jogokat kell alkalmazni, a felhasználói azonosítókat nem szabad megosztani a felhasználók között.
- Ideiglenes jogok meghatározása külső személyek számára csak a tevékenységükhöz szükséges mértékben történhet, kizárólag korlátozott időtartamig. Munkájuk végén, vagy az előre meghatározott időtartam lejárta után a jogokat azonnal meg kell vonni.

A követelmény rendszert évente felül kell vizsgálni és javított formában a **Kontrolling és beszerzési igazgatónak** vagy az ő döntése alapján a **Rendszerkoordinátor** számára is át kell adni. A felülvizsgálatot az **Információbiztonsági felelős** végzi.

6.2 A FELHASZNÁLÓI HOZZÁFÉRÉSEK KEZELÉSE

6.2.1 FELHASZNÁLÓK REGISZTRÁLÁSA ÉS TÖRLÉSE

Formális felhasználóregisztrálási és -törlési folyamatot kell megvalósítani a hozzáférési jogok felhasználók számára történő kiosztása érdekében.

Az érintett **Szakterületi vezetőnek** kell kezdeményezni az új vagy ideiglenes felhasználó fiókjának létrehozását, melyhez a jogosultsági rendtől eltérő jogosultsági kérés esetén az **Információbiztonsági felelős** véleményezése is szükséges. Jóváhagyás után az IT Szolgáltató feladata a felhasználói fiók létrehozása, a kezdeti próbaidős csoporthoz hozzárendelve. Az új munkatárs a teljes szerepkör szerinti jogosultságokat csak a próbaidő lejárta után kaphatja meg, melyet a **Szakterületi vezető** kezdeményez, és az IT Szolgáltató állít be.

Az alkalmazott kilépésének utolsó napján az érintett **Szakterületi vezetőnek,** vagy annak kilépése esetén az Elnök-Vezérigazgatónak értesítenie kell az IT Szolgáltatót a kilépés tényéről. Az érintett felhasználó címtár profilját az IT Szolgáltatónak azonnal le kell tiltania.

Amennyiben adminisztrátor jogkörrel rendelkező alkalmazott távozik, akkor a csoportos adminisztrátori jelszavakat az IT Szolgáltatónak meg kell változtatnia, a Kontrolling és beszerzési igazgatónak értesítenie kell a többi adminisztrátor jogkörrel rendelkező alkalmazottat.

6.2.2 FELHASZNÁLÓI HOZZÁFÉRÉS BIZTOSÍTÁSA

Formális folyamatot kell megvalósítani a felhasználói hozzáférések biztosítására, hogy a hozzáférési jogok kiosztása és visszavonása minden felhasználói típus, minden rendszer és szolgáltatás esetében megtörténhessen.

Munkaviszony kezdetekor, vagy munkakör megváltozása esetén a munkavállalók a *jogosultságnyilvántartások* alapján kell, hogy jogosultságaikat megkapják. A próbaidős kollégák csak azokat a jogosultságokat kaphatják meg, amelyekkel próbaidejük alatt dolgozniuk kell.

Jogosultság változtatási igényt az érintett **Szakterületi vezető** kezdeményezhet, melyet a jogosultsági rendtől (*jogosultságnyilvántartások*) eltérő jogosultsági kérés esetén az **Elnök-Vezérigazgató** hagy jóvá, majd az IT Szolgáltató állít be. Az **Információbiztonsági felelős**

felülbírálhatja a jóváhagyást abban az esetben, ha a biztonsági irányelvek és a lehetséges kockázatok ezt indokolják. Ezt követően értesíteni kell a beállítás tényéről az érintett **Szakterületi vezetőt**.

A *jogosultságnyilvántartásokat* előzetesen az **Elnök-Vezérigazgató** hagyja jóvá.

6.2.3 KIEMELT HOZZÁFÉRÉSI JOGOK KEZELÉSE

Korlátozni és felügyelni kell a kiemelt hozzáférési jogok kiadását és használatát.

A munkatársak kiemelt (adminisztrátori) jogosultságait a lehető legszűkebb körben kell kiosztani. A kiemelt jogosultságok kiosztásának elbírálása minden esetben az **Elnök-Vezérigazgató** döntését igényli, mely döntés meghozatalához mérlegelni kell a felmerülő igényeket és a kiemelt jogosultság kiosztásával járó esetleges biztonsági kockázatokat.

Kiemelt hozzáférések esetén nevesített felhasználói fiókokra kell törekedni. Ahol ez nem lehetséges, ott szükség esetén csoportos azonosítókat lehet használni.

Adminisztrátori hozzáférést (például a **Rendszer koordinátor** távollétében kell egy kollégának munkát végezni a rendszeren) az érintett **Szakterületi vezető** kezdeményezhet, melyet az **Elnök-Vezérigazgató** hagy jóvá, majd az IT Szolgáltató állít be. Ezt követően értesíteni kell az érintett **Szakterületi vezetőt** a beállítás tényéről.

6.2.4 A FELHASZNÁLÓK TITKOS HITELESÍTÉSI INFORMÁCIÓINAK KEZELÉSE

A felhasználók titkos hitelesítési információinak kiadását felügyelet alatt kell tartani egy formális kezelési folyamat segítségével.

A felhasználók hitelesítésének felhasználónévvel és jelszóval kell történnie, melyet a központi címtár kezel.

Minden munkavállaló számára kötelező a hitelesítési adataik titokban tartása.

A jelszavak használatára vonatkozó követelményeket a *„Felhasználói felelősségek”* fejezet tartalmazza.

6.2.5 A FELHASZNÁLÓI HOZZÁFÉRÉSI JOGOK ÁTVIZSGÁLÁSA

A vagyonelemek gazdáinak rendszeres időközönként át kell vizsgálniuk a felhasználók hozzáférési jogosultságait.

A munkatársak számára kiosztott általános és kiemelt jogosultságokat évente felül kell vizsgálni. A felülvizsgálat során meg kell győződni a meglévő jogosultságok érvényességéről. A felülvizsgálatot az **Információbiztonsági felelőssel végzi együttműködve az IT Szolgáltatóval, előzetesen konzultálva a vezetőséggel**.

6.2.6 A HOZZÁFÉRÉSI JOGOK VISSZAVONÁSA VAGY MÓDOSÍTÁSA

Minden alkalmazott és a külső felek összes felhasználója esetében a hozzáférési jogokat az információkhoz és az információfeldolgozó eszközökhöz vissza kell vonni a munkaviszony, a szerződés vagy a megállapodás megszűntetésekor, illetve módosítani kell változás esetén.

A jogosultságok visszavonása és módosítása az IT Szolgáltató feladatköre. Minden munkatárs és külső fél esetében a jogosultságokat vissza kell vonni a munkaviszony, a szerződés, vagy a megállapodás megszüntetésekor, illetve módosítani kell munkakör megváltozása esetén, melyhez az érintett **Szakterületi vezető** jóváhagyása szükséges.

A visszavonás folyamatát az „A munkaviszony megszűnése és megváltozása” fejezet tartalmazza.

6.3 FELHASZNÁLÓI FELELŐSSÉGEK

6.3.1 TITKOS HITELESÍTÉSI INFORMÁCIÓK HASZNÁLATA

A felhasználóktól meg kell követelni, hogy tartsák be a szervezet gyakorlatát a titkos hitelesítési információk használata során.

A Társaságnál három féle hozzáférési szintet különböztetünk meg:

1. Felhasználói hozzáférés
2. Névre szóló adminisztrátori hozzáférés
3. Csoportos adminisztrátori hozzáférés

A **kezdeti jelszavakat** a **Kontrolling és beszerzési igazgató** előzetes jelzése alapján az IT Szolgáltató állítja be és osztja meg SMS-ben az érintett **felhasználóval**.

Valamennyi informatikai rendszer esetén a hozzáférésekhez rendelt jelszavaknak, a hozzáférés szintjétől függetlenül az alábbi alapkritériumoknak kell megfelelni:

- Ne egyezzen meg a felhasználó nevével, telefonszámával, személyi számával, valamint a felhasználóhoz kötődő bármely karaktersorozattal (pl. születési dátum, lakcím).
- Ne egyezzen meg személynévvel.
- Ne egyezzen meg irodalmi, színházi, televíziós, közéleti személyek nevével és egyéb közismert szavakkal, kifejezésekkel.
- Ne tartalmazzon azonos, vagy ismert logika szerint egymást követő karaktereket (pl. 11111, aaaaa, qwert, asdfg, gegegeg).
- Ne utaljon a felhasználóra, munkakörére, munkahelyére.
- Ne legyen könnyen kitalálható, szótárban szereplő.

A felhasználói hozzáféréshez rendelt jelszavakkal szemben támasztott követelmények:

- A hálózati és alkalmazásokhoz tartozó jelszavaknak legalább 8 karakterből kell állniuk és tartalmazniuk kell kis- és nagybetűket, valamint számokat.
- A jelszavak nem lehetnek azonosak a felhasználó névvel, annak becézett formájával, vagy könnyen visszafejthető kifejezéssel.
- A hálózatba kötött számítógépek esetében a felhasználóknak a hálózati, illetve ennek hiánya esetén helyi bejelentkezési jelszavakat három havonta meg kell változtatniuk.
- Ahol ezt az operációs rendszer támogatja, 10 sikertelen bejelentkezés után az operációs rendszernek le kell tiltani a felhasználó fiókját.
- A jelszó megváltoztatásakor az új jelszó nem lehet azonos a korábban használt jelszóval.
- A jelszót más személlyel megosztani tilos.

- A felhasználók jelszavát a felhasználón kívül senki sem ismerheti.
- A jelszót soron kívül meg kell változtatni, ha az illetéktelen személy tudomására jutott, vagy juthatott.

A Társaság munkatársai számára kötelezően betartandó, hogy a napi munkavégzés során használt hitelesítési adataik védelméről gondoskodjanak. Tilos a Társaság erőforrásainak hozzáféréséhez szükséges felhasználóneveket és jelszavakat elárulni, mások számára látható módon feltűntetni.

A titkos hitelesítési információk biztonságos használatáról nagyobb változások esetén oktatást kell tartani, mely az **Információbiztonsági felelős** feladata.

6.4 RENDSZER- ÉS ALKALMAZÁS- HOZZÁFÉRÉS FELÜGYELETE

6.4.1 INFORMÁCIÓHOZ VALÓ HOZZÁFÉRÉS KORLÁTOZÁSA

A hozzáférés-felügyeleti szabály szerint korlátozni kell az információkhoz és az alkalmazási rendszerek funkcióihoz való hozzáférést.

A Társaság rendszereihez és alkalmazásaihoz való illetéktelen logikai hozzáférés megakadályozására jelszavas védelmet kell alkalmazni. A felhasználók kötelesek a bejelentkező nevükhöz tartozó jelszavakat megőrizni. A saját bejelentkező névhez tartozó jelszót elárulni, mások által is elérhető módon feljegyezni tilos!

A Társaság minden alkalmazottjára nézve kötelező a *„Felhasználói felelősségek”* fejezetben szereplő követelményeknek megfelelő jelszavak használata a szervezeti eszközök és szolgáltatások hitelesítéséhez.

Amennyiben egy jelszó illetéktelen személy tudomására jutott, vagy bármilyen módon nyilvánosságra került, azt a jelszót a **Kontrolling és beszerzési igazgatónak** vagy az ő döntése alapján a **Rendszerkoordinátornak**, vagy a jelszó gazdájának azonnal meg kell változtatnia. Az esetet az **Információbiztonsági felelős** tudomására kell hozni, aki arról incidenskezelési űrlapot tölt ki, majd ki kell vizsgálnia, milyen körülmény vezetett a jelszó kompromittálódásához.

6.4.2 BIZTONSÁGOS BEJELENTKEZÉSI ELJÁRÁSOK

Ahol azt a hozzáférés-felügyeleti szabály megköveteli, a rendszerekhez és alkalmazásokhoz való hozzáférést egy biztonságos bejelentkezési eljárással kell felügyelet alatt tartani.

A belső rendszerekbe történő belépéskor a központi címtárat kell használni – amennyiben az adott alkalmazás/szolgáltatás képes rá –, ettől eltérni csak a **Kontrolling és beszerzési igazgató** jóváhagyásával lehet.

A külső megbízható szakmai rendszerek (például képző központok, konferencia központok stb.) esetén a céges e-mail címmel történő regisztráció ajánlott, ettől eltérni csak az **Kontrolling és beszerzési igazgató** engedélyével lehet.

A nem szervezethez, hanem személyhez köthető regisztrációk esetén engedélyezett a privát bejelentkezési információk használata.

6.4.3 JELSZÓKEZELŐ RENDSZER

Az **Elnök-Vezérigazgató** által használt jelszavak tárolásához olyan jelszókezelő rendszert kell alkalmazni, amely megfelelő védelemmel látja el a Társaság birtokában lévő titkos hitelesítési információkat.

