a Magyarság Háza Nonprofit
Korlátolt Felelősségű Társaság

INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Kiadva: az 3/2021. (07.30.) számú ügyvezetői utasítással

.....

Csibi Krisztina
ügyvezető

Magyarság Háza Nonprofit Korlátolt Felelősségű Társaság
MAGYARSÁG HÁZA

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Név:	**Magyarság Háza Nonprofit Korlátolt Felelősségű Társaság**
Rövidített név:	**Magyarság Háza Nonprofit Kft.**
Székhely:	**1051 Budapest, Zrínyi utca 5.**
Cégjegyzékszám:	**Cg.01-09-335243**
Vezetve:	**a Fővárosi Törvényszék Cégbírósága nyilvántartásában**
Adószám:	**26615374-2-41.**
Statisztikai számjel:	**26615374-9499-572-01.**
Honlap:	**http://www.magyarsaghaza.net**
Telefonszám:	**0036 (1) 795 6606**
E-mail cím:	**info@magyarsaghaza.net**
Képviseli:	**Csibi Krisztina ügyvezető, önállóan**
továbbiakban:	**Adatkezelő / Munkáltató / Üzemeltető / Társaság**

Jelen Informatikai Biztonsági Szabályzat (a továbbiakban: Szabályzat) a Magyarság Háza Nonprofit Korlátolt Felelősségű Társaság (a továbbiakban: **Társaság** vagy **Üzemeltető, Munkáltató**) által alkalmazott informatikai rendszer, illetőleg informatikai eszközök használatának rendjére vonatkozó belső szabályait tartalmazza.

A jelen Szabályzat megállapítása és módosítása a Társaság mindenkori vezető tisztségviselőjének hatáskörébe tartozik.

Jelen Szabályzat mindenkor érvényes változata a számítógépes hálózaton és a Társaság székhelyén érhető el. A kinyomtatott példány a vezető tisztségviselő aláírásának hiányában nem tekintendő hivatalos példánynak.

Hatályba léptetve: 2021.július 30. napján

Magyarság Háza Nonprofit Korlátolt Felelősségű Társaság
képv.: Csibi Krisztina ügyvezető, önállóan

Magyarság Háza Nonprofit Korlátolt Felelősségű Társaság

TARTALOM

I. ÁLTALÁNOS RENDELKEZÉSEK

I./1. A Szabályzat célja

(1) A jelen Szabályzat célja egyrészt, hogy a Társasággal foglalkoztatásra irányuló jogviszonyban álló személyekben erősítse az informatikai biztonsági tudatosságot, és biztosítsa a szakmai felkészültséget az informatikai biztonsági szabályoknak való megfeleléshez azáltal, hogy részletes tájékoztatást nyújt az információbiztonság, és különösen az adatbiztonság körében irányadó, kötelező erejű rendelkezésekről. A Szabályzat célja, hogy a Társaság szervezetén belül az informatikai rendszerrel összefüggő döntések meghozatalában közreműködő személyek megfelelő felkészültségét biztosítsa a védelmi előírások megfelelő alkalmazásához.

(2) A jelen Szabályzat a Társaság által végzett informatikai tevékenységeket szabályozza a Társaság birtokában álló informatikai eszközök és szoftverek használatára vonatkozó egységes szabályozás kialakítása és technikai szabályok meghatározása által.

(3) A jelen Szabályzat célja, hogy a benne rögzítetteknek megfelelő eljárási rend alkalmazásával a Társaság biztosítsa az elektronikus információs rendszereinek biztonságát, és az informatikai rendszerek, eszközök használata, alkalmazása során biztosítsa az információbiztonság követelményeinek érvényesülését, és megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát, biztosítsa a biztonságos üzemeltetés alapvető szabályait, az ellenőrizhető informatikai környezet kialakításához szükséges feltételeket, a használathoz és üzemeltetéshez kapcsolódó magas szintű szabályokat, az alapvető biztonsági normákat és követelményeket.

(4) A Szabályzat célja, hogy a Társaság működése és szolgáltatásai során biztosítsa a Társaság által kezelt, feldolgozott, továbbított, valamint tárolt adatok kockázattal arányos védelmét (bizalmasság, sértetlenség és rendelkezésre állás) a felmerülő veszélyforrások ellen.

(5) A Szabályzat célja továbbá a Társaság által megfogalmazott általános elektronikus információbiztonsági irányelvek érvényre juttatásának biztosítása, az ehhez szükséges egyes elektronikus információbiztonsági szerepkörök, feladatok, folyamatok szabályainak, eljárásainak, követelményeinek a meghatározása az elektronikus információbiztonsággal összefüggésben.

(6) A Szabályzat célja továbbá:
- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása;
- a Társaság által üzemeltetett informatikai rendszerek rendeltetésszerű használatának biztosítása;
- az üzembiztonságot szolgáló karbantartás és fenntartás;
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése;
- az adatállományok tartalmi és formai épségének megőrzése;
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása;
- az adatállományok biztonságos mentése;
- az informatikai rendszerek zavartalan üzemeltetése;
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

(7) A jelen Szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzembehelyezésen keresztül az üzemeltetésig. A jelen Szabályzat az információbiztonság általános érvényű előírását tartalmazza, és meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

I./2. A szabályozott szervezet adatai

Név:	**Magyarság Háza Nonprofit Korlátolt Felelősségű Társaság**
Rövidített név:	**Magyarság Háza Nonprofit Kft.**
Székhely:	**1051 Budapest, Zrínyi utca 5.**
Cégjegyzékszám:	**Cg.01-09-335243**
Vezetve:	**a Fővárosi Törvényszék Cégbírósága nyilvántartásában**
Adószám:	**26615374-2-41.**
Statisztikai számjel:	**26615374-9499-572-01.**

Honlap:	**http://www.magyarsaghaza.net**
Telefonszám:	**0036 (1) 795 6606**
E-mail cím:	**info@magyarsaghaza.net**
Képviseli:	**Csibi Krisztina ügyvezető, önállóan**
továbbiakban:	**Adatkezelő / Munkáltató / Üzemeltető / Társaság**

I./3. A Társaság Informatikai Felelőse, elérhetőségei, jogállása

Név:	**Fülep Márk**
Telefonszám:	+36704142474
E-mail cím:	info@tartalomszures.com
Jogállása:	A Társaság Informatikai Felelősének fő szerepe, hogy összefogja, koordinálja, és ellenőrizze a Társaság informatikai tevékenységeit, információbiztonsági intézkedéseit. Informatikai Felelősnek kinevezhető mind belső munkatárs, mind külső szolgáltató.

I./4. A Szabályzat hatálya

I./4.1. A Szabályzat személyi hatálya

(1) Jelen Szabályzat személyi hatálya kiterjed a Társaság belső állományában foglalkoztatott munkavállalókra, és a Társasággal foglalkoztatásra irányuló egyéb jogviszonyban állókra, így különösen az iskolaszövetkezeti tagokra, és a munkaerő-kölcsönzés keretében foglalkoztatott munkavállalókra, továbbá a Társaság informatikai rendszerének használati jogosultságával rendelkező külső személyekre is, azzal a megjegyzéssel, hogy a Társaság által használt elektronikus információs rendszerek külső üzemeltetőire, fejlesztőire, szerződéses úton történő egyéb alkalmazóira jelen Szabályzat rendelkezéseinek megtartását szerződésben rögzíteni kell.

I./4.2. A Szabályzat tárgyi hatálya

(1) Jelen Szabályzat tárgyi hatálya kiterjed a Társaság elektronikus információs rendszereinek minden erőforrására (szolgáltatások, infrastruktúra, technológia, szoftverelemek, hardverelemek, adathordozók, adatok), kiterjed a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, időjüktől és az adatok fizikai megjelenési formájuktól függetlenül, kiterjed a rendszer- és felhasználói programokra, kiterjed az adatok felhasználására vonatkozó utasításokra, kiterjed az adathordozók tárolására, felhasználására.

(2) A jelen Szabályzat hatálya és Társaság által alkalmazott védelmi intézkedések köre kiterjed:
- a Társaság által használt valamennyi informatikai berendezésre, beleértve a berendezések műszaki dokumentációját is;
- rendszerprogramokra és a felhasználói programokra;
- az alkalmazott hardver eszközökre és azok működési biztonságára,
- az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
- adathordozókra, azok tárolására és felhasználására, beleértve a feldolgozásra beérkezés és a felhasználókhoz történő eljuttatás folyamatait is.

I./4.3. A Szabályzat területi hatálya

(2) A jelen Szabályzat területi hatálya kiterjed a Társaság székhelyére, minden telephelyére, továbbá mindazon objektumokra és helyiségekre, ahol a Társaság esetlegesen elektronikus információs rendszereket használ, működtet, üzemeltet vagy fejleszt.

I./4.4. A Szabályzat időbeli hatálya

(1) A Jelen Szabályzat időbeli hatálya **2021. augusztus 1.** napjától visszavonásig terjed.

