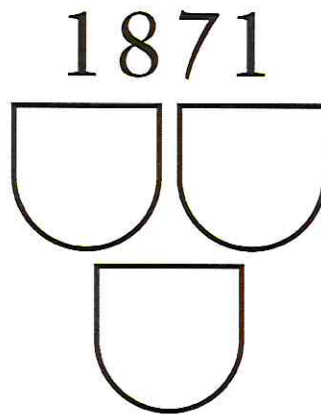


# MAGYAR KÉPZŐMŰVÉSZETI EGYETEM



## INFORMATIKAI SZABÁLYZAT

Elfogadta a Szenátus a 40/2020. (VII. 03.) számú határozatával.



.....  
**Radák Eszter**  
rektor



# TARTALOMJEGYZÉK

Az Egyetem informatikai működésének általános szabályai .....	3
1. § Értelmező rendelkezések .....	3
2. § Az Informatikai Szabályzat célja és hatálya.....	4
3. § Az informatikai feladatellátás szervezeti keretei, működési rendje .....	5
4. § Az Informatikai Osztály osztályvezetőjének feladatai.....	6
5. § A rendszergazda feladatai .....	7
6. § A WEB–mester feladatai.....	8
7. § A Szerverüzemeltető feladatai.....	8
8. § Informatikai eszközök kezelése, használata.....	9
9. § Jogosultságok .....	10
10. § Informatikai szolgáltatások.....	12
Informatikai biztonság .....	14
11. § Az informatikai biztonság szabályozásának célja .....	14
12. § Az informatikai rendszerek biztonsági besorolásai .....	14
13. § Védelmet igénylő, az informatikai rendszerre ható elemek .....	15
14. § Felelősségi körök .....	15
15. § A védelmet igénylő adatok és információk .....	16
16. § Az informatikai eszközbázist veszélyeztető helyzetek.....	16
17. § Az informatikai eszközök védelme .....	17
A szoftverhasználat rendje .....	20
18. § A szoftverhasználattal kapcsolatos szabályok .....	20
19. § Szoftverhasználattal kapcsolatos feladatok .....	20
20. § Adatkezelés, adatvédelem.....	21
21. § Intézkedések .....	22
22. § Záró rendelkezések .....	23
1. sz. melléklet: Felhasználói nyilatkozat .....	24
2. sz. melléklet: Kilépő felhasználói nyilatkozat .....	25
3. sz. melléklet: Megismerési nyilatkozat.....	26

A Magyar Képzőművészeti Egyetem (a továbbiakban: Egyetem) Szenátusa a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény, valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) alapján, összhangban az Egyetem Adatvédelmi és adatkezelési, valamint a közérdekű adatok megismeréséről és közzétételéről szóló szabályzattal (a továbbiakban: Adatvédelmi Szabályzat), a Szervezeti és Működési Szabályzatban (a továbbiakban: SZMSZ) foglalt jogkörében az egyetemi informatikai rendszer kialakításával, fenntartásával, üzemeltetésével, fejlesztésével és védelmével kapcsolatosan a következő Szabályzatot alkotja.

## AZ EGYETEM INFORMATIKAI MŰKÖDÉSÉNEK ÁLTALÁNOS SZABÁLYAI

### 1. § Értelmező rendelkezések

**Biztonsági esemény:** Az informatikai rendszer védelmi állapotában bekövetkezett illetéktelen változás, melynek hatására az informatikai rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.

**Egyetemi számítógépes hálózat:** Az adatátviteli vonalak (típusuk szerint Ethernet, optikai), aktív és passzív hálózati elemek, továbbá minden hálózatra kötött számítógépes munkahely, eszköz (PC, hálózati nyomtató, hálózati tároló stb.) és szerver összessége, függetlenül attól, hogy az mely szervezeti egység használatában van.

**Eszköz:** minden informatikai eszköz (számítógép, szerver, nyomtató, passzív és aktív hálózati elem)

**Felhasználó:** az a személy, aki az Egyetem valamely informatikai szolgáltatását igénybe veszi.

**Funkcionalitás:** Az informatikai rendszer megfelelő tervezésének és üzemeltetésének köszönhetően az adat tartalmi és formai használhatóságának biztosítása.

**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.

- *Zárt a védelem*, ha az összes releváns fenyegetés figyelembe lett véve a védelmi intézkedések megtervezésénél és megvalósításánál.
- *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.
- *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.
- *Folyamatos a védelem*, ha az időben változó körülmények és viszonyok ellenére is megszakítás nélkül valósul meg.

**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.

**Incidens:** A szolgáltatás alapvető működésétől eltérő esemény, mely fennakadást vagy minőségcsökkenést okoz, vagy okozhat a szolgáltatásban.

**Informatikai biztonságpolitika:** Az intézmény minden munkatársa és az informatikai rendszer minden felhasználója számára meghatározza, hogy melyek az informatikai rendszerek által kezelt adatok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzésével kapcsolatos biztonsági elvek, szabályok és előírások.

**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.

**IT vagy informatikai szolgáltatás:** Az Egyetemen használt IT (information technology) vagyis információs technológiai/informatikai rendszerrel nyújtott szolgáltatás.

**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 megsérülne, vagy megsemmisülne. Az eredeti szoftverről készített további másolat jogosulatlan másolásnak minősül, és megsérti a szoftvert védő és használatát szabályozó licenc szerződést, valamint a szerzői jogi törvényt.

**Kockázat:** A fenyegetettség mértéke, amely valamely fenyegető tényezőtől 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.

**Megbízható működés:** Az az állapot, amikor az informatikai rendszerek által kezelt adatok és hordozott információk a rendelkezésre állása biztosított, és védettek a funkcionalitás sérülése, elvesztése ellen.

**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.

**Rendelkezésre állás:** Annak a valószínűsége, hogy egy definiált időintervallumon belül az alkalmazás, szolgáltatás a tervezéskor meghatározott funkcionális szintnek megfelelően a felhasználó által használható.

**Szellemi tulajdon:** A törvény szerint az eredeti számítógépes program az azt létrehozó személy vagy vállalat szellemi tulajdona. A számítógépes programokat szerzői jogi törvény védi.

**Szoftver:** A számítógépes programalkotás és a hozzá tartozó dokumentáció akár forráskódban, akár tárgykódban vagy bármilyen más formában rögzített minden fajtája, ideértve a felhasználói programot és az operációs rendszert is.

**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.

**Szolgáltatásért felelős szervezeti egység:** Az IT és telekommunikációs szolgáltatás nyújtására alkalmas infrastruktúrával rendelkező szervezeti egység, mely az adott szolgáltatás nyújtásának feltételeit a felhasználók számára nyilvánosságra hozza.

## 2. § Az Informatikai Szabályzat célja és hatálya

- (1) Jelen Informatikai Szabályzat (a továbbiakban: Szabályzat) célja, hogy az Egyetem 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.
- (2) A Szabályzat személyi hatálya kiterjed az Egyetem valamennyi
  - a) dolgozójára, függetlenül attól, hogy alkalmazására milyen jogviszony keretében kerül sor;
  - b) hallgatójára, függetlenül az oktatás formájától;
  - c) az informatikai szolgáltatásokat nyújtó és igénybe vevő valamennyi szervezeti egységére.

