Örkény István Színház Nonprofit Kft.

ADATVÉDELMI ÉS INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Képviseletre jogosult személy neve: **Mácsai Pál** ügyvezető igazgató

Jelen szabályzatban nem szabályozott kérdésekben az információs önrendelkezési jogról és az információszabadságról szóló törvény, a számviteli törvény és a kapcsolódó jogszabályok vonatkozó előírásai szerint kell eljárni. A szabályzat felülvizsgálata és karbantartása a jogszabályi változások függvényében, de legalább évente történik.

A szabályzat hatályba lépésének időpontja: 2017. október 01.

Örkény István Színház Nonprofit Kft. adatvédelmi és informatika biztonsági szabályzata

A szabályzat (a továbbiakban: Szabályzat) az Örkény István Színház Nonprofit Kft. (továbbiakban: Társaság) nyilvántartásával összefüggő legfontosabb adatvédelmi és informatikai-biztonsági szabályokat tartalmazza különös tekintettel az adatkezeléssel, adattovábbítással és nyilvánosságra hozatallal kapcsolatos adatvédelmi követelményekre.

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Info tv.) 20§/2/ bekezdése előírja, hogy az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő a 6. § (5) bekezdése alapján kezeli, illetve arról kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire i.

1. ADATVÉDELEM

I. Általános rendelkezések

1. Az Adatvédelmi szabályozás célja, a Szabályzat hatálya

1.1. A Szabályzat célja

A szabályzat célja, hogy rögzítse és összefoglalja azokat a követelményeket és biztosítékokat, amelyek a helyi sajátosságokra figyelemmel biztosítják az adatvédelmi és adatbiztonsági szabályok kialakítását.

1.2. A Szabályzat hatálya

1.2.1. A Szabályzat tárgyi hatálya

A szabályzat hatálya kiterjed a Társaságnál a nyilvántartással és a hozzá kapcsolódó iratok jogszabályszerű kezelésével összefüggő teljes adatkezelési és informatikai folyamatra.

1.2.2. A Szabályzat személyi hatálya

A szabályzat személyi hatálya kiterjed a Társaság valamennyi egységére, különös tekintettel a munkaügyre, ahol személyi adatokat használnak, kezelnek, tárolnak, vagy továbbítanak, valamint a betekintésre jogosultakra és az ügykezelés folyamatában személyi irattal érintkezőkre.

1.2.3. A szabályzat időbeli hatálya

A szabályzat időbeli hatálya kiterjed az alapnyilvántartással és a kapcsolódó személyi iratokkal összefüggő teljes adatkezelési és informatikai folyamatra, az irat beérkezésétől, keletkezésétől a megsemmisítésig.

2. A Szabályzat elkészítése az alábbi jogszabályokon alapul

- Magyarország Alaptörvényének VI. fejezetének (2) és (3) pontjában foglalt személyes adatok védelméhez fűződő jog, (Alaptörvény)
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, (Infotv.)
- A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.)
- Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. CVIII. törvény (Ektv.)
- A Polgári törvénykönyvről szóló 2013. V. törvény (Ptk.),
- A Büntető törvénykönyvről szóló 2012. C. törvény (Btk.)

Érintett: Bármely, meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy, jelen esetben a honlap felhasználója.

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.

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

Hozzájárulás: Az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez.

Tiltakozás: Az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.

Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.

Adatkezelés: Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.

Adattovábbítás: Az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Nyilvánosságra hozatal: Az adat bárki számára történő hozzáférhetővé tétele.

Adattörlés: Az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.

Adatmegjelölés: Az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából.

Adatzárolás: Az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából.

Adatmegsemmisítés: Az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.

Adatfeldolgozás: Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik.

Adatállomány: Az egy nyilvántartásban kezelt adatok összessége.