I./5. Irányadó jogszabályok

(1) A Társaságnak az adatok kezelése során különösen, de nem kizárólagosan az alábbi jogszabályokban, határozatokban, ajánlásokban foglalt előírásoknak megfelelően kell eljárnia, a jelen Szabályzatban foglaltak szerint:

- Az Európai Parlament és a Tanács (Eu) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, a továbbiakban: GDPR vagy Rendelet). A rendelet magyar nyelvű szövege elérhető az alábbi linken: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016R0679;

- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.). A törvény hatályos szövege elérhető az alábbi linken: http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.366978;

- Magyarország Alaptörvénye (a továbbiakban: Alaptörvény). A törvény hatályos szövege elérhető az alábbi linken: http://njt.hu/cgi_bin/njt_doc.cgi?docid=140968.356005;

- a Polgári törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.). A törvény hatályos szövege elérhető az alábbi linken: http://njt.hu/cgi_bin/njt_doc.cgi?docid=159096.370225;

- a Polgári perrendtartásról szóló 2016. évi CXXX. törvény (a továbbiakban: Pp.). A törvény hatályos szövege elérhető az alábbi linken: h http://njt.hu/cgi_bin/njt_doc.cgi?docid=198992.377344;

- a Munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.). A törvény hatályos szövege elérhető az alábbi linken: http://njt.hu/cgi_bin/njt_doc.cgi?docid=143164.367080;

- a Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatói, ajánlásai, határozatai. A NAIH határozatai elérhetőek a következő linken: https://www.naih.hu/hatosagi-hatarozatok---vegzesek.html; A NAIH ajánlásai elérhetőek a következő linken: https://www.naih.hu/ajanlasok.html;

(2) A Társaság az alábbi, a tevékenységére nézve nem kötelezően alkalmazandó jogszabályokban lefektetett alapelvek, előírások szerint valósítja meg az információbiztonság megfelelő védelmi szintjét:

- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.), A törvény hatályos szövege elérhető az alábbi linken: https://njt.hu/jogszabaly/2013-50-00-00.22;

- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet szerinti (a továbbiakban: BM rendelet), A rendelet hatályos szövege elérhető az alábbi linken: https://njt.hu/jogszabaly/2015-41-20-0A;

I./6. Fogalom meghatározások, értelmező rendelkezések, főbb rövidítések jegyzéke

(1) Jelen Szabályzat alkalmazásában irányadó **főbb fogalmak**:

- **adat:** az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.

- **adatállomány:** az egy nyilvántartó rendszerben kezelt adatok összessége.

- **adatbiztonság**: a személyes adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.

- **adathordozó:** az adatok tárolására, megőrzésére szolgáló, beépített vagy cserélhető eszközök összefoglaló neve.

- **adat nyilvánosságra hozatala:** az adat bárki számára történő hozzáférhetővé tétele.

- **adattörlés:** az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges.

- **aktív hálózati eszköz**: kapcsolók (switch-ek), forgalomirányítók (router-ek), vezeték nélküli hozzáférési pontok (Acces Pointok), és egyéb eszközök (bridge-ek, tűzfalak, médiakonverterek, modemek, multiplex, rádiórelék, stb.), amelyek segítségével az informatikai rendszer üzemvitele biztosítható.

- **asztali munkaállomás**: a felhasználó rendelkezésére bocsátott számítástechnikai eszköz, mely alapvetően a számítógépből, monitorból, billentyűzetből és egérből, illetve más csatlakoztatható számítástechnikai eszközökből (különösen: mikrofon, kamera, scanner, nyomtató stb.) állhat;

- **bizalmasság:** az informatikai rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;
- **biztonsági esemény:** nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;
- **biztonsági eseménykezelése:** az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;
- **elektronikus információs rendszer:** az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese. Egy elektronikus információs rendszernek kell tekinteni az adott adatgazda által, adott cél érdekében az adatok, információk kezelésére használt eszközök, eljárások, valamint az ezeket kezelő személyek együttesét
- **felhasználó**: az a természetes személy, aki a Társaság informatikai infrastruktúráját használja, vagy információs társadalommal összefüggő szolgáltatásait igénybe veszi.
- **fenyegetés:** olyan lehetséges művelet vagy esemény, amely sértheti az informatikai rendszer vagy az informatikai rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az informatikai rendszer védettségét, biztonságát;
- **fizikai védelem:** fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klímatizálás és a tűzvédelem;
- **foglalkoztatásra irányuló jogviszony***:* minden olyan jogviszony, amelyben a szolgáltatás tárgya természetes személy által ellenérték fejében végzett munka.
- **foglalkoztatott:** a Társasággal foglalkoztatásra irányuló jogviszonyban álló személy. Jelen Szabályzat és a Társaság adatvédelmi dokumentumainak alkalmazásában az iskolaszövetkezeti tagok, saját állományban foglalkoztatott munkavállalók és munkaerő-kölcsönzés céljából foglalkoztatott munkavállalók gyűjtőfogalma.
- **GDPR**: az Európai Parlament és a Tanács (Eu) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről. A rendelet magyar nyelvű szövege elérhető az alábbi linken: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016R0679;
- **hozzáférés:** olyan eljárás, amely valamely elektronikus információs rendszer használója számára - jogosultságának függvényében - meghatározott célra, helyen és időben elérhetővé teszi az elektronikus információs rendszer erőforrásait, elérhetővé tesz a rendszerben adatokként tárolt információkat;
- **informatikai rendszer** (elektronikus információs rendszer): az adatok kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese.
- **információ:** bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret;
- **információbiztonság**: az elektronikus információs rendszer olyan állapota, amelyben a védelem az abban kezelt adatok valamint a rendszer elemeinek szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.
- **kockázat:** a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;
- **kockázatelemzés:** az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;
- **Le- és feltöltés:** valamely számítógépre vagy számítógépről történő adatátvitel. Általában az internet erőforrásai és egy felhasználói PC között zajlik.

- **Licensz*:*** egy szoftver felhasználását szabályzó szerződés
- **mobil eszköz:** olyan kisméretű hordozható számítástechnikai eszköz, amely vezeték nélküli adattovábbításra képes, cserélhető vagy beépített adathordozóval és önálló áramforrással rendelkezik. Ilyen eszköz az okostelefon, tablet, ebook-olvasó stb.
- **PC, gép:** számítógép
- **rendelkezésre állás:** annak biztosítása, hogy az informatikai rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatók legyenek;
- **sértetlenség:** az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az adat az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az informatikai rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az informatikai rendszer eleme rendeltetésének megfelelően használható;
- **Szerver:** minden olyan számítógép vagy funkció, amely más számítógépeket szolgál ki.

II. A SZÁMÍTÁSTECHNIKAI INFRASTRUKTÚRA ELEMEI, CÉLJA

(1) A Társaságnál található számítástechnikai infrastruktúra létének kizárólagos célja a munkavégzés technikai feltételeinek biztosítása.

(2) A számítástechnikai infrastruktúra elemei:
- számítógépek,
- számítógép perifériák (nyomtató, scanner, egér, stb.),
- a számítógép hálózat,
- az irodatechnikai berendezések (fénymásoló, fax, telefon)
- a számítógépeken futó szoftverek,
- a fenti berendezésekhez és szoftverekhez tartozó dokumentációk,
- az adathordozók és mobil eszközök.

(3) Ezen informatikai eszközök, a rajtuk zajló folyamatok, a felhasználó (munkavállalók) által kifejtett aktivitás és a tárolt adatok a Munkáltató által a személyes adatok védelmére vonatkozó előírások tiszteletben tartásával bármikor ellenőrizhetők és rögzíthetők, függetlenül attól, hogy a magáncélú használat engedélyezett-e valamely felhasználó számára vagy sem.

(4) A Társaság informatikai rendszerében létrehozott/keletkezett/generált anyag (pl. Office állományok, digitális jegyzőkönyvek, tervdokumentációk stb.) a Munkáltató tulajdonát, illetve szellemi termékét képezik. A Munkáltató és az adott munkavállaló között fennálló munkaszerződés megszűnésével a felhasználó ezen anyagokra nem jogosult, kivételt ez alól az képezhet, ha a Munkáltató ezt írásban engedélyezi.

III. A TÁRSASÁG INFORMATIKAI BIZTONSÁGGAL KAPCSOLATOS SZERVEZETI RENDSZERE

III./1. A vezető tisztségviselőnek az informatikai biztonság biztosításával kapcsolatos kötelezettségei

(1) A Társaság mindenkori vezető tisztségviselője a Társaság működésének sajátosságait figyelembe véve határozta meg az informatikai biztonság biztosításának szervezetét, a feladat- és hatásköröket. A jelen Szabályzatban előírtak betartatásáért a munkakörében, vagy feladatkörében minden érintett szervezeti egység vezetője felelős. A Társaság foglalkoztatottjai munkavégzésük során kötelesek gondoskodni az informatikai biztonsági előírások érvényesüléséről.

(2) A vezető tisztségviselő hatáskörei és feladatai az informatikai biztonsággal kapcsolatosan:
a) felelős az informatikai eszközöket igénylő munkakörök ellátásához szükséges technikai feltételek biztosításáért;
b) felelős az esetleges biztonsági események kezeléséért;
c) dönt az ügyfelek személyéről, és az informatikai beruházásokat magában foglaló szerződések tartalmáról;
d) felelős az informatikai biztonság érvényesülésére irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért;
e) felügyeli az Informatikai Felelős tevékenységét;
f) ellenőrzi az informatikai biztonsági szabályzatok, utasítások betartását, ennek érdekében vizsgálatot rendelhet el;
g) kiadja, szükség esetén módosítja a Társaság informatikai biztonsággal kapcsolatos szabályzatait;
h) figyelemmel kíséri az informatikai biztonsággal kapcsolatos jogszabályi változásokat;

III./2. A Társaság Informatikai Felelőse (IT Rendszergazda)

(1) A Társaság informatikai biztonság érvényesülését szolgáló rendelkezések megtartásáért felelős és felhatalmazott személyt (a továbbiakban: **Informatikai Felelős**) jelöl ki (jelen Szabályzat **1. számú melléklet**e szerint, írásban), aki köteles a jelen Szabályzatban, valamint a jogszabályokban meghatározott rendelkezéseknek a Társaság mindenkori vezető tisztségviselője, munkavállalói, szerződéses partnerei, illetve a Társasággal foglalkoztatásra irányuló jogviszonyban álló egyéb személyek által történő megtartását elősegíteni, biztosítani és ellenőrizni. Tekintettel arra, hogy az Informatikai Felelős által ellátandó feladat megfelelő informatikai és adatbiztonsági szakismeretet igényel, így a Társaságnál csak olyan személy nevezhető ki Informatikai Felelősnek – akár szolgáltatási szerződés megkötése révén -, rendelkezik a feladatai ellátáshoz szükséges szakképzettséggel.

(2) A Társaság belső Informatikai Felelősének fő szerepe, hogy összefogja, koordinálja, és ellenőrizze a Társaság informatikai tevékenységeit, információbiztonsági intézkedéseit, és Informatikai Felelős felel a Társaságnál előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért.

