MAGYAR TÁNCMŰVÉSZETI FŐISKOLA

INFORMATIKAI SZABÁLYZATA

Hatályos: 2012. november 15. napjától

A MAGYAR TÁNCMŰVÉSZETI FŐISKOLA

INFORMATIKAI SZABÁLYZATA

A Magyar Táncművészeti Főiskola Szenátusa a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény, valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: adatvédelmi törvény) alapján, a Szervezeti és Működési Szabályzatban (a továbbiakban: SZMSZ) foglalt jogkörében a főiskolai informatikai rendszer kialakítása, fenntartása, fejlesztése és védelme érdekében a következő szabályzatot alkotta.

PREAMBULUM

A jelen Informatikai szabályzat célja, hogy a Magyar Táncművészeti Főiskola informatikai rendszerének működési rendjét, az adatok és információbiztonsággal kapcsolatos elveket, szabályokat, az informatikai rendszerrel kapcsolatos biztonsági intézkedéseket, a szoftverhasználat rendjét valamint az elvárt magatartásformákat és betartandó gyakorlatot szabályozza.

Ennek keretében meghatározza különösen:

I. rész. Az informatikai általános működési rendjét

a) az informatikai csoport működési rendjét,
b) a rendszergazda feladatait, jogait és kötelességeit,
c) az informatikai szolgáltatásokat,
d) az informatikai eszközök kezelését, használatát,
e) a felhasználói jogosultságokat.

II. rész Az informatikai biztonság rendjét

a) az informatikai rendszerek biztonsági besorolását
b) a felelősségi köröket
c) az adatvédelmi felelősök feladatait
d) a védelmet igénylő adatok és információk osztályozását, minősítését, hozzáférési jogosultságát
e) az informatikai eszközbázist veszélyeztető helyzeteket
f) az informatikai eszközök környezetének védelmét
g) az informatikai rendszer alkalmazásánál felhasználható védelmi eszközöket és módszereket
h) az informatikai feldolgozás folyamatának védelmét
i) a központi számítógép és a hálózat munkaállomásainak működésbiztonságát
j) az informatikai biztonsági ellenőrzést

III. rész A szoftverhasználat rendjét

a) a szoftverhasználattal kapcsolatos fogalmakat és általános rendelkezéseket
b) a szoftverhasználattal kapcsolatos kötelességeket és jogokat
c) a szoftverek nyilvántartását
d) a szoftverhasználattal kapcsolatos adatkezelést és adatvédelmet.

I. Rész

AZ INFORMATIKA ÁLTALÁNOS MŰKÖDÉSI RENDJE

1. Bevezető rendelkezések

1. § (1) Az informatikai szabályzat (a továbbiakban: szabályzat) személyi hatálya kiterjed a Magyar Táncművészeti Főiskola (a továbbiakban: főiskola) valamennyi dolgozójára, függetlenül attól, hogy alkalmazására milyen jogviszonyban kerül sor, hallgatójára, függetlenül az oktatás formájára, az informatikai szolgáltatásokat nyújtó és igénybevevő valamennyi szervezeti egységére. Amennyiben a főiskola harmadik félnek is lehetőséget biztosít informatikai infrastruktúrájának használatára, akkor harmadik félre nézve is kötelező a szabályzatban foglaltak betartása.

(2) A szabályzat tárgyi hatálya kiterjed:

a) a főiskola tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre,

b) az informatikai folyamatokban szereplő összes fejlesztési, szervezési, programozási, üzemeltetési dokumentációra,
c) a rendszer- és felhasználói programokra,
d) a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
e) az adatok felhasználására vonatkozó utasításokra, valamint
f) az adathordozók tárolására, felhasználására.

(3) A szabályzat az informatika általános működési rendje mellett meghatározza az eszközök használatának módját, feltételeit, biztonsági előírásait, kitér a jogi és etikai kérdésekre is. A szabályzatban foglaltak ismerete és betartása az eszközöket igénybe vevő minden személy (továbbiakban: felhasználó) számára kötelező.

(4) Az eszközöket csak olyan személy használhatja, aki az eszközök használatára engedélyt vagy utasítást kapott, valamint e szabályzatot ismeri. A szabályzat megismerhető és letölthető a főiskola honlapjáról. A felhasználó a szabályzatban foglaltak tudomásulvételét és elfogadását aláírásával igazolja (3. számú melléklet). Az aláírást megtagadó felhasználó nem jogosult az eszközök használatára. Az új felhasználó regisztrációjáról a rendszergazda gondoskodik.

(5) A szabályzatot a jogszabályokban, a főiskola szervezetében vagy működésében, illetve az informatikában a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. A szabályzat összeállításáért, aktualizálásáért a főtitkár a felelős.

2. Az informatikai csoport működési rendje

3. § (1) Az informatikai csoport tagjai a rendszergazdák.

(2) Az informatikai csoport hatásköre:
a) az intézmény informatikai fejlesztésének tervezése, koordinálása, ellenőrzése,
b) az informatikai fejlesztési terv összeállítása és felülvizsgálata,
c) az Internet és az Intranet funkciók fejlesztése, ellenőrzése.

3. A rendszergazda feladata, jogai és kötelességei

4.§ (1) A rendszergazda – a főiskola oktatási, kutatási, művészeti, igazgatási és szolgáltatási feladatinak figyelembevételével – gondoskodik a főiskola számítástechnikai eszközeinek, különösen az informatikai hálózat, a szoftverek és különféle adatbázisok, az informatika terem stb. folyamatos és biztonságos üzemeltetéséről. Munkáját a főiskola szervezeti egységeinek vezetőivel, illetve az egyes szervezeti egységek informatikai ügyekben illetékes munkatársaival együttműködve végzi.

(2) A rendszergazda főbb feladatai:
a) lebonyolítja az informatikai eszközök beszerzését, telepítését, selejtezését, elvégzi az új gépek és egyéb hardver eszközök beállításait, rendszeres ellenőrzéseket végez az előforduló hibák felderítése és elhárítása érdekében,
b) biztosítja az intézményben az alapfeladatok ellátáshoz szükséges szoftverek működését, beleértve az egyes szervezeti egységek (pl.: Gazdasági Hivatal, Rektori Hivatal, Könyvtár, stb.) speciális szoftvereit is, nyilvántartja a szoftvereket és a licencszerződéseket,
c) gondoskodik az üzemeltetés rendjének szabályozásáról és fenntartásáról, a szabályzatban meghatározott szolgáltatások biztosításáról, a szükséges jelentések elkészítéséről,
d) gondoskodik a számítógépek vírusmentességének fenntartásáról és rendszeres ellenőrzéséről. Vírusfertőzés esetén mindent megtesz a fertőzés terjedésének megakadályozására, a fertőzés megszüntetetésére, illetve a szoftverekben okozott károk helyreállítására. A főiskola anyagi lehetőségeihez mérten szorgalmazza vírusvédelmi rendszer kiépítését.
e) részt vesz az informatikai fejlesztési stratégia kialakításában,
f) elkészíti a szakmai dokumentációt a rendszer felépítéséről, működéséről,
g) a szabályzatban foglaltak szerint új hálózati azonosítókat ad ki, a hálózati felhasználókat, a felhasználói jogokat karbantartja, általában gyakorolja a szabályzatban meghatározott jogait,
h) üzemelteti a főiskola szervereit, ügyel azok lehető legmagasabb biztonsági beállításaira,
i) biztosítja a levelezőrendszer folyamatos és biztonságos működését,
j) a technikai háttér figyelembevételével az egyes szervezeti egységek vezetőinek kezdeményezésére gondoskodik biztonsági másolatok készítéséről, illetve intézményi érdekből fontos területeken kezdeményezi a főiskola vezetésénél biztonsági másolatok készítését.

