"Öcsi Hús" Húsipari, Termelő és Kereskedelmi Zártkörűen működő Részvénytársaság
4700 Mátészalka, Széchenyi u. 178.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Kelt, Mátészalka, 2018. október hó 29. napján

Zemlényi Gyula vezérigazgató

1. szabályzat célja

Az Információbiztonsági Szabályzat (továbbiakban: IBSZ) célja, hogy az „Öcsi Hús" Zrt. (továbbiakban: Társaság) által kezelt adatok és információk biztonságát megteremtse, továbbá intézkedéseket, szabályokat, követelményeket fogalmazzon meg, mellyel az információbiztonsági követelményeket a Társaság hatékony működés mellett biztosítani tudja.

2. A szabályzat hatálya

Az IBSZ alanyi hatálya kiterjed az összes, a Társaságnál fő- és mellékállásban foglalkoztatott alkalmazottra, valamint a szerződéses jogviszonyban álló, vállalkozói és egyéb szerződés keretében foglalkoztatott munkavállalóra (a továbbiakban: felhasználók).

A Szabályzat kiterjed minden nemű adatra és információra, mely a Társaság informatikai vagy egyéb eszközén tárolódik, továbbítódik, beleértve minden papíron található adatot és információt mely a Társasághoz, vagy a Társaság tevékenységéhez, működéséhez köthető.

A Szabályzat kiterjed a Társaság által használt valamennyi informatikai rendszerre, eszközre, amely felhasználja, eléri, tárolja, felügyeli, feldolgozza, továbbítja, vagy megőrzi a Társaságnál keletkező, illetve felhasznált adatokat, információkat és kommunikációt.

3. Kapcsolódó dokumentumok, eljárások

Az alábbi szabályzatoknál és eljárásoknál kizárólag a jelenleg hatályos adott dokumentum szolgál referenciaként az IBSZ számára.

- Informatikai Szabályzat
- Adatok mentése, archiválása és visszaállítása
- Szerver szobába való belépési eljárás
- Vészhelyzeti terv

4. Módosítási előírások

Jelen IBSZ naprakészségét a jogszabályi, funkcionális, szervezeti, technológiai, valamint egyéb változásokra tekintettel az ***IT vezető*** az ***igazgatóság tagjaival*** egyeztetve évente egyszer, vagy a Társaság szervezeti felépítését tekintve nagy változást követő 3 hónapon belül felülvizsgálja és jóváhagyatja a módosítási javaslatait.

5. Jogszabályi környezet

A Társaság tevékenységét szabályozó jogszabályok, kormányrendeletek, felügyeleti és egyéb előírások az alábbiak:

- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.),

- Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete - a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet - GDPR).

Az informatikai biztonságra vonatkozó hazai és nemzetközi szabványok, ajánlások az alábbiak:

- ISO/IEC 27001 Informatika. Biztonságtechnika. Információbiztonsági irányítási rendszerek, követelmények,
- ISO/IEC 27002 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve.

6. Az információbiztonság szabályozása

6.1. Az információbiztonság belső szervezete

A szerepek és felelősségek meghatározása kiemelt fontosságú az információbiztonság fenntartása érdekében a Társaságnál. Annak érdekében, hogy ne alakuljanak ki összeférhetetlen szerepkörök, a felelősségeket teljeskörűen definiálni szükséges. Tekintve a Társaság méretét, valamint informatika munkakörben dolgozói számát, az IT biztonságért az ***IT szakértő*** a felelős:

- A Társaság információbiztonsági stratégiájának megtervezése, támogatása, kivitelezése;
- Az információbiztonsági oktatások tartalmának meghatározásáért;
- Az információbiztonsági követelmények meghatározásáért;
- Minden nemű informatikai változtatás, vagy bevezetés esetén, a projekt során az információbiztonságira vonatkozó követelmények meghatározásáért és betartatásáért;
- Információbiztonsági incidensek kezeléséért, kivizsgálásáért;
- Auditok támogatásáért;
- Biztonsági beállítások biztosításáért;
- A külső felekkel való együttműködés kockázatainak azonosítása, szükség esetén a kockázatok csökkentése;

A ***HR*** felelős az alábbiakért az információbiztonsággal összefüggésben:

- Az informatikai környezethez hozzáférő munkatársak kiválasztási folyamatában az információbiztonsági követelmények teljesülésének biztosítása;
- Az információbiztonság kulcsszereplőinek foglalkoztatásával kapcsolatos feladatok és felelősségek meghatározásáért az IT-val együttműködve;

- Az alkalmazások tekintetében a felhasználói hozzáférési jogosultságok visszavonásának kezdeményezése egy felhasználó távozásakor, illetve szervezeten belüli mozgásakor;
- A biztonságtudatosság képzési és oktatási feltételeinek meghatározása és menedzselése.

A ***Felhasználók*** felelősek az alábbiakért az információbiztonsággal összefüggésben: Az IT biztonsággal kapcsolatban a felhasználókra vonatkozó szabályokat, felelősségeket és iránymutatásokat a Felhasználói IT Biztonsági Kézikönyv tartalmazza, de a Társaság minden felhasználójának kötelessége a további IT biztonsági szabályzatok megismerése, továbbá:

- Az informatikai erőforrások rendeltetésszerű használata;
- Az információbiztonsági szabályzatokban, különösen a Felhasználói IT Biztonsági Kézikönyvben rögzített követelmények, előírások betartása;
- Az általa használt alkalmazások felhasználói leírásainak ismerete és az alkalmazások használatakor azok betartása;
- A kezelésében álló alkalmazói rendszerekkel és informatikai eszközökkel kapcsolatos, illetve az általános információbiztonsági oktatásokon való részvétel;
- IT biztonsági események azonnali jelentése az IT Biztonsági Felelős felé.

Külső féllel kötött szerződések biztonsági követelményei

Külső felekkel kötött szerződések esetén az alábbiakat szükséges ellenőriznie az IT Biztonsági Felelősnek:

- Gondoskodik arról, hogy a külső szolgáltatóval kötött informatikai szerződésekben az információbiztonsági követelmények meghatározásra kerüljenek.
- Külső szolgáltatóval kötött informatikai szerződésekben az átfogó, folyamati, adminisztratív jellegű, műszaki, technológiai információbiztonsági követelmények meghatározása megtörtént.
- A meghatározott információbiztonsági követelmények megvalósításának, teljesülésének ellenőrzése, véleményezése.
- Külső féllel szemben támasztott szolgáltatási szintek meghatározása.
- A külső fél által vállalt szolgáltatási szintek ellenőrzése.
- A külső fél korábbi adatbiztonsági incidenseinek ellenőrzése.

6.2. Vagyontárgyak kezelése

6.2.1. Adatok osztályozása

A Társaságnál tárolt és kezelt adatok védelme érdekében ki kell alakítani osztályozási és kezelési módszertant. Az adatok kategorizálásánál figyelembe kell venni az adat sértetlenségét, bizalmasságát és rendelkezésre állását.

Az IT Biztonsági Felelős felelőssége

- A Társaság adatvagyonát felmérni és minden olyan rendszerhez, alkalmazáshoz, mely adatokat tartalmaz, felelőst, adatgazdát kijelölni, akik rendelkeznek a feladatuk ellátáshoz szükséges szakértelemmel és megfelelő erőforrásokat kell biztosítani számukra feladatuk ellátásához;
- az adatokat bizalmassági osztályokba kell besorolni:
    - nyilvános adatok
    - belső adatok
    - bizalmas adatok
- az alkalmazásokat és rendszereket is bizalmassági osztályba kell sorolni, melyet a rendszer által kezelt legszigorúbb bizalmassági osztályba tartalmazó adat határozza meg, azaz ha a legszigorúbb adat, amelyet a rendszer kezel "Belső adat", akkor a rendszer bizalmassági osztálya is ez alapján kerül besorolásra;
- minden harmadik félre vonatkozó bizalmas adatot úgy kell kezelni, mintha a Társaság bizalmas adatai lennének;
- személyes adatokat csak indokolt esetben kell tárolni, kezelni, valamint a GDPR-ban megfogalmazottak szerint kell eljárni velük.