(3) A Társaság Informatikai Felelősét a Társaság mindenkori vezető tisztségviselője választja a Társaság saját állományban foglalkoztatott munkavállalói közül, vagy külső személy (IT Rendszergazda) megbízásával. A Társaság által kijelölt Informatikai Felelős jogviszonyának időtartama a munkaviszonyának, vagy a megbízás ellátására vonatkozó egyéb jogviszonyának (vállalkozási vagy megbízási jogviszony) időtartamához igazodik. Az Informatikai Felelős jogviszonya megszűnik, ha:

a) jogviszonya megszűnik;
b) a tisztségről lemond;
c) meghal;
d) a Társaság mindenkori vezető tisztségviselője a tisztségéből visszahívja;

(3) A Társaság Informatikai Felelősének hatáskörei és feladatai az informatikai biztonság biztosításával kapcsolatosan:

a) az Informatikai Felelős köteles segítséget nyújtani a felhasználóknak az informatikai infrastruktúra használata során;
b) az Informatikai Felelős köteles rendszeresen ellenőrzéseket végezni arra vonatkozóan, hogy a jelen Szabályzat rendelkezéseit a Társaság mindennapi működése és üzletszerű gazdasági tevékenysége során az arra kötelezettek megtartják-e;
c) az Informatikai Felelős jogosult a Társaság legfőbb szerve, vezetősége irányába javaslattal élni a Társaság informatikai biztonságot biztosító gyakorlatának módosítása vonatkozásában;
d) az Informatikai Felelős jogosult javaslatot tenni informatikai biztonságra irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy veszélyeztető körülmények megszüntetésére;
e) az Informatikai Felelős a saját feladatkörébe tartozó informatikai rendszert köteles felügyelni;
f) az Informatikai Felelős felelősséggel tartozik az informatikai rendszer üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért;
g) az Informatikai Felelős köteles gondoskodni a informatikai rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról;
h) az Informatikai Felelős feladata a védelmi intézkedések, eszközök működésének folyamatos ellenőrzése;
i) az Informatikai Felelős felelősséggel tartozik az informatikai rendszer hardver eszközeinek folyamatos karbantartásáért;
j) az Informatikai Felelős köteles gondoskodni a folyamatos vírusvédelemről;
k) az Informatikai Felelős vírusfertőzés gyanúja esetén köteles gondoskodni a fertőzött rendszerek haladéktalan vírusmentesítéséről;
l) az Informatikai Felelős köteles közreműködni a biztonsági események kezelésében;
m) az Informatikai Felelős felelősséggel folyamatosan köteles ellenőrizni az informatikai rendszer adminisztrációját.

III./3. Rendszerüzemeltetést végző foglalkoztatottak

(1) A rendszerüzemeltetést végző foglalkoztatottak a közvetlen szakmai vezetőjük és/vagy az Informatikai Felelősön keresztül szakmai véleményt és javaslatokat fogalmazhatnak meg a szabályozásokkal és eljárásrendekkel, valamint az alkalmazott technológiákkal kapcsolatban.

(2) Minden információs eszköz vagy eszközcsoport, információs rendszer, informatikai szolgáltatás működtetésére informatikai feladatkört ellátó munkatársat kell kijelölni, aki felelős a jelen Szabályzatban és az egyéb IT utasításokban megfogalmazott követelmények szerinti üzembe helyezésért, üzemeltetésért, vagy kivonásért.

(3) A rendszerüzemeltetést végző foglalkoztatottak feladata a szervezeti előírásoknak és a gyártói ajánlásoknak megfelelően a folyamatos működéshez szükséges beállítások elvégzése, munkafolyamatok és ellenőrzések végrehajtása, a dokumentációk naprakészen tartása, a rendszerek felhasználóinak támogatása, valamint ezen tevékenységeik előírásszerű adminisztrálása.

III./4. A Társaság foglalkoztatottjainak, és külső felhasználóknak a jogai és kötelezettségei

(1) A Társaság informatikai rendszereinek felhasználói kötelesek a jelen Szabályzat, valamint az informatikai biztonságra vonatkozó utasítások, jogszabályok rendelkezéseinek megtartására.

(2) A felhasználó a jelen Szabályzat megismerését, és tudomásulvételét követően jogosult a munkavégzéséhez szükséges informatikai infrastruktúrához való teljes, vagy korlátozott hozzáférésre.

(3) A szervezeti egységek vezetői:

a) kötelesek biztosítani és ellenőrizni a vezetésük alá tartozó szervezeti egységnél az informatikai biztonságra vonatkozó utasításokban és a Szabályzatban foglaltak betartását;
b) az informatikai biztonságot veszélyeztető esemény, fenyegetés észlelése esetén haladéktalanul kötelesek értesíteni a Társaság Informatikai Felelősét és a vezető tisztségviselőt;

c) kötelesek gondoskodni arról, hogy a jelen Szabályzat előírásait és változásait az általuk irányított foglalkoztatottak feladatköreiknek megfelelő részletességgel megismerjék.

d) kötelesek gondoskodni arról, hogy a jelen Szabályzat megismerésére vonatkozó, jelen Szabályzat **2. számú Mellékle**tét képező nyilatkozat az általuk irányított foglalkoztatottak által kitöltésre, aláírásra nyilvántartásba vételre és tárolásra kerüljön.

(4) A felhasználó csak és kizárólag abban az esetben jogosult az Informatikai eszközöket (beleértve a szoftvereket is) magáncélra használni, amennyiben a Társaság ezt írásban előzetesen jóváhagyta.

(5) A felhasználó jogosult az engedélyezett magáncélú felhasználás során keletkezett anyagainak elkülönítésére, melynek helyét és maximális tárhelyét az Informatikai Felelős határozza meg.

(6) A magánjellegű anyagokat az Informatikai Felelős áthelyezheti, vagy akár el is távolíthatja, amennyiben úgy ítéli meg, hogy ezen anyagok az informatikai rendszer működését, biztonságát veszélyeztetik. Engedélyezett magánhasználat során keletkezett anyagok áthelyezésének, eltávolításának szükségessége esetén a munkavállalót előre, írásban értesíti a szükséges intézkedésről, lehetőséget biztosítva, hogy a felhasználó ezt maga tegye meg. Amennyiben a felhasználó legkésőbb az értesítést követő munkanapon nem hajtja végre a szükséges intézkedést, úgy az Informatikai Felelős teszi ezt meg.

(7) Az informatikai eszközöket (beleértve a szoftvereket is) a Felhasználó köteles rendeltetésszerűen használni. A nem rendeltetésszerű használatból eredő károkért a felhasználó felelősségre vonható. Nem rendeltetésszerű használat például, de nem kizárólagosan: más felhasználó felhasználónevével való visszaélés, a PC-n, illetve a szerveren tárolt állományok manipulálása, amely következtében adatvesztés következik be, hibás adatok keletkeznek.

(8) A felhasználó számítógépes vagy mobil eszközön végzett munkája során köteles együttműködni az informatikai biztonságért felelős személyekkel.

(9) Amennyiben a felhasználónak tudomására jut, hogy más felhasználó jelen Szabályzat bármely pontját megsértette, vagy megsérteni készül, köteles haladéktalanul értesíteni az Informatikai Felelőst.

(10) Az informatikai biztonságért felelős személyek időnként – az informatikai rendszer hatékonyabb működése érdekében – Informatikai Utasításokat (IT Utasítás) adnak ki – a Társaság vezető tisztségviselőjével előzetesen egyeztetve –, amelyeket elektronikus úton (e-mail-ben) juttatnak el a felhasználóhoz. A felhasználó köteles ezeket az utasításokat elfogadni és betartani. Az IT Utasítások jelen Szabályzat szerves részét képezik, azok be nem betartása jelen Szabályzat megsértésének minősül.

(11) Vétkes kötelezettségszegésnek minősül, amennyiben a foglalkoztatott nem tartja be a jelen Szabályzatban, illetve az IT Utasításokban foglalt kötelezettségeit. A felhasználóval szemben ilyen esetben a munkaszerződésében írt hátrányos jogkövetkezmények alkalmazhatóak.

(12) A felhasználó a jelen Szabályzatban, valamint IT Utasításokban foglalt kötelezettségének megszegésével okozott kárt köteles megtéríteni, ha nem úgy járt el, ahogy az adott helyzetben általában elvárható. A kártérítés mértéke nem haladhatja meg a munkavállaló négyhavi távolléti díjának összegét. Szándékos vagy súlyosan gondatlan károkozás esetén a foglalkoztatott teljes kárt köteles megtéríteni. Nem köteles a foglalkoztatott megtéríteni azt a kárt, amelynek bekövetkezése a károkozás idején nem volt előrelátható, vagy amelyet a Társaság, mint Munkáltató, vagy foglalkoztató vétkes magatartása okozott, vagy amely abból származott, hogy a Társaság a kárenyhítési kötelezettségének nem tett eleget.

(13) **A felhasználók részletes kötelezettségeit, felelősségeit jelen Szabályzat IX./3. fejezete tartalmazza.**

IV. AZ INFORMATIKAI BIZTONSÁGOT VESZÉLYEZTETŐ HELYZETEK

(1) Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrásoknak a felhasználók általi ismerete szükséges annak érdekében, hogy felkészülten, megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek a Társaság által.

IV./1. Környezeti infrastruktúra által okozott ártalmak

(1) **Elemi csapás:** földrengés, árvíz, tűz, villámcsapás, stb.

(2) **Környezeti kár:** légszennyezettség, nagy teljesítményű elektromágneses térerő, elektrosztatikus feltöltődés, a levegő nedvességtartalmának felszökése vagy leesése, piszkolódás (pl. por).

(3) **Közüzemi szolgáltatásba bekövetkező zavarok:** feszültség-kimaradás, feszültségingadozás, elektromos zárlat, csőtörés.

IV./2. Emberi tényezőre visszavezethető veszélyek

(1) **Szándékos károkozás**: illetéktelen hozzáférés (adat, eszköz), adatok- eszközök eltulajdonítása, rongálás (gép, adathordozó).

