KÁBEL TEAM KFT.
1148 Budapest Lengyel u. 15.
Weblap: www.kabelteam.hu
E-mail: info@kabelteam.hu
Tel: 06/1 470-80-40 **Fax:** 06/1 470-80-45

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT (IBSZ)

Az IBSZ célja a Társságunk és az általunk végzett tevékenység, adatkezelés informatikai biztonsági követelményrendszerének és környezetének meghatározása, mely leírja a biztonsági intézkedéseket, azok dokumentálásának és ellenőrzésének feladatait, az ehhez szükséges egyes szerepköröket és a végrehajtás gyakoriságát vagy idejét.

1. IBSZ HATÁLYA

1.1 *IBSZ szervezeti hatálya*

Az IBSZ kiterjed a Társaság információkezeléssel és –feldolgozással kapcsolatos összes folyamatára és tevékenységére, a tulajdonában vagy használatában lévő elektronikus információs rendszerekben előforduló adatokra, továbbá a céggel szerződéses közös ajánlattevői, vállalkozói, alvállalkozói, megbízotti) jogviszonyban álló valamennyi szervezetre, vállalkozóra, amelynek munkavállalói, vagy alvállalkozói a Társaságunk által használt rendszerekhez, illetve az azokon tárolt adatokhoz hozzáféréssel rendelkeznek. Valamennyi vezető kötelessége, hogy mind az által irányított szervezeteknek, munkavállalóknak, mind az általa egyéb módon foglalkoztatottaknak (megbízott, vállalkozó) legyen módjuk a rájuk vonatkozó elvárások és kötelezettségek megismerésére.

1.2 *IBSZ tárgyi hatálya*

Jelen dokumentum tárgyi hatálya kiterjed az informatikai eszközök elhelyezésére szolgáló létesítményekre (épületekre, telephelyekre), a Társaságunknál található összes üzemelő, használatban lévő vagy a jövőben bevezetett, alkalmazott informatikai eszközre, rendszerre, a kezelt adatokra, azok környezetét alkotó rendszerelemre teljes életciklusában a tervezéstől, elkészítéstől, a rendszerből történő teljes kivonásáig, vagy megsemmisítésig.

1.3 *IBSZ személyi hatálya*

Az elfogadott IBSZ kiterjed:

- Társaságunk valamennyi munkaviszonyban foglalkoztatott alkalmazottjára,
- Cégünk valamennyi képviselőjére, vezetőjére, a rendszerek felhasználóira, fejlesztőire, üzemeltetőire.
- a velünk egyéb módon, másféle szerződések alapján közreműködő munkatársra, külső, megbízásos (szerződéses) eseti munkakapcsolatban lévő személyekre is,
- Társsaságunkkal szerződéses, vagy más módon kapcsolatba kerülő természetes vagy jogi személyekre, gazdasági társaságokra a velük kötött megállapodás, vagy titoktartási nyilatkozatok alapján.

Az IBSZ előírásainak érvényesülését a vonatkozó megállapodások, szerződések tartalmának megfelelő kialakításával kell biztosítani és a biztonságért felelős személyek közreműködésével kell megvalósítani.

1.4 *IBSZ kiadás dátuma, érvényessége*

Jelen szabályzat a kiadás napján lép hatályba, és mindaddig érvényesnek tekintendő, amíg annak egy új változata jóváhagyásra nem kerül.

Az IBSZ írásos formában minden résztvevő számára elérhető Társaságunk honlapján, titkárságán, illetve elektronikus formában cégünk szerverén is.

A Szabályzat, illetve mellékleteinek felülvizsgálatára sor kerül minden olyan esetben, amikor a jelen szabályzathoz képest jelentős változás következik be akár a jogszabályi előírások során, akár a cég működése során, de kiemelten az alábbi esetekben:

- évente egy alkalommal, a belső felülvizsgálatok során,
- SzMSz módosítását követően
- az információbiztonságot is érintő jogszabály-változást követően, amennyiben annak hatálya Társaságunkra is kiterjed;
- az információkezelést és –feldolgozást végző vagy támogató folyamatokban, illetve a kezelt adatok körében beállt lényeges változás esetén;
- a cégünk tulajdonában vagy használatában lévő elektronikus információs rendszerekben, illetve azok fizikai környezetében beálló lényeges változás miatt.
- továbbá minden olyan esetben, amikor a Szabályzatban leírtakhoz képest egyéb jelentős változás történik.

A mindenkori felülvizsgálat végrehajtása az Informatikai felelős feladatát jelenti.

2. IBSZ felelőssége:

Társaságunk vezetése jelen szabályzatban megfogalmazott világos iránymutatással, elkötelezettsége kinyilvánításával, az informatikai biztonsággal összefüggő felelősségi körök egyértelmű kijelölésével és elismerésével aktív módon támogatja az informatikai biztonságot a szervezeten belül.

2.1. Informatikai biztonsági vezető

Társaságunk informatikai biztonsági vezetője külsős személy, a cég vállalkozói szerződéssel foglalkoztatott rendszergazdája, Süller József.

Az informatikai biztonság terén stratégiai feladata:

- Társaságunk informatikai biztonsági feladatainak tervezése, meghatározása, irányítása és ellenőrzése.
- Az informatikai biztonsági szabályzatok elkészítése, vagy azokban való közreműködés, a szabályzatok betartatása, a vonatkozó részeinek karbantartása.
- Részvétel a biztonsági események felderítésében, elemzésében és kezelésében.
- Az információbiztonsági tevékenység koordinálása.
- Az adat- és információvédelemmel kapcsolatos veszélyforrások felmérése és elemzése.
- Gondoskodás az informatikai biztonsági szabályzatok naprakészen tartásáról, az abban foglaltak betartásának ellenőrzéséről.

- Az informatikai biztonsági eszközök állapotának figyelemmel kísérése, javaslatot azok cseréjére, bővítésére.
- Az informatikai biztonságra vonatkozó oktatás megszervezi és lebonyolítása.
- Fentieken túl, a mindennapi működés során feladata az informatikai biztonsági feladatok technológiai szintű ellátása is a cégvezetéssel együttműködve.

2.2. Adatgazdálkodás és adatgazda:

A mindenkori ügyvezető felelőssége az adott terület vezetőjével közösen meghatározni az általa irányított üzleti folyamatokhoz tartozó adatkezelés folyamatát, melynek biztonsági megvalósítását az informatikai vezető segítségével és együttműködésével közösen döntik el.