- (3) Amennyiben az Egyetem harmadik félnek is lehetőséget biztosít informatikai infrastruktúrájának használatára, akkor a harmadik félre nézve is kötelező a Szabályzatban foglaltak betartása.
- (4) A Szabályzat tárgyi hatálya kiterjed:
  - a) az Egyetem 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) az adathordozók tárolására, felhasználására.
- (5) 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.
- (6) Az eszközöket csak olyan személy használhatja, aki az eszközök használatára engedélyt kapott, valamint e Szabályzatot ismeri. A felhasználó a Szabályzatban foglaltak tudomásulvételét és elfogadását aláírásával igazolja (3. számú melléklet). Az aláírást megtagadó felhasználó nem jogosult az eszközök használatára.

### **3. § Az informatikai feladatellátás szervezeti keretei, működési rendje**

- (1) Az Egyetemen az informatikai feladatok ellátásáért a kancellár felel. Feladatait az Informatikai Osztály (a továbbiakban: Osztály) útján látja el. Az Osztály munkatársai felett – a kancellár által átruházott hatáskörben – az Informatika Osztály osztályvezetője utasítási jogkörrel rendelkezik.
- (2) Az Osztály feladatait a rendszergazdák, a WEB-mester, valamint a szerverek és a hálózat működését biztosító eszközök üzemeltetését végző külső szolgáltató (továbbiakban: Szerverüzemeltető) útján látja el.
- (3) Az Osztály feladat- és hatásköre:
  - a) az egyetemi számítógépes hálózat és az IT szolgáltatások üzemeltetése;
  - b) a vezetékes telefonhálózat üzemeltetése, karbantartása és fejlesztése, valamint a mobil szolgáltatások kezelése, beszerzése és nyilvántartása;
  - c) a másoló és nyomtató berendezések (fénymásolók, nyomtatók, multi-funkciós berendezések, szkennerek, stb.) üzemeltetése, karbantartása és fejlesztése;
  - d) a felhasználók munkájának támogatása, az incidensek és problémák kezelése;
  - e) operációs rendszerek konfigurálása és telepítése, az operációs rendszerek és az alkalmazások hibáinak feltárása és elhárítása;
  - f) személyes informatikai eszközök (asztali számítógép, notebook, tablet, mobiltelefon stb.) és kiegészítő perifériák (pl. egér, pendrive) telepítése, beüzemelése a felhasználói igények és vezetői jóváhagyás esetén;
  - g) az informatikai fejlesztések tervezése, végrehajtása, koordinálása és ellenőrzése;
  - h) a közbeszerzési terv informatikai beszerzéseket – a 301/2018. (XII. 27.) Korm. rendelettel a Digitális Kormányzati Ügynökség hatáskörébe utalt központosított közbeszerzések, a továbbiakban – érintő részének összeállítása, felülvizsgálata és végrehajtása;
  - i) az Egyetem honlapjának ([mke.hu](http://mke.hu)) és levelezési rendszerének (@mke.hu) karbantartása, felügyelete;
  - j) az Egyetemhez kapcsolódó WEB-oldalak linkelt megjelenítése (pl.: bestofdiploma.hu; dflab.org stb.) a hivatalos honlapon vagy subdomain beállítása (pl.: kurator.mke.hu);
  - k) a jelen Szabályzatban foglaltak betartatása, betartásának ellenőrzése.

- (4) Az Osztály részére feladat – ha jogszabály, belső szabályzat, a kancellár, vagy az osztályvezető másként nem rendelkezik – az osztályvezető útján adható, megkeresés az osztályvezetőnél kezdeményezhető.
- (5) Az Osztály általános ügyintézési határideje – ha jogszabály, belső szabályzat, a kancellár, vagy az osztályvezető másként nem rendelkezik – 5 munkanap.
- (6) Az Osztály munkatársai kötelesek a beérkező megkeresésekre a lehető legrövidebb időn belül választ adni, a feladatokat határidőre végrehajtani. A végrehajtott feladatokról, megkeresésekre adott válaszokról az Osztály munkatársai az osztályvezetőt minden esetben kötelesek tájékoztatni.
- (7) A belső kapcsolattartás elsődleges formája az e-mail. Az e-maileket az Osztály dolgozói napi rendszerességgel, távollét esetén szükség szerinti gyakorisággal kötelesek figyelemmel kíséreni. Az Osztály minden munkatársa köteles e-mailjeit munkaidőben folyamatosan figyelemmel kíséreni, az elektronikus formában megküldött feladatokat végrehajtani.
- (8) Az osztályvezető a hatáskörébe tartozó feladatok tekintetében beszámolási kötelezettséggel tartozik a kancellárnak.
- (9) A kiadott feladatok végrehajtását, az egyetemi szabályzatok betartását az osztályvezető köteles ellenőrizni.
- (10) Az Osztály feladatainak ellátásában részt vevő alkalmazottak foglalkoztatására, az alkalmazottak jogaira és kötelezettségeire, fegyelmi és kártérítési felelősségére vonatkozó rendelkezéseket a foglalkoztatási követelményrendszer tartalmazza.
- (11) Az Osztály munkatársai foglalkoztatásának részletes szabályait a foglalkoztatási követelményrendszer alapján elkészített munkaköri leírás tartalmazza. A munkaköri leírás a kinevezési okirat mellékletét képezi, melyet a munkáltatói jogkör gyakorlója, a kancellár hagy jóvá.
- (12) Az Osztály munkatársainak munkaidejét a munkaköri leírás határozza meg a Foglalkoztatási Szabályzat rendelkezéseinek figyelembe vételével.
- (13) Az Osztály munkatársainak szabadság iránti kérelmét az osztályvezető, az osztályvezető szabadság iránti kérelmét a kancellár hagyja jóvá az erre rendszeresített szabadság-nyilvántartó nyomtatványon.
- (14) Az osztályvezetőt távolléte vagy akadályoztatása esetén általános felhatalmazással az osztályvezető által kijelölt munkatárs helyettesíti. Az osztály munkatársai vonatkozásában a munkaköri leírásban kerül meghatározásra a helyettesítési rend.
- (15) Az Osztály munkatársai kötelesek az Egyetem jó hírnevét megőrizni, valamint a Kjt. szerinti, illetve a Foglalkoztatási Szabályzatban rögzített fegyelmi vétség elkövetésétől tartózkodni.

#### **4. § Az Informatikai Osztály osztályvezetőjének feladatai**

- (1) Az Egyetem informatikai tevékenységének irányítása körében különösen:
  - a) Az Egyetem igényeit, aktuális helyzetét és lehetőségeit figyelembe véve közreműködik a rövid-, közép- és hosszú távú informatikai stratégia meghatározásában. Javaslatot tesz a kancellárnak az elavult informatikai rendszerek és eszközök cseréjére, új eszközök beszerzésére.
  - b) Közreműködik az éves informatikai költségvetés megtervezésében, valamint a közbeszerzési terv informatikai beszerzéseket érintő részének összeállításában.
  - c) A terveknek megfelelő fejlesztéseket, bővítéseket és az eseti, informatikai tárgyú projekteket megtervezi, előkészíti és koordinálja azok megvalósítását.