3. A Szabályzat tartalma

A Szabályzat a következő témákhoz kapcsolódóan tartalmaz előírásokat:

- a személyi iratok kezelésének adatvédelmi követelményei;
- a betekintési jog gyakorlásának szabályai;
- a nyilvántartást kezelő, személyes adatot tartalmazó számítógépes információs rendszer adatvédelmi és adatbiztonsági szabályai;
- egyes adatkezelésekre vonatkozó speciális rendelkezések

II. Részletes szabályok

1. A személyi iratok kezelésének adatvédelmi követelményei

1.1. A személyi irat fogalma

Személyi irat bármilyen anyagon, alakban és bármilyen eszköz felhasználásával keletkezett adathordozó, amely a munkaviszony létesítésekor, fennállása alatt, megszűnésekor, illetve azt követően keletkezik és a munkavállaló személyével összefüggésben adatot, megállapítást tartalmaz.

1.2. A személyi anyag fogalma

A személyi anyag tartalmazza a munkavállaló munkaviszonyával kapcsolatos iratai közül az alapnyilvántartás adatlapját, az önéletrajzot, a bűnügyi nyilvántartó szerv által kiállított hatósági bizonyítványt (az érintett dolgozók esetében), a munkaszerződést és annak módosítását, a végzettséget igazoló bizonyítvány, oklevél másolatát, valamint, a munkaviszonyt megszüntető iratot, a hatályban lévő fegyelmi büntetést kiszabó határozatot. Ezen iratokat együttesen kell tárolni.

1.3. A személyi iratok köre

- a személyi anyag az 1.1. pont meghatározott iratai.
- a munkaviszonnyal összefüggő egyéb iratok;
- a munkaviszonnyal összefüggő más munkaviszonyokkal kapcsolatos iratok;
- a munkavállaló saját kérelmére kiállított vagy az önként átadott adatokat tartalmazó iratok.

1.4. A személyi iratok keletkezése

A munkaviszony létesítésekor összeállításra kerül a munkavállaló személyi irata az 1.2. pont szerint.

A személyi iratra csak olyan adat és megállapítás vezethető, amelynek alapja

- okirat vagy a munkavállaló írásbeli nyilatkozata;
- a munkáltatói jogkör gyakorlójának írásbeli rendelkezése;
- bíróság vagy más hatóság döntése;
- jogszabályi rendelkezés.

A személyi anyagban a személyzeti iratokon kívül más irat nem tárolható.

A személyi anyagot „Betekintési lap" kimutatással kell ellátni, melyen dokumentálni kell a személyi anyagba történő betekintés tényét, jogosultjának személyét, jogszabályi alapját és a betekintés időpontját.

1.5. A személyi iratok iktatása, kezelése

A személyzeti iratokat személyenként kialakított iratgyűjtőben kell őrizni. Az abban elhelyezett iratok kezelése, tárolása, őrzése a személyzeti feladatokat ellátó ügyintéző feladata.

1.6. A személyi iratok megőrzése

A személyzeti iratokból nem kell másolati példányt tenni az iktatóba, azok tárolása a munkaviszony fennállásáig a személyzeti feladatokat ellátó ügyintézőnél történik.

Az iratokat zárható szekrényben kell tárolni, melynek kulcsát a személyzeti feladatokat ellátó ügyintéző, valamint a gazdasági igazgató kezelheti.
A munkaviszony megszűnése esetén a betekintési lapot a lezárást követően irattározni kell.

A személyi anyagot a munkaviszony megszűnésétől számított ötven évig meg kell őrizni.

1.7. A munkavállalók személyi iratai, munkaügyi nyilvántartása

A Társaság, az általa foglalkoztatott személy iratait a munkavállaló írásbeli hozzájárulása esetén kezelheti.

2. Alapnyilvántartás

2.1. Az alapnyilvántartás vezetésének szabályai

Az alapnyilvántartás célja a munkaviszonyból származó jogok gyakorlásához és kötelezettségek teljesítéséhez szükséges adatok kezelésének biztosítása a munkaviszony alanyai számára.

Az alapnyilvántartást a Társaság az általa rendszeresített adatlapon meghatározott adattartalommal az e szabályzat 1. mellékletében meghatározottakra figyelemmel folyamatosan vezeti.
A munkavállaló az adataiban bekövetkező változásokról nyolc napon belül köteles tájékoztatni a munkáltatói jogkör gyakorlóját, aki a változás tudomására jutásától számított nyolc napon belül köteles intézkedni az adatok aktualizálásáról.

