Bartók Kamaraszínház és
Művészetek Háza
Dunaújváros, Bartók tér 1.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Hatályos: **2014.01.01-től**

dr. Borsós Beáta
igazgató

1. **Az Informatikai Biztonsági Szabályzat célja**

Az Bartók Kamaraszínház és Művészetek Háza Informatikai Biztonsági Szabályzatát (továbbiakban IBSZ) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló többször módosított 1992. évi LXVI. törvény, valamint az államtitok és szolgálati titok számítástechnikai védelméről szóló 3/1988. (XI.22.) KSH rendelkezés alapján a következők szerint határozom meg:

Az IBSZ alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát. a Bartók Kamaraszínház és Művészetek Házában (továbbiakban: színház).

Az IBSZ célja továbbá:

- a titok-, vagyon- és 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 üzembe helyezésen keresztül az üzemeltetésig.
A jelen IBSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

2. Az Informatikai Biztonsági Szabályzat hatálya

2.1. Személyi hatálya

Az IBSZ személyi hatálya a színház fő- és részfoglalkozású dolgozójára, illetve az informatikai eljárásban résztvevő más szervezetek dolgozóira, egyéni vállalkozóira egyaránt kiterjed.

2.2. Tárgyi hatálya

- kiterjed a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed az intézmény tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre,
- valamint az informatikai eszközök műszaki dokumentációira,
- kiterjed az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- kiterjed a rendszer- és felhasználói programokra,
- kiterjed az adatok felhasználására vonatkozó utasításokra,
- kiterjed az adathordozók tárolására, felhasználására.

3. Az adatkezelés során használt fontosabb fogalmak

Adatkezelés: az alkalmazott eljárástól függetlenül az adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is;

Adatfeldolgozás: az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

Adattovábbítás: ha az adatot meghatározott harmadik fél számára hozzáférhetővé teszik.

Adatkezelő: az a természetes vagy jogi személy, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bízhat meg.

Adatfeldolgozó: az a természetes vagy jogi személy, aki vagy amely az adatkezelő megbízásából adatok feldolgozását végzi.

Nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik;

Adatbiztonság: az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

4. Az IBSZ biztonsági fokozata

Intézményünk alapbiztonsági fokozatba tartozik. Intézményünk általános informatikai feldolgozást végez.

5. Kapcsolódó szabályozások

Az IBSZ előírásai összhangban vannak:

- Szervezeti és Működési Szabályzat
- Bizonylati rend,
- Leltárkészítési és leltározási szabályzat,
- Felesleges vagyontárgyak hasznosításának és selejtezésének szabályzata,
- Belső ellenőrzési szabályzat.

6. Védelmet igénylő, az informatikai rendszerre ható elemek

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.
Az informatikai rendszerre az alábbi tényezők hatnak:

- a környezeti infrastruktúra,
- a hardver elemek,
- az adathordozók,
- a dokumentumok,
- a szoftver elemek,
- az adatok,
- a rendszerelemekkel kapcsolatba kerülő személyek.

6.1. A védelem tárgya

A védelmi intézkedések kiterjednek:

- a rendszer elemeinek elhelyezésére szolgáló helységekre,
- 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 vagyoni jogokra

6.2. A védelem eszközei

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

7. A védelem felelőse

A védelem felelősei:

- adatvédelmi felelős: a műszaki vezető
- rendszergazda: a Monos Consulting Kft. (Németh Tamás).

A jelen szabályzatban foglaltak szakszerű végrehajtásáról az intézmény adatvédelmi felelősének kell gondoskodnia.

7.1. Adatvédelmi felelős feladatai

- ellátja az adatfeldolgozás felügyeletét
- ellenőrizni a védelmi előírások betartását
- ellátja az informatikai titokvédelmi munka szervezését és felügyeletét
- kialakítja a védelmi eszközök alkalmazására vonatkozó döntés előkészítése érdekében a szakterületek bevonásával a biztonságot növelő intézkedéseket,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,(CD, DVD)
- a Szervezeti és Működési Szabályzat adatvédelmi szempontból való véleményezése,
- az adatvédelmi feladatok ismertetése, oktatása,
- védelmi rendszer érvényesülésének ellenőrzése,

- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- felelős az intézmény informatikai rendszere hardver eszközeinek karbantartásának koordinálásáért és időszakos tesztjeiért,
- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- tevékenységéről rendszeresen beszámol az intézmény vezetőjének

7.2. Rendszergazda feladatai

- 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 folyamatos ellenőrzése
- ellenőrzi a vásárolt szoftverek helyes működését, vírusmentességét, a használat jogszerűségét
- a vírusvédelemmel foglalkozó szervezetekkel kapcsolatot tart,
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek izolálásáról,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működése és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer önadminisztrációját,
- javaslatot tesz a rendszer szűk keresztmetszetének felszámolására,
- egyeztetés a jegyértékesítő rendszer üzemeltetőjével programmódosítások esetén, ill. a szükséges mentések elvégzésével kapcsolatban.