- d) A különböző szervezeti egységek részéről felmerülő informatikai igényeket egyeztetni, és azokra mindenki számára megfelelő megoldásokat keres.
- e) A beszerzések és fejlesztések során irányítja, koordinálja és ellenőrzi az informatikai területet érintő folyamatokban résztvevő belső munkatársak, külső beszállítók és minden érintett személy munkáját.
- f) A napi szintű működés során koordinálja és ellenőrzi a rendszergazdák, a WEB-mester és a külső üzemeltető cégek és szolgáltatók munkáját.
- g) Gondoskodik az informatikai tárgyú szabályzatok kidolgozásáról és frissítéséről.
- h) Közreműködik az informatikai üzemeltetést is érintő szabályzatok véleményezésében.
- i) Elkészíti az Egyetem informatikai vonatkozású tevékenységeire irányuló külső- és belső ellenőrzések során a beadandó dokumentációt.
- j) Törekszik a nyújtott informatikai szolgáltatások minőségének folyamatos javítására.

## **5. § A rendszergazda feladatai**

(1) A rendszergazda feladatai különösen:

- a) Felhasználókkal való folyamatos és közvetlen kapcsolattartás, kommunikáció.
- b) Felhasználói bejelentések alapján konfigurációs beállítások végrehajtása.
- c) Felhasználók teljes körű informatikai szoftveres és hardveres támogatása, az incidensek kezelése.
- d) Rendszergazdai teendők ellátása, operációs rendszerek konfigurálása és telepítése, az operációs rendszerek és az alkalmazások hibáinak feltárása és elhárítása.
- e) Napi szintű felhasználói gépeket érintő informatikai feladatok és problémák megoldása.
- f) Hálózati üzemeltetési feladatok. Hálózati hibák felderítése, hibaelhárítás:
  - MS Windows, valamint Linux alapú kiszolgálókon futó alkalmazások felügyelete;
  - az intézmény számítástechnikai eszközeinek, különösen az informatikai hálózat, a szoftverek és különféle adatbázisok, informatika terem stb. folyamatos és biztonságos üzemeltetéséről való gondoskodás.
- g) Az alapfeladatok ellátáshoz szükséges szoftverek működési környezetének biztosítása, beleértve az egyes szervezeti egységek (pl.: Gazdasági Osztály, Tanulmányi Osztály, Könyvtár stb.) speciális szoftvereit is.
- h) A számítógépek vírusmentességének fenntartásáról való gondoskodás, annak rendszeres ellenőrzése, az internet működésének folyamatos ellenőrzése.
- i) Új hálózati azonosítók kiadása, a felhasználók felhasználói jogainak karbantartása.
- j) A szoftverek és a licenyszerződések nyilvántartása.
- k) A számítástechnikai eszközök szabályos használatának ellenőrzése, megrendelésének lebonyolítása, telepítése, beállítása, selejtezése, rendszeres ellenőrzése, a hibák felderítése és elhárítása.
- l) HelpDesk feladatok ellátása, incidenskezelés, felhasználók teljes körű informatikai támogatása (környezet: MS Windows, Ms Office, MAC OS, Poszeidon iktatóprogram, Neptun, Forrás.NET gazdálkodási program stb.).
- m) Informatikai eszközök életciklus kezelése (pl. eszköz beszerzési tevékenységek, leltározási tevékenységek, üzembe helyezés, selejtezés, raktározás stb.).
- n) A tanórák illetve az egyéb események, rendezvények hangosítása, és multimédiás támogatása.
- o) A közösen (elsősorban oktatástechnikai célokra) használt eszközök kölcsönzésének lebonyolítása, azok kiadása, visszavétele az erre vonatkozó szabályok szerint.

## 6. § A WEB–mester feladatai

(1) A WEB–mester feladatai különösen:

- a) az Egyetem WEB–lapjának ([mke.hu](http://mke.hu)) kezelése, karbantartása és frissítése napi rendszerességgel;
- b) a WEB–lapon megjelenítendő új információs anyagok előkészítése, illetve a már előkészített anyagok WEB–lap arculatának elkészítése, publikálása;
- c) az Egyetem aktuális tartalmainak feltöltése, hírendszerbe szervezése és kezelése;
- d) a WEB–lapon lévő anyagok folyamatos tartalmi és arculati, valamint helyesírási javítása, frissítése, áthelyezése;
- e) kreatív, konstruktív kezdeményezések a honlap látogatottságának növelésére;
- f) az Egyetem munkatársaitól kapott információt rendszerezi az Informatikai Tanács által meghatározott honlap térkép (site map) és információ-felelősség szerint, valamint javaslattétel a honlap térképpel kapcsolatos döntésekben;
- g) az Egyetem belső (intranet) oldalának kezelése;
- h) az Egyetemhez kapcsolódó WEB-oldalak linkelt megjelenítése (pl.: [bestofdiploma.hu](http://bestofdiploma.hu); [dflab.org](http://dflab.org) stb.) a hivatalos honlapon;
- i) felhasználókkal való folyamatos és közvetlen kapcsolattartás, kommunikáció az egyetemi WEB–lapokkal kapcsolatban az [info@mke.hu](mailto:info@mke.hu) postafiókon keresztül;
- j) javaslattétel a WEB–s alkalmazás szükséges módosítására, cseréjére vagy fejlesztések elvégzésére.

## 7. § A Szerverüzemeltető feladatai

(1) A Szerverüzemeltető – szerverek és a hálózat működését biztosító eszközök üzemeltetését végző külső szolgáltató – feladatai különösen:

- a) Gondoskodik a(z)
  - hálózati komponensek és szolgáltatások;
  - adatbázis jellegű komponensek és szolgáltatások;
  - webkiszolgálók és szolgáltatások;
  - levelező rendszerek;
  - fájlszolgáltatások;
  - szerverek és szerver operációs rendszerek;
  - gazdasági– és adminisztrációs rendszerek;
  - tanulmányi rendszer;
  - egyéb speciális komponensek/rendszerek (pl. nyomtatás management rendszer)folyamatos üzemszerű működéséről, a frissítések elvégzéséről és a felmerülő hibák elhárításáról.
- b) Gondoskodik az informatikai biztonsággal, valamint a tanúsítványokkal kapcsolatos feladatok ellátásáról.
- c) Ellenőrzi a felsorolt feladatok végrehajtását, szükség esetén intézkedéseket fogalmaz meg az Informatikai Osztály osztályvezetője részére.
- d) A már bevezetett és a későbbiekben tervezett szerver szolgáltatások optimális kialakításához, használatához szakmai tanácsadást nyújt az Informatika Osztály osztályvezetője számára a meglévő felhasználási trendek, és az igényelt új funkciók alapján.