6.2.2. Informatikai eszközök leltározása

A Társaságnál használt informatikai eszközöket nyilvántartásba kell venni.

Az IT Biztonsági Felelős felelőssége:

- a Társaság informatikai vagyontárgyairól vagyonleltárt készítsen;
- évenként felülvizsgálja az informatikai vagyonleltárt.

Az informatikai leltárnak az alábbiakat tartalmaznia kell (ahol értelmezhető az adott paraméter):

- a vagyontárgy típusa (szoftver, hardver, adat, üzleti folyamat);
- a vagyontárgy formátuma (elektronikus, papír, eszköz);
- a vagyontárgy kiépítése, architektúrája, moduljai;
- a vagyontárgy fellelhetőségének helye;
- a vagyontárgy telepítésének, használatbavételének idejét;

- a vagyontárgyhoz kapcsolódó licence információkat;
- a vagyontárggyal kapcsolatos felelősségeket.

6.2.3. Az informatikai vagyontárgyak felelősei

Az IT Biztonsági Felelős felelőssége:

- A Társaságban kijelölni a vagyontárgyakért felelős vezetőket és felhasználókat;
- naprakész állapotban, dokumentáltan vezetni az informatikai vagyonleltárt.

6.2.4. A vagyontárgyak elfogadható használata

Informatikai eszközök beszerzése

Az informatikai eszközök beszerzésével kapcsolatos szabályokat a "Informatikai Szabályzat" II. pontja tartalmazza.

Informatikai eszközök kezelése, használata

A beszerzést és nyilvántartásba vételt követően az informatikai eszközök üzembe helyezését kizárólag az IT alá tartozó munkatársak végezhetik. Az üzembe helyezést követően az eszközök átadása átadás-átvételi jegyzőkönyv aláírása mellett kerül sor, melynél a felhasználó nyilatkozik a felelősségéről az adott eszközt illetően.

Az eszközök elvárt kezelésénél minden felhasználónak legalább az alábbiakat kötelezően be kell tartania:

- Hiba esetén azonnal kötelesek jelezni a hibát az IT szakértő felé;
- Kötelesek betartani a munka és tűzvédelmi, biztonsági előírásokat, szabályokat;
- Tilos az eszközöket megbontani, felbontani, nem rendeltetésszerű használat alá kitenni;

A notebook-okkal kapcsolatos szabályokat az *"Informatikai Szabályzat"* III. pontja tartalmazza.

Informatikai eszközök selejtezése

Az eszközök selejtezésére vonatkozó szabályokat az "Informatikai Szabályzat" VIII. pontja tartalmazza

6.3. Személyi biztonság

A megfelelő munkaerő kiválasztása fontos része az informatikai biztonság fenntartásának. Új munkaerő felvételnél fontos ellenőrizni, hogy a jelölt képes e megfelelően betartani az információbiztonsági elvárásokat, melyet a Társaság elvár.

6.3.1. Átvilágítás

Tekintve, hogy a Társaság jogilag nem kötelezett semmilyen típusú átvilágításra a munkaerőt figyelembe véve, a HR felelős azért, hogy meghatározza mikor szükséges részletesebb háttérvizsgálat egy-egy új jelentkező esetében a foglalkoztatást megelőzően, a betöltendő munkakör kockázataival arányos mértékben.

6.3.2. A foglalkoztatás feltételei

Az HR felelős azért, hogy

- a munkavállalóval kötendő szerződésben rögzítésre kerüljenek a kockázatokkal arányos titoktartási követelmények és a foglalkoztatás egyéb kikötései.

A Section Managerek (SM) felelőssége, hogy

- A foglalkoztatás során megköveteljék az információbiztonsági szabályzatokban meghatározott előírások betartását és végrehajtását.

6.3.3. Oktatás, képzés

Az IT Biztonsági Felelős és a HR közösen felelősek az alábbiakért:

- Rendszeres információbiztonsági oktatások tartása a felhasználók számára az információbiztonság fenntartása érdekében;
- Adatok biztonsági osztályba sorolásának megfelelő oktatása;
- A biztonsági események jelentésével, kezelésével kapcsolatos oktatás;
- A legfrissebb fenyegetésekkel, veszélyforrásokkal, a védelmet szolgáló biztonsági eszközökkel, technikákkal kapcsolatban az informatikai és az információbiztonsági munkatársak részére.

Az IT Biztonsági Felelős felel

- hogy csak a megfelelő oktatásban részesült munkavállalók férhessenek hozzá a releváns rendszerekhez;
- a belső információbiztonsági oktatások tartalmának megfelelőségéért.

6.4. Hozzáférés menedzsment

6.4.1. Hozzáférés menedzsment üzleti követelményei

- A hozzáférési jogosultságok kialakítását, szabályozását az informatikai oldal elvárásai, és a Társaság feladatai összehangolásának figyelembevételével kell meghatározni.
- A jogosultsági rendszer használható és biztonságos megvalósítása érdekében felhasználói csoportokat kell kialakítani.
- A csoportok számára a munkavégzésükhöz szükséges minimális jogosultságokat tartalmazó hozzáférési rendszer kialakítása szükséges.

- A használt rendszerekben gondoskodni kell a felhasználók egyedi azonosításáról.
- Külső személyek (támogatók stb.) számára ideiglenes jogosultság biztosítása szükséges, továbbá a tevékenység naplózását biztosítani kell.
- Korlátozni kell az IT munkatársak felhasználói jogosultságát.

A kialakított követelményrendszer aktualitását legalább évente egyszer vizsgálni kell és a változásoknak megfelelően módosítani szükséges. A jogosultságokat a Section Managerek határozzák meg a saját területük anyagait illetően. Az IT szakértőnek a jogosultságokról az illetékes Section Manager által aláírt listával kell rendelkeznie, módosításra az SM írásos engedélyével kerülhet sor.

Az ellenőrzés során vizsgálni kell:

- a kialakított csoportok aktualitását;
- a felhasználók nem rendelkeznek-e több vagy kevesebb joggal, mint amit a munkakörük megkíván;
- az ideiglenesen kiosztott jogok, kilépett dolgozók jogosultságai visszavonásra kerültek-e.

6.4.2. Hozzáféréssel kapcsolatos igények kérésének módja

A munkavállalók részére a számítógépes rendszerekhez történő hozzáférést, annak módosítását a HR kéri. A kilépő munkatárs számítógépes hozzáférésének megszüntetési kérelmét szintén a HR kezdeményezi.

- Jogosultság csak a munkaköri feladatok ellátásához igényelhető.
- A felhasználó munkaviszonyának megszűnése esetén jogosultságait a munkaviszony megszűnésének ismertté válásakor azonnal korlátozni kell, illetve a munkában töltött utolsó nap végén véglegesen vissza kell vonni.

6.4.3. Jelszómenedzsment

A Társaság informatikai rendszereihez való illetéktelen logikai hozzáférések megakadályozására bejelentkezési jelszavakat kell létrehozni mind a felhasználók, mind a rendszergazdák számára.

- A jelszókövetelmények meghatározása, kockázatarányos módon, az adott rendszer technikai lehetőségeit figyelembe véve az IT Biztonsági Felelős felelőssége.
- A jelszavak kiosztása minden esetben zártan kell, hogy történjen.

A felhasználói jelszavak meghatározásának a következő kritériumok figyelembe vételével kell történnie:

- Minimális hossz: 8 karakter;
- Érvényessége: 60-90 nap;
- Megváltoztatás esetén az utolsó 10 jelszó használata nem megengedett,

- A jelszavak komplexitásánál az alábbiak közül valamennyi elvárásnak teljesülnie kell
    - Kisbetű;
    - Nagybetű;
    - Szám;

Jelszavakat kizárólag megfelelő kulcshosszúságú irreverzibilis titkosítással (kriptográfia hash algoritmus) kell tárolni az informatikai rendszerekben. A megfelelő hash függvények kiválasztása az IT Biztonsági felelős felelőssége.