A jelszókezelő program használatával szemben támasztott követelmények:

- Jelszócsere esetén szükséges a jelszókezelő programban tárolt jelszavakat frissíteni.
- A jelszavakat védő mesterjelszót úgy kell megválasztani, hogy eleget tegyen a jelszavakkal szemben támasztott alapkritériumoknak és megfeleljen az alábbi követelményeknek is:
    - A jelszó minimális hossza 12 karakter.
    - A jelszónak tartalmaznia kell a kisbetű, nagybetű, szám és speciális karakter kategóriákból legalább hármat.

6.4.4 KIEMELT JOGOKKAL BÍRÓ SEGÉDPROGRAMOK HASZNÁLATA

Az olyan kiemelt jogokkal bíró segédprogramok használatát, melyek képesek lehetnek arra, hogy felülírják a rendszer- és alkalmazásszintű védelmi intézkedéseket, korlátozni kell, és szoros felügyelet alatt kell tartani.

Rendszerkoordinátori és technikai felhasználót csak az azt megkövetelő műveletekhez szabad alkalmazni.

A technikai felhasználók jogkörét úgy kell kialakítani, hogy csak a szükséges jogosultságokkal rendelkezzenek, melyet a **Kontrolling és beszerzési igazgatónak** vagy az ő döntése alapján a **Rendszerkoordinátornak** évente felül kell vizsgálni.

6.4.5 A PROGRAMOK FORRÁSKÓDJÁHOZ VALÓ HOZZÁFÉRÉS FELÜGYELETE

A Társaság sem belső sem külső erőforrásokkal nem fejleszt alkalmazásokat, ezért ezt a fejezetet kizártuk az alkalmazhatóságból.

Korlátozni kell a programok forráskódjához való hozzáférést.

7 TITKOSÍTÁS

7.1 TITKOSÍTÁSI INTÉZKEDÉSEK

7.1.1 SZABÁLY A TITKOSÍTÁSI INTÉZKEDÉSEK TÉTELÉRE

Az információk védelme érdekében ki kell alakítani és be kell vezetni egy titkosítási intézkedések tételére vonatkozó szabályt.

Titkosítási eljárásokkal védjük a legalább B-3 és S-3 adatbiztonsági kategóriába sorolt adataink bizalmasságát és sértetlenségét.

A Társaság által jóváhagyott titkosítási megoldás a 7-Zip, melyet jelszavas védelemmel kell ellátni.

Az üzleti partnerek dokumentumainak titkosítására használt program minden esetben a partnerek igényei alapján kerül kiválasztásra. Az ilyen módon titkosított állományokat elektronikus levélben, vagy személyesen pendrive-on kell kézbesíteni.

A dokumentumok titkosításához rendelt jelszavakkal szemben támasztott követelmények:

- A jelszavak minimális hossza 8 karakter.
- A jelszavaknak tartalmaznia kell kis- és nagybetűt, számot és speciális karaktert.

7.1.2 KULCSKEZELÉS

A Társaság egy külső, harmadik fél által hitelesített tanúsítvánnyal rendelkezik, mely a www.kartonpack.hu domain névre lett kiállítva. A tanúsítvány negyedéves időtartamra szól.

8 FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG

8.1 BIZTONSÁGI TERÜLETEK

8.1.1 FIZIKAI BIZTONSÁGI HATÁR

Fizikai határokat kell megadni és alkalmazni, hogy megvédjék az olyan területeket, ahol érzékeny vagy kritikus információk vagy információ-feldolgozó eszközök helyezkednek el.

A Társaság fizikai biztonságának határát a teljes intézménytér képezi. Azon belül biztonsági zónákat kell kialakítani annak érdekében, hogy a fizikai és környezeti biztonság több fokozatban valósulhasson meg.

A biztonsági zónákat a bennük folyamatosan tárolt információk bizalmasságára, sértetlenségére és rendelkezésre állására vonatkozó osztályozási szintek alapján, illetve az információkezelő eszközök kockázati besorolása alapján kell kialakítani.

A Társaság telephelyei:

- 1024 Budapest, Ady Endre utca 19. A. ép.
- 4030 Debrecen, Galamb utca 11.

A Társaságnál négy biztonsági zónát kell megkülönböztetni:

- **1. szintű biztonsági zóna**: Termelőüzem, illetve minden felhasználó számára elérhető területek.
- **2. szintű biztonsági zóna**: Raktár, műszaki előkészítő.
- **3. szintű biztonsági zóna**: Műszaki vezetőség, irodák és vezetői irodák.
- **4. szintű biztonsági zóna**: Technikai helyiség (switch).

A Társaság budapesti telephelyén csak vezetői irodák találhatók, így az a 3. számú biztonsági zónába sorolandó.

8.1.2 FIZIKAI BELÉPTETÉSI INTÉZKEDÉSEK

A biztonsági területeket megfelelő beléptetési intézkedésekkel kell védeni annak érdekében, hogy csak az arra jogosult személyek léphessenek be oda.

Az egyes zónákon belül külön beléptetési követelmények kell definiálni.

Zóna követelmények	1. szintű zóna	2. szintű zóna	3. szintű zóna	4. szintű zóna
Belépés, beléptetés	A beléptetés portaszolgálaton keresztül történik. A belépő személyt a portás azonosítja.	Külön kulcs, a kulcs a portán vehető fel. A kulcs naplózása folyamatos (felvétel-leadás).	Külön kulccsal zárható.	Külön kulcs, a kulcs a portán vehető fel. A kulcs naplózása folyamatos (felvétel-leadás).

7. Fizikai beléptetési intézkedések

8.1.3 IRODÁK, HELYISÉGEK ÉS LÉTESÍTMÉNYEK VÉDELME

Az irodák, helyiségek és létesítmények fizikai védelmét meg kell tervezni, és azt alkalmazni kell.

Az egyes zónákon belül külön védelmi követelmények kerültek kialakításra, melyeket az alábbi táblázat tartalmaz.

Zóna követelmények	1. szintű zóna	2. szintű zóna	3. szintű zóna	4. szintű zóna
Tűzvédelem	Porral oltó berendezések biztosítottak.	Füstérzékelő berendezés. Porraloltó berendezések biztosítottak.	Budapest: Füstérzékelő berendezés. Porral oltó berendezések biztosítottak. Debrecen: Porral oltó berendezések biztosítottak.	Porral oltó berendezések biztosítottak.
Biztonsági felügyelet	0-24 órás élő erős portaszolgálat.	0-24 órás élő erős portaszolgálat.	Budapest: 8-20 órás recepció. Debrecen: 0-24 órás élő erős portaszolgálat.	0-24 órás élő erős portaszolgálat.
Riasztórendszer	Nincs.	Nincs.	Nincs.	Nincs.

8. Irodák, helyiségek és létesítmények védelme

8.1.4 KÜLSŐ ÉS KÖRNYEZETI FENYEGETÉSEKKEL SZEMBENI VÉDELEM

A természeti katasztrófák, a rosszindulatú támadás vagy a balesetek elleni fizikai védelmet meg kell tervezni, és azt alkalmazni kell.

Az egyes zónákon belül külön követelmények kerültek kialakításra, melyeket az alábbi táblázat tartalmaz.

Zóna követelmények	1. szintű zóna	2. szintű zóna	3. szintű zóna	4. szintű zóna
Természeti katasztrófák kockázatainak csökkentése	Villámvédelem.	Villámvédelem.	Villámvédelem.	Villámvédelem.
Klimatizálás	Nincs.	Raktár: Nincs. Műszaki előkészítő: Oldalfali split klímák.	Oldalfali split klímák.	Oldalfali split klímák.

9. *Külső és környezeti fenyegetésekkel szembeni védelem*

8.1.5 MUNKAVÉGZÉS BIZTONSÁGI TERÜLETEKEN

Eljárásokat kell kialakítani és alkalmazni a biztonsági területeken való munkavégzésre.

Az 1., 2. és 3. szintű biztonsági zóna esetén az általános munkavédelmi és egyéb pontokban megfogalmazott előírások betartása kötelező.

Kiemelt biztonsági területnek a 4. szintű zóna minősül. Ezen helyiség esetén fokozott óvatossággal kell eljárni, szem előtt tartva az ott lévő infrastruktúra rendelkezésre állását és az életvédelmi szempontokat. A helyiségben külső partner munkavégzése csak kísérővel történhet. Továbbá tilos olyan tevékenységek végzése, amely nem köthető hibaelhárítási, vagy karbantartási, illetve egyéb IT üzemeltetési feladatokhoz:

- Pihenés, étel-, italfogyasztás,
- normál felhasználói tevékenység,
- raktározási tevékenység,
- engedély nélküli helyiség karbantartás (festés, mázolás stb.).

8.1.6 SZÁLLÍTÁSI ÉS RAKODÁSI TERÜLETEK

Az olyan belépési pontokat, mint a szállítási és rakodási területek, illetve más olyan pontokat, ahol jogosulatlan személyek juthatnak be a telephelyekre, felügyelet alatt kell tartani, és ha lehetséges, el kell határolni az információ-feldolgozó eszközöktől, hogy el lehessen kerülni a jogosulatlan hozzáférést.

Amennyiben a Társaság területén karbantartási vagy egyéb munkavégzés folyik a 2., 3. és 4. biztonsági szintre sorolt zónák ajtajainak folyamatos nyitvatartása nem, vagy csak folyamatos

felügyelet mellett engedélyezett. Utóbbi esetben a felügyeletet annak a szervezeti egységnek/személynek kell ellátni, aki a munkavégzést előkészítette.

8.2 BERENDEZÉS

8.2.1 BERENDEZÉSEK ELHELYEZÉSE ÉS VÉDELME

A berendezéseket úgy kell elhelyezni és védeni, hogy csökkenjenek a környezeti fenyegetésekből és veszélyekből eredő kockázatok, illetve a jogosulatlan hozzáférés lehetőségei.

A Társaság informatikai rendszereit legalább a biztonsági zónák követelményeinek megfelelően védeni kell, csökkentve ezzel az illegális tevékenységekből és a külső hatásokból adódó kockázati tényezőket.

A munkaállomások hardver konfigurációját a felhasználóknak tilos módosítani, bármilyen okból belenyúlni.

Minden munkatárs felelősséggel tartozik a munkája ellátására biztosított berendezések rendeltetésszerű használatáért. Amennyiben egy eszköz rendeltetésszerű használata nem biztosított, azt elsősorban a **Kontrolling és beszerzési igazgatónak** vagy az ő döntése alapján a **Rendszer koordinátornak** kell jelezni.

A nyomtatók és egyéb közös használatú IT eszközök esetén a **Kontrolling és beszerzési igazgató** vagy az ő döntése alapján a **Rendszerkoordinátor** felelős az eszközök rendeltetésszerű használatáért. Amennyiben a felhasználó észleli, hogy az eszköz rendeltetésszerű használata nem biztosított, azt elsősorban a **Szakterületi vezetőnek** vagy az ő döntése alapján a **Kontrolling és beszerzési igazgatónak** kell jelezni.

8.2.2 KÖZMŰSZOLGÁLTATÁSOK

A berendezéseket védeni kell az áramkimaradások, illetve a közműszolgáltatások hibáiból eredő egyéb megszakítások ellen.

A hardver eszközök fizikai biztonságának érdekében az épületüzemeltetésnek minimálisan a következő védelmeket kell kialakítania:

- **Villámvédelem**: Az épületgerincen, valamint az épület sarkain villámvédelem van telepítve, melyet rendszeresen felül kell vizsgáltatni.
- **Túlfeszültség-védelem**: A túlfeszültség-védelmet a telepített UPS eszközök látják el a hálózati eszközök, a megfigyelőberendezések, valamint a biztonsági kivilágítás esetében.

8.2.3 KÁBELBIZTONSÁG

Az energiaellátási, valamint az adatátviteli vagy információszolgáltatásokat támogató távközlési kábeleket védeni kell a lehallgatástól, a zavarásoktól vagy a károsodástól.

A hálózati gyengeáramú, illetve nagyfeszültségi kábeleket külön nyomvonalon a mechanikai sérülésektől védett módon kell elhelyezni.

A kábeleknek zárt, nem megbontható csatornában kell futniuk, azokat a szolgáltató rendezőiben és a központi szerverteremben kell végződtetni.

8.2.4 BERENDEZÉSEK KARBANTARTÁSA

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

Rendszeres karbantartást kell végezni és ellenőrizni kell a berendezések működőképességét, melynek felelőse az IT Szolgáltató, a **Kontrolling és beszerzési igazgató** vagy az ő döntése alapján a **Rendszerkoordinátor**.

Kiemelt karbantartási feladatot jelentenek azok az eszközök, amelyek mozgó alkatrészekkel és energiatárolásra alkalmas megoldásokkal rendelkeznek:

- Klíma
- Szünetmentes tápellátás

A fenti eszközök esetén a karbantartásokat legalább évente kell elvégezni.

8.2.5 VAGYONELEMEK ELTÁVOLÍTÁSA

Előzetes jóváhagyás nélkül nem szabad berendezéseket, információkat vagy szoftvereket a telephelyről kivinni.