## 8. § Informatikai eszközök kezelése, használata

- (1) A Szabályzat alkalmazása tekintetében eszköznek tekintendők:
  - a) a számítógépek;
  - b) a számítógép perifériák (pl. nyomtató, szkennер, egér, billentyűzet, kártyaolvasó stb.);
  - c) a számítógép hálózat;
  - d) a számítógépeken futó szoftverek;
  - e) a fenti berendezésekhez, szoftverekhez tartozó dokumentációk;
  - f) az adathordozók.
- (2) Az eszközök pontos jegyzékét az Egyetem tárgyi eszköz nyilvántartása 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 korlátozhatja.
- (3) A számítástechnikai eszközök telepítését, elhelyezését, az előírásoknak megfelelő üzembe helyezését kizárólag a rendszergazdák végezhetik. Ezáltal érvényesíthető az eszközökkel, szoftverekkel kapcsolatos garancia és jótállás.
- (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, 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, gépterem teljesen területén élelmiszert fogyasztani, vagy azokat kicsomagolt állapotban tartani.
  - f) Tilos az eszközöket, és azok részeit áthelyezni, burkolatukat, elektromos csatlakozásaikat megbontani.
  - g) Tilos a számítógépre engedély nélkül szoftvert telepíteni, illetve letörölni.
  - h) A számítógépeket szétszedni, konfigurációjukat, beállításait és a rajtuk lévő jelzéseket (pl. nyilvántartási szám, gyáriszám stb.) megváltoztatni szigorúan tilos! Amennyiben ezen jelölések sérülését, eltűnését észleli a felhasználó, köteles azt haladéktalanul bejelenteni az Osztálynak.
  - i) A felhasználók kötelesek minden meghibásodást, egyéb igényt írásban jelezni az Osztály részére a [support@mke.hu](mailto:support@mke.hu) e-mail címen.
  - j) Elektromos meghibásodás, pl. zárlat gyanúja esetén az eszközt feszültség mentesíteni kell. Ha a meghibásodás a gépterem elektromos hálózatában keletkezik, úgy az egész géptermet feszültség mentesíteni kell a főkapcsolóval.
- (5) Az eszközök használatát az arra kijelölt személy (tanár, oktató, rendszergazda) ismerteti. 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 informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.
- (7) Az intézmény felhasználói kötelesek oly módon használni az informatikai eszközöket, szolgáltatásokat és a hálózatot, hogy magatartásukkal az Egyetem hitelét, jó hírét és érdekeit ne sértsék.

## 9. § Jogosultságok

- (1) Az eszközök és informatikai szolgáltatások használatának módját a felhasználói jogosultságok és hozzáférések szabályozzák. A felhasználók különböző jogosultságokkal rendelkezhetnek, melyeket jelen Szabályzat alapján, jogosultsági szinteknek megfelelően kell meghatározni. A minimum jogosultsági szint mindenkit megillet, aki az intézménnyel közalkalmazotti jogviszonyban áll, munkájához az szükséges, és aláírásával igazolja, hogy a Szabályzat tartalmát megismerte, annak betartását vállalja. Hallgatók esetében a Szabályzat betartásának elfogadása a számítógépekre történő bejelentkezéskor megjelenő bejelentkezési üzenet elfogadásával történik. A további jogosultsági szinteket a minimum és normál szint kiegészítésekként kell értelmezni.
- (2) A hozzáférések biztosítása tekintetében a minimális hozzáférés elvét kell alkalmazni, a szabályozatlan esetekben a hozzáférés tiltottnak, illetve az adott jogosultság nem meglévőnek számít.
- (3) Az új felhasználó regisztrációjáról a munkahelyi vezető írásbeli jelzése ([support@mke.hu](mailto:support@mke.hu)) alapján a rendszergazda gondoskodik. A regisztráció érdekében az alábbi adatok megadása szükséges:
- a) név;
  - b) szervezeti egység;
  - c) beosztás;
  - d) e-mail cím személyi azonosító része a 10. § (2) e) pontban foglaltak figyelembevételével;
  - e) jogosultsági szint a (6) bekezdésnek megfelelően;
  - f) igényelt kritikus informatikai rendszerekhez – 12. § (2) – történő hozzáférés.
- (4) Az egyedi igényeket a közvetlen munkahelyi vezetőtől kell kérni, aki – egyetértése esetén – továbbítja az igényt az Osztály részére ([support@mke.hu](mailto:support@mke.hu)).
- (5) 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.
- (6) A felhasználói jogosultságok szintjei:

Szint	Jogosultak	Jogok
Hallgató (minimumjogok)	Az intézmény bármely hallgatója	<ul style="list-style-type: none"> <li>- bejelentkezés a hallgatói számítógépekre (Neptun kóddal és jelszóval);</li> <li>- könyvtári adatbázisok és a könyvtári nyomtatás/szkennelés használata;</li> <li>- WiFi hálózat.</li> </ul>
Normál	Az intézmény közalkalmazottja	<ul style="list-style-type: none"> <li>- az egyetemi informatikai szolgáltatások használata felhasználó számára biztosított felhasználói fiókokkal;</li> <li>- a felhasználó számára biztosított munkaállomás és mobil eszközök használata;</li> <li>- jóváhagyott szoftverek használata a felhasználó számára biztosított eszközökön;</li> <li>- 50 GB méretű postafiók az egyetem által üzemeltetett (MS Office365) levelezőrendszerben;</li> <li>- az „ORG” megosztások használata a számára jóváhagyott hozzáférési jogosultságokkal;</li> <li>- a telephelyi számítógéphálózatok használata;</li> <li>- WiFi és dolgozói WiFi hálózat.</li> </ul>

Oktató, tanár	Az intézmény oktatói, kutatói, tanárai	- hozzáférés a Neptun rendszerhez WEB-es felületen keresztül
Gazdasági Osztály	A Gazdasági Osztály dolgozói	- hozzáférés külön engedéllyel a gazdasági rendszerekhez (Forrás.NET, KIRA stb.); - a „work” megosztások használata a számára jóváhagyott hozzáférési jogosultságokkal.
Tanulmányi Osztály	A Tanulmányi Osztály dolgozói	- hozzáférés külön engedéllyel a tanulmányi rendszerekhez (Neptun kliens használata)
Könyvtár	Könyvtár alkalmazottai	- hozzáférés külön engedéllyel a könyvtári rendszerekhez
Rendszergazda	Az adott feladatokra kijelölt személy	- speciális jogok, pl. a levelező rendszer, fájl szerverek vagy a WEB oldalak karbantartásával kapcsolatos feladatok ellátásához
Tartományi rendszergazda	Az intézményi rendszer/hálózat/szerver üzemeltető	- korlátlan jogosultság az intézmény összes tartományi munkaállomásán és szerverén