(2) **Nem szándékos, illetve gondatlan károkozás:** figyelmetlenség (ellenőrzés hiánya), szakmai hozzá nem értés, a megváltozott körülmények figyelmen kívül hagyása, vírusfertőzött adathordozó behozatala, biztonsági követelmények és gyári előírások be nem tartása, adathordozók megrongálódása (rossz tárolás, kezelés), a karbantartási műveletek elmulasztása.

V. A BIZTONSÁGI ESEMÉNYEK ÉS INCIDENSEK KEZELÉSE

(1) A Társaság informatikai rendszereibe bekerülő, illetve ott keletkező adatok, információk informatikai rendszerekben történő adatfeldolgozásával, működésével, üzemeltetésével és tárolásával kapcsolatban felmerülő biztonsági és elektronikus információbiztonsági események kezelése érdekében esemény és incidenskezelési szabályozást kell létrehozni.

(2) A biztonsági esemény és incidenskezelés informatikai feltételrendszerének kialakításáért az Informatikai Felelős (IT Rendszergazda) a felelős.

(3) A Társaságnál kialakított biztonsági esemény és incidenskezelés során legalább a következőket kell teljesíteni:
- Az incidens bejelentését követően be kell azonosítani és kategorizálni kell a biztonsági eseményt és kategóriától függően a megfelelő személyt értesíteni kell.
- A biztonsági és elektronikus információbiztonsági események tárolására, kezelésére, követésére belső rendszert kell kialakítani, amelybe automatikusan, vagy a felelős informatikai feladatokat ellátó munkatárs útján manuálisan kerülnek be a biztonsági események.
- Megfelelő kompetenciával rendelkező incidenskezelő foglalkoztatott/csoport kijelölése, mely szükség esetén bevonható az incidens elhárításába, kezelésébe.

VI. FIZIKAI VÉDELMI INTÉZKEDÉSEK

VI./1. Általános követelmények

(1) A Társaság köteles érvényre juttatni az informatikai rendszerének fizikai védelmi követelményeit, megvalósítva a zárt (az összes releváns fenyegetést figyelembe vevő), teljes körű (a rendszer összes elemére kiterjed), folyamatos (megszakítás nélkül valósul meg, a kockázatokkal arányos (a védelem költségei arányosak a potenciális kárértékekkel) védelmet.

(2) A Társaságnak gondoskodnia kell az illetéktelen behatolást vagy hozzáférést, valamint a szándékos károkozást vagy véletlen katasztrófát megakadályozó, szükséges mértékű – kockázatokkal arányos – védelmi intézkedések alkalmazásáról. Ennek érdekében a Társaság:
- ellenőrzés alatt tartja a be- és kilépési pontokat, naplózza a fizikai belépéseket;
- ellenőrzés alatt tartja a székhelyen belüli, belépésre jogosultak által elérhető helyiségeket;
- kíséri a létesítménybe alkalmi belépésre jogosultakat (vendégeket), és figyelemmel kíséri a tevékenységüket;
- megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközöket;
- felügyeli a fizikai behatolás riasztásokat és a felügyeleti berendezéseket;
- védi az elektronikus információs rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben;
- az elsődleges áramforrás kiesése esetére szünetmentes áramellátást biztosít az elektronikus információs rendszer szabályos leállításához vagy a hosszútávú tartalék áramellátásra történő átkapcsoláshoz;
- az informatikai eszközökhöz megfelelő tűzelfojtó berendezéseket alkalmaz, és tart karban;
- szabályozza, továbbá figyeli és ellenőrzi a székhelyre bevitt, onnan kivitt információs rendszerelemeket, és nyilvántartást vezet ezekről;

VI./2. Beléptetési rendszer

(1) A Társaság a jogosulatlan személyek belépésének kiszűrésére alkalmas beléptetési rendszert köteles alkalmazni, melynek működtetésével biztosítja, hogy a személyes adatok tárolási helyeként szolgáló helyiségeibe jogosulatlan személyek ne léphessenek be.

(2) Ennek érdekében a Társaság belső termeibe csak olyan személyek léphetnek be, akik személyazonosságukat igazolták, és akik belépési jogosultságáról a Társaság ügyfélszolgálatának munkatársai meggyőződtek.

VI./3. Kíséret

(1) A Társaság köteles ellenőrzése alatt tartani az irodahelyiségén belüli, belépésre jogosultak által elérhető helyiségeket, azzal, hogy a Társaság saját állományú munkavállalói kötelesek elkísérni az irodahelyiségbe eseti belépésre jogosultakat és figyelemmel követni a tevékenységüket.

VI./4. Jogosultsági szintek

(1) A Társaság foglalkoztatottjai kötelesek a védendő adatokat, technikai eszközöket zárható szekrényben, zárható iroda helyiségben elhelyezni, mely helyiségbe belépni, onnan védendő adatokat tartalmazó iratot, technikai eszköz kivenni csak az illetékes foglalkoztatott jóváhagyásával lehet, mely jóváhagyás megadására a meghatározott jogosultsági szintek alapján kerül sor.

(2) A Társaság ügyvezetése köteles összeállítani, és jóváhagyni és kezelni a Társaság irattárának, valamint az elektronikus információs rendszereknek helyt adó helyiségekbe belépésre jogosultak listáját, továbbá rendszeresen köteles felülvizsgálni a belépésre jogosult személyek listáját, és eltávolítani a belépésre jogosult személyek listájáról azokat, akik a belépésre már nem jogosultak, valamint intézkedni a beléptetési jogosultságot igazoló dokumentum visszavonása, érvénytelenítése, törlése, megsemmisítése iránt. iránt.

VI./5. Asztali munkaállomások

(1) A Társaság munkavállalói a munkavégzés, feladatteljesítés folyamán kizárólag úgy hagyhatják el azt a helyiséget, ahol az általuk folytatott munkavégzés zajlik, hogy a rájuk bízott adathordozókat elzárják, a számítógépeket jelszóval zárolják, vagy az adott helyiséget, illetőleg az egész irodahelyiséget bezárják.

(2) A Társaság irodahelyiségében az asztali munkaállomásokat olyan módon kell elhelyezni, hogy az azokon szereplő adatokra kizárólag az arra jogosultak láthassanak rá.

VII. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

(1) A Társaság adminisztratív védelmi intézkedésekkel, szervezési intézkedésekkel, szabályzatokkal, ellenőrzésekkel (audit), oktatással is köteles az informatikai biztonságot biztosítani.

(2) **Informatikai Biztonsági Szabályzat:** A Társaság elsődleges adminisztratív intézkedésként jelen Szabályzatot tette közzé, melynek betartása minden foglalkoztatott lényeges munkaköri kötelezettségének minősül. A Társaság jelen Szabályzatban megfogalmazta és dokumentálja, valamint a Társaság kommunikációs rendszerein keresztül kihirdeti és informatikai rendszerében hozzáférhetővé teszi az informatikai biztonsági rendelkezéseit. A jelen Szabályzatot az informatikában - valamint a Társaságnál - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. A jelen Szabályzat folyamatos naprakészen tartása az Informatikai Felelős feladata.

(3) **Oktatás:** A Társaság az informatikai rendszer felhasználóit rendszeresen, és szükség esetén alkalmi jelleggel is köteles információbiztonsági oktatásban részesíteni. Az oktatásban ki kell térni arra, hogy az elektronikus információs rendszereket csak olyan személyek használhatják, akik megfelelő számítástechnikai, informatikai, valamint szakmai ismeretekkel rendelkeznek az adott rendszer, szoftver alkalmazásához. Az oktatással gondoskodni kell arról, hogy a felhasználókban tudatosodjanak az alapvető információbiztonsági fogalmak, illetve ismerjék meg a munkájuk során felmerülő információbiztonsági fenyegetettségeket.

(4) **Biztonság tudatosság képzés:** A rendszerüzemeltetést végző személyek kötelesek gondoskodni arról, hogy új elektronikus információs rendszerek bevezetését szoftver bemutató, illetve részletes rendszer használat, tesztelés, dokumentáció megismerés előzze meg az érintett felhasználók tekintetében.

(5) **Informatikai biztonsági kockázatelemzés:** Az informatikai biztonsági kockázatelemzés célja azoknak az informatikai, fizikai és humán tényezőknek a feltárása, amelyek kockázatot hordoznak magukban, ezáltal veszélyeztetve a Társaság megfelelő működését, illetve, további célja, hogy számszerűsíthető módszerekkel megbecsülje a fenyegető tényezők bekövetkezési gyakoriságát és hatását, majd a kockázatok összehasonlítása érdekében számszerűsítse a releváns kockázatokat. A felmerült kockázatok kezelésére, a kockázatokkal arányos intézkedési terveket kell készíteni az Informatikai Felelős közreműködésével, melyek az alábbiakat kell, hogy tartalmazzák:

- a kockázatok csökkentésére tett javaslatokat a technikai eszközök megváltoztatására, vagy fejlesztésére (pl.: új védelmi eszközök alkalmazása, vagy a jelenlegi átkonfigurálása),

- a kockázatok csökkentésére tett javaslatokat az érvényben lévő szabályozás megváltoztatására,
- a kockázatok csökkentésére tett javaslatokat a személyi állományra vonatkozóan (pl.: motiváció, a fegyelmi eljárások szigorítása, oktatás, stb.),
- a kockázatok tudatos felvállalására irányuló javaslatot, ha a védelmi intézkedés költségvonzata nagyobb, vagy közel azonos, mint a fenyegetettség által elszenvedhető anyagi kár.

VIII. LOGIKAI VÉDELMI INTÉZKEDÉSEK

(1) A Társaság logikai védelmi intézkedésekkel is köteles az informatikai biztonságot biztosítani.