(3) A rendszergazda a (2) bekezdésben meghatározott feladatok ellátásában együttműködik különösen a lokális hálózatok működéséért felelős munkatársakkal, de a feladatmegosztás során nem mellőzheti, és nem háríthatja más

személyre ellenőrzési, nyilvántartási kötelezettsége teljesítését, különösen az informatikai beszerzésekre vonatkozó engedélyezést, ellenjegyzést.
(4) A rendszergazda (vagy az általa ezzel megbízott informatikus) kötelessége, hogy feladatai körében az informatikai eszközök beszerzésére, javítására, karbantartására, stb. vonatkozó tanszéki, hivatali előterjesztésekben (kérelmekben) 5 munkanapon belül érdemben eljárjon.

4. Informatikai eszközök kezelése, használata

5. § (1) A szabályzat alkalmazása tekintetében eszköznek tekintendők:
a) a számítógépek,
b) a számítógép perifériák (pl. nyomtató, scanner, egér, stb.),
c) a számítógép hálózat,
d) az irodatechnikai berendezések (pl. fénymásoló, fax, telefon),
e) a számítógépeken futó szoftverek,
f) a fenti berendezésekhez, szoftverekhez tartozó dokumentációk,
g) az adathordozók.
(2) Az eszközök pontos jegyzékét az intézményi leltár tartalmazza. Az informatikai szolgáltatásokat a felhasználói jogosultság átadásának napjától lehet igénybe venni. Egy adott informatikai eszközzel igénybe vehető szolgáltatások körét az eszköz működtetéséért felelős szervezeti egység vezetője határozza meg.
(3) A számítástechnikai eszközök telepítése, elhelyezése, az előírásoknak megfelelő üzembe helyezése kizárólag az informatikai munkatársak feladata. Ezáltal érvényesíthető a beszerzéssel kapcsolatos garancia és jótállás.
Az eszközök gépek üzembe helyezése után az informatikai munkatársak gondoskodnak az eszközökhöz tartozó dokumentációk és egyéb anyagok (telepítő lemezek stb.) átadásáról, az átadásról átvételi jegyzőkönyv készül.
(4) Az eszközök kezelése, használata során az alábbi szabályok betartásával kell eljárnia minden felhasználónak:
a) Minden olyan előírást be kell tartani, amely az eszközök kezelési útmutatójában, ennek hiányában az intézmény által kiadott kezelési útmutatóban szerepel.
b) Be kell tartani a szoftverek/dokumentumok használata, illetve létrehozása során a szerzői jogokra vonatkozó jogszabályokat.
c) Be kell tartani a munka-, és tűzvédelmi előírásokat.
d) Tilos az eszközök közelében enni, inni, dohányozni.
e) Tilos szaktantermek, géptermek teljesen területén élelmiszert fogyasztani, vagy azokat kicsomagolt állapotban tartani.
f) Tilos az eszközöket, és azok részeit áthelyezni, burkolatukat, elektromos csatlakozását megbontani.
g) Tilos a számítógépre szoftvert telepíteni, illetve engedély nélkül letörölni.
h) A felhasználók kötelesek minden meghibásodást, egyéb igényt írásban jelezni - a főtitkár egyidejű értesítése mellett - a rendszergazdának, az it@mtf.hu e-mail címen.
i) Elektromos meghibásodás, pl. zárlat gyanúja esetén az eszközt áramtalanítani kell. Ha a meghibásodás a gépterem elektromos hálózatában keletkezik, úgy az egész géptermet áramtalanítani kell a főkapcsolóval.
(5) Az eszközök használatát az arra kijelölt személy (tanár, oktató, rendszergazda) ismerteti. A feladata az eszközök kezelésének bemutatása, az ahhoz kapcsolódó speciális tudnivalók ismertetése is. Minden felhasználó csak azokat az eszközöket használhatja, amelyek használatára engedélyt kapott, és amelynek kezelésére kioktatták. A használható eszközök körének meghatározása a felhasználói jogosultság kiadásával párhuzamosan történik.
(6) Az intézmény felhasználói kötelesek oly módon használni a hálózatot, hogy magatartásukkal az intézmény hitelét, jó hírét és érdekeit ne sértsék.

5. Jogosultságok

6. § (1) Az eszközök használatának módját a felhasználói jogosultság szabályozza. A felhasználók különböző jogosultságokkal rendelkezhetnek, melyeket jelen szabályzat alapján, a meghatározott jogosultsági szinteknek megfelelően kell meghatározni. A minimum jogosultsági szint mindenkit megillet, aki az intézménnyel hallgatói vagy közalkalmazotti, illetve munkavégzésre irányuló egyéb jogviszonyban áll, és aláírásával igazolja, hogy a szabályzat tartalmát megismerte, annak betartását vállalja.
(2) Minimum jogosultsági szint adható, pl. előkészítő évfolyam esetén az intézménnyel hallgatói jogviszonyban nem állók részére is. A további jogosultsági szinteket a minimum szint kiegészítéseként kell értelmezni.
(3) Az egyedi igényeket a munkahelyi felettestől kell kérni, aki továbbítja az igényt a rendszergazdának.
(4) A felhasználótól a jogosultsági szintjének megfelelő jogot megtagadni csak indokolt esetben lehet. A jogosultsági szinteknek megfelelő szabályok betartása a lokális hálózati eszközök használata esetén is kötelező.

(5) A felhasználói jogosultságok szintjei:

SZINT:	JOGOSULTAK:	JOGOK:
Hallgató (minimumjogok)	Az intézmény bármely hallgatója, előkészítő évfolyam növendéke, vendég	Általános azonosító, mely lehetővé teszi az oktatáshoz, munkához szükséges adatok elérését, Internet használat
Alap	Az intézmény bármely alkalmazottja	Egyéni azonosító, Internet használat, saját könyvtár a szerveren
Oktató, tanár	Az intézmény oktatói, kutatói, tanárai	Alap + hozzáférés a tanári könyvtárakhoz és a tanulókkal kapcsolatos adminisztrációs adatokhoz
Gazdasági Hivatal	A Gazdasági Hivatal dolgozói	Alap + hozzáférés a gazdálkodással és a dolgozókkal kapcsolatos adatokat tartalmazó könyvtárakhoz
Rektori Hivatal	A Rektori Hivatal alkalmazottai	Alap + hozzáférés a munkaköri feladatok által meghatározott, szükséges adatbázisokhoz, a jogosultságoknak megfelelően
Tanulmányi Osztály	Tanulmányi osztályok alkalmazottai	Alap + hozzáférés a hallgatói tanulmányi adatokat tartalmazó könyvtárakhoz
Könyvtár	Könyvtár alkalmazottai	Alap + hozzáférés a könyvtári adatállományokat tartalmazó könyvtárakhoz
Adminisztrátor	Az adott feladatra kijelölt személy	Speciális jogok, pl. a levelező rendszer, vagy a web oldalak karbantartásával kapcsolatos feladtok ellátásához
Rendszergazda	Az intézmény rendszergazdája	Korlátlan jog

(6) A speciális feladatok (pl. postamesterség, webmesterség stb.), illetve az azokhoz tartozó jogok alapértelmezésben a rendszergazdát illetik meg. Ezek a jogok egy-egy jól elhatárolható hálózati adminisztrációs feladat elvégzéséhez rendelhetők, s a rendszergazda beleegyezésével külön megállapodás alapján más személynek átadhatók. A speciális jogok, illetve az ezekhez tartozó azonosítók magáncélra nem használhatók fel. Ezek használata csak a szükséges rendszeradminisztráció erejéig történhet. Az ehhez szükséges kiemelt jogokat a rendszergazda biztosítja. Amennyiben a rendszergazda úgy ítéli meg, hogy a speciális feladatot ellátó személy a rendszer biztonságát veszélyezteti, úgy joga van a kiemelt jogok használati lehetőségét felfüggeszteni. A felfüggesztés tényéről és okairól köteles haladéktalanul beszámolni az érintett személy munkahelyi felettesének.
(7) Az intézményben a lokális hálózatok eszközeinek használati rendjét a szabályzat alkalmazásán felül az alábbi személyek hivatottak meghatározni:

Rektori Hivatal	Főtitkár
Gazdasági Hivatal	Gazdasági főigazgató
Intézetek	Intézetigazgatók
Tanszékek	Tanszékvezetők
Tanterem	Oktatásvezető tanár