2.2 Az alapnyilvántartás módja

A Társaságnál az alapnyilvántartás vezetése a NOVITAX Bér- és HR programmal, elektronikusan történik.

2.3. Az alapnyilvántartás vezetéséért felelős személyek

A nyilvántartás vezetésével kapcsolatos feladatokat a gazdasági igazgató által megbízott munkavállaló láthatja el.
Az alapnyilvántartásban szereplő személyes adatok védelméért, az adatkezelés jogszerűségéért, valamint az előírt adatszolgáltatásokért a Társaság vezetője felelős.

3. A betekintési jog gyakorlásának szabályai

A Társaságnál vezetett alapnyilvántartásba - eljárásában indokolt mértékig - jogosult betekinteni, illetőleg abból adatokat átvenni:

- saját adataiba a munkavállaló,
- a munkavállaló felettese,
- az ellenőrzést végző,
- a fegyelmi eljárást lefolytató testület vagy személy,

Az adatkezelő köteles a helytelen adatot haladéktalanul helyesbíteni, illetve törölni.
A munkavállaló a róla nyilvántartott iratokról másolatot vagy kivonatot kaphat, valamint jogosult megismerni, hogy a nyilvántartásban szereplő adatait kinek, milyen célból és milyen terjedelemben továbbították.

4. A nyilvántartásban és a személyi iratokban szereplő személyes adatokat kezelők személyes felelőssége

A jogviszonnyal összefüggő adatok kezeléséért felelős

- a Társaság vezetője,
- az érintett foglalkoztatott felettese,
- a személyzeti feladatot ellátó ügyintéző,
- a foglalkoztatott a saját adatainak közlése tekintetében,

tartozik felelősséggel.

A Társaság vezetője köteles gondoskodni:

- az adatvédelmi szabályzat kiadásáról, szükség szerint módosításáról;

- az ellenőrzés módszereinek és rendszerének kialakításáról és működtetéséről;
- a jogviszonnyal összefüggő adatok védelmével kapcsolatos követelmények Társaságon belüli közzétételéről.

5. A nyilvántartást kezelő, személyes adatot tartalmazó számítógépes információs rendszer adatvédelmi és adatbiztonsági szabályai

5.1. A számítógépes információs rendszer célja

A jogviszonnyal összefüggő személyes adatokat tartalmazó számítógépes információs rendszer védelmének szabályozása azt a célt szolgálja, hogy biztosítsa az adatkezelés fizikai biztonságát, a működtetés rendjét.

A rendszerbe csak jelszó használatával lehet belépni.

A feldolgozás során keletkezett hibás, aktualitásukat vesztett, vagy feleslegessé vált kinyomtatott adatokat kidobni nem lehet! Azokat be kell zúzni, olvashatatlanná kell tenni, ezután lehet elszállításukról gondoskodni.

6. Egyes adatkezelésekre vonatkozó speciális rendelkezések

6.1. A Társaság Facebook oldalának használata

A Társaság Facebook oldalára a látogatóinknak lehetőségük van hozzászólni, képet feltölteni.
A hozzájárulás elküldésével, kép feltöltésével az érintett személy hozzájárul neve, profilképe, hozzászólása és a feltöltött képe nyilvánosságra hozatalához, és megjelenítéséhez.
Más személyeket ábrázoló képek az érintett személyek írásbeli hozzájárulása nélkül nem tölthetők fel.

Az adatkezelés kizárólag a www.facebook.com oldalon történik, így az adatkezelés időtartamára, módjára, illetve az adatok törlési és módosítási lehetőségeire a facebook.com oldal szabályozása az irányadó.

6.2. Elektronikus megfigyelőrendszer használata

Társaságunk a székhelyén, telephelyén az emberi élet, testi épség, személyi szabadság, az üzleti titok védelme és a vagyonvédelem érdekében elektronikus megfigyelőrendszert alkalmaz, amely kép,- hang,- vagy kép- és hangrögzítést is lehetővé tesz.