A Biztonsági felelősnek az alábbiakra kell felhívni a munkavállalók figyelmét a jelszó választásánál és használatánál:

- tartsa titokban a jelszavait;
- kerülje a jelszavak papírra rögzítését, hacsak nem tudja azt biztonságosan tárolni;
- mindannyiszor és mindakkor cseréljen jelszót, ha bármi jel mutat arra, hogy a rendszer vagy jelszó veszélyeztetve van;
- nem alapoz olyanra, amelyet bárki könnyen kitalálhat, vagy az illető személyével kapcsolatos adatokból kinyerhet, például nevekből, telefonszámokból, születési adatokból stb.
- nem tartalmaz azonos karaktereket, illetve sem csupa számokból, sem csupa betűkből álló csoportokat
- ne osztozzon mással egyéni felhasználói jelszavakon

Adminisztrátori felhasználókhoz tartozó jelszavak tárolása

- A kiemelt jogosultságokkal rendelkező felhasználókhoz tartozó jelszavakat a Társaság erre a célra kijelölt páncélszekrényében kell tárolni.

6.4.4. Felügyelet nélkül hagyott informatikai eszközök

A Társaság munkavállalóinak az informatikai biztonság megtartása érdekében felelősséggel kell bánniuk a munkaeszközeikkel, valamint környezetükkel.

Ennek érdekében a következő szabályokat kell betartaniuk:

- A munkaállomást jelszavas képernyővédővel kell védeni. A képernyővédő indításának maximum 15 perc kihasználatlanság után meg kell történnie.
- A jelszavas képernyővédő paramétereinek beállítása az IT szakértő feladata.
- Ha a felhasználó a munkaidő végén távozik, a munkaállomást mindig ki kell kapcsolnia. Ez alól kivételt képeznek a hosszan futó adatfeldolgozások, valamint a távoli elérésű számítógépek. Ezekben az esetekben azonban a munkaállomást zárolni kell.

6.4.5. Hálózati szintű hozzáférés ellenőrzése

Külső hálózattal való hálózati összeköttetés esetén az **IT Biztonsági Felelős** köteles arról gondoskodni, hogy csak az arra jogosult személyek juthassanak információhoz a Társaság adatállományából.

6.4.6. A rendszerek használatának monitorozása

A hálózat használatát ellenőrizni kell, a felhasználók által használt forgalmat figyelembe véve. A levelező rendszerrel kapcsolatos felügyeleti információkat az *"Informatikai Szabályzat"* VI. pontja tartalmazza.

6.4.7. Távoli elérés, távmunka

A laptopokkal rendelkező és ideiglenesen azt külső helyszínen használó munkavállalók számára elengedhetetlen a hálózat távoli elérése. Ennek érdekében a Társaságnál VPN alapú távoli elérés támogatott.

Távoli elérés használatára vonatkozó előírások:

- A VPN bejelentkezéshez külön felhasználó nevet és jelszót kell használniuk a felhasználóknak. A szükséges beállításokat az **IT Biztonsági Felelős** végzi el.

6.4.8. Mobil eszközökre vonatkozó szabályok

A Társaságnál használatban levő laptopok esetében a biztonsági követelmények magasabbak, mint a Társaság épületeiben használt PC-k esetében, mivel fizikailag könnyebben elérhetőek a támadók számára.

- A hordozható számítógépek merevlemezeit titkosítani szükséges egy korszerű titkosítási mechanizmus által, mely lehet a Windows beépített BitLocker megoldása, vagy egyéb elismert, titkosításra szakosodott cég termékének e funkciója.
- Jelszavas képernyővédő használata 5 perc elteltével szükséges.
- A hordozható számítástechnikai eszközöket szigorúan óvni kell. Gondoskodni kell az eszközök fizikai védelméről és nyilvános helyen (például személygépkocsiban, szemmel látható helyen) nem szabad felügyelet nélkül hagyni őket.
- A számítógép eltulajdonítása esetén azonnal értesíteni kell az **IT Biztonsági Felelőst,** aki intézkedik a megfelelő személyek értesítéséről.

6.4.9. Okostelefon használatra vonatkozó szabályok

A készülékeken nincsen korlátozva az alkalmazások telepítése, a felhasználó felelőssége, hogy milyen alkalmazásokat telepít az eszközökre, azonban nem megbízható forrásból a telepítés tilos. Kizárólag a hivatalos alkalmazás-boltokból engedélyezett az alkalmazások beszerzése.

- Az eszközökön az operációs rendszerek frissítése kötelező. Ezek a frissítések valamennyi esetben biztonsági javításokat is tartalmaznak, ezért ezek nem telepítése veszélyezteti a telefon biztonságát.

- A felhasználó kötelessége megelőzni a készülék eltulajdonítását. Amennyiben ez mégis megtörténik, azt haladéktalanul jelezni köteles az IT Biztonsági Felelős felé.
- Csak olyan okostelefon használható a Társaság adatainak kezelésére, tárolására, mely központilag, távolról menedzselhető, tiltható.
- Az okostelefonok IT általi biztonsági beállításait megváltoztatni tilos: 2 perc inaktivitás után a telefonnak zárolódnia kell; minimum 4 karakteres jelszavas védelem szükséges; 5 sikertelen jelszóbeírás után le kell tiltani a további próbálkozásokat 30 perces időtartamra.
- Bluetooth kapcsolaton keresztül csak azonosított eszközök csatlakozhatnak egymáshoz, automatikusan nem, a felhasználó felelőssége, hogy mely egyéb eszközzel engedélyezi a Bluetooth kapcsolat felépítését.
- Okostelefonok csak titkosított csatornán keresztül csatlakozhatnak a hálózatba kapcsolt számítógépekhez, előzetes azonosítás után.
- Nyilvános Wi-Fi-k használata nem javasolt, kizárólag, ha a felhasználó teljesen megbizonyosodott, hogy az megbízható forráshoz tartozik (pl.: ügyfél, állami hivatal). Hotelek, éttermek és egyéb nyilvános helyeken a Wi-Fi-k használata nem engedélyezett.

6.5. Fizikai biztonság

- A szerverszoba a pénzügyi irodában található, kulccsal csak a biztonsági szolgálat és a társaság tulajdonosai rendelkeznek.
- A klíma a szerverszobában redundáns, a falak tűzbiztosak.
- Tűzjelző és tűzoltó készülék rendelkezésre áll.

A szerverszobába való belépéssel kapcsolatos szabályokat a *"Szerver szobába való belépési eljárás"* tartalmazza.

- A szerverek áramellátását (minden kritikus rendszerelemre tekintettel) szünetmentes áramforrással kell biztosítani (legalább az eszközök szabályos leállását lehetővé tevő kapacitással).

6.6. Üzemeltetés biztonsága

6.6.1. Üzemeltetési szabályzatok

A Társaság informatikai rendszereinek üzemeltetéséért és adminisztrálásáért, valamint az üzemeltetéssel kapcsolatos dokumentált eljárásokért (üzemeltetési szabályozások) az IT Biztonsági Felelős van kijelölve. Ő a felelős azért, hogy az üzemeltetési tevékenységekhez szabályzat is készüljön, melyeket az érintett területeknek el kell juttatnia, valamint az ő feladata a szabályzatok évenkénti felülvizsgálata.

6.6.2. Kapacitástervezés

Annak érdekében, hogy a Társaságnál, a rendszerek működése és az új rendszerek bevezetése a lehető leghatékonyabban történjen, szükséges az informatikai

rendszerek működéseinek mérése, mellyel az informatika rendelkezésre állását, bizalmasságát, és sértetlenségét is optimális mértékben lehet fenntartani. A mérések módjainak meghatározásáért valamint a mérésekben szereplő paraméterek kijelöléséért az **IT Biztonsági Felelős** van megbízva, akinek jelentési kötelezettsége van az **Adminisztrációs igazgató** felé.

6.6.1. Kriptográfiai óvintézkedések

Az adatok védelméről kriptográfiai eljárások segítségével kell gondoskodni. Az Társaságnál az üzletileg kritikus rendszerek esetén kell a megfelelő kriptográfiai eszközök használatát bevezetni, illetve szabályozni, ezzel biztosítva az üzletileg kritikus adatok sértetlenségét, bizalmasságát.