(8) A felhasználók a számítógép-hálózat szolgáltatásait a felhasználói azonosító és az ahhoz tartozó jelszó segítségével vehetik igénybe. Az egyéni azonosítók igénylésének módja, feltételei és használatukkal kapcsolatos részletes tudnivalók az informatikai beléptető jegyen vannak feltüntetve.
(9) A felhasználói azonosítók kezelésének szabályai:

a) Minden felhasználó csak a saját azonosítójával használhatja a hálózatot.
b) Minden felhasználó felel a rábízott felhasználói azonosító és az ahhoz rendelt jogok biztonságáért.
c) Az azonosító használatát még a tulajdonos jelenlétében sem lehet átengedni másnak.
d) A felhasználói azonosítóhoz tartozó jelszót csak annak birtokosa ismerheti.
e) Amennyiben felmerül a gyanú, hogy a jelszó mások tudomására jutott, úgy azt azonnal meg kell változtatni.
f) Amennyiben valaki észleli, hogy más kísérletet tesz a felhasználói jelszavak megszerzésére, azt azonnal jelezni kell a rendszergazdának és a munkahelyi felettesnek.
g) Minden más személy jelszavának vagy adatainak megszerzésére irányuló cselekedet fegyelmi felelősségre vonást von maga után.

h) A felhasználói azonosító tulajdonosa elsődlegesen felel az azonosító használatával elkövetett szabálytalanságokért. Akkor is felelősségre vonható, ha bebizonyosodik, hogy azt nem ő használta, de gondatlansága folytán jutott az azonosító illetéktelen személyhez.
i) Ennek érdekében a felhasználó a számítógépes munkahely elhagyásakor minden alkalommal köteles kilépni a hálózatból.
j) A felhasználó jelszó átadását senki sem kérheti, még a rendszergazda sem.

6. Informatikai szolgáltatások

7. § (1) Az informatikai szolgáltatásokat az informatikai csoport nyújtja a szabályzat üzemeltetői előírásainak megfelelően. Az informatikai céllal üzemeltett informatikai eszközök használatával az alábbi szolgáltatások vehetők igénybe:

a) a számítógépekre telepített oktató és irodai szoftverek használata,
b) saját adatterület az adatok és a levelezés tárolására (alapesetben 2 MB),
c) a számítógéppel készített anyagok nyomtatása,
d) internet hozzáférés (elsősorban www, ftp, mail),
e) intranet szolgáltatás (www, fájl szerver),
f) dokumentumok archiválása,
g) dokumentumok másolása, sokszorosítása,
h) dokumentumok digitalizálása.

(2) A felhasználók státuszuk és jogosultságuk szerint vehetik igénybe ezeket a szolgáltatásokat, a szabályzat rendelkezéseinek betartása mellett. A szolgáltatások használata során be kell tartani a szerzői jogokra vonatkozó jogszabályokat is.

a) Központi hálózat, internetelérés
A központi hálózatot az informatikai csoport üzemelteti és fejleszti. Az informatikai csoport végzi a központi IP tartomány felosztását, a központi hálózat passzív és aktív elemeinek konfigurálását, hálózati menedzsmentjét.
b) Web szolgáltatások
A főiskola központi webszerverét és az intézmény hivatalos honlapját az informatikai csoport működteti. A honlap tartalmáért a rektor a felelős, az ő általa megbízott szerkesztők jogosultak a tartalom létrehozására, módosítására és törlésére.
A főiskola tanszékeinek és egyéb egységeinek lehetőségük van saját információk publikálására, a megbízott szerkesztők közreműködésével. Ebben az esetben a megjelenített tartalomért az adott szervezeti egység vezetője a felelős.
A meglévő domain nevekkel kapcsolatos feladatokat az informatikai csoport látja el, új domain regisztrálására a rektor adhat engedélyt.
Intranet szolgáltatás
c) A főiskola anyagi lehetőségeihez mérten gondoskodik az intranet kiépítéséről, üzemeltetéséről.
A szolgáltatást a főiskola oktatói és nem oktató dolgozói vehetik igénybe. Az intranet elsősorban a nem publikus, illetve munkafázisban lévő dokumentumok tárolására és megosztására, továbbá belső hírek, információk közzétételére szolgál. Az intranet üzemeltetését az informatikai csoport végzi, tartalmát a Rektori Hivatal megbízott munkatársa szerkeszti.
d) Fájl- és adatbázis szerver szolgáltatás
A csoportmunka, valamint a hálózati alkalmazások használatának elősegítésére az informatikai csoport fájl- és adatbázis szervereket üzemeltetnek. A szervereken lehetőség van intézményi egységek közös dokumentumainak, állományainak elhelyezésére, minden munkatárs által elérhető multimédiás tartalmak, adatbázisok közzétételére, munkaállomások mentéseinek tárolására.
e) Intézményi alkalmazások üzemeltetése
Az intézmény saját szerverein üzemeltet olyan egyedi alkalmazásokat, melyek egy vagy több egység feladatainak ellátásához szükségesek (pénzügyi alkalmazások, tanulmányi rendszerek). A szolgáltatás magában foglalja a szerver és kliens oldali szoftver komponensek installálását, karbantartását, frissítését, jogosultságok beállítását, a rendszer biztonsági mentését.
f) Elektronikus levelezési szolgáltatás
A főiskola oktatói, tanárai, valamint az egyéb munkakörben alkalmazottjai jogosultak a levelezési szolgáltatás használatára. Levelezési címeket az informatikai csoporttól lehet igényelni az alábbi címképző irányelvek figyelembe vételével:
- az általános felhasználói e-mail cím vezeteknev.keresztnev@mtf.hu alakú,
- egyes esetekben funkcióhoz kapcsolódó e-mail címek is kioszthatók, pl. rektor@mtf.hu,

- szükség esetén az intézményi egységek a saját nevükre utaló címet, vagy alias-t használhatnak, pl. tanulmanyi@mtf.hu

g) Rendszerüzemeltetési szolgáltatás
Az informatikai csoport az alábbi üzemeltetési szolgáltatásokat nyújtja a felhasználók részére:
- munkaállomások installálása, felügyelete, karbantartása,
- perifériák telepítése, karbantartása,
- vírusvédelmi eszközök üzemeltetése,
- hardver- és szoftverhibák elhárítása,
- biztonsági mentés elvégzése, visszatöltése,
- alkalmazói szoftverek használatával kapcsolatos tanácsadás,
- ügyfélszolgálat (helpdesk).

II. Rész

AZ INFORMATIKAI BIZTONSÁG RENDJE

7. Bevezető rendelkezések

8. § (1) A főiskola az intézményben működtetett informatikai rendszerekre, a tárolt adatokra és információfeldolgozásra vonatkozóan szabályozza az információbiztonsággal kapcsolatos elveket, szabályokat, ezért az informatikai rendszerrel kapcsolatos biztonsági intézkedéseket, valamint az elvárt magatartásformákat és betartandó gyakorlatot az alábbiakban határozza meg:

8. Az informatikai biztonság szabályozásának célja

9. § (1) A szabályozás 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 szabályozás célja továbbá:

a) a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
b) az üzemeltetett informatikai rendszereket fenyegető veszélyek megelőzése, elhárítása,
c) az üzembiztonságot szolgáló karbantartás és fenntartás,
d) az adatok feldolgozása és további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
e) az adatállományok tartalmi és formai épségének megőrzése,
f) az adatállományok biztonságos mentése,
g) az informatikai rendszerek zavartalan üzemeltetése,
h) az adatvédelem és adatbiztonság feltételeinek megteremtése.