- (7) A speciális feladatok (pl., WEB–mesterség, felhasználó adminisztráció stb.), illetve az azokhoz tartozó jogok alapértelmezésben a tartományi rendszergazdát illetik meg. Ezek a jogok egy-egy jól elhatárolható hálózati adminisztrációs feladat elvégzéséhez rendelkezhetők, és a tartományi rendszergazda beleegyezésével külön megállapodás alapján más személynek (pl. WEB–mester, rendszergazda) 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 tartományi rendszergazda biztosítja. Amennyiben a tartományi 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 közvetlen munkahelyi vezetőjének.
- (8) Az Egyetemen a lokális hálózatok eszközeinek használati rendjét a Szabályzat alkalmazásán felül az egyes szervezeti egységek vezetői, tantermek esetében az oktatásvezető tanárok hivatottak meghatározni:
- (9) A felhasználók a számítógépes hálózat szolgáltatásait a felhasználói azonosító és az ahhoz tartozó jelszó segítségével vehetik igénybe. A felhasználói azonosítókat a közvetlen munkahelyi vezető kérésére a rendszergazdák hozzák létre.
- (10) A felhasználói azonosítók kezelésének szabályai:
- Minden felhasználó csak a saját azonosítójával használhatja a hálózatot.
  - Minden felhasználó felel a rábízott felhasználói azonosító és az ahhoz rendelt jogok biztonságáért.
  - Az azonosító használatát még a tulajdonos jelenlétében sem lehet átengedni másnak.
  - A felhasználói azonosítóhoz tartozó jelszót csak annak birtokosa ismerheti.
  - Amennyiben felmerül a gyanú, hogy a jelszó mások tudomására jutott, úgy azt azonnal meg kell változtatni.
  - Amennyiben valaki észleli, hogy más kísérletet tesz a felhasználói jelszavak megszerzésére, azt azonnal jelezni kell a [support@mke.hu](mailto:support@mke.hu) címen és a munkahelyi felettesnek.
  - Minden más személy jelszavának vagy adatainak megszerzésére irányuló cselekedet és azzal történő visszaélés 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 az általa használt programokból és a számítógépről (operációs rendszerből) is.
  - j) A felhasználói jelszó átadását senki sem kérheti, még az Osztály munkatársai sem.
- (11) A felhasználói jelszavakkal szemben támasztott követelmények:
- a) A jelszónak legalább 8 karakter hosszúnak kell lennie
  - b) A jelszónak tartalmaznia kell az alábbi négy karaktercsoportokból legalább háromba tartozó elemet:
    - latin ábécé kisbetűi (a-tól z-ig);
    - latin ábécé nagybetűi (A-tól Z-ig);
    - számok (0-tól 9-ig);
    - speciális, az ábécébe nem tartozó karakterek (pl.: „,”, „!”, „\$”, „#”, „%”).
  - c) A jelszó nem tartalmazhatja a hozzá tartozó felhasználói fiók nevének egyetlen legalább három karakterből álló összefüggő részét sem.
  - d) A jelszavakat 90 naponta meg kell változtatni.
  - e) Az új jelszó nem egyezhet meg az előző 5 jelszó egyikével sem.
  - f) Új jelszót csak minimum egy nap elteltével lehet megváltoztatni.
  - g) A jelszavakat nem lehet visszafejthető titkosítással, vagy titkosítás nélkül tárolni.

## **10. § Informatikai szolgáltatások**

- (1) Az informatikai szolgáltatásokat az Osztály nyújtja a jelen Szabályzat előírásainak megfelelően. Az informatikai céllal üzemeltetett informatikai eszközök használatával az alábbi szolgáltatások vehetők igénybe:
- a) a számítógépekre telepített oktató- és irodai szoftverek használata;
  - b) hálózati alapszolgáltatás (vezetékes és vezeték nélküli hálózatok, internet elérés, telephelyi kapcsolatok);
  - c) levelezőrendszer (@mke.hu);
  - d) fájlszolgáltatások (saját „home” és központi adatterületek az adatok tárolására);
  - e) ügyviteli szolgáltatások (Gazdasági Osztály, valamint Jogi és Humánpolitikai Osztály alkalmazásai);
  - f) központi tanulmányi rendszer (Neptun);
  - g) webszolgáltatások (publikus és belső);
  - h) nyomtatási szolgáltatások (nyomtatás, másolás és szkennelés direkt és kártyás azonosítással);
  - i) iktató rendszer (dokumentumok digitalizálása és archiválása);
  - j) távmunka és távoktatás támogatás (egyetemi hálózaton kívüli munkavégzés biztosítása).
- (2) A felhasználók státuszuk és jogosultságuk szerint vehetik igénybe az alábbi szolgáltatásokat, jelen Szabályzat, valamint az Adatvédelmi Szabályzat rendelkezéseinek, a személyiségi jogokra, illetve a személyes adatok védelmére irányuló jogszabályok betartása mellett.
- a) Hálózati alapszolgáltatás: Az Egyetem telephelyein használható vezetékes és vezeték nélküli belső TCP/IP hálózatok, az elérhető Internet kapcsolatok, DHCP, DNS és a hálózathozzáférés-védelmi rendszerek kezelése, és biztosítása a felhasználók számára. Ide tartozik az Epreskert és a főépület között kialakított telephelyek közötti VPN kapcsolat is. A

- központi hálózatot az Osztály üzemelteti és fejleszti, végzi a központi IP tartomány felosztását, a központi hálózat passzív és aktív elemeinek konfigurálását, hálózati menedzsmentjét.
- b) Publikus és belső WEB szolgáltatások: Az Egyetem központi WEB szerverét az Osztály működteti külső szerver parkban. A meglévő domain nevekkel kapcsolatos feladatokat az Osztály látja el azzal, hogy új domain regisztrálására, vagy meglévő megszüntetésére csak a kancellár adhat engedélyt.
- c) Fájlszolgáltatások: a vándorló profilok, a home területek, más osztályok speciális célú megosztott könyvtárai, az intézményi szervezeti egységei számára fenntartott területek és a mentések készítésére szolgáló területek.
- d) Ügyviteli szolgáltatások és központi tanulmányi rendszer: Az intézmény saját szerverein üzemeltet olyan egyedi alkalmazásokat, melyek egy vagy több egység feladatainak ellátásához szükségesek (pl.: gazdasági/pénzügyi/HR alkalmazások, tanulmányi és iratkezelő rendszerek). A szolgáltatás magában foglalja a szerver és kliens oldali szoftver komponensek installálását, karbantartását, frissítését, jogosultságok beállítását, a rendszer biztonsági mentését.
- e) Levelezőrendszerek: A @mke.hu és a @kepzo.hu címekhez tartozó levelezési- és csoportmunka támogatási szolgáltatáscsomag, illetve a publikus WEB szerveren az alkalmazások számára elérhető SMTP szolgáltatás együttese. Az Egyetem oktatói, tanárai, hallgatói, valamint az egyéb munkakörben alkalmazott munkatársai jogosultak a levelezési szolgáltatás használatára. Levelezési címeket az Osztálytól lehet igényelni az alábbi címképző irányelvek figyelembe vételével:
- az általános felhasználói e-mail cím [vezeteknev.keresztnev@mke.hu](mailto:vezeteknev.keresztnev@mke.hu) alakú;
  - egyes esetekben funkcióhoz kapcsolódó e-mail címek is kioszthatók, pl. [rektor@mke.hu](mailto:rektor@mke.hu);
  - szükség esetén az intézményi egységek elsősorban terjesztési listák formájában a saját nevükre utaló címet, vagy ALIAS-t használhatnak, pl. [tanulmanyi@mke.hu](mailto:tanulmanyi@mke.hu).
- f) Nyomtatási szolgáltatások: Az Egyetem munkaállomásaira és a hálózatára csatlakoztatott nyomtatók, lapolvasók és multifunkciós eszközök kezelését, a nyomtató kiszolgáló kezelését, és a kártyával igénybe vehető nyomtatási lehetőségek kezelését magába foglaló szolgáltatás.
- g) Távmunka és távoktatás támogatása: Távmunka és távoktatási lehetőségek biztosítása hálózaton kívüli munkaállomásoknak WEB-es, VPN és terminál szerver szolgáltatások segítségével történik.
- h) Rendszerüzemeltetési szolgáltatás: Az Osztály különösen 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).