A Társaság területéről csak azon eszközöket lehet eltávolítani, melyek erre rendeltetésszerűen hivatottak az alábbiak mentén:

- A felhasználók számára átadott, a munkavégzéshez szükséges mobil eszközök,
- vezetői és kulcsos gépjárművek,
- szervizeléshez szükséges eltávolítás,
- további eszközök az érintett **Szakterületi vezető** engedélyével.

A munkavégzéshez szükséges eszközök csak őrzötten hagyhatóak, más eszközök esetén az „*Őrizetlenül hagyott felhasználói berendezések”* fejezetben foglaltak lépnek érvénybe.

Szervizeléshez történő eltávolítás csak a **Kontrolling és beszerzési igazgató** vagy az **Elnök-Vezérigazgató** engedélye alapján történhet, mely esetén a „*Berendezések biztonságos eltávolítása vagy újrafelhasználása”* fejezetben leírtak érvényesek. Ez esetben átvételi nyomtatványt kell kérni a külső szerviztől, melyet az eszköz gazdájához el kell juttatni vagy megőrzés mellett bemutatni.

Szoftvereket, berendezéseket és más, a Társaság tulajdonát képező dolgot kizárólag az **Elnök-Vezérigazgató** jóváhagyásával lehet a Társaság telephelyéről eltávolítani. Ez alól kivételt képeznek a munkavégzésre átadott munkaállomások, melyek saját felelősségre eltávolíthatók.

8.2.6 BERENDEZÉSEK ÉS VAGYONELEMEK BIZTONSÁGA A TELEPHELYEN KÍVÜL

A telephelyen kívüli vagyonelemeket annak figyelembevételével kell biztonságban tartani, hogy a szervezet telephelyein kívüli munkavégzésnek milyen különböző kockázatai lehetnek.

A Társaság telephelyén kívül történő munkavégzés esetén az egyes berendezések és vagyonelemek használata során figyelembe kell venni az adott munkakörnyezet kockázati paramétereit, például:

- Informatikai eszközöket felügyelet nélkül hagyni tilos.

- Idegen hálózathoz történő csatlakozás előtt biztosítani kell az informatikai eszközök megfelelő védelmi szintjét (személyi tűzfal, vírusvédelem).

8.2.7 BERENDEZÉSEK BIZTONSÁGOS ELTÁVOLÍTÁSA VAGY ÚJRAFELHASZNÁLÁSA

Minden olyan berendezést, amely adattároló eszközt tartalmaz, ellenőrizni kell annak érdekében, hogy arról az összes érzékeny adatot és jogvédett szoftvert letörölték-e vagy biztonságosan felülírták-e az eltávolítás vagy az újrafelhasználás előtt.

Az egyes adattárolásra alkalmas eszközök csak teljes újratelepítés vagy a háttértár teljes felülírása után távolíthatók el, vagy használhatók fel újra. A felülírást csak minősített, erre a célra rendszeresített eszközökkel szabad végrehajtani.

Engedélyezett eljárás az adathordozók mágneses felülírása. Ebben az esetben a felülírást végző külső partnertől bizonyítványt kell megkövetelni az adatmegsemmisítés sikerességéről.

Újrafelhasználás esetén az eszközöket úgy kell átadni, hogy azok további rendeltetésszerű használata biztosított legyen.

8.2.8 ŐRIZETLENÜL HAGYOTT FELHASZNÁLÓI BERENDEZÉSEK

A felhasználóknak biztosítaniuk kell, hogy az őrizetlenül hagyott berendezések megfelelő védelem alatt álljanak.

Az irodában az őrizetlenül hagyott tárgyak védelmében az alábbi szabályok szerint kell eljárni:

- Külsős személy csak felügyelet mellett tartózkodhat a termelőüzem, a raktár, az irodák, illetve a technikai szoba területén.
- A magántulajdonú tárgyak csak saját felelősségre hagyhatóak őrizetlenül.
- Az iroda helyiségekben a céges eszközök őrizetlenül hagyhatóak, azok eltűnését azonnal jelezni kell.

Minden egyéb helyen tilos őrizetlenül hagyni a felhasználói berendezéseket.

8.2.9 TISZTA ASZTAL ÉS TISZTA KÉPERNYŐ SZABÁLYA

Alkalmazni kell a tiszta asztal szabályát a papírokra és a cserélhető adattároló eszközökre, valamint a tiszta képernyő szabályát az információ-feldolgozó eszközökre.

A tiszta asztal és tiszta képernyő szabály értelmében védeni kell a Társaság információs vagyonát, beleértve a **Felhasználó** íróasztalán tárolt érzékeny, papír alapú információkat, és a munkaállomásokon tárolt elektronikus adatokat, az alábbi szempontok szerint:

- A monitorokat úgy kell elhelyezni, hogy a lehető legkisebb betekintést engedjék meg illetéktelenek számára.
- Az épületen kívülről a monitorokra való rálátást akadályozni kell.
- Amennyiben egy felhasználó rövid időre őrizetlenül hagyja munkaállomását, köteles azt zárolni, hosszabb idő esetén kijelentkezni, vagy lekapcsolni.
- A napi munkavégzés végeztével a munkaállomásokat le kell kapcsolni.

- A napi munkavégzés végeztével a legalább B-2 és S-2 adatbiztonsági kategóriába sorolt papír alapú anyagokat zárható szekrénybe, a B-4 és S-4 adatbiztonsági kategóriába soroltakat páncélszekrénybe el kell zárni.
- Nyomtatók, faxok és fénymásolók esetén ügyelni kell arra, hogy illetéktelenek ne férhessenek hozzá a dokumentumokhoz.
- Az íróasztalokon bizalmas eszközök (tokenek, belépőkártyák, kulcsok és egyéb adattárolásra alkalmas eszközök) felügyelet nélkül nem hagyhatók, a felhasználó köteles gondoskodni azok biztonságos tárolásáról.
- A munkaállomásokon legfeljebb a B-2 és S-2, azok asztalán csak a B-1 és S-1 adatbiztonsági kategóriába sorolt adatokat szabad tartósan tárolni.

9 AZ ÜZEMELÉS BIZTONSÁGA

9.1 ÜZEMELTETÉSI ELJÁRÁSOK ÉS FELELŐSSÉGEK

9.1.1 DOKUMENTÁLT ÜZEMELTETÉSI ELJÁRÁSOK

Az üzemeltetési eljárásokat dokumentálni kell, és rendelkezésére kell bocsátani minden felhasználónak, akinek szüksége van rájuk.

A megbízható és biztonságos üzemeltetés érdekében szabályokat, eljárásokat kell kidolgozni az informatikai rendszerekhez kapcsolódó folyamatok – javítások, karbantartások, szoftvertelepítések és beállítások stb. – végrehajtására, melyet az **Kontrolling és beszerzési igazgató és az Elnök-Vezérigazgató** hagy jóvá.

Az üzemeltetési eljárásokat dokumentálni szükséges annak érdekében, hogy az elvégzett feladatok nyomon követhetőek legyenek.

Az eljárásokban meg kell, hogy jelenjenek:

- Standard változások
- Jóváhagyási folyamat
- Biztonsági incidens kezelése
- Frissítés (patch menedzsment)
- Mentési eljárás
- Kialakított monitoring
- Rendszeres állapot és kapacitás ellenőrzés

A központi szolgáltatásokra az alábbi dokumentációkat kell elkészíteni és frissíteni az eljárások alapján:

- Üzleti funkció leírása, melynek tartalmaznia kell, hogy az adott eszközön milyen üzleti szolgáltatás valósul meg, vagy milyen szolgáltatáshoz kapcsolódik.
- Rendszerterv, melynek tartalmaznia kell a rendszer általános szakmai leírását és minden egyedi beállítást.
- Üzemeltetési dokumentáció, melynek tartalmaznia kell az összes „standard” változást és a hozzá kapcsolódó jóváhagyási folyamatokat.
- Helyreállítási terv, melynek tartalmaznia kell a mentésből történő helyreállítás menetét.

9.1.2 VÁLTOZÁSFELÜGYELET

Felügyelet alatt kell tartani a szervezetben, az üzleti folyamatokban, az információ-feldolgozó eszközökben és rendszerekben bekövetkező olyan változásokat, melyeknek hatása van az információbiztonságra.

A Társaság szervezeti, üzleti és informatikai változásait, amelyek hatással vannak az információbiztonságra, felügyelet alatt kell tartani.

A Társaság információ-feldolgozó rendszerén végzett bármilyen fejlesztést, vagy jelentős változást csak az **Elnök-Vezérigazgató** engedélyével szabad megvalósítani. Ez alól kivételt képeznek az informatikai rendszerelemek konfigurációja, biztonsági frissítése, jogosultságainak változása.

A változtatás végrehajtójának folyamatosan egyeztetnie kell az **Információbiztonsági felelőssel**, aki érvényesíti a változás biztonsági követelményeit.

Változások esetén az érintett üzemeltetési dokumentációkat frissíteni és követni kell, mely a változás végrehajtójának a feladata. Az információbiztonságot érintő változásokról az **Információbiztonsági felelőst** tájékoztatni kell.

Az üzemeltetési folyamatok részletes szabályozását az üzemeltetési dokumentációkban kell megvalósítani.

9.1.3 KAPACITÁSKEZELÉS

Az erőforrások használatát megfigyelés alatt kell tartani, optimalizálni kell és előrejelzéseket kell készíteni a jövőbeni kapacitásszükségletekre, hogy biztosítani lehessen a szükséges rendszerteljesítményt.

A Társaság erőforrásainak használatát optimalizálni kell és előrejelzéseket kell készíteni a jövőbeni kapacitásszükségletekre, hogy biztosítani lehessen a szükséges rendszerteljesítményt. Az erőforrások megfigyelése elsősorban a **Kontrolling és beszerzési igazgató** vagy az ő döntése alapján a **Rendszer koordinátor** feladata, akinek az előre látható bővítési szükségletekről az **Elnök-Vezérigazgatót,** kell értesítenie.

9.1.4 A FEJLESZTÉSI, A TESZTELÉSI ÉS AZ ÜZEMI KÖRNYEZETEK ELKÜLÖNÍTÉSE

A fejlesztési, tesztelési és üzemi környezeteket el kell különíteni, hogy csökkenteni lehessen a jogosulatlan hozzáférés kockázatait vagy a változtatásokat az üzemi környezetben.

A Társaság nem alkalmaz jelenleg fejlesztési és tesztelési környezeteket, mivel nincsenek alkalmazás típusú szolgáltatásai.

9.2 VÉDELEM A ROSSZINDULATÚ SZOFTVEREK ELLEN

9.2.1 INTÉZKEDÉSEK A ROSSZINDULATÚ SZOFTVEREK ELLEN

Észlelő, megelőző és helyreállító intézkedéseket kell megvalósítani a rosszindulatú szoftverek elleni védekezés érdekében, és ezeket kombinálni kell megfelelő felhasználói tudatossággal.

Kliensek esetén:

A munkaállomásokra vírusvédelmi rendszert kell telepíteni, azt frissíteni és központilag menedzselni kell. A felhasználó nem tilthatja le a vírusirtót és annak funkcióit nem korlátozhatja. Az operációs rendszert központi policy alapján rendszeresen frissíteni kell.

- Az ismeretlen forrásból származó elektronikus leveleket tilos megnyitni. A levél fertőzöttségének elbírálásához az alábbiakat kell figyelembe venni:

- A levél feladója ismert személy-e, illetve várható-e levél a feladótól? Figyelem, fertőzött levél ismert személytől, vagy ismerősnek tűnő forrásból is származhat!
- A levél tárgya: gyanús a levél, ha az nem munkaköri feladatokkal kapcsolatos.
- A levél címzettje: fertőzött lehet a levél, ha szokatlanul sok a címzettje.
- A levél nyelvezete: fertőzött lehet a levél, ha idegen nyelven, vagy nem a szokásos kommunikációs nyelven íródott.
- A levél csatolmánya: gyanús lehet a levél, ha az alábbi kiterjesztésű csatolt állományt, például .bat, .com, .exe, .dll, .sys, .bit, .pif, .hlp .txt, vagy beágyazott linket (URL) tartalmaz.

A fertőzöttnek ítélt elektronikus levelet megnyitás nélkül törölni kell.

A Társaság elektronikus levelező rendszerét magánjellegű levelezésre használni tilos!

Szerverek esetén

A szerverekre vírusvédelmi rendszert kell telepíteni, azt frissíteni és központilag menedzselni kell. Az operációs rendszert központi policy segítségével rendszeresen frissíteni kell. Levelező szerver esetén SPAM szűrő alkalmazása szükséges.

Hálózaton

Jelenleg a vezetékes hálózaton csak a szükséges portok patchelése megengedett. A vezeték nélküli hálózaton személyhez köthető hitelesítés szükséges.

A vendég WiFi elérést el kell különíteni a Társaság belső hálózataitól.