(2) A jelen szabályozással megvalósuló információbiztonsági politika célja, hogy a főiskola szervezeti egységei részére egységes és általános értelmezést adjon az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége, rendelkezésre állása és funkcionalitása biztosítása érdekében követendő irányelvekre. Az irányelvek figyelembe vételével meghatározható az informatikai biztonsági szabályozás alapján minősített adatokat kezelő informatikai rendszerek biztonsági osztályba sorolása; kidolgozhatóak a konkrét, rendszer szintű informatikai biztonsági szabályozások, amelyek az informatikai rendszer teljes életciklusában meghatározzák a szabványos biztonsági funkciók tervezéséhez, megvalósításához, üzemeltetéséhez és megszüntetéséhez a szükséges alapelveket és követelményeket.
(3) A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzembe helyezésen keresztül az üzemeltetésig.
(4) A jelen szabályozás az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

9. Az adatkezelés során használt fontosabb fogalmak

10. § (1) Fogalmak

Adatkezelés: az alkalmazott eljárástól függetlenül az adatok 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 rögzítése.
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.
Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.
Adatkezelő: az a természetes vagy jogi személy, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.
Adatfeldolgozó: az a természetes vagy jogi személy, aki vagy amely az adatkezelő megbízásából adatok feldolgozását végzi.
Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele.
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.
A főiskola számítógépes hálózata: részét képezik a következő típusú eszközök: adatátviteli vonalak (típusuk szerint Ethernet, optikai), aktív és passzív hálózati elemek, továbbá minden hálózatra kötött számítógépes munkahely (PC, hálózati nyomtató) és szerver függetlenül attól, hogy az mely főiskolai egység tulajdonában vagy használatában van.
Eszköz: informatikai eszköz (számítógép, szerver, nyomtató, passzív és aktív hálózati elem)
Felhasználó: az a személy, aki a főiskola valamelyik informatikai szolgáltatását igénybe veszi.
IT szolgáltatás: a Főiskolán használt IT rendszerrel nyújtott szolgáltatás.
Adatvédelem: az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény hatálya alá eső adatkör védelme.
Biztonsági esemény: Az informatikai rendszer védelmi állapotában beállt illetéktelen változás, melynek hatására az informatikai rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.
Informatikai biztonság: Az informatikai biztonság az az állapot, amikor az informatikai rendszer által kezelt adatok védelme — bizalmasság, hitelesség, sértetlenség, rendelkezésre állás és funkcionalitás szempontjából — zárt, teljes körű, a kockázatokkal arányos és folyamatos.

- Teljes körű a védelem, ha a védelmi intézkedések az informatikai rendszer összes elemére, az ISO/OSI szabvány szerinti összes rétegére, valamint a végpontok közötti összes elemre kiterjednek.
- Zárt a védelem, ha az összes releváns fenyegetés figyelembe lett véve a védelmi intézkedések megtervezésénél és megvalósításánál.
- Folyamatos a védelem, ha az időben változó körülmények és viszonyok ellenére is megszakítás nélkül valósul meg.
- Kockázattal arányos a védelem, ha kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékek összegével és a megvalósított védelmi intézkedések következtében a kockázatok elviselhető mértékűre mérséklődtek.

Rendelkezésre állás: annak a valószínűsége, hogy egy definiált időintervallumon belül az alkalmazás a tervezéskor meghatározott funkcionalitási szintnek megfelelően a felhasználó által használható.
Funkcionalitás: az informatikai rendszer megfelelő tervezésének és üzemeltetésének köszönhetően az adat tartalmi és formai használhatóságának biztosítása.
Információvédelem: az informatikai rendszerek által kezelt adatok által hordozott információk védelme a bizalmasság, a hitelesség és a sértetlenség sérülése, elvesztése ellen. Az információvédelem az informatikai biztonság egyik alapterülete.

Megbízható működés: az informatikai rendszerek által kezelt adatok által hordozott információk védelme a rendelkezésre állás, és a funkcionalitás sérülése, elvesztése ellen. A megbízható működés az informatikai biztonság másik alapterülete.
Informatikai biztonságpolitika: A főiskola informatikai biztonságpolitikája az intézmény minden munkatársa és az informatikai rendszer minden felhasználója számára meghatározza, hogy az informatikai rendszerek által kezelt adatok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzésével kapcsolatosan milyen biztonsági elveket, szabályokat és előírásokat kell betartani.
ISO/OSI szabvány: A Nemzetközi Szabványosítási Szervezet (ISO) által kibocsátott a nyílt informatikai rendszerek összekapcsolását lehetővé tevő architektúrára vonatkozó ISO/OSI 7498-1 (magyar megfelelője: MSZ OSI 7498-1) szabvány illetve a nyílt rendszerek biztonsági architektúrájára vonatkozó ISO/OSI 7498-2 (magyar megfelelője: MSZ OSI 7498-1) szabvány.
Üzletmenet-folytonosság és katasztrófa-elhárítás tervezés: Az informatikai rendszer és a benne kezelt adatok, valamint a környezetüket képző összes rendszerelem csoportra vonatkozó védelmi intézkedések meghatározására irányuló tervezési tevékenység üzemzavarok és katasztrófa esetére. A védelmi intézkedések érvényesítésével az adatok védelme és/vagy visszaállíthatósága valósítható meg üzemzavar vagy katasztrófa események estén. Angol nyelvű elnevezése: Business Continuity Planning (rövidítése: BCP) és Disaster Recovery Planning (rövidítése: DRP).
Kockázat: A fenyegetettség mértéke, amely valamely fenyegető tényezőből ered, és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázatot a kárnagyság és a bekövetkezés gyakoriság szorzataként definiáljuk egy megadott időtávon.
Szolgáltatásért felelős szervezeti egység: az IT és telekommunikációs szolgáltatás nyújtására alkalmas infrastruktúrával rendelkező önálló szervezeti egység, mely az adott szolgáltatás nyújtásának feltételeit a felhasználók számára nyilvánosságra hozza.
DRP: Disaster Recovery Plan – Katasztrófa utáni helyreállítási terv: magába foglalja az üzletmenet működés szempontjából kritikus adatok, hardver, és szoftver működésének újraindítását természeti vagy ember által okozott katasztrófák esetén.
BCP: Business Continuity Plan – Üzletmenet (működés) folytonossági terv: az üzletmenet működés fenntartása érdekében teendő intézkedések összessége, ha az adott üzleti folyamat vagy alkalmazás végrehajtása, működtetése valamilyen természeti vagy ember által okozott katasztrófa miatt akadályokba ütközik.
SLA: Service Level Agreement – Szolgáltatási szint megállapodás: egy olyan írásos megállapodás, mely két fél között jön létre: a szolgáltató (a jelen szabályzat alkalmazása során a szolgáltatásért felelős szervezeti egység) és a szolgáltatás felhasználója között. Az SLA meghatározza a két fél között nyújtandó szolgáltatás tartalmát és feltételeit.
ITIL: Information Technology Infrastructure Library: egy olyan nemzetközileg elfogadott keretrendszer (de facto szabvány), mely a magas szintű IT szolgáltatások nyújtását a „legjobb gyakorlatok gyűjteménye" elv mentén szabályozza. Az ITIL olyan üzleti (működési) folyamatokat ír le, melyek mind a minőségi mind a gazdaságos szolgáltatás elérését támogatják az informatika területén.
Incidens: A szolgáltatás standard működésétől eltérő esemény, mely fennakadást vagy minőségcsökkenést okoz, vagy okozhat a szolgáltatásban.
Probléma: A probléma egy állapot, mely gyakran több hasonló tünetet produkáló incidens alapján ismerhető fel. A probléma azonosítható lehet egyetlen jelentős incidens alapján is, mely valamilyen hibára utal, melynek oka nem ismert, de hatása jelentős.

10. Az informatikai rendszerek biztonsági besorolásai

11. § (1) A főiskola adatai különböző biztonsági fokozatba tartozhatnak. (üzleti titkok, pénzügyi adatok, illetve a főiskola belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas adatok).
(2) Kritikus rendszerek (A)
Az intézmény működése szempontjából kritikus, az intézmény egészére kiterjedő rendszerek, amelyek szenzitív, illetve személyes adatokat tartalmaznak. Adatvédelmi szempontból kiemelt védelmet igényelnek.

a) Bér- és Munkaügyi rendszer,
b) Gazdasági, ügyviteli rendszer,
c) Dokumentumkezelési, iktatási rendszer,
d) Tanulmányi rendszer,
e) Központi levelezési rendszer,
f) Intézményi szerver (web, mail, authentikációs, stb) kiszolgálók.