## INFORMATIKAI BIZTONSÁG

### 11. § Az informatikai biztonság szabályozásának célja

- (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 az Egyetem szervezeti egységei részére egységes és általános értelmezést adjon az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége, rendelkezésre állása és funkcionalitása biztosítása érdekében követendő irányelvekre.
- (3) A Szabályzatban meghatározott védelemnek működni 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.

### 12. § Az informatikai rendszerek biztonsági besorolásai

- (1) Az Egyetem rendszerei a működésben betöltött szerepük alapján kritikus rendszerek, kiemelt rendszerek és normál rendszerek kategóriájába sorolhatók.
- (2) Kritikus rendszerek (A): Az Egyetem működése szempontjából kritikus, az intézmény egészére kiterjedő rendszerek, amelyek szenzitív, illetve személyes adatokat, illetve a működés szempontjából kiemelten fontos adatokat tartalmaznak. Adatvédelmi szempontból kiemelt védelmet igényelnek. Ide tartoznak:
  - a) bér- és munkaügyi rendszer;
  - b) gazdasági, ügyviteli rendszer;
  - c) dokumentumkezelési, iktatási rendszer;
  - d) tanulmányi rendszer;
  - e) központi levelezési rendszer;
  - f) könyvtári rendszer;
  - g) központi fájlrendszerek;
  - h) A feniték megbízható működését biztosító intézményi szerverek (adatbázis, autentikációs, stb).
- (3) Kiemelt rendszerek (B): Az Egyetem működése szempontjából kiemelt rendszerek, amelyek elsősorban technikai jellegűek, a rajtuk tárolt adatok nem személyes jellegűek. Ide tartoznak:

- a) Telekommunikációs hálózat,
  - b) Kommunikációs rendszerek.
- (4) Normál rendszerek (C): A vagy B kategóriába nem sorolt, az Egyetem napi működése szempontjából nem kritikus vagy kiemelt, illetőleg az Egyetemnek csak egyes részeire kiterjedő rendszerek. Különösen:
- informatikai géptermekek;
  - nyomtatási rendszerek;
  - publikus weboldalak;
  - vezeték nélküli hálózat.

### **13. § Védelmet igénylő, az informatikai rendszerre ható elemek**

- (1) Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és a 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, előírászerű felhasználására, reprodukálhatóságára.
- (4) A védelem eszközei: A mindenkor 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.

### **14. § Felelősségi körök**

- (1) Az Egyetem intézményi szintű vezetése, illetve az Egyetem további vezetői felelősek a saját területükön az informatikai biztonsági szabályokban foglaltak betartatásáért.
- (2) Az informatikai biztonság felelősei a rendszergazdák, akik információbiztonsági kérdésekben az Informatikai Osztály osztályvezetőjének tartoznak beszámolási kötelezettséggel. A rendszergazda feladata az informatikai biztonság körében különösen:
- a) javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására;
  - b) meghatározza a védett adatok körét;
  - c) ellátja az adatkezelés és adatfeldolgozás felügyeletét;

- d) ellenőrzi a védelmi előírások betartását;
  - e) az adatvédelmi feladatok ismertetése;
  - f) a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli;
  - g) a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről;
  - h) ellenőrzi a szoftverek használatának jogszerűségét.
- (3) A Szerverüzemeltető informatikai biztonsággal kapcsolatos feladatai:
- a) felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért;
  - b) gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról;
  - c) feladata a védelmi eszközök működésének folyamatos ellenőrzése;
  - d) gondoskodik a folyamatos vírusvédelemről;
  - e) folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását;
  - f) javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére, illetve bevezetésére;
  - g) ellenőrzi a rendszer adminisztrációját.
- (4) Az Egyetem informatikai rendszerének felhasználói (rendszergazdák, felhasználók, hallgatók, vendégek, külső felhasználók) kötelesek betartani a jelen Szabályzatban leírtakat, továbbá kötelesek jelenteni az Osztálynak ([support@mke.hu](mailto:support@mke.hu)), ha biztonsági problémát okozó jelenséget (biztonsági incidenst) észlelnek.

## **15. § A védelmet igénylő adatok és információk**

- (1) Az Egyetem minősített adatokat nem kezel. Az adatokhoz történő hozzáférést, azok megismerhetőségét a szükséges minimális jogosultságok megadásával kell biztosítani. Alapelve, hogy mindenki csak ahhoz az adathoz és csak olyan módon férhessen hozzá, amire a munkájához szüksége van.
- (2) 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.
- (3) 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).

## **16. § Az informatikai eszközbázist veszélyeztető helyzetek**

- (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:
    - földrengés;
    - árvíz;
    - tűz;



- villámcsapás stb.
- b) környezeti kár:
- légszennyezettség;
  - nagy teljesítményű elektromágneses térerő;
  - elektrosztatikus feltöltődés;
  - a levegő nedvességtartalmának felszökése vagy leesése;
  - piszkolódás (pl. por).
- c) közüzemi szolgáltatásba bekövetkező zavarok:
- feszültség–kimaradás;
  - feszültségingadozás;
  - elektromos zárlat;
  - csőtörés.

### (3) Emberi tényezőre visszavezethető veszélyek

- a) Szándékos károkozás:
- behatolás az informatikai rendszerek környezetébe;
  - illetéktelen hozzáférés (adat, eszköz);
  - adatok– eszközök eltulajdonítása;
  - rongálás (gép, adathordozó);
  - megtevesztő adatok bevitele és képzése;
  - zavarás (feldolgozások, munkafolyamatok).
- b) 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.

(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.

## **17. § Az informatikai eszközök védelme**

- (1) Védett helyiségnek kell tekinteni azokat a helyiségeket, ahol adatok feldolgozására, tárolására alkalmazott informatikai erőforrások találhatóak. A védett területek zárt területnek minősülnek, ezért védelmükről ennek megfelelően kell gondoskodni. Az Egyetemen védett területnek minősül:
- a) a szerverhelyiség;
  - b) aktív hálózati elemek elhelyezésére szolgáló helyiségek, rendező szekrény (rack);
  - c) számítástechnikai eszközzel felszerelt valamennyi iroda.
- (2) Vagyonvédelmi előírások:

- a) a szerverhelyiségeket és a rendező szekrényeket (rack) biztonsági zárral 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 Egyetem vezetőjének azonnal jelenteni kell;
- d) az informatikai eszközöket csak a megfelelő jogosultsággal rendelkező felhasználók használhatják.

