Hatályos: 2020. december 01.-től …….sz. példány

Jóváhagyom: ……
Fogarasi László bv. ezredes, bv. főtanácsos
ügyvezető

A DUNA PAPÍR KFT. INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Készítette: ……..
Nagy Attila mb. informatikus

Tartalom

1. Bevezetés

A Duna Papír Kft. Informatikai Biztonsági Szabályzatát (továbbiakban IBSZ) az informatikai rendszerrel kapcsolatos adatvédelem és adatbiztonság megteremtése érdekében - az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. Törvény (a továbbiakban: Isztv.), és az Európai Parlament és a Tanács (EU) 2016/679 általános adatvédelmi rendelete (GDPR), amelyek részletesen szabályozzák a személyes adatok védelmével, és a közérdekű adatok nyilvánosságával kapcsolatos legfontosabb teendőket, illetőleg az alapvető jogok érvényesülését – az alábbiak szerint szabályozom:

2. A szabályzat célja

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

A szabályzat célja továbbá, hogy az informatika alkalmazása során biztosítsa a társaság munkafolyamataiban az alábbiakat:

- az adat-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását,
- az üzemeltetett számítógépek, informatikai eszközök, valamint azok kiegészítő eszközeinek rendeltetésszerű használatát,
- a számítógépes rendszerek zavartalan üzemeltetését,
- az üzembiztonságot szolgáló karbantartást és fenntartást,
- az adatok számítógépes feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetését, illetve minimális mértékre csökkentését,
- az adatállományok tartalmi és formai épségének megőrzését,
- munkaállomásokon lekérdezhető adatok körének meghatározását,
- adatállományok biztonságos mentését,
- a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását,
- az adatvédelem és adatbiztonság feltételeit, azaz a személyes adatok kezelésére használt informatikai rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, rendelkezésre állását és ellenálló képességét; fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását vissza lehet állítani, valamint az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

3. Az Informatikai Biztonság Szabályzat Hatálya

3.1 A szabályzat személyi hatálya

E szabályzat személyi hatálya a Duna Papír Kft. valamennyi jogviszonyban álló munkavállalójára, valamint szerződéses és egyéb munkaviszony keretében foglalkoztatott ügyviteli és fizikai munkavállalókra terjed ki.
A személyes adatok védelméért, az adatkezelés jogszerűségéért a társaság ügyvezetője a felelős.

3.2 A szabályzat tárgyi hatálya

E szabályzat tárgyi hatálya kiterjed:

- a társaság tulajdonában lévő valamennyi számítástechnikai, informatikai berendezésre, valamint ezek műszaki dokumentációjára is;
- a rendszer- és felhasználói programokra;
- a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül;
- az adatok felhasználására, tárolására vonatkozó utasításokra;
- az adathordozók tárolására, felhasználására;
- valamint a számítástechnikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési dokumentáció).

A szabályzat előírásait alkalmazni kell a társaság belső szervezeti egységei által vezetett nyilvántartások, adatbázisok és valamennyi egyedileg kezelt adat, elektronikus szolgáltatások illetőleg dokumentumok esetében. A társaság által nyilvántartott adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, sérülés, törlés vagy megsemmisülés ellen.

Iratokat, adatokat a munkaköri feladat ellátásán kívül a munkahelyről kivinni, a munkahelyen kívül feldolgozni, tárolni csak az ügyvezető engedélyével lehet, azzal a feltétellel, hogy az irat, adat tartalmát illetéktelen személy nem ismerheti meg.

Az iratok tárolása, kezelése során fokozottan ügyelni kell arra, hogy illetéktelen személyek ne ismerhessék meg azok tartalmát. A munkavégzés céljára szolgáló irodákat távozáskor kulcsra kell zárni. Az irodahelyiségek nyitvatartása miatti illetéktelen hozzáférés esetén az érintett fegyelmi felelősséggel tartozik.

3.3 Szervezeti hatálya

Az IBSZ személyi hatálya kiterjed az adott vállalkozásra, a vállalkozás információkezeléssel és feldolgozással kapcsolatos összes tevékenységére és folyamatára, a szervezet tulajdonában használatban lévő összes információs rendszerben előforduló adatokra, illetve a szervezettel szerződéses jogviszonyban álló valamennyi szervezetre, melynek munkavállalói vagy alvállalkozói a szervezet által használt rendszerekhez, vagy az ezekben tárolt adatokhoz bármiféle hozzáféréssel

rendelkeznek. A szervezet kötelezettsége, hogy az adott szervezetnek legyen módja a rá vonatkozó elvárásokat, kötelezettségeket megismerni.
Az itt nem szabályozott kérdésekben a szervezet Szervezeti és Működési Szabályzata a mérvadó.

4. Az adatkezelés során felhasznált legfontosabb fogalmak

- Adat: a természetes vagy mesterséges objektumok, folyamatok, állapotok jellemzői illetőleg azok részleteinek érzékelhető formában történő megjelenítése. Adat tágabb értelemben jelenthet szöveget, számot, rajzot, térképi részleteket vagy bármely más információt a megjelenési módjára vagy formájára való tekintet nélkül.