Az adatok idegen kézbe kerülésének megakadályozása érdekében a kockázattal arányos titkosítási eljárásokat kell alkalmazni a titkos adatállományok tárolásakor és továbbításakor. A kockázati besorolást, valamint a titkosítási metódust az IT Biztonsági Felelős határozza meg.

Amennyiben technikailag nem megoldható valamely szoftver esetében a meghatározott titkosítási metódus használata, az **IT Biztonsági Felelős és Adminisztrációs igazgató** jóváhagyásával alacsonyabb besorolásnak megfelelő titkosítás is alkalmazható.

A jelszavak és személyes adatok titkosításának meghatározása kiemelt fontossággal bír, melyeknél csak igazgatók jóváhagyásával csökkenthető a titkosítás mértéke.

A megfelelő kriptográfiai eljárásokat az adatok besorolási kategóriái alapján az **IT Biztonsági Felelős** határozza meg.

6.6.2. Vírusvédelmi tevékenységek szabályozása

Az informatikai infrastruktúra és az adatok védelmének biztosítására szolgáló eljárások között alapvető a hatékony vírusvédelem kiépítése és folyamatos működtetése, amely megvédi az informatikai rendszereket a rosszindulatú, romboló hatású programok elterjedése ellen.

A Társaság vírusvédelmét az Trend Micro vírusirtó rendszere valósítja meg.

Ez a modul felelős a friss vírusadatbázisok letöltéséért, azok kliens gépekre való telepítéséért. Az aktív védelem kikapcsolása tilos a felhasználók számára. A hordozható számítógépek vírusadatbázisainak frissítéséért a számítógép felhasználója felelős. A Társaság hálózatára való csatlakozásakor a vírusadatbázis-frissítés és - ellenőrzés automatikusan megtörténik, melynek beállítása és ellenőrzése az **IT** feladata. Amennyiben az ilyen gép internetre csatlakozásakor a frissítés automatikusan nem történne meg, a frissítést manuálisan kell kezdeményezni.

Az **Informatikai szakértő** ezzel kapcsolatos feladatai:

- a vírusdefiníciós állományok naprakészen tartása,

- a felhasználók oktatása a vírusvédelem működési és esetleges frissítési módjairól,
- új program üzembe helyezése, mentett adatállomány visszatöltése, valamint vírusfertőzés alapos gyanúja esetén rendkívüli vírusellenőrzés végrehajtása,
- vírusfertőzés esetén a felhasználók értesítése, a vírusirtás elindítása és lezárása, az ő vezetésével történik a fertőzött számítógépek vírusmentesítése,
- vírusfertőzés esetén ellenőrizni kell mindazon adathordozót, amelyek a számítógéppel a vírusfertőzésig kapcsolatba kerültek. Ha az **IT szakértő** olyan adathordozót talál, amely eltávolíthatatlan vírussal fertőzött, azt meg kell semmisíteni, kivéve akkor, ha nyomozati okokból a rosszindulatú szoftver elemzésére van szükség. Ebben az esetben az adathordozót az érintett gépből ki kell szerelni.

6.6.3. Mentési, archiválási, visszatöltési tevékenységek szabályozása

A Társaságnál minden informatikai rendszerre mentési, visszatöltési, archiválási folyamatot kell kidolgozni. Az eljárásokat az "Adatok mentése, archiválása és visszaállítása" szabályzat tartalmazza részletesen.

6.6.4. Szoftverek kezelése

Az informatikai biztonság megvalósításához hozzájárul a szoftvereszközök jogszerű használata, valamint szoftverek biztonságos kezelése, melyet a Társaság kiemelten korlátoz. A szoftverekkel kapcsolatos szabályokat az *"Informatikai szabályzat"* IV. pontja fejti ki bővebben.

A felhasználókra nézve kiemelt fontosságú, hogy a felhasználók kizárólag jogtiszta szoftvereket használhatnak, melynek elmulasztása fegyelmi eljárást vonhat maga után, valamint figyelmeztetést.

6.7. Kommunikáció biztonsága

6.7.1. Cserélhető adathordozók

Üzleti titkot, személyes adatot, vagy egyéb nem nyilvános adatot USB tárolóra, CD-re, vagy DVD lemezre csak titkosítva szabad másolni az illetéktelen hozzáférés megakadályozása céljából.

Adathordozók tárolására vonatkozó szabályok:

- figyelembe kell venni a gyártó által meghatározott tárolási környezetre vonatkozó paramétereket, a tároló helynek tűzbiztos, elektromágneses hatásoktól védett helynek kell lennie.

A Társaság hivatalos helyiségeiben található adathordozók a tárolás helyéről csak az **IT szakértő** engedélyével távolíthatók el a betekintésre jogosultak által. Az adathordozók átadásáról az iktatókönyvet kell vezetni. Az adathordozót szállítás során védeni kell minden sérüléstől és káros fizikai hatástól.
A kiszállításnak, rendeltetési helyre való megérkezésnek, illetve visszaszállításnak dokumentáltnak kell lennie. Az adathordozók használata során figyelni kell a gyártó által meghatározott selejtezési időpontra, ezen idő után nem biztonságos a használatuk.

Az elavult, meghibásodott hardverek és eszközök selejtezéséről az *"Informatikai szabályzat"* VIII. pontja ír részletesen. Egyéb esetben történő selejtezésről szintén az „"Informatikai szabályzat" VIII. pontja ír.

6.7.2. Elektronikus levelezés biztonsága

Az elektronikus levelezés lehetővé teszi az alkalmazottak és partnerei közötti adatcserét és információáramlást. Annak érdekében, hogy levelező rendszer használatából eredő támadások lehetősége minimálisra csökkenjen, a Társaság felhasználói csak az IT által engedélyezett szoftvert használhatják, akiknek biztosítania kell a ki- és bemenő levelek vírusellenőrzését és a spam-szűrést.

A ki- és bemenő levelek méretkorlátozását 5 MB–ban kell megállapítani, valamint a nem kívánatos fájltípusokra (futtatható állományok stb.) szűrést kell végezni. A beállítások megvalósítása az **IT szakértő** feladata.

Az elektronikus levelezésre vonatkozó általános szabályokat az „"Informatikai szabályzat" VI. pontja határozza meg

- A felhasználók kötelesek naponta ellenőrizni e-mail üzeneteiket. A munkavégzéssel kapcsolatosan már nem használható leveleket rendszeresen el kell távolítani a felhasználók postafiókjából.
- A levelet csak akkor szabad megnyitni, ha a levél megbízható feladótól származik. Nem szabad megnyitni például az angol nyelven írt, nyereményekre és ismeretlen, megrendelt küldeményekre utaló leveleket, ezeket haladéktalanul törölni kell. Az információbiztonsági oktatásokon elhangzottaknak megfelelően kell a linkeket megnyitni, abban az esetben is, ha a küldő ismerősnek tűnik. Ha a felhasználó bizonytalan a levéllel kapcsolatos teendőt illetően, köteles az **IT szakértő** segítségét kérni.
- A felhasználóknak tilos láncleveleket készíteni és továbbítani. Tilos továbbá más felhasználóktól, illetve külső hálózatról kapott támadó, vagy „szemét" („junk") jellegű, a hálózat túlterhelését célzó e-mailek megnyitása, továbbítása. Az ilyen levelek automatikus kiküszöböléséhez az **IT szakértő** segítséget nyújt.
- A felhasználóknak tilos a Társaság nevében olyan e-mailt küldeni, csatolt fájlt megjelentetni elektronikus hirdetőtáblákon vagy egyéb fórumokon, melyek:
  - a Társaság hírnevét, vagy az ügyfelekkel való kapcsolatát ronthatják, illetve a SEH ügyfeleinek érdekét sérthetik,
  - a Társaság bizonyos területekre vonatkozó álláspontját képviselik, fejezik ki,
  - szerzői jogokat sérthetnek,
  - vírusokkal fertőzhetnek meg bármely hálózatot.

- A felhasználók az céges e-mail címükkel semmilyen levelezőlistára, hírcsoportra nem iratkozhatnak fel, nem jelentkezhetnek be.
- A felhasználók személyes levelezésre a Társaság levelező szoftverét nem használhatják.
- A felhasználó által küldött elektronikus leveleket a felhasználónak saját nevével, azonosítható módon kell aláírnia. Nem használható a SEH elnevezése egyedüli aláírásként.