(3) Kiemelt rendszerek (B)
Az intézmény működése szempontjából kiemelt rendszerek, amelyek elsősorban technikai jellegűek, a rajtuk tárolt adatok nem személyes jellegűek.

a) Telekommunikációs hálózat,
b) Kommunikációs rendszerek.

(4) Normál rendszerek (C)

A vagy B kategóriába nem sorolt, az intézmény napi működése szempontjából nem kritikus vagy kiemelt, illetőleg az intézménynek csak egyes részeire kiterjedő rendszerek:

a) Informatikai terem
b) Könyvtári rendszer

11. Védelmet igénylő, az informatikai rendszerre ható elemek

12. § (1) Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.

(2) Az informatikai rendszerre az alábbi tényezők hatnak:

a) a környezeti infrastruktúra,
b) a hardver elemek,
c) az adathordozók,
d) a dokumentumok,
e) a szoftver elemek,
f) az adatok,
g) a rendszerelemekkel kapcsolatba kerülő személyek.

(3) A védelmi intézkedések kiterjednek:

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

(4) 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.

12. Felelősségi körök

13. § (1) Az informatikai biztonsági politikának ki kell fejeznie a vezetés elkötelezettségét az általános biztonság és az informatikai biztonság megfelelő szintjének kialakítása és fenntartása mellett.

(2) A főiskola intézményi szintű vezetése, illetve a főiskola további vezetői felelősek a saját területükön az informatikai biztonsági szabályokban foglaltak betartatásáért.

(3) Az adatvédelem felelősei az informatikai csoport tagjai, a rendszergazdák, akik információbiztonsági kérdésekben a főtitkárnak tartoznak beszámolási kötelezettséggel.

(4) A főiskola informatikai rendszerének felhasználói (rendszergazdák, munkatársak, hallgatók, vendégek, külső felhasználók) kötelesek betartani a jelen szabályzatban leírtakat, továbbá kötelesek jelenteni az informatikai csoportnak, ha biztonsági problémát okozó jelenséget (biztonsági incidenst) észlelnek.

13. Adatvédelmi felelősök feladatai

14. § (1) Az informatikai csoport feladatai:

a) az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
b) javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására.
c) meghatározza a védett adatok körét,
d) ellátja az adatkezelés és adatfeldolgozás felügyeletét,
e) ellenőrzi a védelmi előírások betartását,
f) az adatvédelmi feladatok ismertetése,
g) évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását,
h) ellenőrzi a szoftverek használatának jogszerűségét.

(2) A rendszergazda információbiztonsággal kapcsolatos feladatai:

a) a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli,
b) felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
c) gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,

d) feladata a védelmi eszközök működésének folyamatos ellenőrzése,
e) gondoskodik a folyamatos vírusvédelemről
f) a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
g) folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
h) javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére,
i) ellenőrzi a rendszer adminisztrációját.

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

15. § (1) Az adatok és információk jelentőségük és bizalmassági fokozatuk szerint osztályozhatóak:
a) közlésre szánt, bárki által megismerhető adatok,
b) minősített, titkos adatok.
(2) Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek az adat az érdekkörébe tartozik.
(3) Az adatok feldolgozásakor meg kell határozni a hozzáférési jogosultságot. A kijelölt dolgozók előtt az adatvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.
Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.
(4) Az információhoz való hozzáférést lehetőség szerint a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység – adatbázisokhoz való hozzáférés, a fájlba vagy mágneslemezre történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető.
(5) Az adatok védelmét, a feldolgozás – az adattovábbítás, a tárolás - során az operációs rendszerben és a felhasználói programban alkalmazott, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver adatvédelem).

15. Az informatikai eszközbázist veszélyeztető helyzetek

16. § (1) 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.
(2) Környezeti infrastruktúra okozta ártalmak
a) elemi csapás:
b) földrengés,
c) árvíz,
d) tűz,
e) villámcsapás, stb.
f) környezeti kár:
g) légszennyezettség,
h) nagy teljesítményű elektromágneses térerő,
i) elektrosztatikus feltöltődés,
j) a levegő nedvességtartalmának felszökése vagy leesése,
k) piszkolódás (pl. por).
l) közüzemi szolgáltatásba bekövetkező zavarok:
m) feszültség-kimaradás,
n) feszültségingadozás,
o) elektromos zárlat,
p) csőtörés.
(3) Emberi tényezőre visszavezethető veszélyek
Szándékos károkozás:
a) behatolás az informatikai rendszerek környezetébe,
b) illetéktelen hozzáférés (adat, eszköz),
c) adatok- eszközök eltulajdonítása,
d) rongálás (gép, adathordozó),
e) megtévesztő adatok bevitele és képzése,
f) zavarás (feldolgozások, munkafolyamatok).
Nem szándékos, illetve gondatlan károkozás:
a) figyelmetlenség (ellenőrzés hiánya),
b) szakmai hozzá nem értés,

c) a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
d) a megváltozott körülmények figyelmen kívül hagyása,
e) vírusfertőzött adathordozó behozatala,
f) biztonsági követelmények és gyári előírások be nem tartása,
g) adathordozók megrongálása (rossz tárolás, kezelés),
h) a karbantartási műveletek elmulasztása.

(4) A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

16. Az informatikai eszközök környezetének védelme

17. § (1) Védett helyiségnek kell tekinteni azokat a helyiségeket, ahol a bizalmas adatok feldolgozására, tárolására alkalmazott informatikai erőforrások találhatók. A védett területek zárt területnek minősülnek, ezért védelmükről ennek megfelelően kell gondoskodni.

A főiskolán védett területnek minősül:

a) szerverhelyiség,
b) aktív hálózati elemek elhelyezésére szolgáló helyiség (rendező), rack szekrény,
c) Gazdasági Hivatal,
d) Rektori Hivatal,
e) Informatikai Csoport.

(2) Vagyonvédelmi előírások

a) a szerverhelyiségeket és a (rendező) rack szekrényeket biztonsági zárakkal kell felszerelni,
b) a szerverhelyiségbe és az aktív hálózati elemek elhelyezésére szolgáló helyiségbe való be- és kilépés rendjét szabályozni kell,
c) a fenti védett területekre történő illetéktelen behatolás tényét az intézmény vezetőjének azonnal jelenteni kell,
d) az informatikai eszközöket csak a megfelelő jogosultsággal rendelkező felhasználók használhatják,

(3) Az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

(4) Tűzvédelem

a) A szerverhelyiség a „D" mérsékelt tűzveszélyességi osztályba tartozik.
b) A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.
c) A szerverhelyiségbe biztosítani kell a megfelelő tűzoltó készüléket.
d) A nagy fontosságú, pl. törzsadat-állományokat két példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni. Ezen adatállományok kijelölése a szervezeti egységek vezetőinek a feladata.

17. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

18. § (1) A számítógépek és szerverek védelme

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

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

(2) Hardver védelem

a) A berendezések hibátlan és üzemszerű működését biztosítani kell.
b) A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.
c) Az üzemeltetést, karbantartást és szervizelést az informatikai csoport végzi, esetenként külső szerviz szolgáltatás igénybevételével.

(3) A munkák szervezésénél figyelembe kell venni:

a) a gyártó előírásait, ajánlásait,
b) a tapasztalatokat.

18. Az informatikai feldolgozás folyamatának védelme

19. § (1) Az adatrögzítés védelme:

a) adatbevitel hibátlan műszaki állapotú berendezésen történjen,
b) tesztelt adathordozóra lehet adatállományt rögzíteni,
c) a bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
d) 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.

(2) Adathordozók védelme

a) az adathordozókat a tűz- és vagyonvédelmi előírásokat betartva olyan módon kell elhelyezni, hogy tárolás közben ne sérüljenek, károsodjanak,
b) az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről az egységeknek nyilvántartást kell vezetni,
c) a használni kívánt adathordozót a tárolásra kijelölt helyről kell kivenni, és használat után oda kell visszahelyezni,
d) a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,
e) adathordozót másnak átadni csak engedéllyel szabad.