- Adatállomány: az egy nyilvántartásban kezelt adatok összessége.

- Adatkezelés: az alkalmazott eljárástól függetlenül adatokon végzett bármely művelet vagy műveletek összessége, így például az adatok gyűjtése, felvétele, rögzítése, tárolása, felhasználása, összekapcsolása, szolgáltatása, megjelenítése stb.

- Adatkezelő: az a belső szervezeti egység, amely a személyes, illetőleg a közérdekű adatok körébe tartozó adatok, dokumentumok kezelését, szolgáltatását ellátja.

- Adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.

- Adatközlő: az a belső szervezeti egység, amely az adatfelelős által szolgáltatott adatokat a jogszabályokban meghatározott módon közzéteszi.

- Adattovábbítás: az adatot meghatározott harmadik személy számára történő hozzáférhetővé tétele.

- harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek

- Adatvédelem: az adatokhoz való illetéktelen hozzáférés, a meghibásodás, a megsemmisülés stb. megakadályozása; a személyes adatok esetében kiegészül az adott személy személyes adatai jogellenes gyűjtése, kezelése, tárolása, felhasználása elleni védelemmel.

- Adattörlés: az adatok felismerhetetlenné tétele olya módon, hogy a helyreállításuk többé nem lehetséges.

- Információ: jelentéssel bíró adat megjelenési módjára vagy formájára való tekintet nélkül.

- Kötelezően közzéteendő közérdekű adat: az Isztv 26. § (2) – (3) bekezdésében meghatározott körbe tartozó adat.

- Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, melynek nyilvánosságra hozatalát vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

- Közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személye adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

- Különleges adat: a faji eredetre, nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális éltre vonatkozó személyes adat, továbbá az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

- Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele.

- Személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;

- Elektronikus tájékoztató szolgáltatás (tájékoztatás): az elektronikus közigazgatási szolgáltatás körén kívüli ügyintézésről elektronikus úton hozzáférhetővé tett általános jellegű információs szolgáltatás.

- Interaktív szolgáltatás: az egyszerű tájékoztatáson túlmenően olyan szolgáltatás (például letölthető űrlapok, kereső rendszerek, tematikus tájékoztatók), amely csak a használó aktivitását igényli, a szolgáltatást nyújtó szerv által előkészített dokumentumok kitöltéséhez, felhasználásához.

- alkalmazói program (alkalmazói szoftver): olyan program, amelyet az alkalmazó saját speciális céljai érdekében vezet be, és amely a hardver és az üzemi rendszer funkcióit használja;

- felhasználó: az a személy (vagy szervezet), aki (amely) egy vagy több informatikai rendszert használ feladatai megoldásához;

- felhasználói jog: az a jogosultság a hálózaton, amely a felhasználó számára szükséges és elégséges munkájának elvégzéséhez;

- gépterem (iroda): az a helyiség, amelyben a társaság dolgozói hozzáférhetnek a számítástechnikai eszközökhöz és szolgáltatásokhoz;

- hálózat: két vagy több számítógép összekapcsolása, amely informatikai rendszerek legkülönbözőbb komponensei között adatcserét tesz lehetővé;

- hardver: az informatikai rendszer eszközeit, fizikai elemeit alkotó része;

- informatika: a számítógépes információrendszerek tudománya, amely elméletet, szemléletet és módszertant ad a számítógépes információrendszerek tervezéséhez, fejlesztéséhez, szervezéséhez és működéséhez;

- informatikai biztonság: olyan előírások, szabványok betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és bizalmasságát érintik, és amelyeket az informatikai rendszerek vagy komponenseik alkalmazása során biztonsági megelőző intézkedésekkel lehet elérni;

- munkaállomás: egy operátor vagy felhasználó számára, adott típusú feladathoz felszerelt számítógép vagy terminál;

- rack szekrény: üvegezett, biztonságos fém szekrény, amelyben hálózati eszközöket, szervereket üzemeltetnek;

- rendszerprogram (rendszer szoftver): olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardvereit használhassuk és az alkalmazói programokat működtethessük. A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.

- szerver: olyan hálózatra kapcsolt központi szerepet betöltő számítógép, amelynek alapvető feladata, hogy más, a hálózatra kapcsolt számítógépek vagy terminálok számára az erőforrásait megossza;

- szerverszoba: az a légkondicionált, biztonsági berendezésekkel ellátott helyiség, ahol a szerverek vannak, és csak a kijelölt személyeknek engedélyezett a belépés;

- vírus: önállóan nem működő programrész, amely illegálisan készült egy felhasználói program részeként. A felhasználói program alkalmazása során átterjedhet más, az informatikai rendszerben lévő rendszer- illetve felhasználói programra, sokszorozva önmagát és egy beépített feltételhez kötötten (pl. konkrét időpont) pusztítást indít el.

5. Az adatkezelés, az adatvédelem követelmény rendszere

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.