- A felhasználók üzleti titkokat tartalmazó levelet, dokumentumot nyilvános levelező rendszer felé (pl.: gmail.com) küldeni, továbbítani, csak üzleti folyamathoz kapcsolódóan lehet. A felhasználók munkavégzéshez kapcsolódó anyagokat saját nyilvános levelezőrendszerükre és nyilvános fájlmegosztó szolgáltatások tárhelyeire nem küldhetnek.

6.7.3. Internet szolgáltatások

A Társaság informatikai rendszereit fenyegető veszélyek száma nő az Internetre való kapcsolódással. Az így keletkező veszélyforrások kiküszöbölése a szükséges technikai feltételek megteremtésével és az előírások betartásával lehetséges.

A Táraság internet használattal kapcsolatos szabályait az "Informatikai szabályzat" V. pontja tartalmazza.

Az **IT szakértő** feladata a felhasználók Internethez való hozzáférésének, a bejövő és kimenő adatforgalom naplózásának kialakítása az esetleges visszaélések kiszűrése érdekében. Ennek támogatására a Társaság a Barracuda megoldását használja. Ezzel együtt minimalizálni kell a személyes Internet használatot, és ügyelni kell a Társaság szakmai jó hírnevére.

A böngésző Internet biztonságát közepesnél alacsonyabbra állítani tilos.

A **felhasználókra** vonatkozó szabályok:

- az Internetes szolgáltatásokat kizárólag az **IT** által lehetővé tett módon, hálózaton keresztül vehetik igénybe.
- az Internetről csak a munkavégzéshez szükséges adatállományok, táblázatok, tölthetők le, a hálózatra csatlakoztatott gépre, amelyeket a vírusvédelmi rendszernek automatikusan kell ellenőriznie.
- file-ok letöltése nem megengedett abban az esetben, ha a számítógép „Nem biztonságos hely"-et jelez. Tilos továbbá a több MB méretű zenei és video típusú file-okat letölteni.

6.8. Informatikai rendszerek fejlesztése és karbantartása

A Társaság informatikai rendszereinek módosítását, továbbfejlesztését, valamint új szoftverek fejlesztését az üzleti oldal elvárásaihoz kell igazítani.

6.8.1. Fejlesztőkkel szemben támasztott követelmények

A fejlesztést végző külső vállalkozóval kötött szerződésben meg kell fogalmazni azokat a kötelezettségeket, szankciókat, amelyek a feladat hiányos, vagy nem a specifikációnak megfelelő teljesítése esetén lépnek érvénybe, ki kell térni a forráskód átadására, átvizsgálására vonatkozó elvárásokra, amelyek az informatikai biztonságot növelik, és a lehetséges betörések számát hivatottak csökkenteni.

A belső fejlesztési projektek és szoftverek esetében meg kell határozni az eredménytermékek és programkódok tulajdonosát.

6.8.2. Tesztrendszerek kialakítása

Minden egyes alkalmazás üzembe helyezését meg kell előznie egy tesztelési folyamatnak, amelyet az éles környezettől elkülönített teszt környezetben kell elvégezni. Az üzembe helyezés tényét külön dokumentumban rögzíteni kell, melynek felelőse az IT Biztonsági Felelős.

Az informatikai rendszerek fejlesztése során az IT Biztonsági felelős felelőssége hogy a fejlesztés elkülönüljön tesztelési és éles környezetekre az alábbi intézkedések betartása mellett:

- a fejlesztési és az éles szoftvert különböző környezetben kell futtatni;
- hozzáférési jogosultságok megfelelő kialakításával biztosítani kell, hogy a fejlesztők és nem üzleti tesztelők ne férhessenek az éles rendszerhez;
- gondoskodni kell arról, hogy a fejlesztői rendszerekben ne legyenek éles adatok.

6.8.3. Tesztelési környezet kialakítása

A tesztelés környezetének kialakítása az IT Biztonsági Felelős feladata. A tesztkörnyezet kialakításánál figyelembe kell venni az alábbiakat:

- a tesztelést végző személyeket az IT Biztonsági Felelős jelöli ki a felhasználók közül az üzleti oldal igényeit figyelembe véve;
- a tesztelők nem férhetnek hozzá a program forrás könyvtárához;
- a tesztelést végzők jogosultságait másképp kell meghatározni, mint a fejlesztőkét;
- a tesztelési környezetnek maximálisan meg kell felelnie az éles környezethez funkcionalitásában és környezetében egyaránt.

6.8.4. Tesztadatok biztonsága

A tesztelésnél használt adatokat a szoftverek lehetőségeit figyelembe véve nem éles adatokból kell meghatározni. Az adatok tesztkörnyezetbe való betöltéséért az **IT szakértő** a felelős. Fejlesztői környezetben éles adatok használata nem megengedett, kivéve, ha arról külön utasítás érkezik az IT Biztonsági Felelőstől valamilyen technikai okból adódóan.

6.8.5. Változáskezelés az informatikai rendszerek fejlesztésében

A Társaságnál a változások kezelésére eljárást kell kidolgozni, amely biztosítja a tervezett és végrehajtott változások nyomon követését és visszakereshetőségét.

Amennyiben bármely felhasználónak igénye van valamely informatikai rendszer, vagy alkalmazás megváltoztatására, vagy továbbfejlesztésére, azt közölnie kell az **IT szakértővel** elektronikus levelezés által.

Az **IT szakértő** feladata:

- a változtatásra, fejlesztésre vonatkozó igény szükségességének megítélése;

- erőforrás szükségletének felbecsülése;
- várható hatásainak felmérése;
- az igény támogatása esetén javaslat előterjesztése;
- a változás kivitelezésének koordinálása, beleértve a verziókezelés megvalósítását és dokumentálását.

Az igény elfogadásáról a **Gazdasági vezető** dönt, aki egyeztet az Ügyvezető Igazgatóval.

A kivitelezés megkezdése előtt az **IT vezetőjének** gondoskodnia kell arról, hogy a szükséges dokumentációk elkészüljenek és a rendszer visszaállítható legyen a legutolsó működőképes állapotra.

Az elkészült változtatást tesztelésnek kell alávetni és csak a teszt sikeres lezajlása után kerülhet sor az üzembe helyezésre. A működő rendszert az **IT szakértőnek** meghatározott időközönként ellenőriznie kell. Rendellenes működés esetén a rendszert további fejlesztésnek, illetve tesztelésnek kell alávetni.

6.8.6. Vásárolt és megrendelt programok változtatására vonatkozó előírások

A vásárolt programok esetében figyelembe kell venni a szerzői jogra vonatkozó hatályos törvényi szabályozásokat. A tulajdonjogokat a licencszerződések szabályozzák.
Biztonsági előírások a vásárolt és megrendelt programok változtatásával kapcsolatban:

- A Társaság által vásárolt, vagy számára kifejlesztett szoftverek (és a hozzájuk tartozó dokumentumok) másolása és átadása harmadik félnek - ha a licencszerződés ezt nem teszi lehetővé – szigorúan tilos.

6.9. Információbiztonsági incidensek kezelése

Informatikai biztonsági incidensek észlelése esetén a legfontosabb, hogy a bejelentés mielőbb megtörténjen a felhasználók felől, melynek módja a következő:
A felhasználóknak azonnal jelenteni kell az alábbi esetekben az **IT Biztonsági Felelősnek**:

- bármilyen adat sérülését, kiszivárgását, vagy jogszerűtlen belső használatát fedezték fel, vagy ennek gyanúja áll fenn;
- felismert vagy felismerni vélt védelmi gyengeséget, sérülékenységet, hiányosságot, biztonsági rést fedeztek fel.

A felhasználóknak telefonon vagy e-mailen szükséges értesíteni az **IT Biztonsági Felelőst**, mely során tájékoztatják az incidens paramétereiről. A bejelentés anonim módon is történhet, mely során szükséges jelezni, hogy a felhasználó szeretne anonim maradni. Ebben az esetben az **IT Biztonsági Felelős** nem adja tovább a bejelentő adatait.