2.3. Felhasználók

Felhasználó: Társaságunk valamennyi, papíralapú vagy elektronikus információs rendszert használó munkatársa.

Külső felhasználó: Társaságunkkal kapcsolatban álló külső felek (megbízási, vállalkozói szerződés alapján jogosult vállalkozók, alkalmazottjaik, egyéb munkatársaik), akik szerződéses jogviszony alapján, cégünk biztonsági szabályainak és elvárásainak betartása mellett férhetnek hozzá elektronikus információs rendszereinkhez.

A külső felhasználók hozzáférését a hozzáférés indokának megszűnte után azonnal, ill. az együttműködés lejártakor automatikusan meg kell szüntetni.

2.4. Külső szolgáltatók

A külső szolgáltatók és együttműködő partnerek igénybevétele esetén a szolgáltatási megállapodásokban (szerződésekben) kell kikötni a szolgáltatásra érvényes biztonsági követelményeket és szabályozást. Biztosítani kell a Társaságunk számára az ellenőrzés feltételeit.

Minden érintett szereplővel titoktartási nyilatkozatot kell kikötni, melynek aláírásával felvállalja, hogy a birtokában levő információval nem él vissza.

A külső felekkel kötött megállapodásoknak vagy szerződéseknek pontosan tartalmazniuk kell:

- a megállapodásban részt vevő felek kölcsönös kötelezettségét,
- a joganyagokra vonatkozó felelősséget, pl. adatvédelmi jogszabályok kérdésében,
- szellemi tulajdonjogokat és a szerzői jog átruházását, valamint az együttes csoportmunka védelmét,
- a tevékenységük pontos meghatározását,
- a hozzáférési jogosultságaikat,
- a hozzáférés módját, idejét és korlátait, különös tekintettel a helyszíni munkavégzésre
- a biztonsági előírásainak- és kontrolljainak elfogadását,
- a titoktartási nyilatkozataikat,
- az ellenőrzés feltételeit, valamint az ezekről szóló jelentések meghatározását,
- a szerződésben lefektetett felelősségek auditálásának jogát, vagy az auditok további külső féllel történő elvégeztetésének jogát,
- a karbantartás és rendszerkövetés kérdéseit
- a problémamegoldás folyamatát – ha lehetséges – az előre nem látható események figyelembevételével,

- a biztonsági eseményekről és a biztonság megsértéséről szóló jelentések, értesítések és kivizsgálások esetére vonatkozó intézkedéseket,
- a szerződés teljesítésébe további alvállalkozók bevonásának feltételeit, titoktartásra vonatkozó megállapodásokat.

Külső felek szolgáltatásaival kapcsolatos változásoknál biztosítani kell, hogy a változásokat csak a megfelelő jogosultságokkal lehessen kezdeményezni, és a végrehajtás ellenőrzött és dokumentált körülmények között történjen az igény felvetésétől az átadás-átvételig.

Minden harmadik féllel kötött megállapodás esetében rögzíteni kell a jelen Szabályzat által meghatározott biztonsági követelményeket. Ennek teljesítése érdekében informatikai biztonsági vonatkozású szerződést az ügyvezető csak az Informatikai biztonsági vezetővel való egyeztetést követően köthet.

Jelenleg adatokat nem adunk tovább küldő, harmadik félnek.

2.5. Alapkövetelmények

A Társaság levelezési rendszerében, elektronikus információs rendszereiben tárolt és feldolgozott adatok vonatkozásában az egyes ügyviteli és üzemeltetési folyamatok eljárási szabályaiban előírásakor (még szóbeli előírásai során is) gondoskodni kell arról, hogy az adatok sértetlensége az adatkezelés során megőrződjön.

Az adatosztályozási fejezet szerinti „magas” vagy „kritikus” biztonsági osztályba sorolt adatokat:

a) a bevitel után titkosítottan kell tárolni, kezelni vagy továbbítani,
b) külső adatátviteli csatornák használata során meg kell győződni arról, hogy az átvitel során nem történt adatmódosulás, illetve
c) hogy az átvitel megtörtént.

Információbiztonsági szempontból az adat-előkészítési folyamatok ügyviteli szabályainak:

a) gondoskodniuk kell az adatrögzítést megelőző megfelelő jóváhagyási eljárásról;
b) biztosítaniuk kell a munkaállomás és a felhasználó egyértelmű azonosítását és gondoskodniuk kell azok folyamatos használatáról;
c) biztosítaniuk kell a rögzített adat és a forrásdokumentum közötti kapcsolat (iktatószám, vagy más alkalmas egyedi azonosító) rögzítését;
d) biztosítaniuk kell az adatok teljes körűségét, pontosságát és érvényességét;
e) biztosítaniuk kell, hogy a jóváhagyott adatok teljes körűsége, pontossága és érvényessége az előkészítés további szakaszaiban is fennáll;
f) tartalmazniuk kell a hibásnak minősülő forrásdokumentumok kezelésének eljárásait;
g) tartalmazniuk kell a hibásan rögzített adatokkal kapcsolatos javítási és eszkalációs (problémamegoldó, menedzselő) eljárásokat;
h) tartalmazniuk kell az egyes forrásdokumentumok biztonsági osztályainak megfelelő követelmények teljesítésének módját.

Az adatfeldolgozást végző alkalmazásoknak tartalmazniuk kell a hibák megelőzését, felfedezését és korrigálását szolgáló funkciókat.

Az adatfeldolgozási folyamatok ügyviteli és informatikai üzemeltetési szabályainak megállapításakor gondoskodni kell a feldolgozások során a feldolgozott vagy visszautasított tranzakciók naplózásáról, és biztosítani kell, hogy az adatok teljes körűsége, pontossága és érvényessége a feldolgozási tevékenységek folyamán megmaradjon.

Fentieknek megfelelően Társaságunknál a beérkezett adatokat egy központi szerver erősen védett ügyféladatbázisában tároljuk, kifejezetten korlátozott, védett hozzáféréssel és titkosítva. A biztonsági mentések szintén titkosítva kerülnek tárolásra, helyben tükrözött (RAID0) merevlemezeken, külön külső USB merevlemezen valamint megfelelő biztonságú felhő tárhelyen.