5.1 A társaság belső szervezeti egységei

a) szakmai feladataik ellátása során kizárólag az adott feladat, a tevékenység megítélése, az adott döntés előkészítése érdekében, a vonatkozó jogszabályok rendelkezései alapján feltétlenül szükséges – és a személyes adatok körébe tartozó – adatok gyűjtését, tárolását, rendezését, felhasználását, nyilvánosságra hozatalát, archiválását, irattározását, stb. láthatják el;

Az adatkezelőt fokozott felelősség terheli az adatok jogszabályszerű kezeléséért és szolgáltatásáért.
E szabályzatot a Duna Papír Kft. Szervezeti és Működési Szabályzatával, és Adatvédelmi és adatbiztonsági szabályzatával összhangban kell alkalmazni.

5.2 Az adatvédelem folyamatában a védelem tárgya:

a) a társaság működése során keletkezett személyes és közérdekű adatok teljes köre, keletkezésüktől a megsemmisítésükig,
b) az adathordozók fizikai jellegüktől függetlenül, amelyek személyes, illetőleg közérdekű adatokat tartalmaznak. Az adathordozók lehetnek papír alapú iratok, kimutatások, listák, térképek, műszaki dokumentációk, mágneses adathordozók, informatikai rendszerek, hardver, szoftver
c) az a fizikai környezet, ahol az adatállomány kezelése, tárolása történik.
d) az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra

5.3 Az adatkezelés alapkövetelményei

A feladatok ellátása során az adott feladat szerinti ügymenet részeként biztosítani kell az adatkezelés szabályainak a maradéktalan betartását, a személyek adatainak védelmét a jogellenes felhasználástól.

Az adatkezelés során biztosítani kell:

a) az adott egyén szempontjából fontos adatok helyes, pontos kezelését. A hibás adat előfordulása esetén annak észlelésekor társaságtól, valamint az érintett kezdeményezésekor a pontosítást haladéktalanul teljesíteni kell;

b) az adott személy adatai kizárólag a jogszabály rendelkezéseivel összhangban kerüljenek feldolgozásra, rögzítésre, felhasználásra, illetőleg ne kerüljenek illetéktelenek birtokába;

c) a személyes adatoknak a közérdekű adatokkal való együttes alkalmazásuk esetén nem akadályozhatják a közérdekű adatok nyilvánosságát, szolgáltatását;

d) a különböző célú adatok, adatállományok (adatbázisok) folyamatos vezetését, aktualizálást és az adathordozó fajtájától független folyamatos rendelkezésre állását és elérhetőségét az arra jogosultak számára. A személyes adatok tekintetében minden esetben biztosítani kell a zárt kezelést és a jogszabályok szerinti előírásoknak megfelelő hozzáférést;

e) a különböző adatok, adatállományok (adatbázisok) valódiságát, pontosságát, részletességét, hitelességét;

f) a különböző adatok, adatállományok (adatbázisok) jellegétől függően azok bizalmas, illetőleg az adott területre vonatkozó jogszabályok szerinti kezelését;

g) a társaság gondozásában készült információs rendszerek, adatbázisok folyamatos működését és szükség szerinti folyamatos hozzáférés lehetőségét, a folyamatos aktualizálást, a közérdekű adatok folyamatos a jogszabályoknak megfelelő szolgáltatását;

az adatrendszer (akár számítógépes, akár manuális) fizikai biztonságát. Az adatok és az adathordozó eszközök összességében jelentős értéket képviselnek. Megsemmisülésük esetén újra előállításuk többletmunkát és költséget igényel.

5.4 Az adatvédelem eszközei

Az adatvédelem eszközeiként kell kezelni és folyamatosan biztosítani mindazon igazgatási, iratkezelési, szervezési, személyi, műszaki, technikai, informatikai és egyéb intézkedéseket, melyek elengedhetetlenek az egyes adatok, adatállományok (adatbázisok) zavartalan működéséhez, és védelmet nyújtanak ahhoz, hogy

a) illetéktelenek ne jussanak a különböző személyes adatokhoz (személyes adatokat tartalmazó adatbázisokhoz), dokumentumokhoz,

b) a különböző adatok (adatbázisok) dokumentumok megsérülésére, meghibásodására ne kerüljön sor

az adatkezelés során ismeretek hiánya, hozzá nem értés miatt, emberi mulasztásból károsodásra, adatok, dokumentumok megsemmisülésére ne kerüljön sor

5.5 Személyi feltételek biztosítása

A személyes adatok kezelésével kapcsolatos teendőket a hatáskörükben e feladattal megbízott munkavállalók láthatnak el, amelyet a társaság adatvédelmi és adatbiztonsági

szabályzatában az adatvédelem szervezetére vonatkozó leírás részletesen tartalmaz. A folyamatos ügyintézés érdekében a megfelelő helyettesítésről gondoskodni kell. A közérdekű adatok folyamatos szolgáltatásáért a társaság ügyvezetője felelős. Felelős a szakterületet jól ismerő és az elektronikus adatkezelésben, tájékoztatásban jártas személy(ek) kijelöléséért.

A jelen szabályzatban foglaltak szakszerű végrehajtásáról a társaság adatvédelmi felelősének kell gondoskodnia. Az adatvédelmi felelős feladatait a munkaköri leírás, valamint az Isztv. 24§ (2) bekezdése tartalmazza.