Az összegyűjtött információk alapján az **IT Biztonsági Felelős** megvizsgálja az incidenst, hogy valóban valós-e, valamint elhárításra szorul. Továbbá azt is ellenőriznie szükséges, hogy az incidens informatikai biztonsági eseményből származik-e.

6.9.1. A biztonsági események kategorizálása

A biztonsági események kategorizálása az alábbi szempontok szerint történik:

- az esemény által érintett rendszerek kritikussága;
- az esemény által érintett munkaállomások, foglalkoztatottak száma;
- az esemény által érintett adatok;
- az esemény által kialakult károk és esetleges károk és hatások mértéke.

6.9.2. Az incidensek kategorizálása

- alacsony kategória
  - kevés foglalkoztatottat érint
  - csak támogató rendszert érint
  - csak nyilvános adatot érint
  - kár értéke minimális
- magas kategória
  - sok foglalkoztatottat érint
  - üzletileg kritikus rendszert is érint
  - bizalmas adatot is érint
  - kár értéke jelentős
- személyes adatokat érintő incidens
  - alapértelmezettként magas kategóriába tartozik
  - bármilyen személyes adatot érint

6.9.3. Kategóriák szerinti intézkedés

Alacsony kategória esetén: Az **IT Biztonsági Felelős** eszkalálja a probléma megoldását az általa kijelölt dolgozó felé. A kijelölt személy javaslatot tesz a probléma megoldására, melyet az **IT Biztonsági Felelős** jóváhagy. Jóváhagyás esetén a korábban kijelölt személy folytatja az incidens elhárítását, kivéve, ha az **IT Biztonsági Felelős** mást jelöl ki az incidens megoldására.
Minden kategória esetén: Az **IT Biztonsági Felelős** vezeti az elhárítását az incidensnek, mely során magasabb beosztású vezetők bevonása is szükséges lehet. A későbbi – hasonló – incidensek megelőzése érdekében megoldási javaslatot az **IT Biztonsági Felelősnek** kell tennie, melyet az Ügyvezető Igazgatónak is jóvá kell hagynia. Jóváhagyás esetén az **IT Biztonsági Felelős** az általa kidolgozott módon kezdi meg az incidens alap okainak elhárítását.
Szüksége esetén az incidens kivizsgálásába be kell vonni az érintett szállítót is.

Személyes adatokat érintő incidens esetén: Az **IT Biztonsági Felelősnek** azonnal értesíteni szükséges a kijelölt **Adatvédelmi Felelőst** az incidens mértékéről, és az érintett személyes adatokról, mely után a továbbiakat az **Adatvédelmi Felelős** bevonásával szükséges folytatni a magas kategóriában megfogalmazottak alapján.

1. számú melléklet – Felhasználói IT Biztonsági Kézikönyv

Bevezető

A Felhasználói IT Biztonsági Kézikönyv (továbbiakban: Kézikönyv) a magasabb szintű információbiztonsági szabályzatokban megfogalmazott irányelvek alapján rögzíti a felhasználókkal szemben támasztott követelményeket, kötelezettségeket és a felhasználókat napi munkájuk során érintő információbiztonsági szabályokat.

A Kézikönyv célja

A Kézikönyv célja, hogy a felhasználó számára röviden, érthetően összefoglalja azokat az információbiztonsági követelményeket, amelyeket a Társaság szabályzatokban rögzített.

A Kézikönyv Hatálya

A Kézikönyvben leírtak végrehajtása a dokumentum hatálya alá tartozó személy(ek)re munka-, büntető- és/vagy polgári jogi felelősség terhe mellett kötelező.
A Kézikönyv alanyi hatálya kiterjed az összes, a Társaságnál fő- és mellékállásban foglalkoztatott alkalmazottra, valamint a szerződéses jogviszonyban álló, vállalkozói és egyéb szerződés keretében foglalkoztatott munkavállalóra (a továbbiakban: felhasználók).
A Kézikönyv kiterjed minden nemű adatra és információra, mely a Társaság informatikai vagy egyéb eszközén tárolódik, továbbítódik, beleértve minden papíron található adatot és információt mely a Társasághoz, vagy a Társaság tevékenységéhez, működéséhez köthető.
A Kézikönyv kiterjed a Társaság által használt valamennyi informatikai rendszerre, eszközre, amely felhasználja, eléri, tárolja, felügyeli, feldolgozza, továbbítja, vagy megőrzi a Társaságnál keletkező, illetve felhasznált adatokat, információkat és kommunikációt.

A Felhasználók szerepe az információbiztonságban

A Társaság legnagyobb vagyonát, azaz az információs vagyont a felhasználók kezelik, ezért az információbiztonsággal kapcsolatos törekvések sikerességében kritikus szerepet játszik a felhasználói tájékozottság, biztonságtudatosság.

A felhasználóknak ismerniük kell az általuk kezelt információk és adatok fontosságát, tisztában kell lenniük a fenyegetésekkel, valamint megfelelő ismeretekkel kell rendelkezniük arra vonatkozóan is, hogy milyen módon képesek gondoskodni a rájuk bízott adatok és információk biztonságáról, azaz az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzéséről.

Szankciók

A szabályok nem- vagy hiányos ismeretének, megsértésének akár egyező következményei is lehetnek, mint a tudatos, rosszindulatú visszaéléseknek.

Amennyiben a felhasználó megszegi a szabályzatokban foglaltakat és pénzügyi vagy reputációs kárt okoz ezzel a Társaság számára, úgy felelősségre vonásra fog kerülni, mely történhet pénzügyi kár esetén az okozott kár megtérítésével is.

A jelen szabályzatban leírtak megszegése esetén a cselekmény megvalósíthatja a Btk. (2012. évi C. törvény a Büntető Törvénykönyvről) alábbi pontjait

- személyes adattal visszaélés (Btk. 219. §)
- üzleti titok megsértése (Btk. 418. §)
- információs rendszer felhasználásával elkövetett csalás (Btk. 375.§)
- védelmet biztosító műszaki intézkedés kijátszása (Btk. 386. §)
- tiltott adatszerzés (Btk. 422.§)
- Információs rendszer vagy adat megsértése (Btk. 423.§)
- információs rendszer védelmét biztosító technikai intézkedés kijátszása (Btk. 424. §)

A Társaság informatikai rendszereivel kapcsolatba kerülő személyek esetén (akik nem a Társaság munkavállalói) a Társaság a Polgári Törvénykönyvről szóló 2013. évi V. törvény kártérítésre vonatkozó szabályai szerint intézkedik.

A felhasználók felelőssége és feladatai

- Az információbiztonsági törekvéseknek való megfelelés érdekében a felhasználóknak a jelen dokumentumban definiált szabályokat, valamint az informatikai és információbiztonsági szabályokat ismerniük kell és be kell tartaniuk.
- A felhasználó köteles a munkája során az elvárt gondosságnak megfelelően viselkedni, kommunikálni, a Társaság értékeit megőrizni, a biztonságot megtartani és haladéktalanul jelezni minden gyanús eseményt.
- A felhasználó feladata munkájának ellátása érdekében a hozzá rendelt informatikai eszközök eredményes, rendeltetésszerű használata, betartva a használatra vonatkozó, a Társaság által meghatározott szabályokat.
- A felhasználó felelőssége a Társaság által használt alkalmazói rendszerek felhasználói leírásainak ismerete és az alkalmazások használatakor azok pontos betartása.
- A felhasználók felelőssége a szellemi tulajdonjogok védelme érdekében a vonatkozó törvényi, jogszabályi előírások betartása.
- A felhasználók felelősek a Társaság által kezelt adatok biztonsága érdekében az adatok kezelésére vonatkozó szabályok betartásáért.
- A felhasználó kötelessége az előírt informatikai (biztonsági) oktatáson való részvétel, az oktatási anyag elsajátítása és legjobb tudása szerint történő alkalmazása a munkája során.
- A felhasználó a nevében (hozzáférésével) elkövetett minden szabálysértésért és az így okozott esetleges kárért viseli a felelősséget, kivéve ha kétséget kizáróan bizonyításra kerül, hogy hozzáférésével más személy élt vissza.
- A felhasználóknak figyelemmel kell lennie a Társaság rendelkezésre álló erőforrásaira, ezért a jelentősebb kapacitásigényű feladatok végrehajtását (pl. nagyobb állományok nyomtatása) lehetőség szerint ütemezze terhelési csúcsidőszakon kívülre.
- A felhasználó felelős a számítógépén lokálisan tárolt állományokért, adatokért, szoftverekért. E felelőssége kiterjed az állományok megsemmisüléséből, illetéktelen hozzáférésből eredő és a szerzői jog megsértésével okozott károkra.