Az elektronikus megfigyelőrendszer adott területen történő alkalmazásának tényéről jól látható helyen, jól olvashatóan, a területen megjelenni kívánó harmadik személyek tájékoztatását elősegítő módon figyelemfelhívó jelzést, ismertetést helyeztünk el.

A rögzített felvételeket felhasználás hiányában maximum 3 (három) munkanapig őrizzük meg.

2. INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

1. Az Informatikai Biztonsági Szabályzat célja

Az Informatikai Biztonsági Szabályzás (továbbiakban: IBSZ) alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa a Társaságnál az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek az érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az IBSZ célja továbbá:

- a titok-, a munka-, a vagyon- és a tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése,
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

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

2. Az IBSZ hatálya

2.1. Személyi hatálya

Az IBSZ személyi hatálya a Társaság valamennyi dolgozójára, illetve az informatikai eljárásban résztvevő más Társaságok dolgozóira egyaránt kiterjed.

2.2. Tárgyi hatálya

- kiterjed a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,

- kiterjed a Társaság tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre, valamint a gépek műszaki dokumentációira is,
- kiterjed az informatikai folyamatban szereplő összes dokumentációra,
- kiterjed a rendszer- és felhasználói programokra,
- kiterjed az adatok felhasználására vonatkozó utasításokra,
- kiterjed az adathordozók tárolására, felhasználására.

3. Fogalmi meghatározások

3.1. Az adatkezelés során használt fontosabb fogalmak

érintett: bármely meghatározott, személyes adat alapján azonosított vagy azonosítható természetes személy;

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

hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez;

tiltakozás: az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri;

adatkezelő: a Társaság, aki az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja.

adatkezelés: az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése;

adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;

adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

adatmegjelölés: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

adatmegsemmisítés: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;

adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése.

adatállomány: az egy nyilvántartásban kezelt adatok összessége;

adatvédelmi incidens: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

3.2. Üzemeltetési fogalmak meghatározása

Hozzáférés (account): a felhasználó azonosítója adott rendszerben. Az account-ot meghatározza: felhasználónév és a jelszó.

Felhasználó (user): az a személy, aki az adott rendszer használatára jogosított account-ot kapott

Bejelentkezés (login): az a folyamat, melyben a felhasználó account adatait egy rendszer számára érvényesítés céljából megadja

Tartomány (domain vagy körzet): rendszeradminisztrációs egység, ahol az account definiálva van

Felhasználói név (user name): az account része, mely a felhasználót az adott rendszerben egyedileg azonosítja

Jelszó (password): a felhasználó által választott betű és/vagy számkombináció, mely a felhasználót igazolja. A házirendben meghatározott szabályoknak eleget kell tegyen

Erőforrás (resource): egy informatikai eszköz szolgáltatása, melyet feladatok elvégzésére fel lehet használni

Rendszergazda: Az a személy aki adott alkalmazás fölött az összes hozzáférési jogot gyakorolja

4. Az IBSZ biztonsági fokozata

A Társaság adatai különböző biztonsági fokozatba tartozhatnak. (színházi titkok, pénzügyi adatok, a nyílt adatok feldolgozására, tárolására alkalmas adatok)

A Társaság alapbiztonsági fokozatba tartozik, így általános informatikai feldolgozást végez.

5. Kapcsolódó szabályozások

Az IBSZ-t az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:

- Szervezeti és Működési Szabályzat,
- Bizonylati rend,
- Felesleges vagyontárgyak hasznosításának és selejtezésének, valamint a Leltárkészítési és leltározási szabályzat,
- Belső ellenőrzési kézikönyv,
- Belső kontroll rendszer.

6. Védelmet igénylő, az informatikai rendszerre ható elemek

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.

6.1. A védelem tárgya

A védelmi intézkedések kiterjednek:

- a rendszer elemeinek elhelyezésére szolgáló helyiségekre,
- 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,
- a személyhez fűződő és vagyoni jogokra.