A társaság informatikusa végzi az informatikai védelmi rendszer biztosítását, a vírusvédelmi szoftverek frissítését, valamint biztosítja a rendszer üzemképességét, és a műszaki ellátást, biztonsági másolatot készít, segíti, ellenőrzi a társaság dolgozóinak számítástechnikai munkáját.

5.6 Fizikai, technikai védelem

5.6.1 Tűzvédelem

A szerverszoba, illetve az informatikai eszközöket tartalmazó irodák a "D" tűzveszélyességi osztályba tartoznak, amely mérsékelt tűzveszélyes üzemet jelent.
A szerverszobára vonatkozó tűzvédelem feladatait, sajátos előírásait a társaság tűzvédelmi szabályzata tartalmazza.

5.6.2 Vagyonvédelem, fizikai biztonság

- a szerverszobát, irodákat biztonsági zárakkal kell felszerelni;
- a szerverszobába való be- és kilépés rendjét szabályozni kell, a szerverhez és a szerverszobához való hozzáférés korlátozott, meghatározott informatikus munkatársra, más személy benntartózkodását a társaság ügyvezetője és helyettesei engedélyezhetik.
- szerverszoba kulcsát a társaság informatikus tárolja, onnan csak az arra feljogosítottak vehetik fel;
- munkaidőn túl az irodákban, illetve a szerverszobában csak engedéllyel lehet tartózkodni;
- az irodahelyiségekben elhelyezett számítástechnikai eszközöket csak az arra kijelölt munkavállalók használhatják;
- a számítástechnikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

5.6.3 Adathordozók védelme, tárolása, hordozása és karbantartása

- a munkaasztalon csak azok az adathordozók lehetnek, amelyek az aktuális feldolgozáshoz szükségesek;
- az adathordozókat jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak;
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni;
- adathordozót más intézménynek átadni csak az adatvédelmi felelős engedélyével lehet;
- az adathordozók megőrzésének idejét, ha másképp nincs rendelkezés, a felelős vezető határozza meg;
- olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért, selejtezni kell. Selejtezendő:

a) a fizikailag sérült, javíthatatlan;
b) gyári, raktározási hibát követően felhasználásra alkalmatlan (deformálódott);
c) véglegesen elhasználódott adathordozó.

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni. Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adattárolókról törlő program segítségével kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

A selejtezést a Selejtezési Szabályzatnak és a társaság Iratkezelési Szabályzatának megfelelően kell lefolytatni, Az adathordozókat a Leltározási Szabályzatnak megfelelően kell leltározni.

5.6.4 Adatvédelmi feladatok

- az adatbevitel hibátlan műszaki állapotú berendezésen történhet;
- csak hibátlan adathordozóra lehet adatállományt rögzíteni;
- adatrögzítő szoftver védelme: a programokat, adatokat ellenőrző funkciókkal, amennyiben szükséges titkosítással kell ellátni;
- a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen hozzáférési szinten férhet hozzá a programokhoz és adatokhoz (alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá);
- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak. A fontosabb file-okat tartalmazó adattárolókról másolatot kell időnként készíteni. A másolt lemezek csak az illetékes vezető engedélyével adhatók ki.

5.6.5 Vírusvédelem

A munkaállomásokon és szervereken, ha másképp nincs rendelkezés, heti rendszerességgel vírusellenőrzést és vírusirtást kell tartani.

A vírusvédelmi programok adatbázisát naprakészen kell tartani.

Vírusfertőzés okozta hiba gyanúja esetén azonnal szólni kell az illetékes szakembernek, informatikusnak. Amennyiben nincs erre lehetőség (pl. munkaidőn kívül), a feldolgozásban lévő adatokat el kell menteni, majd a programból kilépve a gépet ki kell kapcsolni. A gépet addig bekapcsolni nem szabad, amíg azt az arra illetékes szakember, informatikus meg nem vizsgálta. A vírusfertőzést jelenteni kell a társaság ügyvezetőjének, még akkor is, ha semmi hiba nem történt a fertőzés folyamán, valamint a társaság ügyvezetőjének ki kell deríteni a fertőzés lehetséges okait, és a szükséges védelmi intézkedést meg kell hoznia.

5.6.6 Szoftvervédelem

Az üzemeltetésért felelős informatikusnak biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek az illetékes felhasználók számára.

Rendszerszoftver védelem:

a) a rendszerszoftver módosításához az illetékes engedélye szükséges;
b) a módosítással egy időben a dokumentációban is át kell a változtatásokat vezetni;
c) a rendszerszoftver-eseményekről és a változtatásokról nyilvántartást kell vezetni (eseménynapló).

Programhoz való hozzáférés, programvédelem:

a) A kezelés folyamán az illetéktelen hozzáférést és próbálkozást ki kell zárni.
b) Gondoskodni kell arról, hogy a tárolt programok, adatállományok ne károsodjanak, a követelményeknek megfelelően működjenek
c) A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt.