Segítségnyújtás

Amennyiben valamelyik felhasználónak kérdése, kérése, panasza van informatikai területtel kapcsolatosan, azt az **IT szakértő** számára jelentheti e-mail segítségével.

Adatok kezelése

Az adatok bizalmassági osztályokba való besorolása:

- Nyilvános adatok: olyan adatok, mely formalizált módon el lettek fogadva a nyilvános közzétételre. Ilyenek lehetnek a Társaság weboldalára kirakott hírek vagy a Társaság éves jelentései, valamint bármilyen platformon a Társaság által nyilvánosságra hozott tartalom.
- Belső adatok: védendő adatok, hiszen a Társaságból kikerülése kárt okozhat a Társaság számára, azonban a Társaság munkavállalói számára hozzáférhetőek. Ilyenek lehetnek a szabályzatok, bizonyos munkaanyagok, tájékoztatók, oktatási anyagok, stb.
- Bizalmas adatok: erősen védendő adatok, melyekhez a Társaságon belül csak azon munkavállalók férhetnek hozzá, akiknek a munkafolyamataik szerint feltétlenül szükséges. Ilyenek az ügyfelek személyes, és különleges adatai, a dolgozók adatai, üzleti tervek, szerződések, a Társaság szellemi termékei, auditok jelentései, stb.

A Társaság adatai jelenleg jellemzően számítógépes rendszerekben és adatbázisokban, valamint papíron tárolódnak, melyekre egyenlően szükséges tekinteni, azonban kezelésüknél az elvárt követelmények különböznek fizikai mivoltukból adódóan.

Papír alapú adatok kezelése

- A papír alapú dokumentumokat minden esetben elzárva kell tárolni felhasználás után.
- Tilos a Társaság adatait tartalmazó papírokat engedély vagy munkakörből adódó felhatalmazás nélkül kivinni a Társaság telephelyeiről.
- Tilos a Társaság adatait tartalmazó papírokat szemeteskukába dobni, ez alól az irodai szemetesek sem kivételek.
- Tilos a Társaság adatainak illetéktelen sokszorosítása, nyomtatása, egyéb felhasználása.
- Tilos a Társaság adatait tartalmazó dokumentumokat a munkaasztalon, üzenőfalon, nyitott fiókban, szekrényen tárolni. A Tiszta Asztal Politika részletesen rendelkezik a "Tiszta asztal, tiszta képernyő" elvről, mely a Társaság munkavállalói számára kötelező.

Elektronikus adatok kezelése

- Elektronikus adatnak tekinthető minden számítógépes rendszerben, vagy adatbázison, webes felületen található adatot.
- Tilos az adatokhoz történő illetéktelen hozzáférés vagy ennek szándékos kísérlete.
- Az elektronikus adatok munkafolyamaton kívüli létrehozása, módosítása, törlése, bármely csatornán történő továbbítása a **Section Manager** engedélye nélkül tilos.

Informatikai eszközök használata

A Társaság által biztosított informatikai eszközök használatának célja a felhasználó munkaköri tevékenységéhez kapcsolódó feladatainak elvégzése.
Az informatikai eszközök használata csak azonosítás után kezdhető meg, ami a felhasználónevének és jelszavának megadását jelenti.

A felhasználóknak tilos:

- az informatikai eszközöket fizikailag megbontani: alkatrészeket cserélni, be-, kiszerelni.
- az informatikai eszközök konfigurációjukat, beállításaikat és a rajtuk lévő jelzéseket (pl. nyilvántartási szám, gyári szám, stb.) megváltoztatni. Amennyiben ezen jelölések sérülését, eltűnését észleli a felhasználó, köteles azt haladéktalanul bejelenteni az IT egyik alkalmazottjának.
- az asztali számítógépek és más, nem hordozható informatikai eszközök fizikai helyének, gyengeáramú informatikai kábelezésének megváltoztatása.
- az informatikai eszközök villamos kábelezésének megváltoztatása.

Hordozható informatikai eszközök kezelése

- Mobil eszközök lopás elleni védelmét minden körülmények között meg kell valósítani (vagyis nem szabad a kocsiban hagyni, bárhol felügyelet nélkül hagyni, nyilvános helyen használni, ahol ráláthatnak a monitorra, stb.).
- Hordozható eszközökön a Társaság adatai csak titkosított módon tárolhatók.
- Otthoni munkavégzés esetén VPN kapcsolat használatával engedélyezett az otthoni internethálózat használata, azonban nem védett környezetben (pl: internetkávézó, hotel, stb.) történő hálózatra csatlakozásból eredő károkért a felhasználó felelős.
- A mobil informatikai eszközöket a felhasználó köteles rendszeres időközönként behozni és hálózatra csatlakoztatni a biztonsági frissítések és egyéb kötelező hálózati beállítások és szabályok lefutása érdekében.

A notebook-okkal kapcsolatos szabályokat az *"Informatikai szabályzat"* tartalmazza.

Okostelefonok kezelése

- A készülékeken nincsen korlátozva az alkalmazások telepítése, a felhasználó felelőssége, hogy milyen alkalmazásokat telepít az eszközökre, azonban nem megbízható forrásból a telepítés tilos. Kizárólag a hivatalos alkalmazás-boltokból engedélyezett az alkalmazások beszerzése.
- Az eszközökön az operációs rendszerek frissítése kötelező. Ezek a frissítések valamennyi esetben biztonsági javításokat is tartalmaznak, ezért ezek nem telepítése veszélyezteti a telefon biztonságát.
- A felhasználó kötelessége megelőzni a készülék eltulajdonítását. Amennyiben ez mégis megtörténik, azt haladéktalanul jelezni köteles az **IT szakértő** felé.
- Csak olyan okostelefon használható a Társaság adatainak kezelésére, tárolására, mely központilag, távolról menedzselhető, tiltható.
- Az okostelefonok IT általi biztonsági beállításait megváltoztatni tilos.
- Bluetooth kapcsolaton keresztül csak azonosított eszközök csatlakozhatnak egymáshoz, automatikusan nem, a felhasználó felelőssége, hogy mely egyéb eszközzel engedélyezi a Bluetooth kapcsolat felépítését.
- Okostelefonok csak titkosított csatornán keresztül csatlakozhatnak a hálózatba kapcsolt számítógépekhez, előzetes azonosítás után.
- Nyilvános Wi-Fi-k használata nem javasolt, kizárólag, ha a felhasználó teljesen megbizonyosodott, hogy az megbízható forráshoz tartozik (pl.: ügyfél, állami hivatal). Hotelek, éttermek és egyéb nyilvános helyeken a Wi-Fi-k használata nem engedélyezett.

Szoftverek kezelése

A szoftverek kezelésével kapcsolatosan az alábbiak betartása kötelező a felhasználók számára:

A felhasználóknak tilos:

- a számítógépre bármilyen szoftver komponenst installálni;
- telepített szoftverek eltávolítása, konfigurációk módosítása;
- illegális szoftverek továbbá egyéb termékek és állományok szerzői jogot sértő módon történő tárolása, telepítése és használata.
- BIOS vagy operációs rendszer beállításokat módosítani.

Hozzáférések kezelése

- A felhasználók hozzáféréseit a felettes vezetők jóváhagyásával az **IT szakértő** állítja be. Amennyiben a felhasználó valamilyen hibából fakadóan többlet jogosultságot tapasztal munkája során, köteles jelenteni azt a felettese vagy az **IT szakértő** felé. Bármilyen hibásan beállított jogosultságból adódóan elkövetett cselekvés, vagy a többlet jogosultság észlelése utáni bejelentés elmaradása később a felhasználó felelősségre vonását eredményezheti.