(3) Adathordozók megőrzése, másolása, leltározása

a) az adathordozók megőrzési idejét a törvényekben meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani,
b) sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni: biztonsági illetve archív adatállomány előállítása másolásnak számít,.
c) a szoftvereket és adathordozókat a leltározási szabályzatban foglaltaknak megfelelően kell leltározni.

(4) Mentések, file-ok védelme

a) az adatfeldolgozás után biztosítani kell az adatok mentését,
b) a munkák során létrehozott általános dokumentumok mentése az azt létrehozó felhasználók feladata,
c) a felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie, az archiválásban az informatikusoknak kell segítséget nyújtani,
d) a szervereken tárolt adatokról a mentést rendszeresen el kell végezni, a mentésért a rendszergazdák a felelősek.

(5) Programhoz való hozzáférés, programvédelem

a) az informatikai csoportnak biztosítani kell, hogy a rendszerszoftverek naprakész állapotban legyenek és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára,
b) a kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni,
c) gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

(6) Programok nyilvántartása

A programokról a leltározásért felelős szervezeti egységnek naprakész nyilvántartást (szoftver leltárt) kell vezetni.

19. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

20. § (1) Központi gépek

a) Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.
b) A központi gépek háttértárairól folyamatosan biztonsági mentést kell készíteni.
c) Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.
d) A vásárolt szoftverekről biztonsági másolatot kell készíteni.

(2) Munkaállomások

a) Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
b) Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell.
c) A főiskola informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.
d) Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.
e) Az informatikai eszközt és tartozékait helyéről elvinni csak az eszköz leltárfelelőse tudtával és engedélyével szabad.

20. Informatikai biztonsági ellenőrzés

21. § (1) Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése illetve annak megakadályozása, hogy az megismétlődjön.
(2) A munkafolyamatba épített ellenőrzés során az IBSZ rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

III. Rész

A SZOFTVERHASZNÁLAT RENDJE

21. A szoftverhasználattal kapcsolatos fogalmak

22. § (1)Szoftverrel kapcsolatos fogalmak

a) A szoftver: a számítógépi programalkotás és a hozzá tartozó dokumentáció (a továbbiakban: szoftver) akár forráskódban, akár tárgykódban vagy bármilyen más formában rögzített minden fajtája, ideértve a felhasználói programot és az operációs rendszert is.

b) A szoftverek beszerzése és használata során figyelembe kell venni a szerzői jogra vonatkozó rendelkezéseket, és a szoftvert kísérő licenc szerződés feltételeit.
A licenc szerződés megsértésével törvénysértést követ el:
- aki a szoftvert, vagy annak dokumentációját, beleértve a programokat, alkalmazásokat, adatokat, kódokat és kézikönyveket a szerzői jog tulajdonosának engedélye nélkül lemásolja vagy terjeszti;
- aki szerzői jog által védett szoftvert egyidejűleg két vagy több gépen futtat, hacsak ezt a szoftver licenc szerződése külön nem engedélyezi;
- az a szervezet, amely tudatosan vagy akaratlanul munkatársait arra ösztönzi, kötelezi, vagy számukra megengedi, hogy illegális szoftvermásolatokat készítsenek, használjanak, vagy terjesszenek;
- aki az illegális szoftvermásolást tiltó törvényt megsérti azért, mert valaki erre kéri vagy kényszeríti;
- aki szoftvert kölcsön ad úgy, hogy arról másolatot lehessen készíteni, vagy aki a kölcsönkért szoftvert lemásolja;
- aki olyan eszközöket készít, importál, vagy birtokol, amelyek lehetővé teszik a szoftver védelmét szolgáló műszaki eszközök eltávolítását, vagy ilyen eszközökkel kereskedik.

(2) Értelmező rendelkezések

a) Szellemi tulajdon: A törvény szerint az eredeti számítógépes program az azt létrehozó személy vagy vállalat szellemi tulajdona. A számítógépes programokat szerzői jogi törvény védi, amely kimondja, hogy az ilyen művek engedély nélküli másolása törvénybe ütköző cselekedet.

b) Szoftver licenc szerződés: Egy adott szoftver esetében a licenc szerződés határozza meg a szerzői jog tulajdonosa által megengedett szoftverhasználat feltételeit. A szoftverhez adott licenc szerződésre külön utalás történik a szoftver dokumentációjában, vagy a program indításakor megjelenő képernyőn is. A szoftver ára tartalmazza a szoftver licencét, és megfizetése kötelezi a vevőt, hogy a szoftvert kizárólag a licenc szerződésben leírt feltételek szerint használja.

c) Jogosulatlan másolás: A szoftver licenc szerződés, amennyiben eltérően nem rendelkezik, a vevőnek csak egyetlen "biztonsági" másolat készítését engedélyezi, arra az esetre, ha az eredeti szoftver lemeze meghibásodna, vagy megsemmisülne. Az eredeti szoftver bármely további másolása jogosulatlan másolásnak minősül, és megsérti a szoftvert védő és használatát szabályozó licenc szerződést, valamint a szerzői jogi törvényt.

d) Illegális szoftverhasználat: Az illegális szoftverhasználat azt jelenti, hogy valaki egy számítógépes programot jogosulatlanul másol le és használ, ezzel megsértve a szerzői jogi törvényt, valamint a szerzőnek a szoftver licenc szerződésben leírt feltételeit. Aki szoftvert illegálisan használ, az a szerzői jogi törvény értelmében büntetőjogi törvénybe ütköző cselekedetet követ el.

e) Új szoftver beszerzések:
- Az egyedi beszerzéssel, ajándékozással, pályázat útján megszerzett szoftver.
- Amennyiben egy eszköz beszerzése során az ár már tartalmazza (OEM- Original Equipment Manufacturer) a szoftver árát.
- Már meglévő termék frissítése (UPGRADE), vagy

– bármilyen más törvényes módon megszerzett szoftver.

22. Általános rendelkezések

23. § (1) A főiskolán tilos az szerzői jogról szóló törvénybe ütköző szoftverhasználat.
(2) Az egység vezetője, illetőleg megbízottja felel az érintett szervezeti egységeknél és az ott elhelyezett eszközök tekintetében a legális szoftvergazdálkodásért, amit ezen szabályzat betartásával és betartatásával valósít meg.
(3) A főiskola nevében beszerzett licencek hasznosításáról, illetve a szervezeti egység által beszerzett szoftver szervezeti egységen kívüli hasznosításáról – amennyiben azt licencszerződés lehetővé teszi, és a szervezeti egység ehhez hozzájárul – az informatikai csoport javaslata alapján az illetékes vezető dönt. Az informatikai csoport javaslatot tehet a szoftver licencek újrahasznosításáról, amennyiben azt szakmai indokok alátámasztják.
(4) Az e szabályzatban nem szabályozott kérdésben az informatikai csoport javaslata alapján az illetékes vezető jogosult dönteni, és a szükséges intézkedéseket megtenni.
(5) Az informatikai csoport gondoskodik a jogtiszta szoftverhasználat érdekében történő alkalomszerű, – de legalább évenkénti – ellenőrzésről. Az ellenőrzésekről jegyzőkönyv készül, ami a szükséges intézkedések megtételére is javaslatot tesz, amit az illetékes vezetőnek és a főtitkárnak kell átadni.

23. Szoftverhasználattal kapcsolatos kötelességek és jogok

24. § (1) A rendszergazda kötelességei:
a) A számítógép által futtatott szoftverek telepítése, konfigurálása (A számítógép beépített gyári szoftverét is beleértve) a felhasználó(k) igényei szerint;
b) A telepítés során tájékoztatja a felhasználót, az egység vezetőjét, a szoftver licencében rögzített jogokról és kötelezettségekről;
c) Amennyiben a szoftvert a gyártó kívánja telepíteni, akkor ezt csak a rendszergazda jelenlétében végezheti. Az egyedi fejlesztésű programok gyártó által történő telepítése esetén a rendszergazda ellenőrzi, hogy csak a szerződésben szereplő legális szoftverek kerülnek telepítésre;
d) Már meglévő szoftvereket azonnali hatállyal nyilvántartásba venni;
e) A szoftverállományban történő változást (új szoftver beszerzését, stb.) az informatikai csoport által karbantartott nyilvántartásban két héten belül a kötelező adatszolgáltatás eredményeképpen fel kell venni, illetve aktualizálni kell.
f) Rendszeresen ellenőrzi a szoftverhasználatot.