5.7 Hardver védelem

- A számítógépeket óvni kell folyadéktól, túlzott páratartalomtól és hőigénybevételtől;
- a számítógép közelében ételt és italt fogyasztani tilos;
- a szerverszobában klímaberendezés használata ajánlott;
- szervereknél biztosítani kell a szünetmentes feszültségforrást és rack szekrényben vagy szerverszobában kell elhelyezni;
- a számítógép-hálózat csatornáit lehetőség szerint külön kábelcsatornában kell vezetni, melyre jól látható helyekre rá kell írni a hálózat típusát;
- a fali csatlakozók megbontása szigorúan tilos;
- csak földelt aljzatokat lehet használni számítógép üzemeltetéséhez;
- a lengő kábeleket úgy kell elhelyezni, hogy azok balesetet ne okozhassanak, alapelv: sűrűn használt utat szabadon kell hagyni;
- a számítógépek belsejébe nyúlni, és ott bárminemű változtatást okozni tilos, csak az illetékes szakember (társaság informatikusa), illetve a szervizek szakemberei nyúlhatnak bele;

5.8 Hálózatvédelem

Alapelvek

Csak olyan eszközök kapcsolhatók a szervezet hálózatába, melyek a szervezet biztonsági architektúrájával összehangban vannak. Tilos olyan munkaállomás, mobil eszköz használata, amely rendelkezik nem bizalmas hálózati kapcsolattal.
Naprakész nyilvántartást kell vezetni az engedélyezett protokollokról, illetve a hálózatvédelem informatikai biztonsági architektúra elemeinek beállításáról.
A szervezet számítógép hálózatának vezeték nélküli szegmensein, valamint nem bizalmas csatornán keresztül csak titkosított adatkapcsolatot lehet kialakítani.

Hálózat biztonsága

A belső hálózatokon csak az engedélyezett protokollok használhatóak. A belső hálózaton engedélyezett protokollokat az üzemeltetők javaslata, illetve az informatikai vezető határozza meg. Hordozható eszközöket – notebookokat, tableteket, okostelefonokat csak a rendszergazda által elvégzett és jóváhagyott ellenőrzés után lehet a szervezet számítógép hálózatára kapcsolni. A számítógép hálózatban a felhasználók hitelesítési adatait (bejelentkező nevek, jelszavak) csak titkosítva lehet továbbítani.

Felelősség

A hálózat és az adattovábbítás biztonsági eljárásaival kapcsolatos feladatok az informatikai vezető felelőssége.

5.9Informatikai védelem

1. A szerverszobában a társaság informatikusán, valamint az informatikai rendszer üzemeltetését végző gazdálkodó szervezet munkatársán kívül más nem tartózkodhat. Más személyek benntartózkodását a társaság ügyvezetője engedélyezheti.

2. Üzemidőn kívül az ajtókat zárva kell tartani. A szerverszoba kulcsát a hivatali informatikus tárolja, onnan csak az arra feljogosítottak vehetik fel. Munkaidőn kívül idegen személy csak felügyelet mellett tartózkodhat a gépteremben.

3. Az irodákban/szerverszobában a folyamatos, higiénikus munkavégzés feltételeit kell megőrizni.

4. A szerverszobába ételt, italt bevinni és ott elfogyasztani szigorúan TILOS!

5. A szerverszobába égő cigarettával belépni és ott dohányozni, valamint tüzet okozó tevékenységet folytatni szigorúan TILOS!

6. A szerverszoba takarítását csak a társaság informatikusának felügyelete mellett, legalább havonta egyszer, a kijelölt személy végezheti.

7. A berendezések belsejébe nyúlni TILOS! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak a társaság informatikusa és a szervizek szakemberei végezhetik.

8. A számítógépeket csak rendeltetésszerűen és az ütemezett munkák elvégzésére lehet használni. Tilos a számítógépeken játszani, illetve az informatikai rendszer biztonságát veszélyeztető tevékenységet végezni.

9. Adathordozókat csak a társaság informatikusa engedélyével lehet be- és kivinni a szerverszobából.

10. Az elektromos hálózatba más – nem a rendszerekhez, illetve azok kiszolgálásához tartozó – berendezéseket csatlakoztatni nem lehet.

11. A számítógép javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetmentes használat, a szakszerűség, a vonatkozó érintésvédelmi szabályok és az esztétikai követelményeket. Nem végezhető olyan javítás, szerelés, átalakítás vagy bármely beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat. A fenti rendelkezések megsértése esetén az elkövetővel szemben az adatvédelmi felelős fegyelmi felelősségre vonást kezdeményezhet