Hordozható adattárolók kezelése

Az adathordozók logikai védelmét az operációs rendszer és az ehhez tartozó ellenőrző, filekezelő rutinok alkalmazásával lehet biztosítani.

Az informatikai eszközök üzemeltetéséért elsősorban az IT Szolgáltató, a **Kontrolling és beszerzési igazgató**, illetve az ő döntése alapján a **Rendszerkoordinátor** felelős. Kötelesek gondoskodni a feldolgozások igényeinek megfelelő adathordozók biztosításáról, beleértve a biztonsági másolatok eszközigényeit, illetve az üzemeltetés biztonságát növelő generációs adatállományok alkalmazását is. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval kell ellátni. Az azonosítókat mind emberi, mind informatikai olvasásra alkalmas formába kell feltüntetni.

Tilos a privát adathordozókat szolgálati célra igénybe venni, illetve tilos szolgálati adathordozókat magáncélra igénybe venni.

Ismeretlen forrásból származó USB pendrive-ot tilos a számítógépekbe helyezni. Üzleti partnerektől kapott pendrive-ok esetén vírusellenőrzést kell végezni, ahol erre lehetőség van. Az ismerten fertőzött pendrive-okat arra elkülönített munkaállomáson ellenőrizni és vírusmentesíteni kell.

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

Az adathordozók szállítása csak megfelelő módon kialakított fémdobozban történhet, melyeket a Társaság épületén kívül kell tárolni.

Az adathordozókról nyilvántartást kell vezetni. Az azonosító adaton kívül a felírás és megőrzés dátumát, védettség tényét, jogosultsági és illetékességi adatokat, valamint az adathordozó kiadására és visszavételezésére vonatkozó információkat kell tartalmaznia. A nyilvántartásnak naprakészen követnie kell az adathordozók fizikai mozgását. A nyilvántartás vezetéséért elsősorban a **Kontrolling és beszerzési igazgató** vagy az ő döntése alapján a **Rendszerkoordinátor** is felelős.

Az adathordozók megőrzési idejét a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló többször módosított 1995. évi LXVI. törvényben foglaltak, továbbá Társaságunk Bizonylati rendjében és Iratkezelési szabályzatában foglaltak alapján az adatkezelő határozza meg.

Mobil eszközök kezelése

Ismeretlen forrásból tilos bármilyen szoftvert vagy alkalmazást telepíteni. Telefonokon nem szabad megkérdőjelezhető (illegális) módosítást végezni.

9.3 MENTÉS

9.3.1 INFORMÁCIÓK MENTÉSE, FILEOK VÉDELME

Mentési célból másolatokat kell készíteni az információkról, szoftverekről és rendszerképekről, és ezeket rendszeresen tesztelni kell egy egyeztetett mentési szabály szerint.

Az informatikában a legnagyobb értéket a számítógépen tárolt adatok jelentik. Ezek védelmében meghatározó jelentőségű a biztonsági másolatok készítése.

A mentések folyamata:

- A mentéseket naponta kell végrehajtani.
- A mentésből a rendszerek, a szoftverkörnyezet beállításainak, valamint a tárolt adatoknak teljes körűen visszaállíthatónak kell lennie a mentés pillanatának állapotára.
- Az éles adattároló és -feldolgozó eszközök esetében az adatokat havonta legalább 2 példányban kell menteni, és egymástól fizikailag elkülönült helyiségben elzárt, az éles adattároló, -feldolgozó eszköz helyiségének tűzterétől elkülönülő térben, tűzbiztos helyen kell tárolni.
- A mentett adatokhoz csak az arra jogosultak férhetnek hozzá.

A munkák során létrehozott Word és Excel dokumentumok mentése az azt létrehozó munkatársak (**Felhasználók**) feladata, azonban valamennyi munkaállomás fájlszerverre történő mentését meg kell oldani.

A Társaság adatait – különös tekintettel a pénzügyi és számviteli adatokra, valamint a könyveléssel kapcsolatos adatokra – kezelő adattároló egységek (szerverek) esetében legalább napi szintű mentéseket kell biztosítani.

A levelezések mentése külső szolgáltató szerverén (Microsoft Office365) történik.

Az adatállományok fájlvédelme során gondoskodni kell arról, hogy azok ne károsodjanak.

9.4 NAPLÓZÁS ÉS MEGFIGYELÉS

Az információhoz való hozzáférést 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 havonta át kell tekinteni, és a jogosulatlan hozzáférést vagy annak a kísérletét az ügyvezetésnek azonnal jelenteni kell.

A naplófájlok áttekintéséért, értékeléséért a **Kontrolling és beszerzési igazgató** a felelős.

9.5 AZ ÜZEMELŐ SZOFTVEREK FELÜGYELETE

9.5.1 SZOFTVEREK TELEPÍTÉSE AZ ÜZEMELŐ RENDSZEREKRE

Eljárásokat kell megvalósítani az üzemelő rendszereken elvégzendő szoftvertelepítések felügyeletére.

A rendszerekre történő szoftvertelepítések végrehajtása előtt vírusellenőrzést és előzetes tesztelést kell lebonyolítani, amennyiben az indokolt. Az ilyen módon ellenőrzött szoftverek telepítését karbantartási ablakban kell végrehajtani, hogy ne zavarja a munkatársak napi munkáját.

Az informatikai rendszereken csak jogtiszta, egyedileg engedélyezett szoftverek használhatók, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak.

Visszaállítási tervet kell készíteni a „*Változásfelügyelet*” alfejezetben leírtak alapján.

9.6 A MŰSZAKI SEBEZHETŐSÉGEK FELÜGYELETE

9.6.1 MŰSZAKI SEBEZHETŐSÉGEK FELÜGYELETE

Kellő időben meg kell szerezni az információkat a használatban lévő információs rendszerek műszaki sebezhetőségeiről, értékelni kell a szervezet kitettségét ezeknek a sebezhetőségeknek, és megfelelő intézkedéseket kell hozni a kapcsolódó kockázatok kezelésére.

Az **Információbiztonsági felelősnek** havi szinten figyelnie kell a megjelenő sérülékenységekről szóló jelentéseket, amelyekről tájékoztatnia kell a **Kontrolling és beszerzési igazgatót**. A **Kontrolling és beszerzési igazgatónak** vagy az ő döntése alapján a **Rendszerkoordinátornak** ellenőriznie kell a Társaság információs rendszereinek érintettségét és szükséges esetben javaslatot kell tennie az **Elnök-Vezérigazgató** felé a javítás elvégzésére. Jóváhagyás esetén a **Kontrolling és beszerzési igazgatónak** vagy az ő döntése alapján a **Rendszerkoordinátornak** be kell ütemeznie, majd végre kell hajtania a biztonsági javítások telepítését először teszt környezetben, majd azt követően éles környezetben is a javítások súlyosságának sorrendjében.

9.6.2 KORLÁTOZÁSOK A SZOFTVERTELEPÍTÉSRE

Meg kell állapítani és be kell vezetni a felhasználók általi szoftvertelepítést vezérlő szabályokat.

A Társaság szervereire csak a **Kontrolling és beszerzési igazgató** vagy az ő döntése alapján az IT Szolgáltató, illetve a **Rendszerkoordinátor** telepíthet szoftvereket, melyekért felelősséggel tartozik.

A Társaság munkaállomásaira normál rend szerint csak az IT Szolgáltató, a **Kontrolling és beszerzési igazgató** vagy az ő felügyelete mellett a **Rendszerkoordinátor** telepíthet szoftvereket.

A **Kontrolling és beszerzési igazgató** vagy az ő döntése alapján az IT Szolgáltató, illetve a **Rendszerkoordinátor** feladata évente ellenőrizni a szoftverintegritást. Amennyiben engedély nélküli szoftvertelepítést észlelt, ennek tényéről értesíti az **Elnök-Vezérigazgatót**.

Mobil eszközök esetén csak legális szoftverek telepíthetőek, melyekért az eszközgazdák felelnek.

9.7 AZ INFORMÁCIÓS RENDSZEREK AUDITÁLÁSÁVAL KAPCSOLATOS MEGFONTOLÁSOK

9.7.1 AZ INFORMÁCIÓS RENDSZEREK AUDITÁLÁSÁVAL KAPCSOLATOS INTÉZKEDÉSEK

Az auditkövetelményeket és az üzemelő rendszerek ellenőrzésére is kiterjedő tevékenységeket gondosan meg kell tervezni és meg kell állapodni azokban, hogy az üzleti folyamatok megzavarását minimalizálni lehessen.

Jelen szabályzatot az **Információbiztonsági felelős** köteles évente felülvizsgálni, a nagyobb változásokat folyamatosan követni.

Az **Információbiztonsági felelős** kötelessége, hogy évente a szabályzat hatálya alá tartozó tárgyi eszközökön auditot végezzen. Az audit tevékenységeket gondosan meg kell tervezni, hogy az üzleti folyamatok megzavarását minimalizálni lehessen.

10 A KOMMUNIKÁCIÓ BIZTONSÁGA

10.1 A HÁLÓZATBIZTONSÁG FENNTARTÁSA

10.1.1 HÁLÓZATI INTÉZKEDÉSEK

A hálózatokat gondozni és felügyelni kell, hogy a rendszerekben és az alkalmazásokban meg lehessen védeni az információkat.

A Társaság hálózatára, csak nyilvántartott és jóváhagyott eszközökkel léphetnek be a munkatársak, vagy külső ügyfelek.

A belső használatú (nem guest) vezeték nélküli hálózat esetén 802.1x protokoll használata kötelező.

10.1.2 A HÁLÓZATI SZOLGÁLTATÁSOK BIZTONSÁGA

Minden hálózati szolgáltatásra meg kell határozni a biztonsági mechanizmusokat, a szolgáltatási szinteket és a kezelési követelményeket, és be kell építeni a hálózati szolgáltatási megállapodásokba függetlenül attól, hogy ezeket a szolgáltatásokat házon belülről vagy kiszervezett formában nyújtják.

Az egyes rendelkezésre állási idők teljesítéséhez optimalizálni szükséges a(z):

- Hibaészlelési folyamatokat
- Incidenskezelési folyamatokat
- Visszaállítási folyamatokat

10.1.3 ELKÜLÖNÍTÉS A HÁLÓZATOKBAN

Az információszolgáltatások, a felhasználók és az információs rendszerek különböző csoportjait el kell különíteni a hálózatokban.

A Társaság hálózatát szét kell választani a felhasználásnak megfelelő alhálózatokra, hogy az egyes rendszerek egymástól logikailag elkülöníthetőek legyenek a hálózati forgalom tekintetében.

Az alábbi szolgáltatásokat védett hálózati szegmensbe kell helyezni:

- Publikált szolgáltatások
- Teszt szolgáltatások
- Éles szolgáltatások

10.2 INFORMÁCIÓÁTVITEL

10.2.1 SZABÁLYOK ÉS ELJÁRÁSOK AZ INFORMÁCIÓÁTVITELRE

Formális átviteli szabályokat, eljárásokat és intézkedéseket kell bevezetni, hogy meg lehessen védeni az információk átvitelét minden típusú kommunikációs eszköz használata esetén.

A munkatársak és alvállalkozók csak úgy használhatják a Társaság kommunikációs csatornáit (e-mail, telefon), hogy azzal ne sértsék meg a törvényi előírásokat és a Társaság érdekeit.

Nem biztonságos hálózaton fájl és információküldést csak titkosított és hitelesített csatornán keresztül lehet végezni, vagy titkosítani kell az állományt.

Biztonságos hálózaton a legalább B-2 és S-2 adatbiztonsági kategóriába sorolt információkat jelszóval védett állományban, a legalább B-3 és S-3 adatbiztonsági kategóriába sorolt információkat a fájl titkosításával kell küldeni.

10.2.2 MEGÁLLAPODÁSOK AZ INFORMÁCIÓÁTVITELRE

A megállapodásoknak foglalkozniuk kell az üzleti információk biztonságos átvitelével a szervezet és a külső partnerek között.

Az információátvitel során be kell tartani az adott ügyfél, partner által kért vagy előírt szabályokat. Külső partnerek esetén titoktartási nyilatkozatban ki kell térni az információátvitel szabályaira.

A Társaság üzleti partnereinek adatait csak az **Elnök-Vezérigazgató** és az ügyfél együttes hozzájárulásával adhat át harmadik fél számára.

10.2.3 ELEKTRONIKUS ÜZENETKÜLDÉS

Az elektronikus üzenetekben lévő információkat megfelelően védeni kell.

Az elektronikus üzenetekben lévő információk védelme érdekében be kell tartani a *„Védelem a rosszindulatú szoftverek ellen”* fejezetben megfogalmazott szabályokat.

Elektronikus üzenetküldés esetén a legalább B-2 és S-2 adatbiztonsági kategóriába sorolt információkat jelszóval védett állományban a fájl titkosításával kell küldeni.

Magán levelezési címre üzleti partner specifikus információit továbbítani tilos.