2.6. Alapkövetelmények betartása

Társaságunk a munkavállalók adatait külön programban (Nexon, Bérenc), jelszavakkal védetten tárolja egy külön tűzfal és vírusírtó szoftverekkel ellátott számítógépen. Az adatokhoz csak jogosult személyek férhetnek hozzá. Megalakulásunk óta nem volt munkaügyi adatvesztés, információvesztés, adatvédelmi incidens ezen a téren.
Szerződéskötéseknél, amennyiben a szerződéskötő fél magánszemély, az adatait, a számviteli és adózási jogszabályi előírásoknak megfelelően bekérjük, tároljuk és őrizzük a jogszabályban előírt őrzési kötelezettségnek eleget téve.
Mind a megrendelő, mind a munkavállaló magánszemély adatait harmadik félnek csak jogszabályi kötelezettség esetén adjuk ki, előírt adatszolgáltatási követelményeknek eleget téve. Pl. nem fizetés esetén követelésbehajtónak, ügyvédnek adjuk át, más harmadik félnek nem.
Az adatok tárolását, lezárását jogszerűen, határidőben elvégezzük.

Társaságunk a következő adatbázisokkal dolgozik: Microsoft SQL server 2008 R2. amely a Nexon tárolására alkalmas számítógépen található. Szerződések tárolása a tartományi szerver dokumentumok mappájában találhatóak.

2.7. Adatcsere, adattovábbítás

Amennyiben társaságunknál adatcsere, adattovábbítás történik, gondoskodni kell annak biztonságáról. Ennek érdekében a szervezetek között olyan megállapodást kell kötni, amely mindkét fél által támasztott követelményeknek megfelel.

A külső szervezetekkel történő adatcserét csak a szervezettel kötött megállapodás alapján lehet végezni, melyben rögzíteni kell az adattovábbítás technikai és adminisztratív eljárásait.
Társaságunk a hálózaton történő elektronikus levelezésre a Microsoft Exchange Online rendszerét használja, a kliens gépeken ezt a Microsoft Outlook alkalmazással érik el a felhasználók, vagy böngészőn keresztül megfelelő titkosított protokoll segítségével (SSL) valamint laptopon, tableten és mobiltelefonokon szintén az előírt megbízható szoftvereken keresztül. Az Outlook alkalmazásban a felhasználók csak saját elektronikus levelesládájukhoz férhetnek hozzá.

Biztosítani kell az elektronikus üzenetekben továbbított információk biztonságát és rendelkezésre állását. Ehhez meg kell határozni azokat az eljárásokat, amelyeket az elektronikus üzenetek továbbítása során alkalmaznak.

2.8. Hálózati határvédelem

Az elektronikus információs rendszerek csak a Társaságunk biztonsági architektúrájával összhangban elhelyezett informatikai biztonsági eszközökön felügyelt interfészeken keresztül kapcsolódhatnak külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

A bizalmas és a nem bizalmas hálózatokat csak a kiépített tűzfalon keresztül lehet összekapcsolni.

Tilos olyan munkaállomást vagy mobil eszközt csatlakoztatni a cég hálózatára, amely nem bizalmas hálózati kapcsolattal is rendelkezik.

A rendszergazda naprakész nyilvántartást vezet az engedélyezett portokról, protokollokról, és a hálózati határvédelem informatikai biztonsági architektúra elemeinek beállításairól.

A cég számítógép-hálózatának vezeték nélküli hálózati szegmensein wifi (melyeket WPA2 titkosítás védi) valamint a nem bizalmas csatornán keresztüli bizalmas kapcsolat során titkosított adatkapcsolatot kell kialakítani. Ez az informatikai vezető feladata a munkaüggyel és a cégvezetővel közös megállapodások alapján.

Laptopon tárolt adatok védelme lopás ellen a merevlemezek titkosítása pl A VeraCrypt egy ingyenes nyílt forráskódú merevlemez titkosítási szoftver Windows, Mac OSX és Linux operációs rendszerekhez, vagy a Microsoft saját bitlocker szoftverét használjuk.

Tűzfalak alkalmazása szerver és kliens gépek esetén a Windows beépített tűzfala alkalmas adataink védelmére. Valamint a hálózati eszközeinkben (3com router) szintén tűzfal gondoskodik a behatolások kiszűrésére.

Kliens gépek esetén teljes vírusvédelem a Norton360 vírusvédelmi szoftver, mely tartalmaz tűzfalat, levélszemét szűrőt és VPN védelmet.

Biztonságos távmunka kialakítása, biztosítása – távoli asztali kapcsolaton és titkosított VPN-en keresztül.

Hardver és szoftverleltár vezetése az informatikai vezető feladata a könyvelés tárgyi eszköz nyilvántartásával együttműködve.
Ugyancsak ő gondoskodik évek óta rendszeresen és naprakészen a számítógépek operációs rendszerének/szoftvereinek folyamatos frissítéséről, az adatok sérülékenységének időszakos teszteléséről.

2.9. Hálózati adatátvitel biztonsága

A belső hálózatokon az adatforgalomban kizárólag engedélyezett portok/protokollok használhatók, melyek körét az informatikai vezető határozza meg és évente felül is vizsgálja.

Hordozható számítógépeket, tableteket, okostelefonokat csak a rendszer-üzemeltető által elvégzett ellenőrzés után lehet Társaságunk számítógép-hálózatára kapcsolni.

Számítógép-hálózatunkban a felhasználói hitelesítés adatait (felhasználó azonosító, jelszó) titkosítva kell továbbítani.

Az adatcsere, adattovábbítás biztonsági eljárásaival kapcsolatos feladatok elvégzése, ellenőrzése, korrekciója az Informatikai biztonsági vezető felelőssége.

3. Adatmentés

Az adatmentés célja az elviselhetetlen mértékű adatvesztés megakadályozása, és az elvárt időn belüli adatvisszaállítás biztosítása.

3.1. Információk biztonsági mentése

Társaságunk kezelésében lévő szerverekről az elektronikus formában tárolt információról biztonsági mentéseket kell készíteni.

Az egyéb eszközökön lévő adatokról javasolt.

A cégünk olyan mentési rendet alakított ki, ami biztosítja az adatok visszaállíthatóságát az elvárható követelmények szerint (elvárt visszaállítás idő, maximálisan elviselhető adatvesztés stb.).

A mentések gyakoriságát, a mentés módját, a használt adathordozót és a tárolási helyet a fentiek figyelembevételével választottuk ki és kötöttünk rá szerződést az Informatikai biztonsági vezetővel.

Az érintettek számára oktatás megtörténik, a teljes visszaállítási eljárás többször is tesztelésre került.