(2) **Szoftverhasználat korlátozásai:** A Társaságnál kizárólag olyan szoftvert és hozzátartozó dokumentációt lehet használni, amelyek megfelelnek a rájuk vonatkozó szerződésben foglalt elvárásoknak. A vezető tisztségviselő, illetőleg az Informatikai Felelős által engedélyezett, megfelelő licence-el rendelkező szoftvereket lehet használni, melyekről leltár készül. Szabad vagy nyílt forráskódú vagy ingyenes szoftverek használatbavételét az Informatikai Felelős engedélyezi. A felhasználók semmilyen alkalmazást nem telepíthetnek a munkaállomásaikra. A rendszerprogramok, illetve a felhasználói alkalmazások telepítését a munkaállomásokra csak a rendszerüzemeltetést ellátó személyek végezhetik el. A felhasználók semmilyen szoftvert nem telepíthetnek, sem fizikai adathordozón sem pedig letöltéssel az Informatikai Felelős jóváhagyása nélkül. Minden, a felhasználóhoz tartozó szoftvert az Informatikai Felelősnek jóvá kell hagynia, és csak akkor telepíthető, ha az adott telepítés nem jelent biztonsági kockázatot az elektronikus információs rendszerek számára, és ha a telepítés nem sért olyan licencszerződést, amely az adott szoftverre vonatkozik.

(3) **Ügymenet folytonosság tervezése:** A Társaság a folyamatos ügymenet biztosítása érdekében tervet készít az elektronikus rendszerek kiesése esetében az elvégzendő feladatokra. A folytonosság védelme érdekében a munkaköri leírásokban, belső szabályozásban, illetve megbízási szerződésekben rögzíteni kell az esetleges katasztrófa okozta helyzetek kezelési rendjét, és helyreállítási teendőit.

(4) A részletesebben szabályozott logikai védelmi intézkedések (adathordozók védelme, hozzáférés-felügyelet, rendszerüzemeltetés) külön fejezetekben kerültek szabályozásra.

IX. AZ EMBERI ERŐFORRÁSOK BIZTONSÁGA

IX./1. A foglalkoztatásra irányuló jogviszony kezdetekor fellépő kötelezettségek

(1) A foglalkoztatásra irányuló jogviszonyban álló foglalkoztatottak a jelen Szabályzat **2. számú Mellékle**tét képező megismerési nyilatkozat aláírásával elismerik, hogy a jelen Szabályzatban meghatározott biztonsági elvárásoknak, előírásoknak eleget tesznek. A nyilatkozat mindenkor aktuális verziójának a felhasználóval történő aláíratása és adminisztrálása a foglalkoztatott közvetlen felettesének a feladata és felelőssége.

(2) A jogviszonyt létesítő foglalkoztatott munkavégzéséhez szükséges infokommunikációs eszközöket és jogosultságokat a foglalkoztatott közvetlen felettese igényli meg a Társaság Informatikai Felelősétől.

(3) Az új belépő foglalkoztatottak számára a jelen Szabályzatban foglalt előírások tudatosítása az Informatikai Felelős felelőssége. Az informatikai biztonsági oktatás tartalmának és felépítésének összhangban kell lennie az új belépő foglalkoztatott által betöltendő munkakörrel, illetve feladatkörrel.

(4) A naprakész informatikai biztonsági oktatási anyagok elkészítése az Informatikai Felelős felelőssége.

IX./2. A foglalkoztatásra irányuló jogviszony fennállása során fellépő kötelezettségek

(1) Az Informatikai Felelős indokolt esetben, de legalább évente egyszer ismételt oktatásról gondoskodik a biztonságtudatosság növelése érdekében, mely során az informatikai biztonságot érintő legfontosabb változásokról részletes tájékoztatást ad a felhasználóknak. Az oktatás tartalmának és felépítésének összhangban kell lennie a foglalkoztatott által betöltött munkakörrel.

(2) Az oktatáson való részvétel minden felhasználó számára kötelező, aki a munkavégzése során informatikai rendszert használ. A részvétel dokumentálása, illetve a megfelelő dokumentálási keretek biztosítása az Informatikai Felelős feladata.

(3) A felhasználóknak a jelen Szabályzatot érintő változásokról, valamint a legfontosabb informatikai biztonsági eseményekről és trendekről az oktatások mellett alkalmi jelleggel kiegészítő tájékoztatást kell nyújtani, mely tájékoztatás az Informatikai Felelős (IT Rendszergazda) feladata és felelőssége.

IX./3. A felhasználók részletes kötelezettségei, felelőssége

(1) **Megismerési és felelősségvállalási nyilatkozat**: A Társasággal foglalkoztatásra irányuló jogviszonyban álló személyeken kívüli, harmadik személynek minősülő felhasználók a bármely jogviszony alapján keletkező, a Társaság informatikai rendszerének bármely elemére vonatkozó használati jogosultságuk esetén a jogviszony kezdetekor a jelen Szabályzat **3. számú Mellékle**tét képező megismerési és felelősségvállalási nyilatkozat aláírásával elismerik, hogy a jelen Szabályzatban meghatározott biztonsági elvárásoknak, előírásoknak eleget tesznek. Azokban az esetekben, amikor a Társaság elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem a Társaság foglalkoztatottja, az információbiztonsági elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás, megkötése során kell, mint kötelezettséget érvényesíteni. A Társaság által rendszeresített nyilatkozat célja a külső felhasználókban is tudatosítani, hogy a lehető legnagyobb gondossággal járjanak el a Társaság által használt elektronikus információs rendszerekben tárolt adatok használatakor, annak érdekében, hogy az adatok bizalmassága, sértetlensége, és rendelkezésre állása a külső felhasználó szándékos, vagy gondatlan magatartásából ne sérüljön, illetve a felelősségük számon kérhető legyen.

(2) **Biztonsági esemény jelentési kötelezettség:** A Társaság által üzemeltetett, vagy alkalmazott információs rendszerrel, a rendszer üzemeltetésével vagy a rendszer elhelyezésére szolgáló helyiséggel kapcsolatban álló felhasználóknak kötelessége jelenteni minden olyan nem kívánt vagy nem várt egyedi vagy sorozatos informatikai biztonsági eseményeket, amelyek nagy valószínűséggel veszélyeztetik a Társaság tevékenységét és fenyegetik az informatikai biztonságot. A bejelentést az Informatikai Felelős, és a Társaság ügyvezetője felé kell megtenni.

(3) **Az elektronikus levelezésre és az internetes böngészésre vonatkozó szabályok:** A Társaság által biztosított levelezőrendszer a munkavégzéssel kapcsolatos ügyintézést szolgálja. A céges levelező kliens beállításait tilos módosítani vagy privát e-mail fiókokat hozzáadni. Ismeretlen helyről származó, gyanús e-mail megnyitásakor a felhasználó köteles mérlegelni, hogy a levél vagy csatolmánya vírust tartalmazhat, és köteles az észlelt kockázatot jelezni az Informatikai Felelős irányába. A céges e-mail címet magáncélra – pl. online regisztrációhoz, hírlevél feliratkozáshoz, fórum feliratkozáshoz – tilos használni. A levelezés során nevesített postafiókokat kizárólag a hozzárendelt felhasználó használhatja, más foglalkoztatott postafiókjának használata tilos. Nem megengedettek továbbá az alábbiakban bemutatásra kerülő viselkedési formák. A Felhasználó nem jogosult a belső informatikai rendszerén kívüli helyszínen/helyszínről, nyilvános eszközről vagy nyilvános csatornán elérni vagy megpróbálni elérni a belső informatikai szolgáltatást, kizárólag a Munkáltató igényei szerint megfelelően védett eszközről, védett csatornán. Kifejezetten tilos az alábbi jellegű alkalmazások használata:

- online rádióhallgatás (kivéve munkavégzés céljából)
- fájlcsere szoftverek használata
- csevegő (chat) -software-ek használata (kivéve Skype, Viber, WhatsApp munkavégzés céljából)
- közösségi oldalak használata (kivéve munkavégzés céljából)
- videómegosztó oldalak használata (kivéve munkavégzés céljából)

(4) **Közösségi média használata:** A közösségi médiákon való kommunikáció a Társaság 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 Társaság jó hírnevét, gazdasági érdekeit veszélyezteti. A közösségi média felületei tilos mások zaklatása, rágalmazása, megfenyegetése. Tilos a közösségi média felületein bárminemű, a Társaság által üzleti titoknak minősített, a Társaság belső működésére, belső folyamataival kapcsolatos, a Társaság munkavállalóival kapcsolatos információk közlése, megosztása. Tilos a Társaság székhelyén, irodáiban készült fénykép, hang-és videófelvétel megosztása.

(5) **A jelszókezelés általános szabályai:** A felhasználó a számítógépre csak saját nevében és jelszavával léphet be, és az alkalmazásokat csak saját nevében használhatja. A jelszavak nem hozhatók nyilvánosságra és nem oszthatók meg senkivel. A jelszavak bizalmasságának megőrzéséért a felhasználó személyesen felel. Ha a felhasználónak a legkisebb gyanúja is felmerül, a jelszó biztonságának integritása felől, azt köteles azonnal megváltoztatni és gyanújáról az Informatikai Felelőst értesíteni. Más felhasználó azonosítóját átmeneti jelleggel sem szabad használni. A felhasználó köteles a jelszavát az előírt gyakorisággal és módon megváltoztatni. A felhasználónak az alapértelmezett jelszavakat az első belépés után kötelessége azonnal megváltoztatni. A felhasználó azonosítójával és jelszavával az informatikai rendszerben végrehajtott műveletekért személyesen felel. Vészhelyzet esetére (indokolt és szükséges, hogy a távollévő munkavállaló anyagaihoz hozzáférjen egy másik munkavállaló) lezárt borítékban, a páncélszekrényben kell tárolni a felhasználónevet, jelszót minden felhasználóra vonatkozóan. Indokolt esetben a lezárt boríték felnyitható vezető tisztségviselői engedéllyel, valamint az Informatikáért Felelőst és az Adatvédelmi Felelőst erről tájékoztatni kell.