10.2.4 BIZALMASSÁGI VAGY TITOKTARTÁSI MEGÁLLAPODÁSOK

A bizalmassági vagy titoktartási megállapodások követelményeit, amelyek a szervezetnek az információk védelmére vonatkozó igényeit tükrözik, azonosítani kell, rendszeresen át kell vizsgálni és dokumentálni kell.

A Társaság háromféle titoktartási megállapodást különböztet meg:

- Munkavállalói titoktartási nyilatkozat
- Partner munkavállalói titoktartási nyilatkozat
- Titoktartási záradék a partneri szerződésekhez

Mindegyik titoktartási megállapodásban definiálni kell a Társaságnak az információk védelmére vonatkozó követelményeit és a kapcsolódó törvényi előírásokat. A meghatározott követelményeket és törvényi előírásokat évente, vagy nagyobb változások esetén az **Információbiztonsági felelősnek** át kell vizsgálnia.

11 RENDSZEREK BESZERZÉSE, FEJLESZTÉSE ÉS KARBANTARTÁSA

11.1 AZ INFORMÁCIÓS RENDSZEREK BIZTONSÁGI KÖVETELMÉNYEI

11.1.1 INFORMÁCIÓBIZTONSÁGI KÖVETELMÉNYEK ELEMZÉSE ÉS MEGHATÁROZÁSA

Az információbiztonsággal kapcsolatos követelményeket tartalmazniuk kell az új információs rendszerekre vagy a már létező információs rendszerek továbbfejlesztésére vonatkozó követelményeknek.

Az információs rendszerek információbiztonsági követelményeit még a tervezés, illetve a módosítás kidolgozásának fázisában rögzíteni kell, a követelményeknek való megfelelést a bevezetés során biztosítani kell.

A követelményektől való eltérést az **Elnök-Vezérigazgató** engedélyezhet. Továbbá be kell tartani az *„Üzemeltetési eljárások és felelősségek”* fejezet *Változásfelügyelet* részében foglaltakat.

A folyamatosan változó környezeti tényezők (szabályozások, technológia, fenyegetettségek stb.) miatt az alkalmazott követelménylistát tartalmi szempontból évente felül kell vizsgálni.

11.1.2 NYILVÁNOS HÁLÓZATOKON NYÚJTOTT ALKALMAZÁSSZOLGÁLTATÁSOK BIZTONSÁGA

Az alkalmazásszolgáltatások által nyilvános hálózatokon keresztül átvitt információkat védeni kell a tisztességtelen tevékenységektől, a szerződéses vitáktól, a jogosulatlan közzétételtől és módosítástól.

A Társaság által nyújtott nyilvános szolgáltatás a Társaság weblapja. A weblap tartalmát csak az **Elnök-Vezérigazgató** engedélyével szabad publikálni. Tilos a honlapon olyan információk közzététele, amelyek a sértik a törvényi megfelelőséget (tisztázatlan szellemi jog, emberi méltóságot sértő közlések, törvény által korlátozott egyéb tevékenységek).

Annak érdekében, hogy a Társaság a weboldal tartalom bizalmasságát biztosítani tudja, évente sérülékenység vizsgálatnak kell alávetni, amelyért elsősorban a Társasággal szerződésben álló szolgáltatók a felelősek. Ezt a felelősséget/kötelezettséget a velük megkötött szerződésekben kell kikötni. Az évenkénti sérülékenység vizsgálat végrehajtásával kapcsolatban, a szolgáltatók szakembereivel való konzultációt a **Kontrolling és beszerzési igazgató** folytatja le, illetve a feladat elvégzéséről készült riportokat szakmai szempontból ő kontrollálja.

11.1.3 AZ ALKALMAZÁSSZOLGÁLTATÁSOK TRANZAKCIÓINAK VÉDELME

A Társaságnak nincs tranzakciós szolgáltatása.

11.2 BIZTONSÁG A FEJLESZTÉSI ÉS TÁMOGATÁSI FOLYAMATOKBAN

11.2.1 SZABÁLY A BIZTONSÁGOS FEJLESZTÉSRE

A rendszerfejlesztések/bevezetések során ügyelni kell, hogy a fejlesztendő/bevezetendő rendszerben érvényesíteni kell a leendő adatosztályozási kategóriának megfelelő információbiztonsági követelményeket.

A fejlesztendő/bevezetendő rendszer specifikálása során az **Információbiztonsági felelős** feladata, hogy a rendszerrel szemben elvárt funkcionális követelményeken túl a biztonsági követelmények is megjelenjenek a specifikációban.

A fenti követelmények teljesülése érdekében az **Információbiztonsági felelőst**, minden a rendszerfejlesztés/bevezetéssel kapcsolatos megbeszélésre, egyéb kommunikációs csatornába be kell vonni, amiért az adott fejlesztési/bevezetési téma felelőse felelős.

A szoftverek és rendszerek fejlesztésére szabályokat kell kialakítani és alkalmazni a fejlesztések során a szervezetben.

11.2.2 RENDSZEREK VÁLTOZÁSFELÜGYELETI ELJÁRÁSAI

A vonatkozó szabályozást az *„Üzemeltetési eljárások és felelősségek”* fejezet *Változásfelügyelet* része tartalmazza.

A fejlesztési életciklus során végrehajtandó rendszerváltoztatásokat felügyelni kell egy formális változásfelügyeleti eljárással.

11.2.3 AZ ALKALMAZÁSOK MŰSZAKI VIZSGÁLATA A MŰKÖDTETŐ KÖRNYEZET VÁLTOZÁSAI UTÁN

A Társaság informatikai szolgáltatásainak infrastrukturális elemeit minden, a működtető környezet változtatása után át kell vizsgálni műszakilag és biztosítani kell, hogy a biztonsági szint azonos, vagy magasabb szinten legyen a változás után.

A fenti követelménynek a Társaság kétféleképpen felel meg:

- Változások után az informatikai rendszereket sérülékenység-vizsgálati teszteknek kell alávetni.
- Az informatikai rendszer konfigurációit, beállításait a jelen szabályzatot figyelembe véve kell a legjobb gyakorlat szerint biztonságossá tenni.

Ha megváltoztatják a működtető környezetet, akkor az üzletkritikus alkalmazásokat meg kell vizsgálni és tesztelni kell annak érdekében, hogy annak ne legyen kedvezőtlen hatása a szervezet működésére és biztonságára.

11.2.4 SZOFTVERCSOMAGOK VÁLTOZTATÁSAINAK KORLÁTOZÁSA

A munkaállomások szoftverintegritásának megőrzése a Társaság valamennyi alkalmazottjának a felelőssége.

A szerverek szoftvercsomagjainak változásait csak az **Elnök-Vezérigazgató** engedélyével, a kritikus ügyviteli folyamatok leállása nélkül szabad végrehajtani.

A szoftvercsomagok módosításait lehetőleg el kell kerülni, korlátozni kell az elengedhetetlen változtatásokra, és minden változtatást szigorúan felügyelni kell.

11.2.5 BIZTONSÁGOS RENDSZEREK TERVEZÉSI ELVEI

Az információs rendszerek biztonságának tervezése során az alábbi irányelveket kell követni:

- Minden rendszer a leendő adat besorolási kategóriának megfelelő védelmi intézkedéseket tartalmazza (jogosultságkezelés, titkosítás stb.).
- Az információs rendszerben bekövetkező incidensek feltárását és követését biztosítani kell (például naplózás).
- A tervezés során ki kell térni az adott rendszer környezetének védelmére.
- Minden releváns információs rendszert védeni kell a rosszindulatú vírusoktól.
- Csak olyan információs rendszereket szabad tervezni, amelynek gyártói támogatottsága hosszútávon biztosított az információbiztonsági sérülékenységek esetén.
- Minden információs rendszerhez olyan, hibatűrési és mentési stratégiát és megoldást kell biztosítani, amely harmóniában van az adott rendszerrel szemben elvárt rendelkezésre állási követelményekkel.

A biztonságos rendszerek tervezésére elveket kell kialakítani, dokumentálni, fenntartani és alkalmazni az információs rendszerek megvalósítása során.

11.2.6 BIZTONSÁGOS FEJLESZTÉSI KÖRNYEZET

A szervezeteknek a rendszerfejlesztési és -integrációs tevékenységek számára olyan biztonságos fejlesztési környezeteket kell létrehozniuk és megfelelően védeniük, amelyek lefedik a rendszerfejlesztés teljes életciklusát.

11.2.7 KISZERVEZETT FEJLESZTÉS

A Társaságban az informatikai szolgáltatások (honlap, informatikai infrastruktúra, SAP rendszerek stb.) fejlesztését hatályos szerződések alapján külső partnerek látják el.

A külső partner önhatalmú fejlesztést nem végezhet, amennyiben a Társaság ilyen szolgáltatást vesz igénybe, pontosan kell meghatározni:

- A fejlesztés tartalmát.
- A fejlesztés során elvárt titoktartási információkat.
- A fejlesztés során elvárt biztonsági elvárásokat.

A külső partner által elvégzett feladatokat mindhárom szempont szerint ellenőrizni kell, amelyért az **Információbiztonsági felelős** a felelős.

A szervezetnek felügyelnie kell és megfigyelés alatt kell tartani a kiszervezett rendszerfejlesztési tevékenységet.

11.2.8 A RENDSZER BIZTONSÁGI TESZTELÉSE

A fejlesztések során el kell végezni a rendszerek biztonsági tesztelését, amelyért elsősorban a **Kontrolling és beszerzési igazgató** vagy az ő döntése alapján a **Rendszerkoordinátor** a felelős.

El kell végezni a biztonsági funkciók tesztelését a fejlesztés során.

11.2.9 A RENDSZER ELFOGADÁSI TESZTELÉSE

Elfogadási tesztprogramokat és ehhez kapcsolódó kritériumokat kell létrehozni az új információs rendszerekre, a továbbfejlesztésekre és az új verziókra.

Az informatikai rendszerek korszerűsítését és az új változatok átvételi követelményeit az **Elnök-Vezérigazgató** határozza meg, és az átvétel előtt elvégezteti a megfelelő rendszervizsgálatokat.

Új információ feldolgozó- vagy tárolóeszköz telepítését, tesztelését az írott beszerzési követelmények teljesülésének ellenőrzését a **Kontrolling és beszerzési igazgató** vagy az ő döntése alapján a **Rendszerkoordinátor** végzi/felügyeli. A tesztelés során meg kell állapítani azt is, hogy a programok a törvényi, jogszabályi és egyéb előírásoknak megfelelnek-e, telepítésre alkalmasak-e. Az ezen tevékenységek során felmerülő esetleges újabb sérülékenységeket és fenyegetéseket felméri és szükség esetén a biztonsági szabályok módosítására, kiegészítésére javaslatokat tesz.

11.3 TESZTADATOK

11.3.1 TESZTADATOK VÉDELME

A tesztadatokat gondosan kell kiválasztani, védeni és felügyelni.

A Társaság nem rendelkezik külön tesztkörnyezettel vagy tesztrendszerrel, nincsenek tesztadatai.

12 SZÁLLÍTÓI KAPCSOLATOK

A szállítókkal történő megállapodás minden esetben az **Elnök-Vezérigazgató** felelőssége, az előkészítésben segítik az egyes szakterületek vezetői.

12.1 INFORMÁCIÓBIZTONSÁG A SZÁLLÍTÓI KAPCSOLATOKBAN

A Társaságnál az alábbi szállítói kapcsolatokat kell megkülönböztetni:

- Általános szállítók
- A Társaság által igénybevett szolgáltató cégek
- Partnerek, melyek által az ügyfelek kiszolgálása történik

12.1.1 INFORMÁCIÓBIZTONSÁGI SZABÁLY A SZÁLLÍTÓI KAPCSOLATOKRA

Információbiztonsági követelményekben kell megállapodni a szállítókkal és ezeket dokumentálni kell annak érdekében, hogy mérsékelni lehessen a szállítóknak a szervezeti vagyonelemekhez való hozzáféréséből eredő kockázatokat.

A szállító cégekkel minden esetben megállapodást kell létrehozni, melyben meg kell határozni a Társaság vagyonelemeire vonatkozó információbiztonsági követelményeket.

12.1.2 A BIZTONSÁG KEZELÉSE A SZÁLLÍTÓI MEGÁLLAPODÁSOKBAN

Minden vonatkozó információbiztonsági követelményt meg kell határozni, és ezekről meg kell állapodni mindazon szállítókkal, akik hozzáférhetnek a szervezet információihoz, ezeket feldolgozhatják, tárolhatják, kommunikálhatják, vagy informatikai infrastruktúraelemeket biztosíthatnak ezekhez.

Az általános szállítói kapcsolatok esetén a szállító cég gazdasági leinformálása szükséges.

A szolgáltató cégek esetén szükséges:

- A cég leinformálása (gazdasági, tulajdoni, jogi helyzetét vizsgálni kell)
- A szerződésben titoktartási, felelősségi rész kialakítása.