Kidolgozásra került a mentések ellenőrzésének (ellenőrző visszatöltés) rendje is (többpéldányos mentés, külső helyszínen tárolás).

A mentési, visszaállítási eljárást évente, a szerződés megújítása során, releváns változások esetén haladéktalanul, az ügyvezető és az informatikai vezető felülvizsgálja és naprakésszé teszi.

3.2. Mentési eljárás

Biztonsági mentéseknek kell készülnie

a) az online elérhető (éles, tartalék, teszt) adatbázisokról és fájlrendszer könyvtárakról,
b) az offline elérhető (archivált) adatbázisokról és fájlrendszer könyvtárakról,
c) szoftverek telepítőkészletéről.

Normál (Teljes-FULL): azaz minden mentési folyamattal mentésre kerül az összes állomány, függetlenül az előző mentés időpontjától és annak státuszától.

A mentéseket ütemezett feladatként, automatikusan kell elvégezni, minden hétköznap.

Az automatikus mentés elindítását munkaidőn túl kell ütemezni, hogy az alkalmazások ne legyenek használatban és ne legyenek nyitott állományok. Emiatt az automatikus mentést 23:00-ra kell ütemezni.

A mentés eredményességét és futási idejét a mentés másnapján az informatikai vezető ellenőrzi.

3.3. Archiválási eljárás

Társaságunknál az informatikai vezető által biztosított központosított archiválás működik megfelelően évek óta.

Az előző heti napi mentések közül a pénteki mentést kell archiválni hétfő reggel.

Az archivált állományokat tartalmazó HDD-ket egyedi azonosítóval kell ellátni, és megfelelő biztonságú helyen kell tárolni.

Az archiválást az Informatikai biztonsági vezető végzi, vagy az általa kijelölt más, megfelelő szakmai felkészültségű személy.

Az archiválás után az utolsó hét előtti napi mentéseket törölni kell.

Az archivált állományokat tartalmazó HDD-ket évente selejtezni kell.

A selejtezés során az egy éven túli archív állományokat tartalmazó HDD-ket alacsony szintű formázással formattálni kell. Az archív állományok selejtezéséről jegyzőkönyvet kell rögzíteni.

3.4. Visszatöltés mentési állományból

A visszatöltés igénylését az adott szervezeti egység vezetője írásban, az ügyvezető szóban, telefonon, email-ben, vagy más elektronikus úton is kezdeményezheti az Informatikai

Az Informatikai biztonsági vezető megvizsgálja, hogy milyen okai vannak a visszatöltési igénynek. Ezek lehetnek:

a) adatvesztés/programhiba;
b) felhasználói hiba;
c) természeti katasztrófa.
d) egyéb.

Amennyiben adatvesztés vagy programhiba történt, az Informatikai biztonsági vezető gondoskodik a hiba elhárításáról. Katasztrófa esetén a Katasztrófatervnek megfelelően jár el.

Az Informatikai biztonsági vezetőnek meg kell vizsgálnia, hogy a visszatöltéssel nem sérülnek, illetve változnak meg az adott rendszer adatai. A visszatöltés jogosságát az Informatikai biztonsági vezető dönti el az adott rendszer adatgazdájával történt egyeztetés után. Amennyiben az ellenőrzés nem talált kizáró okot, és a visszatöltési kérelemben megadott dátumú mentés elérhető, az adott napi állományt vissza kell tölteni a kért helyre.

A sikeres visszatöltés tényét jegyzőkönyvben kell rögzíteni.

4. Biztonsági helyzet- és eseményértékelés

Gondoskodni arról, hogy a biztonsági események és zavarok okozta kár minimális legyen, továbbá, hogy az esetleges hibákból javító intézkedések következzenek.

4.1. Naplózás

Társaságunk elektronikus információs rendszereiben automatikus naplót vezet az elektronikus információs rendszerek biztonsági szempontból lényeges tevékenységekről. Ez a napló alkalmas arra, hogy a későbbiekben ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

Az informatikai biztonsági vezető egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő szervezeti egységgel, hogy növelje a kölcsönös támogatást.

Az informatikai biztonsági vezető megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

Az automatikusan készülő naplókban (naplóbejegyzés generálás) rögzíteni kell legalább az alábbi eseményeket:

- be- és kijelentkezéseket;
- sikertelen bejelentkezési kísérleteket;
- jogosulatlan hozzáférési kísérleteket;
- jogosultság megadáskor a megadott jogosultságokat;
- az operátori konzol riasztásait és üzeneteit;
- a rendszerriasztásokat, meghibásodási jelentéseket;
- felhasználók felvételét, törlését;

- jogosultsági csoportokban beálló változásokat (új csoport létrehozása, jogosultsági csoporthoz tartozó elemi jogosultságok megváltozása, stb.);
- felhasználók jogosultságaiban beálló változásokat;
- naplózási funkciók indítását és leállítását
- naplóállomány létrehozását, törlését; (külön jegyzőkönyvben rögzítve);
- a naplózási konfigurációban beálló változást (külön jegyzőkönyvben rögzítve);
- a rendszerdátum, -idő megváltoztatását;
- hardverkonfiguráció megváltozását;
- nyilvános hálózaton keresztüli kapcsolat létrehozása és bontása, az ellenoldali fél azonosítása, a forgalom jellege és a továbbított vagy fogadott állomány neve, elérési útvonala.

Az eseményekhez a naplózó funkciónak hozzá kell rendelnie (ha lehetséges):

- a felhasználó azonosítóját,
- a számítógép azonosítóját (IP cím),
- az esemény dátumát és időpontját, (a rendszernek a belső rendszerórát kell használnia a naplóbejegyzések időbélyegeinek előállításához, és időbélyegeket kell rögzítenie)
- a hozzáféréskor elért állományokat,
- a használt programot.

A különböző rendszerek naplóállományainak egységes értelmezhetőségének érdekében olyan naplózási architektúrát kell kialakítani, ami biztosítja, hogy:

- ahol csak technikailag lehetséges, a naplózás szerveroldalon történjen,
- a naplózást a lehető legkevesebb számú naplóállomány használatával történjen,
- automatikus mechanizmus gondoskodjon az egyes eszközök rendszerórájának szinkronizálásáról,
- automatizált megoldások támogassák a különböző naplóállományok összefésülését, feldolgozását és elemzését.

Az informatikai vezető gondoskodik arról, hogy a naplóállományokhoz írási jogosultsággal humán felhasználók nem férhetnek hozzá, a naplóállományokból a törlést nem végezhetnek.