6.2. A védelem eszközei

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

7. A védelem felelőse

A védelem felelőse a rendszergazda. A jelen szabályzatban foglaltak szakszerű végrehajtásáról a Társaság adatvédelmi felelősének kell gondoskodnia.

7.1. Adatvédelmi felelős (rendszergazda) feladatai

- ellátja az adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- kialakítja a védelmi eszközök alkalmazására vonatkozó döntés elkészítése érdekében a szakterületek bevonásával a biztonságot növelő intézkedéseket,
- felelős az informatikai rendszerek üzembiztonságáért, biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének, szerviz ellátás biztosításának folyamatos ellenőrzése,
- a Szervezeti és Működési Szabályzat adatvédelmi szempontból való véleményezése,
- az adatvédelmi feladatok ismertetése, oktatása,

- a védelmi rendszer érvényesülésének ellenőrzése,
- felelős a Társaság informatikai rendszere hardver eszközeinek karbantartásáért, és időszakos hardver tesztjeiért,
- ellenőrzi a vásárolt szoftverek helyes működését, vírusmentességét, a használat jogszerűségét,
- vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek izolálásáról,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására.

7.2. Az adatvédelmi felelős (rendszergazda) ellenőri feladatai

- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
- ellenőrzi az informatikai munkafolyamat bármely részét.

7.3. Az adatvédelmi felelős (rendszergazda) jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet az Társaság vezetőjénél,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére, illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

7.4. Adatvédelmi felelős kiválasztása

Az alábbi követelményeknek kell megfelelnie:

- erkölcsi feddhetetlenség,
- összeférhetetlenség - az adatvédelmi felelős funkció összeférhetetlen minden olyan vezetői munkakörrel, amelyben adatvédelmi kérdésekben a napi munka szintjén dönteni, intézkedni kell.
- az informatika szintjén:

  = az informatikai hardver eszközök és a védelmi technikai berendezések ismerete,

  = üzemeltetésben jártasság,

  = szervezőkészség.
- a szakterületre vonatkozó jogi szabályozás ismerete.

7.5. Az adatvédelmi felelős megbízatása

Az adatvédelmi felelőst a Társaság vezetője bízza meg. Az adatvédelmi felelős írásbeli meghatalmazás alapján jogosult ellátni a hatáskörébe tartozó feladatokat.

8. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére az adatvédelmi felelős oktatás formájában biztosítja. Erről nyilvántartást vezet.

8.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t a bekövetkező változásokat követően aktualizálni kell, ami az adatvédelmi felelős feladata.

8.2. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

- közlésre szánt, bárki által megismerhető adatok,
- minősített, titkos adatok.

Az informatikai feldolgozás során keletkező adatok minősítése a gazdasági igazgató feladata. A védelmi utasítások és szabályozások nem mondhatnak ellent a törvények és a jogszabályok mindenkori előírásainak. A titoknak minősülő adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot.

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

Minden dolgozóval, aki az adatok gyűjtése, felvétele, tárolása, feldolgozása, hasznosítása és törlése során információkhoz jut adatkezelési nyilatkozatot kell aláíratni. (2. sz. melléklet)

8.3. Megosztási mappákhoz való hozzáférés

8.3.1. Windows hálózati bejelentkezés

A Társaság által használt hálózati rendszerben az azonosítás olyan account információ felhasználásával történik, melynek részei a felhasználói név és a jelszó, amik együttesen érvényesek.

8.3.2. Alkalmazás szintű bejelentkezés

Ha egy alkalmazás futtatásához vagy annak adatainak eléréséhez felhasználói azonosításra van szükség, és az alkalmazás önálló felhasználó kezeléssel rendelkezik, akkor alkalmazás szintű bejelentkezésre van szükség.

8.4. Account átvétele

- az elkészült account kézbesítéséről az rendszergazda gondoskodik
- az account átadása kizárólag annak tulajdonosának történhet

8.5. Az account felhasználási feltételei

A személyre szólóan kiadott jelszót a felhasználó köteles titokban tartani. Másnak átadni, leírni, vagy egyéb formában rögzíteni tilos! A Társaság vezetője beosztottját jelszavának átadására nem utasíthatja.