12. Védelmi előírások:

- A számítógépeket csak indítójelszóval lehessen elindítani, az indítójelszavat 90 naponta meg kell változtatni.
- Külön figyelmet kell fordítani az IT adminisztrátori hozzáférésekre, amelyek jellemzően széleskörű jogosultságot jelentenek. Olyan esetekben, amikor a rendszerből az adatok le is tölthetők, indokolt további intézkedéseket is megtenni, illetve adott esetben a letöltések technikai blokkolása is indokolt lehet.
- Induláskor minden esetben vírus-ellenőrző programot kell elindítani; A megfelelő anti - vírus szoftver telepítése és a tűzfalak megfelelő alkalmazása és konfigurálása mellett a rendszeres frissítés is kiemelten fontos, illetve a megfelelő belső szabályozás és a tudatosság növelése is (pl. a gyanús csatolmányok megnyitásának mellőzése).
- A feldolgozáshoz szükséges programok elindításához és az adatok hozzáféréséhez jelszóvédelem kell.
- A LIBRA Integrált Pénzügyi Gazdasági Rendszer felhasználói csak jelszavas azonosítást követően léphetnek be a rendszerbe. A felhasználói névnek és a jelszónak minden esetben egyedinek kell lennie.
- Minden esetben a jelszavaknak különbözniük kell.
- Az adatállományokról napi mentést kell készíteni, ezeket a heti mentésekig kell megőrizni;
- A teljes anyagról heti mentéseket kell készíteni, a mentések készítése esetén nem szabad megfeledkezni arról, hogy a mentésben lévő adatokat ugyanolyan magas szinten kell védeni, mint az éles rendszerben lévő adatokat.
- A teljes anyagról a tárgyévet követő év első munkanapján mentést kell végezni.
- Használt eszközök lecserélése esetén gondoskodni kell az adatok törléséről, amely történhet formázással, egyszerű törléssel, vagy egyesesetekben fizikai megsemmisítéssel. Ez a kötelezettség mindenféle eszközre vonatkozik, amely cseréje előtt személyes adatot tartalmazott.

6. Az IBSZ biztonsági fokozata

A hivatal adatai különböző biztonsági fokozatba tartozhatnak. (üzleti titkok, pénzügyi adatok, illetve a hivatal belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas adatok).

Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

7. Védelmet igénylő, az informatikai rendszerre ható elemek

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.

- Az informatikai rendszerre az alábbi tényezők hatnak:
- a környezeti infrastruktúra,
- a hardver elemek,
- az adathordozók,
- a dokumentumok,
- a szoftver elemek,
- az adatok,
- a rendszerelemekkel kapcsolatba kerülő személyek.

7.1 A védelem tárgya

A védelmi intézkedések kiterjednek:

- az alkalmazott hardver eszközökre és azok működési biztonságára,
- az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
- az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára

7.2 A védelem eszközei

A mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

8. A védelem felelőse

A jelen szabályzatban foglaltak szakszerű végrehajtásáról a társaság ügyvezetőjének kell gondoskodnia.

8.1 Adatvédelmi felelősök feladatai

a) Adatvédelmi képviselő feladatai:

- figyelemmel kíséri az adatbiztonsággal és információszabadsággal kapcsolatos változásokat, amelyek alapján indokolt esetben kezdeményezi jelen szabályzat módosítását;-
- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására. -
- ellátja az adatkezelés és adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- az adatvédelmi feladatok ismertetése
- ellenőri tevékenységét adminisztrálja
- ellenőrzi a szoftverek használatának jogszerűségét
- évente egy alkalommal részletesen ellenőrzi az informatikai vezetővel az IBSZ előírásainak betartását-
- a rendszergazda jelenlétében, előzetes bejelentési kötelezettség nélkül ellenőrizheti az informatikai munkafolyamatok adatvédelmet érintő részeit.

b) Informatikus/rendszergazda feladatai:

- a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli
- felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének folyamatos ellenőrzése,
- felelős a hivatal informatikai rendszer hardver eszközeinek karbantartásáért,
- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- gondoskodik a folyamatos vírusvédelemről
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer adminisztrációját.

8.2 Az informatikai biztonsági vezető jogai

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

8.3 Felhasználók

Felhasználó:
a szervezet összes, elektronikus információs rendszert használó munkatársa.

Speciális felhasználó:
adminisztrátori, root, stb. speciális jogosultsággal rendelkező felhasználók. Minden adminisztrátor egy felhasználó is egyben, csak egy speciális fiók abban a tekintetben, hogy ő teljes joggal rendelkezik az adott rendszer felett.

Külső felhasználó:
a szervezettel kapcsolatban álló külső felek a Szervezet biztonsági szabályainak és elvárásainak betartása mellett férhetnek hozzá a Szervezet elektronikus információs rendszeréhez.
A külső felhasználók hozzáférését a hozzáférés indokának megszűnte után azonnal, ill. az együttműködés lejártakor automatikusan meg kell szüntetni. A megszűntetésről késedelem nélkül az Informatikai osztályt értesíteni kell, hogy a megfelelő lépéseket el tudják végezni.

9. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

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

9.1 Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában - valamint a társaságnál - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. Az IBSZ folyamatos karbantartása az informatikus/rendszergazda feladata.

10. Jogosultságkezelés

A jogosultságkezelés célja az erőforrásokhoz és információkhoz való hozzáférési jogok megadásának és megvonásának szabályozása.

10.1 Alapelvek

Minden felhasználó csak azokhoz az erőforrásokhoz, információkhoz jut hozzá, amely a munkavégzéséhez feltétlen szükséges. A felhasználók a szervezet tulajdonában vagy használatában lévő számítógépeken tárolt valamennyi információhoz csak a megfelelő jogosultság ellenőrzését követően férhetnek hozzá, ezzel megvédve az adatokat a jogosulatlan hozzáféréstől.
Az informatikai biztonsági felelős ellenőrzi és dokumentálja az állomány megosztásokat, hogy elkerüljék az esetleges szerzői joggal védett tartalmak megosztását, megjelenítését, végrehajtását, reprodukálását.