Ennek során biztosítja, hogy az elektronikus információs rendszer megvédje a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

A naplóbejegyzéseket az információmegőrzési követelményeknek megfelelő időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

4.2. Incidenskezelés

„Adatvédelmi incidens”: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;
Társaságunk Incidens kezelő rendszert vezetett be, az esetlegesen bekövetkező adatvédelmi incidensek kimutatása, kezelése, jelentése érdekében.
Az informatikai vezető naponta ellenőrzi a naplóállományok bejegyzéseit.

Figyelemmel kíséri a Kormányzati Eseménykezelő Központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseit (http://www.cert-hungary.hu/aggregator/sources/2), és az egyéb forrásból érkező riasztásokat.

Gondoskodik róla, hogy „Incidens" esemény bekövetkeztekor, vagy ennek alapos gyanúja esetén Társaságunk információrendszere lehetőleg automatikusan jelentést generáljon és ezzel értesítse őt az esemény bekövetkeztéről vagy gyanújáról.

Mind erről, mint a munkatársak, felhasználók esetében bekövetkezett információbiztonsági szabályok megsértéséről az informatikai vezető jelentést tesz az ügyvezetőnek.

Ketten együtt minősítik az incidenst a körülmények ismeretében, vagy döntenek bármelyikük javaslata alapján is arról, hogy eseti szakértői megbízást adnak az incidens körülményeinek kivizsgálására.

Az informatikai biztonsági vezető, az incidens súlyának ismeretében dönt a következményekről, az incidens kezeléséről a hibák javításáról.

A biztonsági esemény kivizsgálásának eredményéről értesíti az ügyvezetőt, aki dönt a további esetleges fegyelmi, jogi eljárásról.

Az informatikai biztonságban résztvevők és szükség szerint az informatikai vagy szakmai rendszergazdák bevonásával a riasztásokban szereplő sérülékenység elhárítására haladéktalanul intézkedjenek.

Amennyiben a sérülékenység jellege olyan, hogy annak elterjedése megelőzhető, hogyha a felhasználók például nem nyitnak meg bizonyos web oldalakat vagy egy adott jellegű elektronikus levélben található linkre nem kattintanak, akkor belső figyelmeztetést kell kiadni a cégünk szokásos értesítési rendszerén (pl. e-mail) keresztül.

4.2.1. Adatvédelmi incidens kivizsgálása, jegyzőkönyvezése, nyilvántartásba vétele:

Eljárás adatvédelmi incidens esetén:
Az adatvédelmi incidens bekövetkeztekor a fentiekben előírtak alapján olyan nyilvántartás vezetése került előírásra, amely tartalmazza a NAIH felé megküldendő információkat.
Adatvédelmi incidens részleteinek rögzítéséhez javasolt nyilvántartási rendszert az alábbiakban egy konkrét példával mutatjuk meg.
sorszám, pl 01/2018.
Dátum: pl. 2018.01.28.
Az incidens leírása: pl. titkárság rossz helyre küldött emailt
Tudomásszerzés az incidensről: pl fogadó fél jelezte, maga a titkárság jelezte
Adatvesztés leírása: részletesen, konkrétan, egyértelműen. Pl. Legalább egy harmadik fél tudomást szerzett a szerződésben szereplő személyes adatokról.
Incidens természetes jellegének megnevezése, pl. a példánál: Téves mail küldés. Egy követeléskezelőnek szerettük volna átküldeni néhány adósunk adatait, de a mailcímük eleje megegyezett egy másik partnerével és emiatt tévedésből rossz helyre küldtük ki az adatokat.
Incidenssel érintettek száma, adatai, az adatok bizalmi kategóriája: pl. x db, magas
Az incidens következményeinek hatása: nem felmérhető, nem tudni, lényegtelen
Meghozott intézkedések (korrekció) pl, az érintettek értesítése
Javító intézkedések: Az alkalmazottaink figyelmét ismételten felhívtuk a levelezőrendszer megfelelő használatára, a hibalehetőségekre.
Hatósági értesítés: igen, NAIH értesítés dátuma: xxx
Ügy lezárása és dátuma: pl. 2018.02.01.
Adatvédelmi megbízott elérhetőségei: megadásra kerülnek ide.

4.2.2. Bejelentési kötelezettség

Amennyiben felmerül a gyanú, hogy Társaságunk számítógépes biztonsági incidens áldozatává vált, vagy éppen ennek folyamata alatt van, akkor a jogszabályokban meghatározott esemény bejelentési kötelezettség mellett az informatikai vezető az ügyvezető haladéktalan informálása mellett bejelenti ezen incidens tényét és kapcsolatot tart az érintett, külön jogszabályban meghatározott szervekkel is.

Amint az ügyvezetőnek tudomására jut egy esetleges az adatvédelmi incidens, azt indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomásukra jutott, bejelenteni kötelesek az illetékes felügyeleti hatóságnál, kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudják, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

Az adatvédelmi incidensről szóló bejelentést a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) mindenkori kapcsolati pontjára (http://naih.hu/uegyfelszolgalat,--kapcsolat.html) kell eljuttatni.

A bejelentés összeállításának és beadásának felelőse az informatikai biztonsági vezető.

Az adatvédelmi incidensről szóló bejelentésben legalább:

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
b) közölni kell a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d) ismertetni kell a Társaságunk által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.
e) Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

Társaságunk jogszabályi kötelezettségének megfelelően nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

4.2.3. Az érintett tájékoztatása az adatvédelmi incidensről

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor Társaságunk indokolatlan késedelem nélkül, elvárható időben tájékoztatja az érintettet az adatvédelmi incidensről.

Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az előző pont b), c) és d) pontjában említett információkat és intézkedéseket.

Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

a) Cégünk megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
b) Társaságunk az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

5. Adatkezelés: adatkérés és panaszkezelés menete

Társaságunk felelőssége, hogy gondoskodjon arról, hogy az általunk kezelt személyes adatokról az érintett adatalanyok a megfelelő hatékonysággal és minőségben kapjanak információt és segítséget. Ennek során törekednie kell, hogy az érintett magánszemélyek részére a személyes adatok kezelésére vonatkozó, az alábbiakban ismertetett valamennyi információt és tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, (különösen a gyermekeknek címzett bármely információ esetében).

Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

Ennek érdekében különösen fontos az ügyfélkapcsolati pontokon, mint például a titkárságon (telefon, e-mail), a központi e-mail- kezelésénél, továbbá a telefonos ügyfélszolgálat során az ott dolgozó kollégák adatvédelmi képzése, annak tudatosítása, hogy mindig pontosan tisztában kell lenniük az adatkezelési elvekről és jogszabályokról, a vonatkozó felelősségi körökről, a megfelelő kommunikációról és válaszadási normákról.

5.1. Adatkérés kezelésének jogi alapjai

Társaságunk indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható.

Kapcsolat esetén Társaságunk az érintettre vonatkozó személyes adatokat illetően az érintett rendelkezésére bocsátja a következő információk mindegyikét:

a) Társaságunk képviselőjének a kiléte és elérhetőségei;
b) az adatvédelmi megbízott elérhetőségei;
c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
d) cégünk vagy harmadik fél jogos érdekei, ha van ilyen;
e) adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;
f) továbbá a tájékoztatást az érintettek jogairól.

Az Érintett jogosult arra, hogy Társaságunktól visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

a) az adatkezelés céljai;
b) az érintett személyes adatok kategóriái;

c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
d) adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
e) az érintett azon joga, hogy kérelmezheti a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
f) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;

Végezetül társaságunk az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja.

Az érintett által kért további másolatokért az adminisztratív költségeken alapuló, észszerű mértékű díjat felszámolunk.

Amennyiben az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésére bocsátani Társaságunknak, kivéve, ha az érintett másként kéri.

Az érintett jogosult arra is, hogy kérésére Társaságunk indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

Az érintett jogosult arra, hogy kérésére Társaságunk indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, Cégünk pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, de csak ha az alábbi indokok valamelyike fennáll:

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
c) az érintett az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
d) a személyes adatokat jogellenesen kezelték;
e) a személyes adatokat az uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
f) a személyes adatok gyűjtésére az információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

Az érintett jogosult arra, hogy kérésére Társaságunk korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy cégünk ellenőrizze a személyes adatok pontosságát;
b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
c) Társaságunknak bizonyítottan nincs már szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy

d) az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy Társaságunk jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Társaságunk ezen ügymenet során minden olyan Érintett címzettet tájékoztat valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel.

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a kezelése ellen, ideértve az ezeken alapuló profilalkotást is, ha:

a) az adatkezelés közérdekű vagy közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
b) az adatkezelés egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Ezekben az esetekben Társaságunk a fenti személyes adatokat értelemszerűen nem kezelheti tovább, - kivéve, ha bizonyítja,

- hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben,
- vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak
- vagy jogszabályban előírt kötelezettségek teljesítéséhez szükségesek.

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik.

Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

5.2. Adatkérés kezelésének menete Társaságunknál

Az érintettek kérései bármilyen kommunikációs csatornán befuthatnak a szervezetbe:

- személyesen a cégnél, titkárságon,
- telefonon az ügyfélszolgálaton vagy máshol,
- elektronikus levélben,
- hagyományos levélben, vagy faxon.

Az érintettek kérései lehetnek például:

- adatkérés (milyen adatokat kezel róla a szervezet),
- adatmódosítási kérés,
- adathasználat korlátozás,
- adatletiltás,
- az adatok „elfelejtésének” kérése.

Minden beérkezési csatorna, és bármilyen kérés esetén az érintettek kérését pontosan, változtatás nélkül és haladéktalanul továbbítani kell az adatkezelési megbízottnak, az informatikai biztonsági vezetőnek és az ügyvezetőnek.

Az adatkezelési megbízott feladata az érintettekkel kapcsolatos:

- minden kérés kezelése,
- a szükséges adatok begyűjtése,
- az esetleg szükséges szervezeti vagy technikai módosítások elvégzése,
- a kérések megválaszolása

és az ügyvezető felelőssége ennek megfelelő, jogszabályok szerinti kezelése, a teljes folymat ellenőrzése, az informatikai biztonsági vezető felelőssége pedig az informatikai rendszerben történő lépések megtétele.

Az eljárás során cégünk köteles és jogosult

- az adatkérő személyazonosságát (jogosultságát) ellenőrizni,
- a kért adatok megadásáról, vagy a szükséges feladatok elvégzéséről intézkedni, é
- s a rendelet által megszabott határidőn belül a megfelelő választ az érintettnek megküldeni.

Előirányzott törlési határidő: Adatokat a jogszerű lezárás után követően 30 napon belül töröljük. Minden lehetséges adatot törünk az érintett kérésére.

6. Számítógép használati elvek

Társaságunk minden dolgozója jogosult a munkaköréhez tartozó adat- és információ hozzáféréshez, azok felvitelére és karbantartásra. Ennek érdekében szükséges mobiltelefon, asztali számítógép, és/vagy laptop vagy egyéb mobil számítógépes eszköz, fénymásoló, stb. használatára, melynek biztosítása Társaságunk feladata.

Hangsúlyozzuk, hogy társaságunk az előzőekben nem tételesen felsorolt információ feldolgozó eszközöket (számítógépeket, nyomtatókat, fénymásoló- és fax berendezéseket, scannereket, stb.) munkavégzés céljára biztosítja az azokat felhasználó munkavállalóknak.

Cégünk minden belépő új munkatársa köteles a belépésével egyidejűleg az Informatikai biztonsági szabályzatban és kapcsolódó dokumentumaiban foglaltakat elolvasva megismerni, tudomásul venni.

Az Informatikai biztonsági szabályzatban és kapcsolódó dokumentumaiban foglaltak be nem tartása szankcionálást von maga után, amely akár a munkaviszony megszűntetését, polgári peres vagy büntetőeljárást is magába foglalhat. Társaságunk fenntartja magának a jogot, hogy a bármely felhasználó számára dedikált előjogokat, kiváltságokat azonnali hatállyal visszavonja, illetve megszűntesse, az informatikai célú használatot ellenőrizhesse.

A szervezet vezetője, a közvetlen vezetők, az informatikai biztonsági vezető azonnal köteles intézkedést kezdeményezni cégünk bármely munkatársával (akár külső munkatárssal, alvállalkozó foglalkoztatottjával) szemben is, amennyiben azok megsértik az Informatikai biztonsági szabályzatban és kapcsolódó dokumentumaiban foglaltakat.

A felhasználók kötelesek megőrizni a Társaságunkkal kapcsolatos információk bizalmasságát, függetlenül az információhordozó formájától, amely lehet szóbeli, papíralapú illetve elektronikus.