(3) Tűzvédelem:

- a) A szerverhelyiség a „D” mérsékelt tűzveszélyességi osztályba tartozik.
- b) A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.
- c) A szerverhelyiségben biztosítani kell a megfelelő, elektromos berendezések oltására alkalmas 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.

(4) 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 adatállományt;
- b) biztonsági mentésekről, háttértákról a megsérült adatok visszaállítása;
- c) archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

(5) Hardver védelem:

- a) A berendezések hibátlan és üzemszerű működését biztosítani kell.
- b) A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése, cseréje.
- c) Az üzemeltetést, karbantartást és szervizelést az Osztály végzi, bizonyos esetben külső szerviz szolgáltatás igénybevételével.

(6) A munkák elvégzése során figyelembe kell venni a gyártó előírásait, ajánlásait.

(7) 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 bevitelénél alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

(8) 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 a szervezeti 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.
- (9) 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.
- (10) Mentések, fájlok 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 Osztály munkatársainak kell segítséget nyújtani;
  - d) a szervereken tárolt adatokról a mentést rendszeresen el kell végezni, a mentésért a rendszergazdák a felelősek.
- (11) Programhoz való hozzáférés, programvédelem:
- a) az Osztálynak biztosítani kell, hogy a rendszerszoftverek naprakész állapotban legyenek és a segédprogramok, programkönyvtárak mindig hozzáférhetőek 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.
- (12) A programokról a leltározásért felelős szervezeti egységnek naprakész nyilvántartást (szoftver leltárt) kell vezetni.
- (13) Központi gépek, szerverek védelme:
- a) Szünetmentes áramforrást kell használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén az adatvesztéstől.
  - b) A központi gépek háttértáiról 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.
- (14) Munkaállomások védelme:
- a) Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
  - b) Vírusfertőzés gyanúja esetén az Osztályt azonnal értesíteni kell.
  - c) Az Egyetem 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.

## **A SZOFTVERHASZNÁLAT RENDJE**

### **18. § A szoftverhasználattal kapcsolatos szabályok**

- (1) 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:
  - a) aki a szoftvert, vagy annak dokumentációját, beleértve a programokat, alkalmazásokat, adatokat, kódokat és kézikönyveket a szerzői jog tulajdonosának engedélye nélkül lemásolja vagy terjeszti;
  - b) aki szerzői jog által védett szoftvert egyidejűleg két vagy több gépen futtat, hacsak ezt a szoftver licenc szerződése külön nem engedélyezi;
  - c) az a szervezet, amely tudatosan vagy akaratlanul munkatársait arra ösztönzi, kötelezi, vagy számukra megengedi, hogy illegális szoftvermásolatokat készítsenek, használjanak, vagy terjesszenek;
  - d) aki az illegális szoftvermásolást tiltó törvényt megsérti azért, mert valaki erre kéri vagy kényszeríti;
  - e) aki szoftvert kölcsön ad úgy, hogy arról másolatot lehessen készíteni, vagy aki a kölcsönkért szoftvert lemásolja;
  - f) aki olyan eszközöket készít, importál, vagy birtokol, amelyek lehetővé teszik a szoftver védelmét szolgáló műszaki eszközök eltávolítását, vagy ilyen eszközökkel kereskedik.
- (2) Az Egyetemen tilos az szerzői jogról szóló törvénybe ütköző szoftverhasználat.
- (3) Valamennyi szervezeti egység vezetője felelős az érintett szervezeti egységnél és az ott elhelyezett eszközök tekintetében a legális szoftvergazdálkodásért, amit ezen Szabályzat betartásával és betartatásával valósít meg.
- (4) Az Egyetem nevében beszerzett licenck hasznosításáról, illetve a szervezeti egység által beszerzett szoftver szervezeti egységen kívüli hasznosításáról – amennyiben azt licencszerződés lehetővé teszi, és a szervezeti egység vezetője ehhez hozzájárul – az informatikai osztályvezető javaslata alapján az illetékes vezető dönt. Az informatikai osztályvezető javaslatot tehet a szoftver licenck újra hasznosításáról, amennyiben azt szakmai indokok alátámasztják.
- (5) Az e Szabályzatban nem szabályozott kérdésben az informatikai osztályvezető javaslata alapján az illetékes vezető jogosult dönteni, és a szükséges intézkedéseket megtenni.

### **19. § Szoftverhasználattal kapcsolatos feladatok**

- (1) A rendszergazda feladatai különösen:
  - 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 és a szervezeti 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) Rendszeresen ellenőrzi a szoftverhasználatot.

- f) Bizonyos szoftverek adatait, hozzáférhetőségét az Egyetem dolgozói körében nyilvánosságra hozza – a kellő licenc számának erejéig.
  - g) A szervezeti egységeknek tanácsot ad a szoftverbeszerzés területén.
- (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 alkalomszerűen ellenőrzi az adott szervezeti egységen belül a szoftverek legalitását, a vonatkozó rendelkezések betartását. Az ellenőrzésről jegyzőkönyvet készít, melyet az Osztály osztályvezetőjének ad át.
  - d) A rendszergazda szoftverhasználattal kapcsolatos mindennemű felelőssége megszűnik, ha azt nem ő telepítette. A rendszergazda haladéktalanul köteles a felelősség megszűnését és a kiváltó okokat az Osztály osztályvezetőjének írásban bejelenteni.
- (3) A szervezeti egységek vezetőjének feladatai különösen:
- a) Az Egyetem szoftverhasználati szabályait az alkalmazottakkal ismertetni, betartását ellenőrizni.
  - b) Biztosítani a jogtiszt szoftverek hatékony felhasználását.
- (4) A szervezeti 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.
- (5) A dolgozók otthoni és a hallgatók saját használatában lévő számítógépek tekintetében a szoftverhasználat rendjére az éppen aktuális felsőoktatási szoftver keretszerződések az irányadók.