A partneri kapcsolatok esetén szükséges:

- A cég leinformálás (gazdasági, tulajdoni, jogi helyzetét vizsgálni kell)
- Ismertnek kell lennie a szállítói láncnak.
- A szerződésben ki kell térni az ügyfél adatok bizalmasságára.
- Titoktartási nyilatkozatot kell kialakítani az üzleti adatok védelme érdekében.

12.1.3 INFORMÁCIÓS ÉS KOMMUNIKÁCIÓS TECHNOLÓGIÁK SZÁLLÍTÓI LÁNCA

A szállítókkal kötött megállapodásoknak tartalmazniuk kell azokat a követelményeket, amelyek azokkal az információbiztonsági kockázatokkal foglalkoznak, amelyek az információs és kommunikációs technológiák szolgáltatási és termékellátási láncaival kapcsolatosak.

Az általános szállítói kapcsolatok esetén nincs megfogalmazott követelmény.

A szolgáltató cégek esetén szerződésben ki kell kötni a kommunikáció módját és annak csatornáit.

A partneri kapcsolatok esetén:

- Ki kell kötni a kommunikáció módját és a megfelelő csatornákat.
- Az ügyfél adatokat csak az adatosztályozási szintjének megfelelő követelmények szerint szabad átküldeni, hogy harmadik félhez ne kerülhessen információ.
- Törekedni kell, hogy elkülönüljenek a szakmai és kereskedelmi kapcsolatok.

12.2 A SZÁLLÍTÓI SZOLGÁLTATÁSNYÚJTÁS IRÁNYÍTÁSA

A szállítók között különbséget kell tennünk belső igény kiszolgálását célzó és külső – ügyfél igényt – kiszolgáló szállítók között.

12.2.1 A SZÁLLÍTÓI SZOLGÁLTATÁSOK FIGYELEMMEL KÍSÉRÉSE ÉS ÁTVIZSGÁLÁSA

A szervezeteknek rendszeresen figyelemmel kell kísérnie, át kell vizsgálnia és auditálnia a szállítói szolgáltatásnyújtást.

A belső szolgáltatások esetén az irodai –facility– megrendelések esetén az **Elnök-Vezérigazgató**, míg az informatikai eszközök beszerzése esetén a **Kontrolling és beszerzési igazgató** felelőssége a szállító kapcsolatok, szolgáltatások nyomon követése.

A külső szolgáltatások esetén az **Elnök-Vezérigazgató** felelőssége a szállítói kapcsolatok figyelemmel kisérése.

12.2.2 A SZÁLLÍTÓI SZOLGÁLTATÁSOK VÁLTOZÁSAINAK FELÜGYELETE

A szállítók által nyújtott szolgáltatásokban bekövetkező változásokat, beleértve az információbiztonsági szabályok, eljárások és intézkedések karbantartását és fejlesztését. felügyelet alatt kell tartani, figyelembe véve az üzleti információk kritikusságát, az érintett rendszereket és folyamatokat, valamint a kockázatok újraértékelését.

A belső szolgáltatások esetén, amennyiben a szállítói kapcsolatok során változás történik, a **Kontrolling és beszerzési igazgatónak** és az **Szakterületi vezetőknek** értesíteni kell az **Elnök-Vezérigazgatót**, hogy felügyelni tudja a változásokat.

A külső szolgáltatások esetén, az üzleti partnerekkel kapcsolatot tartó **Felhasználók** kötelesek az **Elnök-Vezérigazgatónak** jelezni, ha a kapcsolatban bármilyen jellegű változás történik, mely üzleti érdeket befolyásol.

Az értesítések alapján az **Elnök-Vezérigazgatónak** gondoskodni kell az üzleti érdekek sérthetetlenségéről és dönteni kell az egyes változások jóváhagyásáról is.

13 AZ INFORMÁCIÓBIZTONSÁGI INCIDENSEK KEZELÉSE

13.1 AZ INFORMÁCIÓBIZTONSÁGI INCIDENSEK ÉS JAVÍTÁSOK KEZELÉSE

13.1.1 FELELŐSSÉGEK ÉS ELJÁRÁSOK

Vezetői felelősségeket és eljárásokat kell kialakítani, hogy biztosítható legyen a gyors, hatásos és rendezett válaszadás az információbiztonsági incidensekre.

A biztonsági incidensek kategóriájába az alábbi események tartoznak:

- Jogosulatlan hozzáférés (informatikai eszközhöz, alkalmazáshoz, adathoz, biztonsági zónához)
- Információs vagyon (eszköz, szoftver, adat stb.) elvesztése, eltulajdonítása, vagy megrongálódása
- Határincidensek, vírusfertőzések
- A mentési feladatok végrehajtásának akadályoztatása
- Működési rendellenességek (eszköz hiba, program hiba, információ rendelkezésre állásának elvesztése, hibás adatok a feldolgozó rendszerben stb.)
- A törvény, vagy a szabályzat megsértésére utaló cselekmények

Az alábbi események kiemelt incidensnek minősülnek:

- Szándékos károkozás (logikai, fizika)
- Gondatlanságból fakadó károkozás (hozzáférési információk megosztása, esemény eltitkolása, levelek magánfiókba történő továbbítása, bizalmas adatok továbbítása illetéktelenek számára stb.)
- Munkaköri kötelmek megszegéséből származó károkozás
- Azonnali kezelést igénylő károkozás (hozzáférési információkkal történő visszaélés stb.)

A bizalmasság és sértetlenség elvesztéséből fakadó incidensek kezelésében résztvevő személyek:

Incidens kategória	Bejelentésért felelős	Kezelésért felelős
Belső IT infrastruktúrát érintő események	Elsősorban **a Kontrolling és beszerzési igazgató** vagy az ő döntése alapján a **Rendszerkoordinátor**	Elsősorban **a Kontrolling és beszerzési igazgató** vagy az ő döntése alapján a **Rendszerkoordinátor**
Munkaállomást érintő események	**Felhasználó**	Elsősorban **a Kontrolling és beszerzési igazgató** vagy az ő döntése alapján a **Rendszerkoordinátor**

Incidens kategória	Bejelentésért felelős	Kezelésért felelős
Adatokat érintő események	**Adatkezelő**	Elsősorban **a Kontrolling és beszerzési igazgató** vagy az ő döntése alapján a **Rendszerkoordinátor**
Törvény-, szabály-, és eljárássértések	**Információbiztonsági felelős**	**Elnök-Vezérigazgató**

10. Incidenskezelésben résztvevő személyek (bizalmasság és sértetlenség)

A rendelkezésre állás sérüléséből fakadó incidensek kezelésében résztvevő személyek:

Incidens kategória	Bejelentésért felelős	Kezelésért felelős
Belső IT infrastruktúrát érintő események	**Felhasználó**	Elsősorban **a Kontrolling és beszerzési igazgató** vagy az ő döntése alapján a **Rendszerkoordinátor**
Munkaállomást érintő események	**Felhasználó**	Elsősorban **a Kontrolling és beszerzési igazgató** vagy az ő döntése alapján a **Rendszerkoordinátor**
Adatokat érintő események	**Adatkezelő**	Elsősorban a **Kontrolling és beszerzési igazgató** vagy az ő döntése alapján a **Rendszerkoordinátor**

11. Incidenskezelésben résztvevő személyek (rendelkezésre állás)

Az incidenskezelést az alábbi eljárás szerint kell végrehajtani:

1. Információbiztonsági események és gyengeségek jelentése a kezeléséért felelős személy részére
2. Incidenst kiváltó ok megszűntetése
3. Esemény felvétele az Információbiztonsági esemény nyilvántartás táblázatba
4. Információbiztonsági események felmérése és döntéshozatal
5. Megkerülő megoldás bevezetése (ha van, és a végleges megoldás azonnal nem léptethető életbe)
6. Incidens elhárítása
7. Incidens lezárása
8. Tanulás az információbiztonsági incidensekből (tapasztalatok és tanulságok levonása)

13.1.2 INFORMÁCIÓBIZTONSÁGI ESEMÉNYEK JELENTÉSE

Az információbiztonsági eseményeket, amilyen gyorsan csak lehet, jelenteni kell a megfelelő vezetői csatornákon keresztül.

A Társaság alkalmazottainak az általuk észlelt, a Társaság informatikai rendszereiben keletkező, vagy más, a Társaságot érintő biztonsági incidenseket jelenteniük kell az adott incidens kezeléséért felelős személynek. Minden incidensről tájékoztatni kell az **Információbiztonsági felelőst,** aki a kiemelt incidensekről jelent az **Elnök-Vezérigazgatónak**.

13.1.3 INFORMÁCIÓBIZTONSÁGI GYENGESÉGEK JELENTÉSE

Meg kell követelni a szervezet információs rendszereit és szolgáltatásait használó alkalmazottaktól és szerződéses munkatársaktól, hogy jegyezzék fel és jelentsék, ha bármilyen információbiztonsági gyengeséget észlelnek vagy gyanítanak a rendszerekben vagy szolgáltatásokban.

A Társaság alkalmazottainak és szerződéses munkatársainak az általuk észlelt, a Társaság informatikai rendszereiben és szolgáltatásaiban jelenlévő biztonsági gyengeséget jelenteniük kell az **Információbiztonsági felelősnek**.

13.1.4 AZ INFORMÁCIÓBIZTONSÁGI ESEMÉNYEK FELMÉRÉSE ÉS DÖNTÉSHOZATAL

Az információbiztonsági eseményeket fel kell mérni, és el kell dönteni róluk, hogy információbiztonsági incidensnek minősülnek-e.

Az incidens kezeléséért felelős személynek felül kell vizsgálnia, hogy a jelentett, észlelt biztonsági események információbiztonsági incidensnek minősülnek-e. Információbiztonsági incidensnek minősül:

- Az információbiztonsági szabályok megsértése
- Az információbiztonsági védelmi rendszer (vírus-, határvédelem stb.) bármely elemének működésképtelenné válása
- Az információbiztonsági sérülékenységek kihasználása (támadás)
- Az informatikai rendszerben végzett olyan illegális felhasználói vagy üzemeltetői tevékenység, amelynek következtében a biztonsági szint lecsökken

13.1.5 VÁLASZ AZ INFORMÁCIÓBIZTONSÁGI INCIDENSEKRE

Az információbiztonsági incidensekre dokumentált eljárások szerint kell reagálni.

Az információbiztonsági incidenseket a kezelésükért felelős személynek kell kivizsgálni, aki szükség esetén további személyeket jogosult bevonni a vizsgálatba. Minden incidenst az Információbiztonsági esemény nyilvántartás táblázatba rögzíteni kell.

13.1.6 TANULÁS AZ INFORMÁCIÓBIZTONSÁGI INCIDENSEKBŐL

Az információbiztonsági incidensek elemzéséből és megoldásából szerzett ismereteket fel kell használni arra, hogy csökkenjen a jövőbeni incidensek bekövetkezésének valószínűsége és hatása.

A dokumentált információbiztonsági incidensek elemzéséből és megoldásából szerzett tapasztalatokat fel kell használni, hogy csökkenjen a jövőbeni incidensek bekövetkezési

valószínűsége és hatása. Azon incidensek esetén, amelyek várhatóan ismétlődhetnek a szervezeten belül (üzemeltetési incidensek), az incidens leírását rögzíteni kell.

13.1.7 BIZONYÍTÉKOK ÖSSZEGYŰJTÉSE

A szervezetnek meg kell adnia és alkalmaznia kell eljárásokat olyan információk azonosítására, gyűjtésére, beszerzésére és megőrzésére, melyek bizonyítékul szolgálhatnak.

Információbiztonsági incidensek kivizsgálásakor az **Információbiztonsági felelős** elrendelheti az incidensek bizonyítékainak összegyűjtését az érintett munkatársaktól az érintett **Szakterületi vezető** jóváhagyásával. Az összegyűjtött bizonyítékul szolgáló információkat minden esetben meg kell őrizni. Az összegyűjtött bizonyítékoknak minimálisan az alábbi információkat kell tartalmaznia:

- Incidens bekövetkezésének ideje
- Incidens megnevezése, leírása
- Incidens bekövetkezésének helye (pontos fizikai vagy logikai hely)
- Incidens okozójának azonosítása (név, felhasználói név, IP cím stb.)

14 A MŰKÖDÉSFOLYTONOSSÁG BIZTOSÍTÁSÁNAK INFORMÁCIÓBIZTONSÁGI VONATKOZÁSAI

14.1 AZ INFORMÁCIÓBIZTONSÁG FOLYTONOSSÁGA

14.1.1 AZ INFORMÁCIÓBIZTONSÁG FOLYTONOSSÁGÁNAK TERVEZÉSE

A szervezetnek meg kell határoznia az információbiztonsági követelményeit, valamint az információbiztonság irányításának folytonossági követelményeit olyan kedvezőtlen helyzetekben, mint pl. egy válság vagy katasztrófa során.