7.2. Az adatvédelmi felelős ellenőri feladatai

- évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását,
- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
- előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

7.3. Az adatvédelmi felelős jogai

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

7.4 Az adatvédelmi felelős kiválasztása

Az alábbi követelményeknek kell megfelelnie:

- erkölcsi fedhetetlenség
- összeférhetetlenség - az adatvédelmi felelős funkció összeférhetetlen minden olyan vezetői munkakörrel, amelyben adatvédelemi kérdésekben a napi munka szintjén dönteni, intézkedni kell.
- Az informatika szintjén:
  - az informatikai hardver eszközök és a védelmi technikai berendezések ismerete
  - üzemeltetésben jártasság
  - szervezőkészség
- szakterületére vonatkozó jogi szabályozás ismerete

7.5 Adatvédelmi felelős megbízatása

Az adatvédelmi felelőst az intézményvezető bízza meg.
Az adatvédelmi felelős írásbeli meghatalmazás alapján, vagy a munkaköri leírásban foglaltak szerint jogosult ellátni a hatáskörébe tartozó feladatokat.

8. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére az adatvédelmi felelős és a rendszergazda oktatás formájában biztosítják. Erről nyilvántartást kötelesek vezetni.

Az Informatikai Biztonsági Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

8.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában - valamint az intézménynél - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell.

Az IBSZ folyamatos karbantartása az adatvédelmi felelős feladata.

9. Az informatikai eszközbázist veszélyeztető helyzetek

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

9.1. Környezeti infrastruktúra okozta ártalmak

- elemi csapás:
  1. földrengés,
  2. árvíz,
  3. tűz,
  4. villámcsapás, stb.
- környezeti kár:
  1. légszennyezettség,
  2. nagy teljesítményű elektromágneses térerő,
  3. elektrosztatikus feltöltődés,
  4. a levegő nedvességtartalmának felszökése vagy leesése,
  5. piszkolódás (pl. por).
- közüzemi szolgáltatásba bekövetkező zavarok:
  1. feszültség-kimaradás,
  2. feszültségingadozás,
  3. elektromos zárlat,
  4. 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 biztonsági-, jelző és riasztó berendezések karbantartásának 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

10.1. Tervezés és előkészítés során előforduló veszélyforrások

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

10.2. A rendszerek megvalósítása során előforduló veszélyforrások

- hibás adatállomány működése,
- 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 környezetének védelme

11.1. Vagyonvédelmi előírások

- az irodák külső és belső helyiségeit biztonsági zárakkal kell felszerelni,

- az irodákba való be- és kilépés rendjét szabályozni kell,
- csak az illetékes dolgozók tartózkodhatnak az irodákban,
- az irodák kulcsainak felvétele illetve leadása csak aláírás ellenében történhet
- a számítógép monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- az informatikai eszközöket csak az intézmény arra felhatalmazott alkalmazottai használhatják,
- az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

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, melyről nyilvántartást kell vezetni,
- a használni kívánt adathordozót (floppy, CD) a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni,
- a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,
- adathordozót másnak átadni csak engedéllyel szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

12. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

12.1. Az irodák védelme

Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben 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

A berendezések hibátlan és üzemszerű működését biztosítani kell.

A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.

Az üzemeltetést, karbantartást és szervizelést az informatikusok végzik.

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.

Alapgép megbontását (kivéve a garanciális gépeket) csak a rendszergazda végezheti el.
Billentyűzet, monitor, nyomtató cseréjének idejét dokumentálni kell.

12.3. Az informatikai feldolgozás folyamatának védelme

12.3.1. Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- tesztelt adathordozóra lehet adatállományt rögzíteni,
- a bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
- az adatrögzítő szoftver védelme. Lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják 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. (alapelv: a tárolt adatokhoz csak az illetékes személyek férjenek hozzá).
    - az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
    -

A szerverek rendszergazda jelszavát a rendszergazda kezeli, kérésre az intézményvezetőnek átadja.