10.2 Hozzáférési jogok

A szervezet csak felhasználónevet és jelszó párost használ az informatikai rendszereinek hozzáféréséhez.

10.3 Jelszókezelés szabályai

A felhasználói jelszavak kezelését szabályozni kell, különös tekintettel arra, hogy

- a felhasználók titokba tartsák azokat, illetve
- megfelelő időközönként azokat megváltoztassák
- biztosítani jelszó kiadásakor csak a jelszó tulajdonosa szerezzen róla tudomást.

A felhasználói jelszavaknak:

- legalább 8 karakterből kell, hogy álljanak,
- lehetőség szerint kis és nagybetűkből álljanak, illetve számokat és írásjeleket is tartalmazzanak,
- a kezdeti jelszavakat első belépés után mielőbb meg kell változtatni
- a jelszavakat legalább 6 havonta cserélni kell.

10.4 Távoli elérés szabályai

Szabályozni kell a szervezet informatikai rendszerihez való távoli hozzáférést. A távoli hozzáférést csak indokolt esetben lehet alkalmazni, a hozzáférés és az adatcserét biztonságos csatornán keresztül kell megvalósítani.
A külső rendszerekből a Szervezet belső hálózatára csatlakozás csak a szervezet ügyvezetőjének előzetes engedélyével lehetséges. A megvalósulás feltételit az Informatikai Biztonsági felelős határozza meg.

Távoli munka esetén a szolgáltatások megkezdése ellőtt végre kell hajtani a hitelesítési eljárást (VPN kapcsolat). A megosztott erőforrások csak a hitelesítés után érhetők el. Csak megfelelően biztosított környezettel, technikai feltételekkel biztosított helyen lehet a távoli elérést biztosítani. Nyilvános hálózatokról, jelszó nélküli wifi hálózatokról a távoli elérést tilos indítani.

A távoli eléréshez külön felhasználói csoportot kell létrehozni. Lehetőség szerint csak olyan rendszerekből engedélyezhető a távoli elérés, amely során a felhasználó csak adatellenőrzésre, adatfeldolgozásra képes, adatmásolás, tárolás, továbbítás távoli rendszerekbe nem lehetséges

11.Adatmentések

Az adatmentések célja az elviselhetetlen adatvesztések megakadályozása, illetve az elvárt időn belüli adatvisszaállítás.

11.1 Általános rendelkezések

Minden szervezet kezelésében vagy használatában lévő, elektronikus formában tárolt információkról biztonsági mentést kell készíteni. Olyan mentési rendet kell kialakítani, ami biztosítja az adatok visszaállítását az elvárt visszaállítási időn belül, illetve ami meghatározza a maximálisan elviselhető adatvesztést.

A mentések gyakoriságát, a felhasznált adathordozókat, tárolási helyüket a fentiek figyelembevételével kell kiválasztani, illetve olyan eljárásrendet kell alkalmazni, ami megfelel azon feltételeknek.

11.2 Mentési eljárásrend

Adatmentéseknek kell készülniük a szervezet számítógépein tárolt dokumentumokról (Word / Excel táblázatokról) Továbbá, mentést kell készteni a szervezet számlázási programjairól. A mentéseket minden nap el kell végezni automatikusan bármiféle felhasználói beavatkozás nélkül. A mentési folyamatokat munkaidőn kívülre kell ütemezni, hogy a mentendő adatállományok ne legyenek használatban, miközben a mentési folyamat tart, mert ez inkonzisztenciát fog okozni a mentett állományokban. Ezért a mentéseket 22:00-ra kell ütemezni. A mentés eredményét a mentés másnapján ellenőriznie kell az Informatikai Biztonsági Felelősnek.

11.3 Archiválási eljárásrend

Minden héten hétfőn a pénteken készült napi mentést archiválni kell. Archiválni az erre kiválasztott azonosítóval ellátott merevlemezre kell, amit az archiválás után vissza kell helyezni tűzvédett páncélszekrénybe. Az archiválásra használt merevlemezeket évente selejtezni kell

11.4 Visszatöltés mentési állományból

A mentések visszatöltésénél meg kell határozni, hogy milyen dátumú visszaállítási állományra van szükség, melyik állományra van szükséges, illetve milyen célból van szükség a visszatöltésre. Az Informatikai Biztonsági Felelős feladata megvizsgálni a visszatöltés okait, ami lehet:

- programhiba által bekövetkezett adatvesztés
- felhasználói rögzítési hiba
- vírus, kártevő által okozott adatvesztés

Bármilyen adatvesztés történik a szervezetnél, értesíteni kell a szervezet tulajdonosát / ügyvezetőt. Amennyiben az adatvesztés esetén vélhetően magánszemélyek adatai is sérültek, értesíteni kell az adatvédelmi tisztviselőt, ennek hiányában az adatvédelmi felelőst.

12.Naplózás

A szervezet elektronikus rendszereiben automatikus naplót kell vezetni, a biztonsági szempontból lényeges tevékenységekről.