8.6. Hozzáférés korlátozása (account zárolása)

A biztonsági előírások és a Társaság érdekei megkövetelik, hogy visszaélések és azok gyanúja esetén a felhasználó rendszerhez/hálózathoz/alkalmazáshoz való hozzáférése korlátozva legyen.

8.7. Manuális korlátozások

- account jogosulatlan használatakor
- jogosultságokkal való visszaélés, károkozás esetén
- a munkavégzésre irányuló munkaviszony megszűnésekor
- az alkalmazott, egyéb foglalkoztatott felettesének indokolt kérése alapján

9. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete fontos, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

9.1. Környezeti infrastruktúra okozta ártalmak

- Elemi csapás: földrengés, árvíz, tűz, villámcsapás, stb.
- Környezeti kár: légszennyezettség, nagy teljesítményű elektromágneses térerő, elektrosztatikus feltöltődés, a levegő nedvességtartalmának felszökése vagy leesése, piszkolódás (pl. por).
- Közüzemi szolgáltatásba bekövetkező zavarok: feszültség-kimaradás, feszültségingadozás, elektromos zárlat, csőtörés.

9.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya), szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a megváltozott körülmények figyelmen kívül hagyása,
- vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),

- a karbantartási műveletek elmulasztása.

A szükséges karbantartás elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

10. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

A Társaság számítógépein tárolt Microsoft Office dokumentumok, legyen az Word, Excel vagy PowerPoint prezentáció, védett anyagnak minősül.

10.1. Tervezés és előkészítés során előforduló veszélyforrások

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

10.2. A rendszerek megvalósítása során előforduló veszélyforrások

- helytelen adatkezelés,
- programtesztelés elhagyása.

10.3. A működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság,
- szervezetlenség,
- képzetlenség,
- szándékosan elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

11. Az informatikai eszközök környezete, azok védelme

11.1. A munkaállomások minimális igénye

A váratlan áramkimaradás esetén a szervert intelligens UPS–sel kell ellátni (szünetmentes tápegység), mellyel az áramkimaradás folyamatosságát biztosítani lehet. Az informatikai eszközöket csak a kijelölt dolgozók használhatják.

11.2. Adathordozók

- könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni,
- a használni kívánt adathordozót (CD, DVD, pendrive) a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni.

11.3. Vírus védelem

11.3.1. Vírusfertőzés gyanús helyzetek

A felhasználó az alábbi vírusfertőzésre utaló jelenségekkel találkozhat:

- A víruskereső program névvel azonosított vírust jelez. A lehető legerősebb vírusjegy.
- Szokatlan számítógép- vagy programviselkedés. Általánosan erős vírusjegy.
- A rendszer működése többszöri újraindítás után is egyértelműen lassabb a megszokottnál. Átlagosan erős vírusjegy.

11.3.2. Teendők vírusfertőzés esetén

Tájékoztatni kell a rendszergazdát a fertőzésről vagy annak gyanújáról.
A vírusvédelmi szoftvert elindítjuk, és megszüntetjük a vírusfertőzést. Ez történhet elsődlegesen a fertőzött állomány javításával (a vírus eltávolítása), ha erre lehetőség van, egyébként a fertőzött állomány törlésével. Ez utóbbi esetben ügyelni kell arra, hogy nem rendszerállományról van-e szó.

A szerverek és munkaállomások vírusvédelmére az alábbi szabályokat kell betartani:

- Minden munkaállomásra és szerverre vírusellenőrző szoftvert kell telepíteni.
- A vírusellenőrző programnak minden újonnan érkezett állománnyal kapcsolatos fájlművelet esetén meg kell vizsgálni az adathordozó tartalmát.
- Biztosítani kell a vírusvédelmet ellátó programok, valamint a vírusok adatait tartalmazó állományok rendszeres, gyártó által kibocsátott verziók telepítésével történő mielőbbi frissítését.