12.3.2. Az adathordozók védelme

Az adathordozók logikai védelmét az operációs rendszer és az ehhez tartozó ellenőrző, file-kezelő rutinok alkalmazásával lehet biztosítani.

Az informatikai eszközök üzemeltetéséért a rendszergazda felelős.

Tilos a privát adathordozókat szolgálati célra igénybe venni, illetve tilos szolgálati adathordozót magáncélra igénybe venni.

12.3.3. Adathordozók tárolása

Az adathordozók tárolására műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani. Intézményünkben a műszaki vezető irodájában elhelyezett lemezszekrény szolgál az adathordozók tárolására.

12.3.4. Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését.

A munkák során létrehozott word és excel dokumentumok mentése az azt létrehozó munkatársak felhasználók feladata.

A személyi anyagok adatállományok mentését havi gyakorisággal az ügyintéző végzi el és a MÁK területi Igazgatósága tárolja.

A főkönyvi könyvelési, analitikus nyilvántartások adatainak mentését a Polisz számviteli rendszer saját szerverén végzi el.

A levelezések mentését vagy a felhasználó vagy kérésre a rendszergazda végzi el.

A felhasználó számítógépén lévő adatokról a rendszergazda készít másolatokat a felhasználó tájékoztatása alapján.

A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentést a rendszergazda végzi..

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.

12.4.2. Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem
A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.

Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

Programok megőrzése, nyilvántartása

A programokról az adatvédelmi felelősnek valamint az analitikus könyvelőnek naprakész nyilvántartást kell vezetni

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

Gondoskodni kell arról, hogy a tárolt programok, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek.

Lokális gépre programot csak a rendszergazda tudtával lehet telepíteni.

A számvitelről szóló többször módosított 2000. évi C. törvény értelmében a intézményünk a gazdasági 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 gépek

Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.

A központi gépek háttértárairól folyamatosan biztonsági mentést kell készíteni. A mentés felülírással készül, így mindig 1 nappal korábbi állapotú adat-visszaállítást kell lehetővé tenni.

Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.

A vásárolt szoftverekről biztonsági másolatot kell készíteni.

13.2. Munkaállomások

A hálózatra idegen programot, adatot másolni csak a rendszergazdával történt egyeztetés után lehet.

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.

Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell.

Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.

Az intézmény informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.

A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.

Az informatikai eszközt és tartozékait helyéről elvinni csak az eszköz leltárfelelőse tudtával és engedélyével szabad.

14. Ellenőrzés

DMJV Polgármesteri Hivatala Belső Ellenőrzési Osztálya az intézmény éves belső ellenőrzési ütemtervében rögzíti az ellenőrzés módját.

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

A munkafolyamatba épített ellenőrzés során az IBSZ rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

15. Záró rendelkezések

Az Informatikai Biztonsági Szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat.

Dunaújváros, 2014. január 1.

dr. Borsós Beáta
igazgató

Kapják:

gazdasági vezető
adatvédelmi felelős - Török Imre
rendszergazda, - Németh Tamás, továbbá
a szabályzat az intézményi **„P" meghajtó Szabályzatok, hirdetmények mappájában is közzétételre kerül.**

Megismerési nyilatkozat

A **Bartók Kamaraszínház és Művészetek Háza 2014. január 1** -től hatályos **Informatikai biztonsági szabályzatában** foglaltakat megismertem. Tudomásul veszem, hogy az abban leírtakat a munkám során köteles vagyok betartatni.

Név	Feladat, hatáskör	Dátum	Aláírás
Hierné Rozsos Ilona	gazdasági vezető	2014.01.01.	
Szendreyné Dani Melinda	főkönyvi könyvelő	2014.01.01	
Török Imre	adatvédelmi felelős	2014.01.01	
Turbucz Zsuzsanna	titkárnő	2014.01.01	
Borsiné Takács Györgyi	jegypénztáros	2014.01.01	
Vitézné Tonka Magdolna	jegypénztáros helyettes	2014.01.01.	
Németh Tamás	rendszergazda	2014.01.01.	
Wachterné Orosz Adrienn	szervező	2014.04.01.	
Horváth Ágnes	pénztáros	2014.04.11.	
Horváth István	munkaügyi ügyintéző	2014.07.01.	