(6) **Mobil és nem mobil eszközök, adathordozók használata:** A nem mobil informatikai eszközök áthelyezése a felhasználó által nem végezhető. A felhasználó felelős a személyes használatra kiadott eszközök rendeltetésszerű használatáért és őrzéséért, továbbá a rábízott informatikai berendezések állapotának, állagának megőrzéséért. Az

informatikai eszközöket a munka befejeztével, illetve a munkaidő végeztével a felhasználónak áramtalanítania kell, amennyiben azok folyamatos üzemben tartása nem indokolt. A saját használatra átvett számítógép rendszerszintű beállításainak módosítása (ebbe nem értendők bele az irodai programok felhasználói beállításai), a felhasználó számára nem engedélyezett. Az informatikai hálózat fizikai megbontása, a számítástechnikai eszközök lecsatlakoztatása (kivételt képeznek a hordozható eszközök), illetve bármilyen számítástechnikai eszköz hálózatra történő fizikai csatlakoztatása és/vagy beszerelése tilos. Az informatikai rendszerekben csak azokat a feladatokat szabad elvégezni, amelyek a felhasználó vagy üzemeltető munkájának ellátásához szükségesek, függetlenül attól, hogy az informatikai rendszer esetleg ennél szélesebb körű tevékenységet enged meg. A Társaság által rendszeresített biztonsági funkciókat (például automatikus képernyővédő-aktiválás) kikapcsolni, megkerülni tilos. A mobil eszközt tilos autóban hagyni, nyilvános helyen lopás lehetőségének kitenni: például, de nem kizárólag asztal mellé letett táskában tárolni, bármilyen külső zsebben tárolni, lezáratlan belső zsebben tárolni. A mobil eszközt tilos idegen informatikai hálózatban használni, kivételt ez alól az alábbi esetek képeznek: ha erre az Informatikai Felelőssel való előzetes egyeztetést követően a vezető tisztségviselő írásban engedélyt ad, illetve amennyiben a foglalkoztatott az otthoni WIFI hálózatát használja, amely WPA vagy WPA2 típusú titkosítással rendelkezik. Tilos az informatikai eszközök közelében enni vagy inni, illetőleg élelmiszert kicsomagolt, italt kibontott állapotban tartani.

(7) **Vírusvédelem:** Amennyiben a munkaállomás indítását követően a felhasználó az tapasztalja, hogy a vírusvédelmi program nem indult el (pl. ikonja nem látható), vagy ki van kapcsolva, akkor a munkavégzés megkezdése nem engedélyezett, az esetleges vírusfertőzésért a felhasználó felel. Ilyen esetben a munkaállomást le kell állítani, és értesíteni kell az Informatikai Felelőst. Amennyiben a felhasználó a vírusvédelmi rendszer által generált riasztás kap, azt haladéktalanul jelentenie kell az Informatikai Felelős felé. A Társaság belső hálózatához nem (vagy régen) csatlakoztatott számítógépen (pl. notebook) a vírusvédelmi rendszer frissítése a felhasználó feladata és felelőssége.

(8) **Szoftverhasználati szabályok:** Kizárólag olyan szoftvereket és dokumentációkat szabad használni, amelyek megfelelnek a vonatkozó szerződésben rögzített szerzői jogi vagy más jogszabályi elvárásoknak. A számítógépeken csak és kizárólag az informatikai feladatok ellátásért, üzemeltetésért felelős szervezeti egység, valamint az erre jogosult külső felek munkatársai telepíthetnek, módosíthatnak, vagy távolíthatnak el bármilyen fajta szoftvert. A Felhasználó nem jogosult önállóan, az Informatikai Felelőssel való egyeztetés és jóváhagyás nélkül szoftvereket telepíteni, sem a saját, sem más, a Társaság birtokában álló számítógépre. A Felhasználó nem jogosult a Társaság birtokában álló szoftvereket magáncélra lemásolni, sem más gépre telepíteni. A Felhasználó nem jogosult önállóan, az Informatikai Felelőssel való egyeztetés és jóváhagyás nélkül szoftvert átállítani, törölni, – ez kiemelten fontos a számítógép biztonságát biztosító szoftverekkel kapcsolatosan, mint például, de nem kizárólag: vírusvédelem, tűzfal, proxy, operációs rendszer biztonsági beállításai. Ez alól kivétel képeznek a személyes munkakörnyezet beállítása (pl. háttérkép stb.), illetve az olyan változtatások, amelyek a felhasználói alkalmazásokon történnek, tipikusan a nyomtatóválasztás, helyesírás ellenőrző nyelvválasztás, egyéb irodai alkalmazások testre szabása.

(9) **Mentés:** A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó felhasználók feladata. A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban a rendszerüzemeltetést végző személyek segítséget nyújtanak. A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért az Informatikai Felelős a felelős.

(10) **Informatikai incidens:** A felhasználó semmilyen körülmények között sem próbálhatja meg maga megoldani az esetleges informatikai incidenseket anélkül, hogy először konzultálna az Informatikai Felelőssel. A felhasználók csak az Informatikai Felelős utasításával és kifejezett engedélyével kísérelhetik megoldani az informatikai incidenseket.

(11) **Egyéb informatikai aktivitás** Kifejezetten tilos olyan tevékenységet folytatni, amelynek célja más felhasználók adatainak jogosulatlan megszerzése, megváltoztatása, letörlése. A felhasználónak tilos más felhasználó nevében tevékenykedni és a felhasználó nem teheti lehetővé mások számára, hogy a nevében tevékenykedjenek. Kifejezetten tilos más felhasználó munkavégzését korlátozó tevékenységet végezni, amennyiben az nem a munkavégzést szolgálja. Munkavégzést korlátozó tevékenység például, de nem kizárólag a sávszélesség foglalása, online zenehallgatás és video megtekintés; nem munka célú levelezés esetén a nagy méretű levelek küldése, fogadása (jellemzően: nagy mellékletek, képek, ppt-k, videók stb.); fájl letöltések, feltöltések (zenék, filmek, játékok stb.). Tilos a rendszer bármely elemének eredeti felhasználási céljától eltérő használata vagy az erre irányuló próbálkozás. A Felhasználónak tilos a hálózati forgalom figyelése, erre alkalmas szoftver telepítése, illetve igénybevétele. Tilos az Informatikai Felelőstől kapott IP címtől eltérő más IP cím használata. Szigorúan tilos olyan anyag továbbítása, letöltése vagy közzététele az interneten, amely a magyar vagy nemzetközi jogszabályokat sérti.

(12) A fenti szabályok rendszeres és szúrópróbaszerű ellenőrzése az Informatikai Felelősnek a feladata és felelőssége.

X. A FELHASZNÁLÓI JOGOSULTSÁG VÁLTOZÁSÁNAK ESETEI

X./1. Munkavégzés tartós szünetelése

(1) A munkavégzés várhatóan egy hónapnál hosszabb tartamú szünetelése – pl. GYES, GYED, hosszantartó betegség stb. – esetén a felhasználó jogosultságait a távollét időszakára fel kell függeszteni, a felfüggesztés kezdeményezése az Informatikai Felelősnél a foglalkoztatott közvetlen felettesének a felelőssége.

X./2. Felülvizsgálat

(1) A korábban kiosztott jogosultságokat legalább félévente felül kell vizsgálni, szükség esetén gondoskodni kell azok módosításáról vagy visszavonásáról, mely a foglalkoztatott közvetlen felettesének a felelőssége.

(2) A kilépő foglalkoztatott közvetlen felettese gondoskodik a jogosultság visszavonásáról, másik feladatkörbe történő áthelyezés esetén pedig az új közvetlen felettes igényli az új jogosultságok megadását az Informatikai Felelőstől.

X./3. Hozzáférési jogosultságok visszavonása

(1) Az összes munkaviszonyban vagy foglalkoztatásra irányuló egyéb jogviszonyban álló természetes személynek az információkhoz és információ feldolgozó eszközökhöz való hozzáférési jogosultságát fel kell függeszteni, amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár. Ha az érintett részéről alaposan feltételezhetően fennállhat az ügymenetet vagy elektronikus információbiztonságot sértő magatartás veszélye, a jogosultságokat még az érintett tájékoztatását megelőzően vissza kell vonni.

(2) A jogosultságok visszavonását az érintett felhasználó közvetlen felettese kezdeményezi, a végrehajtása az adott rendszer üzemeltetésért felelős foglalkoztatott, vagy annak hiányában az Informatikai Felelős feladata.

XI. ADATHORDOZÓK VÉDELME

XI./1. Adathordozók és mobil eszközök igénylése, kiadása és visszavétele, valamint nyilvántartása

(1) A munkavégzéshez adathordozót és mobil eszközt a felhasználók számára az adott foglalkoztatott közvetlen felettese igényelhet. Az igénylés teljesítéséhez az Informatikai Felelős jóváhagyása szükséges, és az adathordozó igénylése kizárólag indokolt esetben hagyható jóvá.

(2) Minden egyes kiadott adathordozóról és mobil eszközről nyilvántartást kell vezetni, továbbá az eszközök visszavétele esetén ennek tényét a kapcsolódó nyilvántartásban rögzíteni kell. A **4. számú Melléklet**ben rögzített nyilvántartások vezetése az Informatikai Felelős, vagy az általa kijelölt munkavállaló felelőssége.

XI./2. Adathordozók használata

(3) A Társaságnál kizárólag a Társaság tulajdonába tartozó adathordozók használata engedélyezett, saját tulajdonú adathordozók használata és a számítógépekhez vagy egyéb eszközökhöz való csatlakoztatása szigorúan tilos.

(4) Az adathordozók használatának feltétele az Informatikai Felelős által biztosított vírusvédelmi eszközzel való folyamatos ellenőrzés.

(5) Az adathordozók kizárólag munkavégzés céljából használhatóak, a Társaság tevékenységének végzéséhez. A felhasználók munkájához nem kapcsolódó adatok tárolása, illetve az adathordozók magáncélú felhasználása nem engedélyezett.

(6) A Társaság helyiségein kívül történő eszközhasználat esetén az adathordozókon tárolt adatokat, dokumentumokat a lehető leghamarabb fel kell másolni a megfelelő hálózati meghajtóra, ezután az adathordozóról pedig törölni kell azokat.