Minden munkatársunk kötelessége jelenteni, ha azt tapasztalják, hogy valaki az informatikai biztonságát cégünknek sérti, vagy a személyes adatkezeléssel kapcsolatos előírásokat nem tartja be. Mind az ügyvezető, mind az adott szervezeti egység vezetője, mind az informatikai vezető köteles a szükséges intézkedéseket megtenni, amennyiben az adatvédelemre, a számítógép vagy az internet használatra vonatkozó eljárásokat a saját vagy külsős munkatárs megsérti.

A felhasználók semmilyen szoftvert nem telepíthetnek az Informatika munkatársának jóváhagyása nélkül, beleértve az Internetről letölthető vagy máshonnan beszerzett ingyenes vagy időszakosan szabadon felhasználható programokat. Új szoftver telepítésének igényét a közvetlen vezetőnek kell bejelenteni.

A szoftverek jogtisztaságára vonatkozó kötelezettségeket jelen szabályzatban foglaltak rögzítik.

Az informatikai vezető több éves tapasztalat alapján megfelelően gondoskodik:

- a hálózat határvédelméről
- a végpontok védelméről
- a biztonságos jelszóhasználatról és jelszó kezelésekről
- kilépők jelszavainak megszüntetéséről, a munkaüggyel közösen együttműködve.

7. Internet használati elvek

Mivel Társaságunk számára az Internet kapcsolat üzletileg kritikus és igen lényeges eleme a működésünknek, ezért annak biztonsága érdekében az Internetet használó munkavállalóknak, külső személyeknek az alábbi szabályokat kell betartaniuk:

- Tilos az Internet illegális (jogszabályokba ütköző) célokra történő használata, mások személyiségi jogainak megsértése; tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték); a szerzői jogok megsértése; software szándékos és tudatos illegális terjesztése,
- Tilos másokra nézve sértő, mások vallási, etnikai, politikai vagy más jellegű érzékenységét sértő, másokat zaklató tevékenység,
- Tilos az Internet hálózathoz kapcsolódó más - hazai vagy nemzetközi - hálózatok szabályaiba ütköző tevékenységek, amennyiben ezek a tevékenységek ezen hálózatokat érintik.
- Tilos a nem a Társaságunk tevékenységéhez kapcsolódó profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése,
- Tilos a hálózat, illetve erőforrásai normális működését megzavaró, veszélyeztető tevékenység,
- Tilos a hálózatot, illetve erőforrásait indokolatlanul, vagy szándékosan túlzott mértékben, pazarló módon igénybevevő tevékenység,
- Tilos az Interneten honlappal rendelkező szállítók, szolgáltatók, azok termékeinek, szolgáltatásainak minősítése,
- Tilos a Társaságunkhoz, a közösségi élethez méltatlan oldalak keresése, látogatása,
- A felhasználók nem tölthetnek le, illetve nem tölthetnek fel az Internetre semmilyen olyan jellegű információt, adatot, szoftvert, amely összeférhetetlen cégünk jelen Informatikai biztonsági politikájával.
- Tilos az Internetről letöltött szoftverek (shareware vagy freeware termékek) Társaságunk informatikai eszközein történő telepítése.
- Fenti szabályok betartása érdekében rögzítésre kerül, hogy mind az ügyvezetőnek, mind a közvetlen vezetőknek, az informatikai biztonsági vezetőnek és/vagy az általuk megbízott személyeknek jogában áll a felhasználók előzetes értesítése nélkül is bármely weboldal

látogatását megtiltani, illetve a weboldalak látogatását oly módon szabályozni, hogy tételesen megadja a látogatható helyek körét.

8. EMAIL, ELEKTRONIKUS LEVELEZÉSI ELVEK

Társaságunk levelezőrendszerében minden munkatárs rendelkezik személyes, kizárólag általa kezelhető postafiókkal, amit csak és kizárólag munkavégzésre használhat.

Társaságunk biztosítja azon SPAM-szűrő rendszereket, tűzfalat és egyéb megoldásokat, amelyek a biztonságos használatot biztosítják.

A levelezőrendszerhez tartozó megosztott postafiókokhoz történő hozzáférés előre meghatározott jogosultság alapján történik Ennek kezelése során be kell tartani a vonatkozó jogszabályokat, és Társaságunk szabályzatait, jogos érdekeit. Az előírások be nem tartása, azok megszegése a mértékétől függően munkajogi, vagy a megvalósított tényállástól függő egyéb szankció alkalmazandó.

A levelező rendszer működését az informatikai vezető monitorozza és működteti.

Társaságunk levelezőrendszerében folytatott minden tevékenységet az előző fejezetekben leírt elveknek megfelelően kell folytatni. Ezeknek az elveknek a betartását cégünk külön figyelmeztetés nélkül is ellenőrizheti, és erről a tényről a munkaszerződésben, a számítógépes jogosultság kiosztásakor, vagy munkáltatói utasításban tájékoztatja a felhasználóit.

Az ellenőrzés célja kizárólag a cég érdekeinek védelme, például a látogatott internetes oldalak és a látogatás időtartamának megfigyelése a munkaidő alatti munkavégzés ellenőrzése okán. Erről jelen IBSZ elolvastatásával, mind a részletes munkavállalói tájékoztató átadásával tájékoztatja Társaságunk dolgozóit, akik ezek aláírásával elismerik a tájékoztatás megtörténtét.

Hangsúlyozzuk, hogy az elektronikus levelezés esetleges munkaáltatói ellenőrzése minden esetben célhoz kötött, aminek a levelek ellenőrzése, megőrzése minden szakaszában meg kell felelni.

A levelezési rendszer paramétereit, beleértve a szűrőfeltételeket, korlátozásokat (mellékletek szűrése: nagyméretű multimédiás file-ok, futtaható file-ok stb.) az informatikaivezető állítja be, az üzleti és biztonsági követelmények figyelembe vételével, és az ügyvezető egyidejű tájékoztatása és engedélye alapján.

9. KÖZÖSSÉGI MÉDIA HASZNÁLATI ELVEK

A közösségi média eszközein és felületein munkaidőben és/vagy Társaságunk informatikai rendszeréből történő kommunikáció nem lehet személyes célú, csak munkával kapcsolatos.

A közösségi média használata nem történhet a munkával kapcsolatos kötelezettségek teljesítésének rovására.

A közösségi média felületeken a munkatársaknak tilos bármilyen olyan tartalom közzététele, amely alkalmas lehet Társaságunk jó hírnevének, jogos gazdasági érdekének veszélyeztetésére.