A Társaság kritikus szolgáltatásait fel kell készíteni a kedvezőtlen helyzetekre, mint például egy válság vagy katasztrófa.

Az üzletmenet-folytonossággal szemben támasztott követelményeket az üzleti hatáselemzés elvégzése után kell meghatározni.

Az üzletmenet-folytonosság (működés-folytonosság) biztosítása érdekében az Üzletmenet-folytonossági felelős (továbbiakban ÜF felelős) feladata a működésfolytonossággal kapcsolatos tevékenységek irányítása: tervezés, megvalósítás, tesztelés, oktatás, monitorozás, karbantartás és a biztonsági követelmények érvényesítése a felsorolt folyamatok során.

Az üzletmenet-folytonossági tervek és azon belül a DR (Disaster Recovery) katasztrófa elhárítási cselekvési tervek célja, hogy megvédjék a vállalatot azoktól a váratlan hatásoktól, amelyek az üzemszerű működést vagy az informatikai rendszerek funkcionalitását veszélyeztetik. Ennek legfontosabb eleme a rendkívüli helyzetekre történő felkészülés. A tervezésnek az a célja, hogy minimalizálja a kockázatokat, és az üzemelési stabilitást egy olyan szinten tartsa, amely a károkhoz mérten optimális költségekkel és gyorsan teszi lehetővé az eredeti állapot helyreállítását.

Az elkészült üzletmenet-folytonossági és katasztrófa elhárítási terveknek megfelelően az üzletmenet-folytonosság megfelelő szintjének biztosításához szükséges készségeket (kompetenciák, tartalék eszközök, tervek stb.) ki kell alakítani.

Oktatásokat kell szervezni, amelynek segítségével az alkalmazottak elsajátíthatják az üzletmenet-folytonossági tevékenységek rájuk vonatkozó feladatait, illetve a kialakított készségek alkalmazását.

A tervek és a készségek alkalmazhatóságáról teszteléssel kell meggyőződni. A tesztelések tapasztalatait minden esetben vissza kell vezetni a tervekre, illetve szükség esetén módosításokat kell végrehajtani a készségekben is.

A tervek elkészítésénél meg kell határozni az ideiglenes, még elfogadható biztonsági szintet, amelyet az üzletmenet-folytonossági és katasztrófa elhárítási incidensek alatt is fenn kell tartani.

14.1.2 AZ INFORMÁCIÓBIZTONSÁG FOLYTONOSSÁGÁNAK MEGVALÓSÍTÁSA

A szervezetnek olyan folyamatokat, eljárásokat és intézkedéseket kell létrehoznia, dokumentálnia, bevezetnie és fenntartania, amelyek biztosítják az információbiztonság folytonosságának elvárt szintjét egy kedvezőtlen helyzetben.

Az üzletmenet-folytonosság biztosítható:

- A kiesett erőforrások megfelelő pótlásával
- Alternatív üzleti folyamatok kialakításával
- A kiesett erőforrások helyreállításával

A kiesett erőforrások megfelelő pótlásához biztosítani kell a szervezetben a humán és technikai erőforrások helyettesíthetőségét. Ezt a szempontot a kompetenciafejlesztésnél is figyelembe kell venni.

Tömeges humán erőforrások kiesése esetén tervekkel kell rendelkezni arra vonatkozóan, hogy krízis helyzetben mely szerepkörök (és a hozzájuk tartozó erőforrások) csoportosíthatók át az alacsonyabb prioritású feladatoktól a magasabb prioritású feladatokra.

A kis megengedett maximális kiesési idővel (<4 óra) rendelkező informatikai erőforrásokra tartalékot kell képezni.

Ha az üzleti folyamatok az őket támogató erőforrások kiesése esetén más módon is működtethetőek (külső szolgáltatások és erőforrások igénybevétele), úgy alternatív üzleti folyamatokat kell dokumentálni annak érdekében, hogy az erőforrások kiesése esetén az üzletmenet-folytonosság fenntartható maradjon.

Amennyiben az üzletmenet-folytonosság alternatív üzleti folyamattal nem biztosítható az üzletmenet-folytonosság fenntartását vagy viszaállítását az üzleti folyamatokat támogató IT erőforrások helyreállításával, DR tervek végrehajtásával kell megoldani.

A működés-folytonosság biztosítására DR terveket kell készíteni a kritikus folyamatokat kiszolgáló eszközökre, melyeket a magas rendelkezésre állásra törekedve kell megvalósítani.

14.1.3 AZ INFORMÁCIÓBIZTONSÁG FOLYTONOSSÁGÁNAK ELLENŐRZÉSE, VIZSGÁLATA ÉS ÉRTÉKELÉSE

A szervezetnek rendszeres időközönként ellenőriznie kell a létrehozott és bevezetett információbiztonsági folytonossági intézkedéseket azért, hogy biztosítani lehessen az intézkedések érvényességét és hatásosságát kedvezőtlen helyzetekben.

A működés-folytonossági tervezéssel kapcsolatos dokumentumokat évente vagy az informatikai rendszerek nagyobb változásánál felül kell vizsgálni, valamint aktualizálni kell, amiért az ÜF felelős felel.

14.2 TARTALÉKOK

14.2.1 INFORMÁCIÓ-FELDOLGOZÓ ESZKÖZÖK RENDELKEZÉSRE ÁLLÁSA

Az információ-feldolgozó eszközöket elegendő tartalékkal együtt kell megvalósítani a rendelkezésre állási követelmények teljesítése érdekében.

15 MEGFELELÉS

15.1 MEGFELELÉS A JOGI ÉS SZERZŐDÉSES KÖVETELMÉNYEKNEK

15.1.1 A VONATKOZÓ JOGSZABÁLYI ÉS SZERZŐDÉSES KÖVETELMÉNYEK AZONOSÍTÁSA

Minden vonatkozó, jogilag kötelező törvényi, szabályozói és szerződéses követelményt és a szervezet ezek teljesítésére irányuló megközelítését egyértelműen azonosítani kell, dokumentálni kell, és napra készen kell tartani minden információs rendszerre és a szervezetre.

A Társaság folyamatainak kialakításakor figyelembe kell venni a vonatkozó törvényi, szabályozói és szerződéses követelményeket, melyek a következők:

Jogszabályok

A vonatkozó jogszabályokat a *„Vonatkozó jogszabályok, ajánlások, belső utasítások és dokumentumok”* fejezet tartalmazza.

Szerződések

A szerződéseket az **Elnök-Vezérigazgató** tárolja és teszi a vezetők számára hozzáférhetővé.

15.1.2 SZELLEMI TULAJDONJOGOK

Megfelelő eljárásokat kell megvalósítani annak érdekében, hogy biztosítani lehessen a jogi, szabályozói és szerződéses követelményeknek való megfelelést a szellemi tulajdonjogok és a jogvédett szoftvertermékek használata terén.

A Társaság és a partnerei között kötött szerződésekben tisztázni kell a szellemi tulajdonjogi viszonyokat a későbbi vitás kérdések elkerülése érdekében.

A Társaság számára fejlesztett szoftverek esetén meg kell követelni, hogy a fejlesztő olyan felhasználási jogokkal ruházza fel a Társaságot, amelyek alkalmasak arra, hogy a fejlesztő cég megszűnése esetén a Társaság a szoftvert tovább fejleszthesse.

15.1.3 A FELJEGYZÉSEK VÉDELME

A feljegyzéseket védeni kell az elveszéstől, a megsemmisüléstől, a hamisítástól, a jogosulatlan hozzáféréstől vagy a jogosulatlan kiadástól, összhangban a jogi, szabályozói, szerződéses és üzleti követelményekkel.

A feljegyzések védelme érdekében a fájlmegosztásra kell menteni az adatokat, amint erre lehetőség van. A papír alapú feljegyzéseket digitalizálni kell, vagy kulccsal zárható szekrényben kell tárolni az irodában.

15.1.4 A MAGÁNTITOK ÉS A SZEMÉLYHEZ KÖTHETŐ INFORMÁCIÓK VÉDELME

A magántitok és a személyhez köthető információk védelmét biztosítani kell, ahogy azt a vonatkozó jogszabályok és szabályozások megkövetelik, ahol helyénvaló.

Az információ feldolgozó rendszer a Társaság tulajdona. Az információ feldolgozó rendszerben magán- és levéltitkot kezelni az alkalmazottak számára tilos.

Amennyiben a felhasználók mégis kezelnek magán- és levéltitkot a rendszerekben, úgy ráutaló magatartással hozzájárulnak ahhoz, hogy azokat a Társaság ellenőrizze.

A munkaállomásokon és mobil eszközökön, továbbá a levelezésben lévő magántitkokhoz csak az adott személy férhet hozzá, távozáskor kérheti ennek elvitelét, melyet az **Elnök-Vezérigazgatónak** kell engedélyezni.

15.1.5 A TITKOSÍTÁSI INTÉZKEDÉSEK SZABÁLYOZÁSA

A titkosítási intézkedéseket a vonatkozó megállapodásoknak, jogszabályoknak és szabályozásoknak megfelelően kell alkalmazni.

A titkosítási intézkedések szabályozásáról a *„Titkosítási intézkedések”* fejezet, a vonatkozó jogszabályokról a *„Vonatkozó jogszabályok, ajánlások, belső utasítások és dokumentumok”* fejezet foglalkozik.

15.2 INFORMÁCIÓBIZTONSÁGI VIZSGÁLATOK

15.2.1 AZ INFORMÁCIÓBIZTONSÁG FÜGGETLEN VIZSGÁLATA

A szervezetnek az információbiztonság felügyeletével és megvalósításával kapcsolatos megközelítését (pl. információbiztonsági intézkedési célok, intézkedések, szabályok, folyamatok, eljárások) független vizsgálatnak kell alávetni előre tervezett időközönként vagy a jelentős változásokhoz kapcsolódóan.

A **Kontrolling és beszerzési igazgatónak** évente kezdeményezni kell az információbiztonság felülvizsgálatát, egy tőle független külső kompetens személy bevonásával.

15.2.2 MEGFELELÉS A BIZTONSÁGI SZABÁLYOKNAK ÉS SZABVÁNYOKNAK

A vezetőknek rendszeresen meg kell vizsgálni a saját felelősségi területükön belül az információfeldolgozás és az eljárások megfelelését a vonatkozó biztonsági szabályoknak, szabványoknak és egyéb biztonsági követelményeknek.

Az **Információbiztonsági felelősnek** évente össze kell gyűjteni a Társaságra vonatkozó szabályokat, szabványokat és egyéb biztonsági követelményeket, melyek által a vezetőségnek felül kell vizsgálni az információfeldolgozás és az eljárások megfelelését.

15.2.3 A MŰSZAKI MEGFELELÉS VIZSGÁLATA

Az információs rendszerek megfelelését a szervezet információbiztonsági szabályainak és szabványainak megfelelően rendszeresen meg kell vizsgálni.

Elsősorban a **Kontrolling és beszerzési igazgató** vagy az ő döntése alapján a **Rendszerkoordinátor** köteles évente felülvizsgálni a Társaság által alkalmazott rendszereket és folyamatokat az információbiztonság szempontjából az **Információbiztonsági felelős** bevonásával.

Az **Információbiztonsági felelősnek** évente meg kell vizsgálnia az információs rendszereket a Társaság információbiztonsági szabályainak és követelményeknek megfelelően.

16 FOGALOMTÁR

Adatgazda: A Társaság adatvagyonáért felelős személy, a Társaságnál ezt a szerepet az **Elnök-Vezérigazgató**, valamint a **Szakterületi vezetők** tölti be.

Adatkezelő: A Társaság által üzemeltetett rendszerekben tárolt adatok, adatcsoportok, adatkörök kezeléséért, menedzseléséért felelős, tipikusan üzleti oldali vezető, akinek a szervezeténél az adat keletkezik.

Bizalmasság: Az információkhoz vagy adatokhoz csak az arra jogosultak és csak az előírt módon férhetnek hozzá. A bizalmasság követelményét a megfelelő hozzáférési jogosultságok beállításával és védelmi intézkedések alkalmazásával lehet elérni.

Eszköz: Mindazon, a Társaság tulajdonát képező vagy általa használt tárgyiasult vagyonelem, melynek, sértetlenségét és rendelkezésre állását az irányítási rendszer keretében védeni kell.

Életciklus: Az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam.

Észlelés: A biztonsági esemény bekövetkezésének felismerése.

Felhasználó: A legalapvetőbb szerepkör, mely a Társaság összes alkalmazottját magába foglalja. A Felhasználó szerepkörön kívül más speciális szerepkörökbe is tartozhat egy-egy alkalmazott.

Fizikai védelem: A fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem.

Hitelesség: Egy információ akkor tekinthető hitelesnek, ha mind tartalmának sértetlensége, mind létrehozójának (küldőjének) kiléte garantálható.

Információbiztonság: Az információ bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása.