(7) Az ismeretlen (nem egyértelműen beazonosítható) tulajdonosú adathordozók használata tilos. Ilyen esetben a talált adathordozót nem szabad a számítógépekhez csatlakoztatni vagy mások számára továbbadni. Az Informatikai Felelős felé haladéktalanul jelenteni kell a megtalálás tényét és át kell adni számára a megtalált adathordozót.

(8) Az Informatikai Felelős a talált adathordozót és a Társaság birtokába kerülésének módját a egyedileg megvizsgálja, majd a vizsgálat lezárását követően az incidensről jelentést készít.

XI./3. Adathordozók tárolása

(1) A nem beépített adathordozókat a napi munkavégzés befejezését követően - amennyiben lehetséges - le kell választani a számítógépekről és elzárva kell tartani (páncélszekrényben, széfben, zárt szekrényben vagy fiókban stb.), erről az adathordozó használójának kell gondoskodnia.

(2) Ügyelni kell arra, hogy ilyen adathordozó semmi esetre se maradjon szem előtt (például asztalon hagyva).

(3) A tárolás során a gyártói előírásokat be kell tartani, és a gyártó által előírt megfelelő környezeti paramétereket biztosítani kell.

XII. HOZZÁFÉRÉS-FELÜGYELET

XII./1. Azonosítás

(1) A Társaság által alkalmazott elektronikus információs rendszereknek minden belső és külső felhasználót egyedileg azonosítaniuk kell, annak érdekében, hogy:
- minden, egy adott időpontban végzett tevékenység összerendelhető legyen egy természetes személlyel;
- az összerendelés egyértelmű, megváltoztathatatlan, később is visszakereshető legyen.

(2) A beépített fiókokat (Guest, Admin, stb.) is vagy nevesíteni kell – átnevezéssel -, vagy le kell tiltani.

(3) A korábban már felhasznált azonosítókat a megszüntetésüktől számított 12 hónapig nem engedélyezett ismételten kiadni, vagy egyéb módon használatba venni.

XII./2. Hitelesítés

(1) A Társaság tulajdonában vagy használatában lévő, összes elektronikus információs rendszer esetében az azonosítást legalább egy hitelesítő mechanizmussal is ki kell egészíteni. A hitelesítés mechanizmus általános módszere a felhasználói azonosítóhoz tartozó jelszó alkalmazása.

(2) A jelszavakkal kapcsolatos minimális elvárások - melyeknél csak szigorúbbakat szabad alkalmazni - minden rendszer esetében:
- a jelszavak hossza legalább 14 karakter kell, hogy legyen;
- a jelszó sem részben, sem egészében nem tartalmazhatja a fiókazonosítót;
- a jelszónak kisbetűt, nagybetűt és számjegyet is tartalmaznia kell:
- a jelszavakat legalább 180 naponként meg kell változtatni;
- az új jelszónak legalább egy karakterében különböznie kell a legutóbb használt 10 jelszó bármelyikétől;

(3) A kezdeti jelszót az első belépéskor meg kell változtatni, továbbá a jelszavak bizalmasságát minden felhasználónak meg kell őriznie, azokat más személy tudomására hozni szigorúan tilos.

(4) A jelszavakat azok kompromitálódása – vagy annak gyanúja – esetén haladéktalanul meg kell változtatni, vagy a hozzájuk kapcsolódó fiókot le kell tiltatni.

XII./3. Engedélyezés

(1) A felhasználók csak a számukra kijelölt feladatok végrehajtásához szükséges és elégséges jogosultságokat kaphatják meg az információkhoz és a rendszer erőforrásaihoz való logikai hozzáférés során.

(2) A nem indokolt, felesleges jogosultságok megszüntetésének érdekében a hozzáférési jogosultságokat rendszeresen felül kell vizsgálni, és az indokolatlan - a legkisebb jogosultság elvével nem megegyező - hozzáféréseket vissza kell vonni. A rendszeres felülvizsgálat végrehajtása a közvetlen felettesek felelőssége.

XII./4. Felügyelet

(1) Legfeljebb öt sikertelen bejelentkezési kísérletet követően az elektronikus információs rendszernek automatikusan zárolnia kell a fiókot – legyen az felhasználói vagy privilegizált, hagyományos vagy technikai – legalább egy óra időtartamra. A zárolást az Informatikai Felelős, vagy az általa kijelölt személy oldhatja fel.

(2) Egymás utáni többszöri zárolásról automatikusan értesíteni kell az Informatikai Felelőst.

(3) Azokat a fiókokat, melyekbe 180 napja nem jelentkeztek be sikeresen, felül kell vizsgálni és szükség szerint gondoskodni azok letiltásáról és deaktiválásáról. A szabály alól kivételt képeznek a munkaállomások operációs

rendszerének lokális technikai – például adminisztrátori – fiókjai, melyek jellegüknél fogva inaktív – használaton kívüli – állapotban vannak.

XIII. RENDSZERÜZEMELTETÉS

XIII./1. Karbantartás

(1) Az elektronikus információs rendszerek és rendszerelemek megfelelő működése érdekében rendszeres karbantartásokat kell végezni.

(2) Az informatikai eszközök tekintetében a karbantartások feltételrendszerének kialakításáért és a karbantartási, javítási tevékenységek szükség szerinti ütemezésű végrehajtásáért az Informatikai Felelős a felelős.

(3) A fizikai védelmet biztosító eszközök, berendezések tekintetében (ideértve a tűzoltó- vagy klímaberendezéseket is) a karbantartások feltételrendszerének kialakításáért és a karbantartási, javítási tevékenységek végrehajtásáért a vezető tisztségviselő felelős, mely kötelezettségének a fizikai védelemért felelős személy kijelölésével tesz eleget.

(4) A Társaságnál a karbantartások és javítások során legalább a következőket kell teljesíteni:
- karbantartásokat előre meg kell tervezni, amely az informatikai eszközök tekintetében az Informatikai Felelős feladata. A karbantartási munkálatok idejét az érintett szervezeti egység vezetőjével egyeztetni kell, és ez alapján előzetesen tájékoztatni kell az érintett felhasználókat. A felhasználók időben történő értesítése az Informatikai Felelős felelőssége.
- A fizikai védelmet biztosító eszközök, berendezések esetében a vezető tisztségviselő által kijelölt, fizikai védelemért felelős személy felelőssége az eszközök és berendezések karbantartási tervének elkészítése, és a végrehajtás irányítása.
- A karbantartásokat és javításokat a szállító vagy a gyártó által előírt módon, és ütemezés szerint kell végrehajtani, és dokumentálni kell.
- Amennyiben egy elektronikus információs rendszer vagy annak egy vagy több elemének karbantartása vagy javítása azt igényli, hogy az adott elektronikus információs rendszer vagy annak egy vagy több eleme kiszállításra kerüljön a Társaságtól, akkor azt az Informatikai Felelőssel való konzultációt követően, a vezető tisztségviselőnek jóvá kell hagynia, vezető tisztségviselői jóváhagyás hiányában semmilyen eszköz és berendezés karbantartás vagy javítás céljából történő kiszállítása a Társaság területéről nem engedélyezett. A jóváhagyás előtt ellenőrizni kell, hogy az eszköz tartalmaz-e adathordozót.
- Karbantartási, javítási vagy cserélési célból bármilyen informatikai eszközt kivinni a Társaság területéről kizárólag az eszköz által esetlegesen tartalmazott adathordozók kivételével (amennyiben ez lehetséges) vagy mentést követően, az adathordozón lévő adatok visszaállíthatatlan törlése után engedélyezett.
- A kiszállítást megelőző vizsgálatok és tevékenységek végrehajtásáért, és azok dokumentálásáért az Informatikai Felelős a felelős.

XIII./2. Vírusvédelem

(1) A Társaság által használ informatikai infrastruktúra egészére kiterjedő, folyamatos vírusvédelem és rendszeres vírusellenőrzés biztosítása érdekében automatikus frissítésű, központilag menedzselhető vírusvédelmi rendszert kell kiépíteni.

(2) Vírusellenőrző alkalmazásokat kell telepíteni mind a munkaállomásokra, mind pedig a szerverekre és informatikai határvédelmi eszközökre.

(3) A vírusvédelmi rendszer kialakításáért az Informatikai Felelős a felelős.

(4) A vírusvédelmi feladatok elvégzéséhez olyan vírusvédelmi programokkal kell rendelkeznie a Társaságnak, amelyek segítségével az előforduló összes platform ellenőrizhető, és ezeknek a programoknak a vírusmeghatározásra szolgáló állományait rendszeresen frissíteni kell.

(5) A Társaság számítógépein legalább hetente egyszer teljes körű vírusellenőrzést kell végezni előre ütemezett módon, automatikusan.

(6) A külső forrásból származó cserélhető adathordozókat használatba vétel előtt automatikus kártékony kód ellenőrzés alá kell vetni.

(7) Megfelelő vírusvédelem nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép és mobil eszköz nem üzemeltethető.

(8) A jogosultságokat úgy kell kialakítani, hogy a felhasználók ne állíthassák le az eszközükön futó vírusvédelmi szoftvert, és nem változtathassák meg annak beállításait.

XIII./3. Mentés

(1) A rendszer legfontosabb elemeinek egyértelmű és visszakereshető azonosítása, illetve az egyes informatikai rendszereket érintő rendkívüli helyzetek megszüntetésének megvalósítása érdekében mentéseket, archiválásokat kell végezni olyan módon, hogy azokból szükség esetén az elektronikus információs rendszer, illetve az abban lévő adatok visszaállíthatók legyenek.

(2) A mentés, archiválás és visszatöltés tervezésének és üzemeltetésének kialakításáért az Informatikai Felelős a felelős.

(3) Biztonsági mentéseknek kell készülniük az alábbiakról:
- az online elérhető adatbázisokról és fájlrendszer könyvtárakról;
- az offline elérhető (archivált) adatbázisokról és fájlrendszer könyvtárakról;
- a szoftverek telepítőkészletéről.

XIII./4. Naplózás

(1) Az elektronikus információs rendszerekben kezelt adatokhoz való hozzáférések nyomon követhetősége, a rendszerek jogosulatlan használatának és a bekövetkezett problémák azonosítása érdekében az eseményeket naplózni kell.