11.4. Tűzvédelem

A Társaság munkaállomásai alacsony kockázati osztályba tartoznak, ami mérsékelt tűzveszélyes üzemet jelent.

A tűzvédelem feladatait, sajátos előírásokat a Társaság Tűzvédelmi szabályzata tartalmazza. A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell. Külön tűzszakaszt kell képezni.

12. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

12.1. A munkaállomások védelme

Elemi csapás (vagy más ok) esetén a bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

12.2. Hardver védelem

Biztosítani kell a berendezések hibátlan és üzemszerű működését. A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése. A karbantartási munkákat tervezetten, körültekintően és gondosan kell elvégezni.

A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlatait, a tapasztalatokat,
- a hardver tesztek által feltárt hibákat.

12.3. Az informatikai feldolgozás folyamatának védelme

12.3.1. Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- a bizonylatokat, adathordozókat csak e célra kialakított és megfelelő tároló helyeken lehet tartani,
- az adatrögzítés szoftver védelme: biztosítani kell továbbá a rögzített tételek visszakeresésének és javításának lehetőségét is.
- hozzáférési lehetőség:
  = a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz.
  = az adatok bevitele során az azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

12.3.2. Adathordozók védelme

A Társaságnál az alábbi adathordozók lehetnek: CD lemez, DVD lemez, pendrive, hordozható winchester, notebook, asztali számítógép, szerver, okos telefon, stb.)
Az informatikai eszközök üzemeltetéséért a rendszergazda felelős, aki köteles gondoskodni a feldolgozások igényeinek megfelelő adathordozók biztosításáról, beleértve a biztonsági másolatok eszközigényeit, illetve az üzemeltetés biztonságát növelő generációs adatállományok alkalmazását is.

12.3.3. Az adathordozók megőrzése

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

12.3.4. Selejtezés, sokszorosítás, másolás

Olyan mágneses adathordozót, amelyet javíthatatlan fizikai károsodás ért selejtezni kell.

Selejtezni kell:

- a fizikailag sérült, javíthatatlan, a gyári, raktározási hibából követően felhasználásra alkalmatlan (deformálódott) CD-t, DVD-t, pendrive-t.
- véglegesen elhasználódott anyagot.

Az alkalmatlan CD-ket, DVD-ket, pendrive-ket fizikai roncsolással használhatatlanná kell tenni.

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

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

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

A selejtezési jegyzőkönyvek nem selejtezhetőek.

Titkos adatokat tartalmazó adathordozókat nem lehet selejtezni.

12.3.5. Leltározás

Az adathordozókat a Leltárkészítési és leltározási szabályzatban foglaltaknak megfelelően kell leltározni.

12.3.6. Mentések, file-ok védelme

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

A mentések folyamata:

- A mentéseket folyamatosan kell végrehajtani.
- A mentésből az adatoknak teljes körűen visszaállíthatónak kell lennie a mentés pillanatának állapotára.
- A szerverek mentését legalább hetente kell elvégezni.
- A mentett adatokhoz csak az arra jogosultak férhetnek hozzá.

Az egyéb mentéseket meghatározott időszakonként el kell végezni. A munkák során létrehozott dokumentumok mentése az azt létrehozó munkatársak feladata:

- A személyi anyagok adatállományának mentését napi gyakorisággal a személyügyes végzi el.
- A könyvvezetés és a pénzügyi könyvvezetés adatainak automatikus mentését a program végzi el.
- A pénztár könyvelés adatainak automatikus mentését napi gyakorisággal a program végzi el.
- Az egyéb analitikus nyilvántartások adatainak mentését naponta kell elvégezni.

12.4. Szoftver védelem

12.4.1. Rendszerszoftver védelem

A rendszergazdának biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

Teendők a következők:

- a rendszerszoftver módosításához az üzemeltetésért felelős vezető engedélye szükséges,
- név szerint kell kijelölni azokat a személyeket, akik a rendszerszoftverben módosításokat végezhetnek,
- a módosítással egy időben, a dokumentációban is a változásokat át kell vezetni, a változtatásokról nyilvántartást kell vezetni.