A munkatársak számára a közösségi média felületeket tilos mások bárminemű zaklatására, megfenyegetésére, rágalmazására vagy becsmérlésére használni.

Tilos megosztani a közösségi média felületeken cégünk által "üzleti titoknak" és/vagy "szigorúan bizalmasnak" minősített, vagy józan belátás alapján annak minősíthető információkat, ide értve Társaságunk belső működésére, folyamataira, infrastruktúrájára vezetőségére, munkavállalóira, alvállalkozóira stb. vonatkozó információkat is.

Tilos a Társaságunk székhelyén, telephelyein és irodáiban készült fényképek, hang- és videó felvételek megosztása.

A személyes adatok védelme érdekében felesleges és személyes érzékeny információt a kollégáink ne osszanak meg senkivel, se e-mail, se közösségi médián keresztül. Nem adhatnak meg, vagy oszthatnak meg személyes adatokat, lakhely-, születési adatokat, telefonszámot, (védett) e-mail címet, bankszámlaszámot, bankkártya adatokat (főleg PIN kódot), semmilyen jelszót. Nem tehetnek közzé önmagukról és a környezetükről kompromittáló fényképeket, videókat, vagy olyanokat, amikből szenzitív információkra lehet szert tenni.

A közösségi média eszközein – különösen - munkaidőben történő kommunikáció megfelelő professzionalizmust kell, hogy visszatükröződjön, megfelelő hangnemet használva. Így például a vulgáris kifejések, mást megalázó viccek nem megengedettek, a nem megfelelő tartalmak nemcsak a közzétevőt, hanem cégünket is leminősíthetik.

Társaságunk szeretné jelen szabályzatban is rögzíteni, hogy a közösségi média felületein megjelentetett publikáció, illetve véleménynyilvánítás minden esetben legyen etikus és félreérthetetlen. Érdemes azt is kinyilvánítani, hogy a szóban forgó tartalom magánvélemény, azaz szubjektív, és nem fogalmaz meg semmilyen objektív, pozitív/negatív kritikát.

10. Informatikai oktatási rend

Társaságunk valamennyi munkatársát, és ahol szükséges, a harmadik fél felhasználóit is, megfelelő képzésben részesíti a szervezet biztonsági szabályairól és eljárásairól már a belépés, kapcsolat felvételének elején is.

Rendszeres időközönként ezeket az ismereteket rendszeresen naprakész ismeretek közlésével fel kell újítani.

Az informatikai biztonsági képzés megtartása az Informatikai vezető felelőssége, de a feltételek biztosítása, a résztvevők jelentésétől való gondoskodás az ügyvezető kötelezettsége.

A képzés foglalja magába a biztonsági követelményeket, a jogi felelősséget, az üzleti óvintézkedéseket, valamint az informatikai eszközök helyes használatát, például a bejelentkezési eljárást, a szoftverek használatát. Az informatikai biztonságtudatossági képzés elvégzését az elektronikus információs rendszer használója aláírásával, vagy más módon (sms, email stb.) igazolja.

Kiemelten fontos az adatkezelési műveletekben vevő személyzet tudatosság-növelése és képzése. Az ilyen felhasználóknak pontosan tisztában kell lenniük a mindenkori adatkezelési rendelkezésekkel, azok etikai és jogszabályi vonatkozásaival, az ebből fakadó személyes kötelezettségeikkel és felelősségeikkel.

A képzést azelőtt kell lefolytatni, még mielőtt a felhasználók megkapnák a hozzáférési jogot (jogosultság) az elektronikus információs rendszerekhez, vagy az adatokhoz.

11. INFORMATIKAI BIZTONSÁG ELLENŐRZÉSI RENDJE

Az informatikai biztonsági szabályzatban előírt eljárások és szabályok érvényesítése hagyományos vezetési eszközökkel történik, melynek elemei:

- eseti vagy rendszeresen ismétlődő ellenőrzés
- felelősségre vonás az ellenőrzéssel feltárt mulasztás miatt
- mulasztások esetén hibamegelőző vizsgálat lefolytatása, korrekciók tétele szükség esetén

Az informatikai biztonság ellenőrzésére vonatkozó feladatokat az ügyvezető és az informatikai vezető közösen határozzák meg, az adatvédelmi megbízott bevonásával. Az ellenőrzések megszervezése és végrehajtása az ügyvezető hatáskörébe tartozik.

A kontrollok kialakításánál elsődlegesen azt kell figyelembe venni, hogy azok által az információbiztonság szintje mérhető legyen.

Rendszeresen ellenőrzi az informatikai vezető a számítógépeknek, szervereknek a logjait, begyűjti és elemzi, biztosítja az adatbázisok és logok anonimizálását, védelmét.

Meg kell határozni az ellenőrzések területeit, a hozzájuk rendelt ellenőrzési célkitűzésekkel.

Az ellenőrzés eredményét minden esetben ki kell értékelni, és a megfelelő következtetéseket le kell vonni, illetve vissza kell csatolni a biztonsági folyamatra. Bizonyítható mulasztás feltárása esetén szükség szerinti mértékű felelősségre vonási eljárást kell kezdeményezni.

Az informatikai biztonsággal kapcsolatos ellenőrzés lehet:

- Megfelelőségi vizsgálat (melynek célja felderíteni, hogy Társaságunk egésze, részterülete rendelkezik-e a törvényi előírásokban meghatározott személyi, eljárási, tárgyi feltételekkel, és azok megfelelően dokumentáltak-e).
- Az informatikai biztonság szintjére vonatkozó vizsgálat (annak ellenőrzésére, hogy a jelen informatikai biztonság szintje megfelel-e üzleti elvárásainknak, jogszabályi kötelezettségeinkek).
- Az informatikai biztonsági szabályok betartásának ellenőrzése azért, hogy Társaságunk jelen IBSZ-ben és egyéb szabályzataiban foglalt előírásokat egy-egy területén az illetékes, érintett személyek ismerik-e, betartják-e.

12. Web-oldal védelme

Társaságunk Web-oldalának biztonságtechnikai védelmét az informatikai vezető biztosítja.
A web-felületről elérhető távmunka védelmét tűzfal és minden olyan egyéb eszköz biztosítja, amit az informatikai vezető megfelelőnek ítél.

Kelt: Bp., 2018.05.27.

…….. ……..……

ügyvezető informatikai vezető