Jelszavak

A Társaságnál használatos szoftvereknél, amennyiben technikailag lehetséges, biztonságos jelszókövetelmények lettek meghatározva. Azonban egyes alkalmazások jelenleg nem támogatják a megfelelő jelszavak megkövetelését, így a felhasználóknak minden alkalmazásnál (beleértve a Windows-os belépési jelszavukat is) az alábbi jelszóbeállítások kötelezőek.

A jelszóválasztással kapcsolatos követelmények:

- legalább 8 karakter hosszú jelszót kell választani;
- a jelszó tartalmazzon az alábbi négy kategóriából legalább háromfélét:
  - nagybetű,
  - kisbetű,
  - numerikus karakter,
- tilos jelszóként a jelszó tulajdonosával kapcsolatba hozható vagy ismert szót, kifejezést választani;
- tilos az informatikai rendszerben ismert parancsot vagy alkalmazás nevet jelszóként használni;
- a jelszó nem lehet azonos a felhasználói azonosítóval és nem is tartalmazhatja azt;
- minden új jelszó kialakításánál törekedni kell arra, hogy szerkezetében ne hasonlítson az előző, lecserélendő jelszóra.

Jelszavak kezelése

- Tilos a jelszó más számára történő felfedése, vagy ennek valószínűsíthetősége esetén a felhasználó köteles azt haladéktalanul megváltoztatni;
- a felhasználók nem adhatják ki jelszavaikat kollégáiknak, még akkor sem, ha helyettesítési tevékenységet lát el távollétünkben;
- a választott jelszavak ne kerüljenek feljegyzésre és ne legyenek bármilyen más módon illetéktelenek számára hozzáférhetők.

A Windows jelszó megváltoztatásához a <CTRL> <ALT> <DEL> billentyűkombinációt kell egyszerre lenyomni, amelynek hatására a megjelenő képernyőn megjelenik a „Jelszó módosítása" / „Change Password" gomb. Erre kattintva lehet a jelszót megváltoztatni (a régi jelszó egyszeri és az új jelszó kétszeri megadása után az OK gombra kell kattintani).

Bizalmas jellegű dokumentumok esetében titkosítani szükséges a fájlokat, melyeket jelszóval szükséges védeni. A jelszavak meghatározásánál a fent részletezett követelmények az irányadóak.
A jelszóval védett fájlok továbbítása esetén a felhasználóhoz a jelszót a fájl átadási csatornájától eltérő csatornán kell eljuttatni (Pl. ha a fájl elküldése e-mailben, akkor a jelszó elküldése sms-ben történjen).

Csatlakoztatható eszközök kezelése

- Saját, felhasználói tulajdonban lévő cserélhető adathordozó használata minden formában tilos;
- CD/DVD írást csak az IT végezhet;
- Cserélhető adathordozóról munkaállomást indítani tilos.
- Nyilvános bizalmassági osztályba sorolt adatot tartalmazó adathordozó kivitele esetén minden esetben alkalmazni kell kriptográfiai eszközzel történő titkosítást az érzékeny adatok védelmében;
- A házon kívülre vitt adathordozók nem hagyhatók felügyelet nélkül (zárt autóban sem). Az adathordozót kézipoggyászban, rejtett módon kell szállítani.
- A szerverek és munkaállomások adathordozóinak Társaságon kívülre történő kivitele csak speciális engedélyekkel lehetséges (csak és kizárólag az IT munkavállalói végezhetnek ilyen tevékenységet.)

Vírusvédelmi szabályok

A Társaságnál a vírusvédelmi tevékenységekért az IT a felelős. Ők telepítik a megfelelő, erre a célra vásárolt szoftvert (Trend Micro), valamint a beállítását is ők végzik.

- A felhasználóknak tilos a vírusvédelmi szoftvert kikapcsolni vagy leállítani.
- Amennyiben a felhasználó a számítógépen vírusra utaló nyomokat (hirtelen lassulás, nem rendeltetésszerű működés, furcsa feliratok vagy üzenetek) talál, akkor azt köteles azonnal jelenteni az IT számára.
- Vírusos állománnyal valaha fertőzött médiát számítógépen alkalmazni szigorúan tilos.

Elektronikus levelezés szabályai

- A Társaságnál az elektronikus kommunikáció hivatalos formája az e-mail.
- A felhasználók az elektronikus levelező szoftvert (Outlook) csak a munkakörükből adódó feladataik elvégzéséhez használhatják, privát levelezésre nem.
- A felhasználóknak kötelező ellenőrizni a tárhelyüket, amennyiben az megtelik, archiválás szükséges, melyhez segítségül kérhetik az IT –t is.
- A biztonságos levelezés érdekében futtatható állományok (pl.: .exe, .com, .pif) fogadása és továbbítása nem megengedett.
- A levelek mérete 5 Mb-ban került maximalizálva, azaz csatolmánnyal együtt, maximum ekkora lehet a levelek mérete.

- Nem nyilvános adatokat a Társaságon kívülre küldeni csak titkosítva engedélyezett.
- Ismeretlen forrásból származó levelekben szereplő linkekre kattintani szigorúan tilos, továbbá a szövegben található kéréseket sem szabad komolyan venni, azonnal törölni kell azokat.

Információbiztonsági események kezelése

Az információbiztonsági események és incidensek jelentése nagy szerepet játszik a Társaságnál az információ biztonságának fenntartásában.

A felhasználóknak azonnal jelenteni kell az alábbi esetekben az **IT Biztonsági Felelősnek**:

- bármilyen adat sérülését, kiszivárgását, vagy jogszerűtlen belső használatát fedezték fel, vagy ennek gyanúja áll fenn;
- felismert vagy felismerni vélt védelmi gyengeséget, sérülékenységet, hiányosságot, biztonsági rést fedeztek fel.

Amennyiben az információbiztonsági incidens feltehetően személyes adatot (is) érint, az **IT Biztonsági felelős** azonnali hatállyal értesíti az **Adatvédelmi felelőst**, aki megteszi a belső adatkezelési szabályzatban foglalt tevékenységeket.

Biztonsági incidensek esetén az **IT Biztonsági felelős** vizsgálja meg az incidenst kiváltó okot, és javaslatot tesz a vezérigazgatónak a kiváltó ok megszűntetésére.

Tiszta asztal, tiszta képernyő politika

- A munka szempontjából lényegtelen, munkához nem kapcsolódó információhordozókat el kell zárni.
- Látogató vagy vendég fogadásakor minden, a látogatáshoz nem kapcsolódó, a látogatás szempontjából lényegtelen dokumentumot vagy iratot el kell zárni.
- El kell zárni az ügyfél- vagy személyes adatokat tartalmazó dokumentumokat, amennyiben már nem tér vissza aznap többet a munkaállomásához.
- A felhasználó a munka befejezését követően köteles minden bizalmas információt a saját vagy a szervezeti egysége részére biztosított, zárt szekrényben elhelyezni.
- A zárt szekrények kulcsainak őrzéséről – önállóan használt szekrény esetén – a munkavállaló gondoskodik. Több munkavállaló által használt szekrények kulcsai zárt szekrényben (fiókban) elhelyezhetők, tárolhatók, amelyek őrzésével a szervezeti egység vezetője felelőst (felelősöket) jelöl ki.
- A fölöslegessé vált, bizalmas információkat tartalmazó dokumentumokat az iratmegsemmisítőben meg kell semmisíteni.
- Azonnal vissza kell vinni minden, más osztályról kapott dokumentumot, ha már nincs rá szüksége a felhasználónak.
- Be kell zárni minden olyan dokumentumot, alkalmazást, amellyel a felhasználó nem dolgozik, szem előtt tartva a hatékonyságot és az ésszerűséget.
- A „tálca" gyorsindító részén csak az általánosan használt irodai alkalmazások indítóikonjai szerepelhetnek.

- A képernyőt zárolni kell minden olyan esetben, amikor arról bizalmas adatok láthatóak illetéktelenek számára vagy a felhasználó elhagyja a munkaállomását.