## **20. § Adatkezelés, adatvédelem**

- (1) Az informatikai eszközök használata során a felhasználók kötelesek betartani az adatkezelésre és adatvédelemre, a közérdekű adatok nyilvánosságára vonatkozó jogszabályokat, valamint az Egyetem Adatvédelmi Szabályzatában foglaltakat.
- (2) Az adatbiztonság érdekében az Egyetem informatikai eszközeit technikailag és jogilag védeni kell a külső behatolás ellen.
- (3) Szerzői jogokkal védett anyagok kezelése érdekében az Egyetem informatikai rendszerébe jogszabályban, szerződésben biztosított felhasználási jog alapján, illetve megfelelő licenc engedély birtokában lehet programokat telepíteni.
- (4) Az Egyetem informatikai rendszerén nem helyezhetők el:
  - a) az emberi és személyiségi jogokba ütköző, diszkriminatív (kirekesztő) jellegű;
  - b) ifjúság– és természetellenes, pornográf (szemérem sértő) jellegű;
  - c) politikai és harcászati célú, az erőszak bármely formáját propagáló;
  - d) reklámozásra és más üzleti célra felhasználható;
  - e) az Egyetemnek, az Egyetem 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) Az Egyetem eszközeivel csak az intézmény számára és személyes célra készíthetők dokumentumok. A személyes célra készült dokumentumok nem szolgálhatnak anyagi haszonszerzés, vagy politikai propaganda céljául.
  - c) A felhasználók adatai az eszközök meghibásodása, vagy bármely más okból megsérülhetnek. Az ebből származó károkért az Egyetem felelősséget nem vállal.
- (6) A felhasználó adatvédelemmel kapcsolatos jogai:
- a) A felhasználó jogosultsága alapján saját adatterülettel rendelkezhet az Egyetem 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 szabályok betartása és betartatása, valamint a rendszer és a hálózat biztonságának megőrzése érdekében az Osztály osztályvezetője ezek megsértésének tényét írásban közli a jogsértő személy munkahelyi felettesével és a kancellárral.

## **21. § Intézkedések**

- (1) A rendszergazda jogosult bármikor ellenőrizni az Egyetem 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 Egyetem eszközeit nem a Szabályzat előírásainak megfelelően használja, úgy felelősségre vonás kezdeményezhető vele szemben. Mivel a szabályok megszegése az Egyetem egész informatikai rendszerének, az Egyetem 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 felhasználó munkahelyi felettesének, az Informatikai Osztály osztályvezetőjének, illetve a munkáltatói jogkör gyakorlójának, aki dönt a felelősségre vonásról.
- (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 korlátozása az elkövetett szabálytalanság függvényében lehet ideiglenes vagy végleges. A rendszergazda az általa hozott korlátozó intézkedéseket a felhasználó munkahelyi felettesének, vagy hallgató esetében a szak-gazda tanszék vezetőjének, valamint az Informatikai Osztály osztályvezetőjének jelenti, aki dönt annak jóváhagyásáról, illetve a továbbiakban szükséges intézkedésekről. A korlátozó intézkedések ellen a munkáltatói jogkör gyakorlójánál lehet panasszal élni.
- (4) Amennyiben az elkövetett vétség feltehetően szabálysértésnek vagy bűncselekménynek minősül, úgy az Informatikai Osztály osztályvezetője köteles azt a kancellárnak jelenteni, aki gondoskodik az esetleges feljelentés megtételéről.
- (5) A felhasználó minden olyan általa okozott kárért teljes körű kártérítési kötelezettséggel tartozik, mely az eszközök rendeltetés, vagy előírás szerinti használatának megszegése miatt történik.

## **22. § Záró rendelkezések**

- (1) Jelen Szabályzat a Szenátus döntését követő napon lép hatályba. A hatálybalépéssel egyidejűleg hatályát veszti az Egyetem korábbi Informatikai Szabályzata.

# 1. SZ. MELLÉKLET: FELHASZNÁLÓI NYILATKOZAT

## Felhasználói nyilatkozat

Alulírott jelen nyilatkozat aláírásával kijelentem, hogy a Magyar Képzőművészeti Egyetem (a továbbiakban: MKE) Informatikai Szabályzatát ismerem és az abban foglaltakat magamra nézve kötelezőnek tekintem. Kijelentem továbbá, hogy a MKE számítógépes rendszeréhez való hozzáférésre jogosító felhasználói nevemet és kezdeti jelszavamat tartalmazó dokumentumot átvettem. A szabályzatok elektronikus formában elérhetők a <http://www.mke.hu/about/dokumentumok.php> címen, valamint nyomtatott formában az informatikai osztály irodájában.

Tudomásul veszem továbbá az alábbiakat:

- a) Az általam kezelt számítástechnikai eszközök nem megfelelő vagy szerzői jogot sértő üzemeltetéséből, hibás beállításából eredő kárért teljes körű felelősség (polgári- és büntetőjogi is) terhel.
- b) A MKE informatikai erőforrásaihoz jogosultságot biztosító jelszavaimat más személynek nem adhatom ki, ezen hozzáférési jogosultsággal/jogosultságokkal elkövetett minden szabálysértésért, a számítógépen lokálisan tárolt, illetve hordozható médián tárolt állományokért, adatokért, szoftverekért és az így okozott esetleges kárért felelősséggel (polgári- és büntetőjogi is) tartozom.

Jelen nyilatkozatban foglaltak betartása az MKE-vel fennálló szerződéses jogviszonyomból eredő lényeges kötelezettségemet képezi.

Kelt (város, dátum): ....., .....

Név (nyomtatott betűvel): .....

Aláírás: .....



## 2. SZ. MELLÉKLET: KILÉPŐ FELHASZNÁLÓI NYILATKOZAT

### Kilépő felhasználói nyilatkozat

Alulírott jelen nyilatkozat aláírásával tudomásul veszem, hogy a Magyar Képzőművészeti Egyetem informatikai rendszerében használt számítógépes hozzáférésem a mai naptól megszűnik. Tudomásul veszem, továbbá, az egyetemi informatikai rendszerben tárolt minden elektronikus anyagom (dokumentumok, levelek, stb.) törlésre kerül, ezek visszaállítására, a későbbiekben nincs lehetőség.

A régi e-mail címemre érkező levelek átirányítását KÉREM a következő címre\*:

privát e-mail címem: .....

A régi e-mail címemre érkező levelek átirányítását NEM KÉREM, az e-mail cím véglegesen törölhető!\*

\*a megfelelőt kérjük aláhúzni!

Budapest, .....

Személynév (nyomtatott betűvel): .....

Aláírás: .....

**Tájékoztatás:** Mivel az egyetemi e-mail postafiók szintén törlődik, amennyiben leveleit még nem töltötte le eddig, ebben az informatikai osztály munkatársa jelen nyilatkozat aláírásakor még segítséget nyújt, a későbbiekben a levelek visszaállítására szintén nincs lehetőség.

Az egyetemi e-mail címre érkező levelek külső, privát e-mail címre történő átirányítására azonban lehetőség van 1 éven át. Ez nem vonatkozik a belső csoportos levelezésre (pl. mindenki@mke.hu) hiszen ezekből a csoportokból a felhasználó eltávolításra kerül. Jelen nyilatkozat aláírásának időpontjától számított egy éven múlva az egyetemi @mke.hu végződésű e-mail cím véglegesen megszűnik, visszaállítására nincs lehetőség.

### 3. SZ. MELLÉKLET: MEGISMERÉSI NYILATKOZAT

#### Megismerési nyilatkozat

Aláírással nyilatkozom, hogy a Magyar Képzőművészeti Egyetem informatikai szabályzatában foglaltakat megismertem.

Sorsz.	Nyilatkozó szervezeti egysége	Nyilatkozó neve	Nyilatkozó beosztása	Nyilatkozó aláírása