Információbiztonsági esemény: Az információ életciklusa (létrehozás, hozzáférés, kezelés, feldolgozás és megsemmisítés) során a normális működéstől, tevékenységtől való eltérést jelző, az információbiztonságot érintő esemény.

Információbiztonsági incidens: Olyan információbiztonsági esemény, vagy azok sorozata, amely az információbiztonsági kontrollokat (védelmi intézkedéseket) károsan befolyásolja, illetve az információbiztonsági, vagy azzal összefüggő szabályok, beállítások megkerülésével, be nem tartásával kapcsolatos, vagy a rendelkezésre állást vagy üzletmenetet olyan mértékben befolyásoló esemény, amely a krízis esemény fogalomkörébe tartozik.

IT Szolgáltató: A Társaság bizonyos (szolgáltatási szerződésben meghatározott) informatikai szolgáltatásokat külső féltől vesz igénybe. Az IBSZ-ben e fél tekinthető az IT Szolgáltatónak.

Katasztrófahelyzet: A Társaság informatikai rendszereit érő bármilyen váratlan esemény, vagy hatás akkor nevezhető katasztrófának, ha:

- A bekövetkező esemény hatására egy vagy több informatikai szolgáltatás kiesett, és
- A kiesett szolgáltatások következtében a Társaság informatikai szolgáltatásainak alaprendeltetésből származó feladatai veszélyeztetve vannak, vagy a működéshez szükséges feltételek megszűnnek, és
- A kiesett szolgáltatásokat a normál működésben meglévő erőkkel, eszközökkel és egyéb készségekkel SLA-n belül helyreállítani nem lehetséges, és
- A normál működésben meglévő erőkkel, eszközökkel és egyéb készségekkel történő helyreállítás időtartamában a Társaság katasztrofális anyagi-, erkölcsi-, vagy jogi károkat szenvedne el.

Kockázatelemzés: Olyan elemző és értékelő jellegű szakértői vizsgálat, amely meghatározott kárértékeken alapulva, a folyamatokat támogató erőforrások – IT rendszer, humán erőforrás, fizikai környezet, kiszervezett tevékenységek – gyenge pontjainak és fenyegetettségeinek elemzése útján meghatározza a fenyegetések bekövetkezése során keletkező potenciális kárértékeket és a fenyegetések bekövetkezési gyakoriságát.

Kockázatértékelés: A Társaságnál alkalmazott jelentésben megegyezik a kockázatelemzéssel, továbbá kiegészül a kockázatok kezelésére alkalmazott ellenintézkedések megfelelőségének értékelésével.

Logikai védelem: Az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.

Napló (naplóállomány): Olyan adatállomány, amely különböző rendszereken, a rendszer működésével, illetve használatával kapcsolatos események gyűjtésére és tárolására szolgál.

Naplóbejegyzés: A naplót alkotó elemi részek, melyek összessége alkotja a naplót. Naplóbejegyzéseket bizonyos felhasználói vagy rendszeresemények bekövetkezését követően állít elő minden eszköz, illetve alkalmazás. A létrejött naplóbejegyzés valamilyen helyi vagy távoli helyen vezetett naplóállományba kerül eltárolásra.

Naplógyűjtő és elemző: Forráseszközökön keletkező naplóbejegyzések központi gyűjtését és elemzését végző rendszer. Feladata a forráseszközök előállított naplóállományok befogadása, tárolása, feldolgozása, majd a beállított szabályrendszere alapján riasztások, jelentések előállítása.

Naplózás: A naplóbejegyzések előállításának és naplóban történő rögzítésének folyamata.

Rendelkezésre állás: Követelmény egy adott rendszer megbízhatóságára. Statisztikailag jellemzi az üzemidő, a rendelkezésre állási tényező és a sebezhetőségi ablak. A rendelkezésre állást véletlen események is fenyegetik, ezért a statisztikai jellemzők garantálása érdekében határozott védelmi intézkedéseket kell megtenni.

Sértetlenség: Egy információ vagy rendszer sértetlen, ha minden kétséget kizáróan megállapítható az a tény, hogy az adat az előállítása óta változatlan maradt, a rendszer pedig a rendeltetésének megfelelően használható.

Tulajdonos: Magyar Állam.

Vagyonelem: Bármi, amelynek a szervezet az információ biztonsága szempontjából értéket tulajdonít, és amelyet védeni kíván. Vagyonelem maga az információ, annak hordozó- vagy feldolgozó eszköze.

Vezetőség: Az **Elnök-Vezérigazgató**, az igazgatók, a minőségirányítás és az értékesítés.

17 A SZABÁLYZAT KARBANTARTÁSA

17.1 A SZABÁLYZAT MÓDOSÍTÁSA

Az Informatikai Biztonsági Szabályzat tartalma, frissítése, karbantartása az **Információbiztonsági felelős** feladata.

17.2 HATÁLYON KÍVÜL HELYEZÉS

Az Informatikai Biztonsági Szabályzat életbe lépésével nem helyez hatályon kívül egyéb szabályozást.

18 MELLÉKLETEK

18.1 HIVATKOZOTT SZABÁLYZATOK ÉS DOKUMENTÁCIÓK

Az alábbi táblázatban került összefoglalásra a dokumentumban hivatkozott szabályzatok és egyéb dokumentációk.

Dokumentum neve
IT eszköz kiosztási lista
Leltározási szabályzat
Iratkezelési szabályzat
Tűzvédelmi szabályzat
Munkavédelmi tájékoztató
Alkalmazotti nyilatkozat
Titoktartási záradék a partneri szerződésekhez

12. Hivatkozott szabályzatok és dokumentációk

18.2 ALKALMAZOTTI NYILATKOZAT MINTA

Név: ..... ,szig. szám: ……..……. a Kartonpack Nyrt. (a továbbiakban: Társaság) munkavállalója kijelentem, hogy információbiztonsági oktatáson 20……-án/én részt vettem és a feladataim ellátásához szükséges ismeretekkel rendelkezem.

Az informatikai eszközök megfelelő használata, illetve az információbiztonsági szabályok betartása közvetett vagy közvetlen védelmet nyújt az információvesztés vagy az információ jogosulatlan személyhez való kerülése ellen.

Tudomásul veszem, hogy a Társaság informatikai rendszerében kezelt szoftverek, fájlok, levelek a Társaság tulajdonát képezik, így azokat a Társaság kijelölt szakemberei ellenőrizhetik.

Minden munkavállalóra egységesen vonatkozó biztonsági szabályok, amelyeknek részletes követelményeit az Információbiztonsági szabályzat (IBSZ) tartalmazza:

Az informatikai eszközök rendeltetésszerű alkalmazása érdekében

- Ügyelek a használatomban lévő informatikai eszközök állagmegóvó tárolására, rendeltetésszerű használatára.
- A biztonságos tárolásról mobileszköz és adat esetén is gondoskodom.
- Amennyiben szervezeti mobiltelefonnal rendelkezem, köteles vagyok a mobiltelefonon:
    - SIM kártya PIN kódot alkalmazni,
    - minimális követelmény szerint legalább 4 karakterből álló jelkódot alkalmazni (a jelkód kiegészíthető egyéb azonosítási módszerekkel, pl.: mintázattal vagy biometrikus azonosítással (ujjlenyomat, arcfelismerés, íriszszkenner), mintázattal történő azonosítás esetén legalább 4 pontból álló mintázat összeállítása szükséges),
    - az automatikus kijelző lezárás funkciót beállítani,
    - az eszköz keresése funkciót engedélyezni (lehetőség szerint), valamint
    - a rendelkezésre álló legfrissebb szoftververzziókat alkalmazni, esetleges információbiztonsági sérülékenységek elkerülése érdekében.

Az informatikai eszközök és adatok biztonságos alkalmazása érdekében

- Csak a Társaság által nyilvántartott és ellenőrzött eszközökkel léphetek be a Társaság hálózatára.
- Kizárólag a Társaság által engedélyezett szoftvereket használom.
- A jelszavaimat és egyéb azonosító kódjaimat titkosan kezelem, azokat nem osztom meg mással.
- A jelszavaimat semmilyen körülmények között nem jelenítem meg a különböző adathordozókon: Jelentéseken, képernyőn, papíron stb.
- Más személy felhasználói azonosítóját és jelszavát nem használom, ezek megszerzésére nem törekszem. Ha ilyen a tudomásomra jut, azt másnak át nem adom, hanem jelzem a

jelszó tulajdonosának és közvetlen vezetőmnek a titkosság megszűnését, és kérem az azonnali jelszómódosítást.
- Az általam menedzselt jelszavakat rendszeresen megváltoztatom.
- Tevékenységem során gondosan járok el és igyekszem megakadályozni illetéktelen személy hozzáférését az informatikai rendszerekhez.
- Tudomásul veszem, hogy csak a munkámhoz feltétlenül szükséges adatok (dokumentumok, levelek stb.) megismerésére vagyok jogosult.
- Az internet és a vállalati levelező rendszer használata során ügyelek arra, hogy az elküldött levelek:
    - Nem tartalmazhatnak olyan információt, amely a Társaság érdekeit sértheti,
    - csak titkosított formában tartalmazhatnak üzleti titkokat és csak munkaköri tevékenység célját szolgálhatják.
- Csak a Társaság által támogatott titkosítási rendszerrel védem adataimat az illetéktelen hozzáféréstől.
- Munkavégzésre nem használok webes levelező alkalmazásokat, erre csak a Társaság vállalati levelező rendszerét használom.
- Nem lehetetlenítem el a vírusellenőrzést.
- Kerülöm az olyan tevékenységet, amelynek célja, vagy előrelátható következménye a Társaság hálózata sértetlenségének, rendelkezésre állásának vagy adata bizalmasságának, sértetlenségének, vagy rendelkezésre állásának bármilyen sérülése.
- Elkerülöm, hogy családtagjaim, ismerőseim bizalmas információk birtokába jussanak otthoni munkám során.
- Nem élek vissza a tudomásomra jutott és az informatikai rendszerben előforduló szoftver és védelmi hiányosságokkal és jelentem az információbiztonsági felelősnek.
- Ügyelek arra, hogy illetéktelen személyek ne olvashassák a monitoron megjelenő információkat.
- Azt a munkaállomást, melyen bejelentkeztem, csak abban az esetben hagyom szabadon, felügyelet nélkül, ha a napi munkavégzés miatt ez indokolt, és:
    - A megnyitott alkalmazásokat a használatot követően bezárom,
    - a munkaállomáson jelszóvédelemmel rendelkező képernyőkímélő (screen saver) van és ezt aktiváltam,
    - vagy a munkaállomásomat zároltam.

Az informatikai eszközök, adatok magánhasználatra történő alkalmazásának elkerülése érdekében

- Nem használom öncélú gazdasági haszonszerzésre vagy egyéb magánjellegű tevékenységre a Társaság által rendelkezésemre bocsátott számítógépet, szoftvert, nyomtatót, és egyéb perifériákat.
- Nem másolom le a munkavégzés céljára nálam telepített szoftvert.
- Magáncélra adatokat nem rögzítek és rögzített céges adatokat engedély nélkül nem viszek ki a Társaság területéről, telephelyeiről.

- A Társaság területére, telephelyeire magántulajdonú adatrögzítésre alkalmas eszközt (pl.: CD-t, DVD-t, pendrive-ot stb.) engedély nélkül nem viszek be.

Szoftverek jogtisztaságának megőrzése

- A Társaság számos külső cégtől vásárolja meg a számítógépes szoftverek licenc engedélyét. A Társaság a szoftver felhasználói szerződéssel nem válik a szoftverek tulajdonosává, és azok dokumentációját és az adathordozókon tárolt program példányait a szoftver tulajdonosának külön engedélye nélkül nem áll jogomban reprodukálni.
- Amennyiben tudomásomra jut, hogy a megvásárolt szoftvert, vagy azzal kapcsolatos dokumentációt nem a fentiek szerint használják, akkor azt köteles vagyok jelenteni a munkáltatói jogkör gyakorlójának.
- Tudomásul veszem, hogy a Büntető Törvénykönyv 385. paragrafusa értelmében az illegális szoftvermásolásban részt vevő személy a törvény értelmében akár 10 évig terjedő szabadságvesztéssel is sújtható.

Jelentési kötelezettségeim

Amennyiben tudomásomra jut, hogy a fenti szabályokat a Társaság munkavállalói közül bárki megsérti, azt köteles vagyok jelenteni a közvetlen vezetőmnek és az Kontrolling és beszerzési igazgatónak.

Záró rendelkezések

A Társaság információs rendszereinek használata során birtokomba kerülő üzleti titkokat és személyes adatokat a vonatkozó szabályok és törvények szerint megőrzöm.

Kijelentem, hogy az itt leírtakat megértettem és azokat magamra nézve kötelezőnek elismerem. Tudomásul veszem, hogy amennyiben az „Alkalmazotti nyilatkozat”-ban leírtakat megszegem, úgy munkajogi, kártérítési és büntetőjogi felelősségem áll fenn.

....., 20..... év ..... hó ..... nap

.....

munkavállaló