Úgy kell kialakítani ezeket a naplóbejegyzéseket, amikből egyértelműen kiderül

- milyen események történnek
- miből származtak az események
- mik voltak az események kimenetelei

Az automatikusan készülő naplófájlokban az következő események körül a lehető legtöbbet rögzíteni kell:

- be- és kijelentkezéseket
- jogosulatlan hozzáférési kísérleteket
- rendszerriasztásokat, meghibásodási jelentéseket
- felhasználók felvitelét, törlését, módosítását
- jogosultsági csoportokban történő változásokat
- a felhasználók jogosultságaiban beálló változásokat.
- naplózási funkciók indítását és leállítását
- naplóállományok létrehozását, törlését
- naplózási konfigurációban történő változásokat
- nyilvános hálózaton való távoli kapcsolódási kísérleteket, kapcsolatok létrehozását, kapcsolatok bontását

A napló fájlokhoz a felhasználóknak írási jogosultsággal nem férhetnek hozzá, a naplófájlokból törlés nem engedélyezett.

13.Képzés, tudatosítás

Folyamatosan biztosítani kell, hogy szervezet tagjai tudatában legyenek az informatikai biztonság fenyegetettségeivel, motiválni kell őket a szervezet informatikai biztonsági szabályzatának betartására. Oktatni kell a szervezet tagjait a biztonsági eljárásokról, a felhasználni informatikai eszközök helyes használatáról annak érdekében, hogy lecsökkentse a szervezet biztonsági kockázatokat.

13.1 Számítógép használati elvek

A felhasználók jogosultak a munkakörükhöz kapcsolódó adathozzáférésekhez, azok karbantartásához.

A szervezethez új belépő kollégának kötelessége a belépéssel együtt a jelen Informatikai Biztonsági Szabályzatot elolvasni, megismerni, tudomásul venni.

A szervezet az adatokat feldolgozó eszközöket /számítógépek, nyomtatók, szkennerek/ köteles munkavégzés céljából biztosítani az azokat használó munkavállalóknak.

A felhasználók nem telepíthetnek semmilyen szoftvert (sem ingyenes, se jogtiszta) a Rendszergazda / Informatikai felelős jóváhagyása nélkül. Nem legális szoftver telepítés a szervezet informatikai eszközeire szigorúan tilos.

Az informatikai biztonsági vezetőnek kötelessége értesíteni a vállalat vezetőjét, amennyiben a Szervezet munkatársai, vagy külső munkatársak a cég Informatikai Biztonsági Szabályzatát megsértik. A szervezet vezetőjének kötelessége intézkedéseket kezdeményezni, esetleg szankcióval élni a szabályzatot megsértő személyekkel szemben

13.2 E-mail használati elvek

A szervezet levelezőrendszerében minden munkatárs rendelkezik személyes, kizárólag általa kezelhető postafiókkal, amelyet csak és kizárólag céges munkavégzésre lehet használni. A levelező rendszer használata során be kell tartani a vonatkozó jogszabályokat, illetve a szervezet szabályzatait. Az előírások megszegése, be nem tartása mértékétől függően munkajogi vagy egyéb szankciók alkalmazhatók.

13.3 Internet használati elvek

A szervezet felhasználóinak a következő szabályokat kell betartaniuk:

- Tilos a szervezet tevékenységéhez kapcsolódó profitszerzést célzó direktmarketing tevékenység.
- Tilos a hálózat, illetve annak erőforrásait indokolatlan mértékben igénybe vevő tevékenység végzése (pl. torrent programok használata).
- A szervezethez méltatlan weblapok látogatása.
- Tilos olyan internetes tevékenység végzése, ami ellentétben van a szervezet Informatikai Biztonsági Politikájával, egyéb szabályzatával.
- Tilos másokra nézve sértő, másokat zaklató tevékenységek végzése.
- Tilos az internetről letöltött, bárminemű szoftver telepítése a szervezet informatikai eszközeire az Informatikai Biztonsági felelős engedélye nélkül.
- A szervezet vezetőinek, közvetlen vezetőknek, az informatikai biztonsági felelősnek, vagy az általuk megbízott személyeknek jogában áll a felhasználók előzetes értesítése nélkül bármely weboldal meglátogatásának tiltása.

13.4 Közösségi média használata

A közösségi médiákon való kommunikáció szervezet eszközein, munkaidőben csak munkával kapcsolatos lehet. A közösségi média használata nem történhet a munkával kapcsolatos munkavégzés rovására.
A közösségi oldalakon tilos olyan tartalom közlése, ami a szervezet jó hírnevét, gazdasági érdekeit veszélyezteti.
A közösségi média felületei tilos mások zaklatása, rágalmazása, megfenyegetése.
Tilos a közösségi média felületein bárminemű, a szervezet által üzleti titoknak minősített, a szervezet belső működésére, belső folyamataival kapcsolatos, a szervezet munkavállalóival kapcsolatos információk közlése, megosztása.
Tilos a szervezet székhelyén, telephelyén, irodáiban készült fénykép, hang-és videófelvétel megosztása.

14.Záró rendelkezések

Jelen szabályzat 2020. december 01. napján lép hatályba.

A 2014. 01.01-től hatályban lévő Informatikai Biztonsági szabályzat hatályát veszti.