(2) A rendszergazda jogai:
a) Új szoftver telepítése csak a rendszergazda – vagy az általa megbízott személy – jogosult;
b) A rendszergazda – jogainak védelme érdekében – jogosult technikai korlátozások bevezetésére;
c) A rendszergazda a számítógép használójának felügyelete mellett rendszeresen és alkalomszerűen ellenőrzi az adott szervezeti egységen belül a szoftverek legalitását, a vonatkozó rendelkezések betartását. Az ellenőrzésről jegyzőkönyvet készít, melyet az egység vezetőjének ad át.
d) A rendszergazda szoftverhasználattal kapcsolatos mindennemű felelőssége megszűnik, ha azt nem ő telepítette. A rendszergazda köteles a felelősség megszűnését és a kiváltó okokat az egység vezetőjének írásban bejelenteni.

(3) Az egységek vezetőjének kötelessége:
a) A főiskola szoftverhasználati alapelveit tartalmazó Szoftver Etikai Kódexet (2. melléklet) az alkalmazottakkal ismertetni, betartását ellenőrizni.
b) Biztosítja a jogtiszta szoftverek hatékony felhasználását.

Az egységek vezetői a szoftverhasználattal kapcsolatos további teendőiket saját hatáskörben hozott egyedi döntésekkel határozzák meg, amelyek nem lehetnek ellentétesek a hatályos jogszabályokkal, és jelen szabályzat rendelkezéseivel.
(4) Az informatikai csoport feladata
a) bizonyos szoftverek adatait, hozzáférhetőségét az intézmény dolgozói körében nyilvánosságra hozza – a kellő licenc számának erejéig;
b) a szervezeti egységeknek tanácsot ad a szoftverbeszerzés területén;

(5) A dolgozók otthoni és a hallgatók saját használatában lévő számítógépek tekintetében, a szoftverhasználat rendjére az éppen aktuális felsőoktatási szoftver keretszerződések az irányadóak.

24. Szoftverek nyilvántartása

25. § (1) Az egységek nyilvántartásának tételesen fel kell sorolnia – amennyiben licenc szerződés nem tiltja - a rendelkezésére álló szoftver licenceket az alábbi adatok feltüntetésével:

a) tételazonosító sorszám;
b) a szoftver gyártója;
c) a szoftver neve;
d) a szoftver verziószáma;
e) a szoftver leírása;
f) a szoftver azonosító sorszáma, szériaszáma;
g) a szükséges hardver környezet;
h) a szükséges operációs rendszer, szoftverkörnyezet;
i) a licenc feltételei: Kik, hányan, hány számítógépen, mettől, meddig használhatják;
j) a szoftver típusa (OEM, frissítés);
k) ezen szoftver alapján frissített szoftver tételazonosítójának sorszáma;
l) a dokumentációt, illetve az eredeti adathordozót birtokló szervezeti egység megnevezése.

25. Adatkezelés, adatvédelem

26. § (1) Az informatikai eszközök használata során a felhasználók kötelesek betartani az adatkezelésre és adatvédelemre, a közérdekű adatok nyilvánossága vonatkozó jogszabályt, valamint a főiskola SZMSZ- ében és egyéb szabályzataiban foglaltakat.

(2) Az adatbiztonság érdekében:

a) A főiskola az adatok védelmét a személyhez fűződő jogok tiszteletbetartásával és az adatvédelmi törvénynek megfelelően biztosítja.
b) A főiskolán nyilvántartott személyes adatokról tájékoztatást, a tárolt adatokhoz való hozzáférést – az érintett személyen kívül – csak az arra jogosult szervnek vagy személynek lehet biztosítani.
c) Az érintett személy, szervezeti egység tény- és adathelyesbítést kérhet.
d) A főiskola informatikai eszközein csak a jogszabályokban megengedett adatokat lehet kezelni.
e) A főiskola informatikai eszközeit technikailag és jogilag védeni kell a külső behatolás ellen.

(3) Szerzői és rokon jogokkal védett anyagok kezelése érdekében a főiskola informatikai rendszerébe jogszabályban, szerződésben biztosított felhasználási jog alapján, illetve megfelelő licencengedély birtokában lehet programokat telepíteni.

(4) A főiskola informatikai rendszerén nem helyezhetők el:

a) az emberi és személyiségi jogokba ütköző, diszkriminatív (kirekesztő) jellegű,
b) ifjúság- és természetellenes, pornográf (szeméremsértő) jellegű,
c) politikai és harcászati célú, az erőszak bármely formáját propagáló,
d) reklámozásra és más üzleti célra felhasználható,
e) a főiskolának, közvetlen környezetének, a főiskola jó hírnevének, a főiskola polgárainak anyagi vagy erkölcsi kárt okozó, információk.

(5) A felhasználó adatvédelemmel kapcsolatos kötelezettségei:

a) Minden felhasználó köteles a biztonságos adatkezelésre vonatkozó általános és helyi előírások betartására.
b) A felhasználók az intézmény hivatalos és nem hivatalos dokumentumait csak előzetes engedély alapján vihetik ki az intézményből.
c) Az intézmény eszközeivel csak az intézmény számára és személyes célra készíthetők dokumentumok. A személyes célra készült dokumentumok nem szolgálhatnak anyagi haszonszerzés, vagy politikai propaganda céljául.
d) A felhasználók adatai az eszközök meghibásodása, vagy bármely más okból megsérülhetnek. Az ebből származó károkért az intézmény felelősséget nem vállal.

(6) A felhasználó adatvédelemmel kapcsolatos jogai:

a) A felhasználó jogosultsága alapján saját adatterülettel rendelkezhet az intézmény szerverén, mely mások számára nem elérhető.
b) A felhasználó jogosultsága alapján saját e-mail címmel rendelkezhet.
c) A felhasználó jogosult személyes adatainak és adatterületének védelmére, azokat személyiségi jogainak betartásával kell kezelni. Adatait kiadni, az általa létrehozott dokumentumokról másolatot készíteni, vagy azokba betekinteni, csak a tulajdonos hozzájárulásával lehet.

(7) Az adatvédelmi jogok betartása és betartatása, valamint a rendszer és a hálózat biztonságának megőrzése érdekében a rendszergazda a jogsértés tényét írásban közli a jogsértő személy munkahelyi felettesével.