12.4.2. Felhasználói programok védelme

12.4.2.1. Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.

A felhasználók jelszavait illetéktelen személyektől gondosan védeni kell. A jelszót nem szabad több személy között megosztani. A jelszót soron kívül meg kell változtatni, ha az illetéktelen személy tudomására jutott, vagy juthatott.

12.4.2.2. Programok megőrzése, nyilvántartása

A programokról naprakész nyilvántartást kell vezetni úgy, hogy a nyilvántartásból egyértelműen megállapítható legyen a program azonosítására és kezelésére vonatkozó adatok.

A számvitelről szóló többször módosított 2000. évi C. törvény értelmében az üzleti évről készített beszámolót, valamint az azt alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá más, a számviteli törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 10 évig meg kell őrizni.

A bizonylat elektronikus formában is megőrizhető, ha az alkalmazott módszer biztosítja az eredeti bizonylat összes adatának késedelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az utólagos módosítás lehetőségét.

13. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

13.1. Központi gép (Server)

A központi gép háttértárairól hetente egy teljes, a többi napon biztonsági mentést kell készíteni. A mentéseket heti egy alkalommal külső adattároló egységre kell másolni. Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.

13.2. Munkaállomások

A Társaság informatikai eszközeiről programot, illetve adatállományokat nem lehet másolni a jogos belső felhasználói igények kielégítésein kívül.

14. Internet hozzáféréssel kapcsolatos intézkedések

A vírusok és az illetéktelen hozzáférések miatt tűzfalat kell konfigurálni. A tűzfal működése közben keletkező állományokat az üzemeltetőnek rendszeresen ellenőrizni kell.

15. Az elektronikus levelezés szabályai

Minden alkalmazott rendelkezik internetes postafiókkal, melyet magáncélokra is használ. Munkaviszonyának megszűnése esetén nem használhatja tovább az e-mail címet, az törlésre kerül, vagy az alkalmazott feladatát továbbiakban ellátó kolléga kezelésébe kerül.

16. Ellenőrzés

A Társaság az éves belső ellenőrzési ütemtervében rögzíti az ellenőrzés módját.

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszerben meglévő veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése, illetve annak megakadályozása, hogy az megismétlődjön.

A folyamatba épített előzetes, utólagos és vezetői ellenőrzés során az IBSZ rendelkezéseinek betartását az adatkezelést végző Társasági egység vezetői folyamatosan ellenőrzik.

Záró rendelkezés

AZ ADATVÉDELMI ÉS INFORMATIKA BIZTONSÁGI SZABÁLYZAT

2017. október 01. napján lép hatályba.

Ezzel egy időben a korábban érvényes szabályzat hatályát veszti.

A szabályzatot módosítani kell

a.) olyan jogszabályi előírás változása esetén, amely érinti a hatályos szabályzat előírásait, valamint

b.) ha a Társaság szerv sajátosságai, működésének változása alapján indokolttá vált.

A módosításokat az ok felmerülésétől számított 90 napon belül kell végrehajtani.

A módosítások elvégzéséért a gazdasági igazgató a felelős.

Budapest, 2017. október 01.

.....
ügyvezető igazgató

.....
gazdasági igazgató

1. sz. melléklet

AZ ALAPNYILVÁNTARTÁS ADATKÖRE

SAJÁT

2. melléklet

ADATKEZELÉSI NYILATKOZAT

Alulírott ..... (név) ..... (lakcím) nyilatkozom, hogy a feladatellátás során tudomásomra jutott információkat megőrzöm, azt illetéktelen személyek részére nem adom át.

A munkavégzés során csak a részemre hozzáférhető adatokkal dolgozom, más adatok hozzáférésére kísérletet sem teszek.

Dátum: 201... .....

.....
aláírás

Megismerési nyilatkozat

A Társaság 2017. ……..…….. –tól hatályos Adatvédelmi és Informatika Biztonsági Szabályzatában foglaltakat megismertem. Tudomásul veszem, hogy az abban leírtakat a munkám során köteles vagyok betartatni.

Név	Beosztás	Dátum	Aláírás