(2) A naplózási környezet feltételrendszerének kialakításáért az Informatikai Felelős a felelős.

(3) A Társaságnál olyan elektronikus naplózási rendszert kell kialakítani, hogy utólag minden esetben meg lehessen határozni, hogy melyik felhasználó, mikor, honnan, milyen bizalmas adathoz, milyen célból (olvasás / létrehozás / módosítás / törlés) fért hozzá.

(4) Elektronikus naplóknál megfelelő jogosultsági beállításokkal kell biztosítani, hogy azokhoz csak a naplózási feladatokkal, illetve a napló adatok ellenőrzésével, vizsgálatával megbízott, arra jogosult személyek férhessenek hozzá.

XIII./5. Az adatátvitel bizalmassága és sértetlensége

(1) A Társaság által használt elektronikus információs rendszernek védenie kell a továbbított információk bizalmasságát és sértetlenségét, ezért olyan adatátviteli rendszert kell a Társaságnak alkalmaznia, amely képes biztosítani az adatátvitel bizalmasságát és sértetlenségét, és ennek érdekében megfelelő védelmi mechanizmust kell kialakítani az adatátvitel során.

(2) Az adatátvitel bizalmasságának, sértetlenségének kialakításáért az Informatikai Felelős a felelős.

(3) A Társaságnak biztosítania kell, hogy a titkosított adathoz csak az arra jogosult – utólag is ellenőrizhető módon – férhessen hozzá. Ennek érdekében az elektronikusan tárolt információt át kell alakítani úgy, hogy az ahhoz hozzáférő személyek meghatározott kulcs, illetve kód ismerete nélkül ne tudják az adatot megfejteni, és ne tudják kinyerni annak információ tartalmát. A módszernek meg kell valósítania, hogy harmadik személy az adatátviteli vagy adattároló eszközhöz való hozzáférése esetén ne jusson hozzá az információhoz.

XIV. ZÁRÓ RENDELKEZÉSEK

XIV./1. A Szabályzat módosítása

(1) A Szabályzat megállapítására és módosítására a Társaság mindenkori vezető tisztségviselője jogosult.

XIV./2. A Szabályzat megismertetése

(1) Jelen Szabályzat rendelkezéseit meg kell ismertetni a Társaság valamennyi munkavállalójával (foglalkoztatottjával), felhasználóval és a munkavégzésre irányuló szerződésekben elő kell írni, hogy betartása és érvényesítése minden munkavállaló (foglalkoztatott) lényeges munkaköri kötelezettsége.

XIV./3. A Szabályzat másolása, felhasználása

(1) Jelen Szabályzat szerzői jogi műnek minősül, tilos a Szabályzat egészének vagy részének, részletének máso lása, többszörözése, újra nyilvánossághoz történő közvetítése, a mű mindenfajta eltorzítása, megcsonkítása, egészben vagy részben történő használata, felhasználása, feldolgozása, értékesítése a szerző írásos hozzájárulása

nélkül. Szabályzat szerzője a Társaság megbízott jogi képviselője, akinek személyéről a Társaság erre irányuló kérésre tájékoztatást nyújt.

(2) Szerzői jogi jogsértés esetén a Társaság közjegyzői ténytanúsítást alkalmaz, melynek összegét a jogsértő felhasználóra hárítja.

XV. MELLÉKLETEK

1. számú melléklet	Informatikai Felelős kijelölése - sablon
2. számú melléklet	Munkaszerződésbe, vagy foglalkoztatásra irányuló egyéb szerződésbe foglalandó kikötés az Informatikai Biztonsági Szabályzat megismeréséről, alkalmazásáról
3. számú melléklet	Megismerési és felelősségvállalási nyilatkozat külső személyek részére - sablon
4. számú melléklet	Adathordozók és mobil eszközök nyilvántartása

1. <u>számú melléklet – Informatikai Felelős kijelölése</u>

INFORMATIKAI FELELŐS KIJELÖLÉSE

Alulírott, _____, mint a **Magyarság Háza Nonprofit Kft.** (székhely: 1051 Budapest, Zrínyi utca 5.) vezető tisztségviselője, egyben a munkáltatói jogkör gyakorlója, az alábbi személyt jelölöm ki az Informatikai Biztonsági Szabályzatban meghatározott Informatikai Felelősi feladatok ellátására:

Informatikai Felelős:

név:	_____
munkakör /belső munkavállaló esetén/:	_____
tevékenység megkezdésének időpontja:	_____
mobil telefonszám:	_____
e-mail cím:	_____

Kelt: Budapest, 2021. év _____ hó __. nap

_____

Magyarság Háza Nonprofit Kft.
képv.: Csibi Krisztina, ügyvezető, önállóan

<u>Tudomásulvételi záradék:</u>

Alulírott, tudomásul veszem, hogy köteles vagyok a vonatkozó Informatikai Biztonsági Szabályzat betartásával ellátni az Informatikai Felelős feladatokat.

Kelt Budapest, 2021. év _____ hó __. nap

_____

_____

2. számú melléklet - Munkaszerződésbe, vagy foglalkoztatásra irányuló egyéb szerződésbe foglalandó kikötés az Informatikai Biztonsági Szabályzat megismeréséről, alkalmazásáról

Munkáltató:

Név:	**Magyarság Háza Nonprofit Korlátolt Felelősségű Társaság**
Rövidített név:	**Magyarság Háza Nonprofit Kft.**
Székhely:	**1051 Budapest, Zrínyi utca 5.**
Cégjegyzékszám:	**Cg.01-09-335243**
Vezetve:	**a Fővárosi Törvényszék Cégbírósága nyilvántartásában**
Adószám:	**26615374-2-41.**
Statisztikai számjel:	**26615374-9499-572-01.**
Honlap:	**http://www.magyarsaghaza.net**
Telefonszám:	**0036 (1) 795 6606**
E-mail cím:	**info@magyarsaghaza.net**
Képviseli:	**Csibi Krisztina ügyvezető, önállóan**
továbbiakban:	**Adatkezelő / Munkáltató / Üzemeltető / Társaság**

Informatikai Felelős és elérhetősége:

Név:	
Telefonszám:	
E-mail cím:	

Munkavállaló:

név:	
lakcím:	
anyja neve:	
továbbiakban:	Munkavállaló

1. A Munkavállaló kijelenti, hogy a Munkáltató az Informatikai Biztonsági Szabályzatát a rendelkezésére bocsátotta és annak tartalmát megismerte, és tudomásul vette, hogy az abban foglaltak betartása lényeges munkaköri kötelezettségének minősül.
2. A Munkavállaló köteles a Munkáltató Informatikai Biztonsági Szabályzatát jelen Szerződés aláírását követő 5 (öt) munkanapon belül részletesen áttanulmányozni, és az esetleges kérdéseivel a Munkáltató Informatikai Felelőséhez fordulni. A Munkavállaló a Munkáltató által biztosított elektronikus információs rendszerek használata során köteles alkalmazni és érvényesíteni az Informatikai Biztonsági Szabályzat rendelkezéseit.
3. A Munkavállaló kötelezettséget vállal arra, hogy:
   a) munkavégzése során maradéktalanul betartja és betartatja az Informatikai Biztonsági Szabályzat rendelkezéseit,
   b) a rendelkezésére bocsátott elektronikus információs rendszereket az előre meghatározott célon kívül más célra nem használja, és nem használtatja fel, valamint a tudomására jutott adatokat nem hozza nyilvánosságra,
   c) a Munkáltatónál rendszeresített biztonsági előírások betartásával és betartatásával megakadályozza az információkhoz való jogosulatlan hozzáférést,
   d) amennyiben az Informatikai Biztonsági Szabályzatban foglaltak megsértését észleli, azt haladéktalanul jelenti a Munkáltatónak, valamint,
   e) biztonsági esemény, incidens esetében az Informatikai Biztonsági Szabályzatban foglaltak szerint jár el.
4. A Munkavállaló tudomásul veszi, hogy a munkaviszonnyal összefüggő magatartása körében ellenőrizhető, a Munkáltató – különösen, de nem kizárólagosan - jogosult a Munkavállaló által munkavégzésre használt számítógépek, telefonok és egyéb eszközök, programok és alkalmazások által naplózott valamennyi - nem magánjellegű - adat megismerésére, azzal, hogy a Munkáltató a magánjellegű használatot kifejezetten megtiltja.

3. számú melléklet – Megismerési és felelősségvállalási nyilatkozat – sablon

FELHASZNÁLÓI FELELŐSSÉGVÁLLALÁSI NYILATKOZAT

Alulírott, _____, mint a _____ (székhely: _____; cégjegyzékszám/nyilvántartási szám: _____) vezető tisztségviselője, mint a **Magyarság Háza Nonprofit Kft.** (székhely: 1051 Budapest, Zrínyi utca 5.) szerződéses partnere, kijelentem, hogy az Informatikai Biztonsági Szabályzatban foglaltakat megismertem, a rám, illetőleg az általam képviselt Társaságra vonatkozó szabályokat megértettem és azokat magamra nézve kötelező érvényűnek elismerem.

Kelt: Budapest, 2021. év _____ hó __. nap

_____

képv.: _____

Nyilatkozattevő

4. Adathordozók és mobil eszközök nyilvántartása

ADATHORDOZÓK NYILVÁNTARTÁSA

Adathordozó nyilvántartási sorszáma	2021/_
Adathordozó egyedi azonosítója	
Adathordozó típusa	
Adathordozó titkosított	igen/nem
Kiadás időpontja	
Átvevő felhasználó neve	
Átvevő jogállása	belső munkavállaló / külső fél
Használatból kivonás indoka	
Visszavétel időpontja	
Átvevő neve	

MOBIL ESZKÖZÖK NYILVÁNTARTÁSA

Mobil eszköz nyilvántartási sorszáma	2021/_
Mobil eszköz egyedi azonosítója	
Mobil eszköz típusa	
Kiadás időpontja	
Átvevő felhasználó neve	
Használatból kivonás indoka	
Visszavétel időpontja	
Átvevő neve	