26. Intézkedések

27. § (1) A rendszergazda jogosult bármikor ellenőrizni az intézmény eszközeinek szabályos használatát. Az ellenőrzés tényét nem köteles előre bejelenteni, de törekednie kell, hogy az ne zavarja feleslegesen a napi munkamenetet.
(2) Ha a felhasználó az intézmény eszközeit nem a szabályzat előírásainak megfelelően használja, úgy fegyelmi eljárás kezdeményezhető vele szemben. Mivel a szabályok megszegése az intézmény egész informatikai rendszerének, a főiskola működésének, mások munkájának biztonságát is veszélyeztetheti, ezért a rendszergazda indokolt esetben, saját hatáskörben azonnal felfüggesztheti a felhasználói jogok gyakorlását. A rendszergazda a szabályok megsértését illetve a felhasználói jogok ideiglenes felfüggesztését haladéktalanul jelenti a munkahelyi felettesnek, illetve a munkáltatói jogkör gyakorlójának, aki dönt a fegyelmi eljárás megindításáról.
(3) A szabályok csekélyebb jelentőségű megszegése esetén a rendszergazda saját hatáskörben olyan mértékben korlátozhatja a felhasználói jogosultságot, ami nem veszélyezteti az alkalmazott munkavégzését, illetve a hallgató tanulmányi kötelezettségeinek teljesítését. A jogosultság megvonása az elkövetett szabálytalanság függvényében lehet ideiglenes, vagy végleges. A rendszergazda az általa hozott korlátozó intézkedéseket a felhasználó munkahelyi felettesének, illetve hallgató esetében a szak-gazda tanszék vezetőjének jelenti, aki dönt annak jóváhagyásáról, illetve a továbbiakban szükséges intézkedésekről. A korlátozó intézkedések ellen a rektornál lehet panasszal élni.
(4) Amennyiben az elkövetett vétség feltehetően bűncselekménynek minősül, úgy a rendszergazda a tudomására jutást követően köteles a felhasználói jogokat azonnal teljes mértékben felfüggeszteni, a felhasználó adatait zárolni, s az intézmény vezetőjének a cselekményt jelenteni.
(5) Az előző pontokban felsorolt jogok a lokális hálózatok vonatkozásában megilletik az azok működéséért felelős személyeket is.
(6) A felhasználó minden olyan általa okozott kárért teljes körű kártérítési kötelezettséggel tartozik, mely az eszközök rendeltetés, vagy előírás szerinti használatának megszegése miatt történik.

Záró rendelkezések

A Szenátus a Magyar Táncművészeti Főiskola Informatikai szabályzatát a 2012. november 14-i ülésén a 42/2012. számú határozatával jóváhagyta.
A jelen szabályzat 2012. november 15-én lép hatályba.
Ezzel egyidejűleg hatályát veszti a 2007. december 12-én kiadott Informatikai szabályzat.
A jelen szabályzat rendelkezéseinek végrehajtásáról az informatikai csoport gondoskodik.

Budapest, 2012. november 14.

Szakály György
rektor

dr. Hobaj Tünde
főtitkár

Mellékletek:

1. *Informatikai beléptető jegy*
2. *Szoftver Etikai Kódex*
3. *Megismerési nyilatkozat*

Informatikai beléptető jegy

Alkalmazott neve: .....

Beosztás: .....

MTF domain azonosító .....

MTF domain jelszó: .....

Igényelt e-mail : .....@mtf.hu

e-mail fiók azonosító .....

e-mail fiók jelszó: .....

MTF levelező szerver POP3/SMTP: mail.mtf.hu

Igényelt rendszerekhez való hozzáférés:

informatikai rendszer megnevezése	Jogosultság*

*Jogosultsági szint:
Hallgató (minimumjogok), Alap, Oktató/tanár, Gazdasági Hivatal, Rektori Hivatal, Tanulmányi, Könyvtár, Adminisztrátor, Rendszergazda

Budapest, 2012. .....

.....
engedélyező (vezető) aláírása

.....
alkalmazott aláírása

Szoftver Etikai Kódex

A szerzői jog által védett számítógépes szoftverek illegális használata és másolása törvénybe ütköző cselekedet, büntetőjogi felelősségre vonással jár, ellenkezik a Magyar Táncművészeti Főiskola (továbbiakban főiskola) politikájával. Az ilyen jellegű szoftvermásolást helytelenítjük és elítéljük, ezért ennek megakadályozására a főiskola a következő alapelveket fogadja el:

1. A főiskola semmilyen körülmények között nem ösztönzi, és nem tűri el az illegális szoftvermásolatok készítését vagy használatát.
2. Minden indokolt szoftverigény kielégítésére a főiskola jogtiszta szoftvert biztosít az összes számítógépre, a megfelelő időben, és a szükséges mennyiségben.
3. A főiskola eleget tesz minden olyan licenc vagy vásárlási feltételnek, amely az általa beszerzett vagy használt szoftverek felhasználását szabályozza.
4. Az illegális szoftvermásolatok készítésének vagy használatának megakadályozása érdekében a főiskola szigorú belső ellenőrzést végez, beleértve a fenti normák betartatására, és a normákat megszegők fegyelmi büntetésre vonatkozó intézkedéseket.
5. A főiskola számos szoftvercég termékeit használja. A főiskola szoftverhasználati politikája és rendje előírja, hogy az alkalmazottak tiszteletben tartsák a szoftverekkel kapcsolatos szellemi tulajdonjogot valamint a használt szoftverek licencszerződéseinek feltételeit. A licencelt szoftver eszközökkel való gazdálkodás megköveteli, hogy a főiskola csak jogtiszta szoftvereket telepítsen a számítógépeire, beleértve a hordozható számítógépeket és szervereket is.
6. A főiskola minden szükséges lépést megtesz, hogy megakadályozza a licencelt szoftverek és a kísérő dokumentációk jogsértő másolását, mind a saját telephelyén, mind máshol, kivéve azt az esetet, ha a másolásra a licenctulajdonostól írásbeli engedélyt kapott. A szoftverek engedély nélküli másolása a Szerzői Jogi törvény szerint bűntettnek minősül.
7. A főiskola nem adhat engedélyt egyetlen alkalmazottnak sem a szoftverek vonatkozó licencszerződését megsértő használatára, beleértve a szoftverek átadását vagy elfogadását üzleti partnerektől, megbízóktól vagy ügyfelektől.
8. A főiskola a szoftverhasználattal kapcsolatosan tájékoztatást nyújt az alkalmazottaknak. A tájékoztatást követően az alkalmazottaknak alá kell írniuk a szoftverhasználattal és licenc gazdálkodással kapcsolatos Alkalmazotti nyilatkozatot. Az új alkalmazottak a belépésüket követő 10 munkanap alatt kapják meg a fenti tájékoztatást.
9. Azok az alkalmazottak,
   - akik a szoftvert, vagy annak dokumentációját a szerzői jog tulajdonosának engedélye nélkül lemásolják vagy terjesztik;
   - akik szerzői jog által védett szoftvert egyidejűleg két vagy több gépen futtatnak, hacsak ezt a szoftvert licenc szerződése külön nem engedélyezi;
   - akik tudatosan vagy akaratlanul munkatársaikat arra ösztönzik, kötelezik, vagy számukra megengedik, hogy illegális szoftvermásolatokat készítsenek, használjanak vagy terjesszenek;
   - akik az illegális szoftvermásolást tiltó törvényt megsértik azért, mert valaki erre kéri vagy kényszeríti Őket;
   - akik szoftvert kölcsön adnak úgy, hogy arról másolatot lehessen készíteni, vagy akik a kölcsönkért szoftvert lemásolják;
   - akik olyan eszközöket készítenek, importálnak, vagy birtokolnak, amelyek lehetővé teszik a szoftver védelmét szolgáló műszaki eszközök eltávolítását, vagy ilyen eszközökkel kereskednek, fegyelmi büntetés lehetőségének vannak kitéve, mely az azonnali elbocsátást is maga után vonhatja.
10. A főiskola fenntartja a jogot arra, hogy megvédje hírnevét, illetve a számítógépes szoftverekbe befektetett beruházásait azáltal, hogy erős belső ellenőrző rendszert alakít ki, melynek célja megakadályozni a szoftverek illegális másolatának készítését és használatát. Ezek az ellenőrzések magukba foglalják a
    - szoftverhasználat gyakori és időszakonként megismétlődő felmérését;
    - a vállalat számítógépeinek előzetesen bejelentett vagy bejelentés nélküli auditját, melynek célja a legalitás biztosítása;
    - A főiskola számítógépein található azoknak a szoftvereknek az eltávolítását, melyekhez nem tartozik érvényes licenc vagy a licenc meglétét igazoló dokumentum;
    - és a fegyelmi eljárásokat (beleértve az elbocsátást is), melynek akkor indulnak, ha egy
    - alkalmazott megsérti a jelen szoftverpolitika rendelkezéseit.

Megismerési nyilatkozat

A Magyar Táncművészeti Főiskola 2012. ..... hatályos **Informatikai szabályzatát** megismertem. Tudomásul veszem, hogy az abban leírtakat a munkám során köteles vagyok betartani.

Név	Beosztás	Dátum	Aláírás

Budapest, 2012. .....