23-17/2015/MMA

IGAZGATÓ

MMA
MAGYAR MŰVÉSZETI AKADÉMIA
Művészetelméleti és Módszertani Kutatóintézet

1121 Budapest, Budakeszi út 38.
Levelezési cím:
1368 Budapest, Pf. 262
Telefon: +36 (30) 427-4743
Email: titkarsag@mma-mmki.hu
Web: www.mma-mmki.hu

A MAGYAR MŰVÉSZETI AKADÉMIA

MŰVÉSZETELMÉLETI ÉS MÓDSZERTANI KUTATÓINTÉZET IGAZGATÓJÁNAK

.11../2015. (XII../XVII) számú utasítása

a Magyar Művészeti Akadémia Művészetelméleti és Módszertani Kutatóintézet

Informatikai biztonsági szabályzatáról

1. A Magyar Művészeti Akadémia Művészetelméleti és Módszertani Kutatóintézet Szervezeti és Működési Szabályzatában biztosított jogkörömnél fogva az MMA Művészetelméleti és Módszertani Kutatóintézet Informatikai biztonsági szabályait az utasításban foglaltak szerint határozom meg.

2. Jelen utasítás az aláírást követő munkanapon lép hatályba.

3. Az MMA Művészetelméleti és Módszertani Kutatóintézet Informatikai biztonsági szabályairól szóló utasítást az Intézet munkatársai számára helyben szokásos módon ki kell hirdetni.

Budapest, 2015. 12. 18.

dr. Kocsis Miklós PhD
mb. igazgató

A Magyar Művészeti Akadémia Művésztelméleti és Módszertani Kutatóintézet (a továbbiakban: Intézet) által működtetett informatikai rendszerekre vonatkozóan a biztonsági és üzemeltetési intézkedések szabályozására, a számítástechnikai eszközök használata, továbbá az adatkezelés folyamatának biztonsági szabályai meghatározására, az informatikai szerepkörök behatárolására és az egyes szereplők informatikai biztonságot érintő feladatai azonosítására az Intézet Informatikai Biztonsági Szabályzatát (a továbbiakban: IBSZ vagy szabályzat) a következők szerint határozom meg:

A szabályzat célja

1. § (1) Az IBSZ alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, és megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát az Intézet informatikai eszköz- és vagyonvédelmének intézményi szintű szabályozása, illetve az üzemeltetési, felhasználói, vezetői teendők és felelősségi körök meghatározása útján.

(2) Az IBSZ célja továbbá az Intézetnél

a) a titok-, a vagyon- és a tűzvédelemre vonatkozó védelmi intézkedések betartása,

b) az üzemeltetett informatikai rendszerek rendeltetésszerű használata,

c) az üzembiztonságot szolgáló karbantartás és fenntartás,

d) az adatok informatikai feldolgozása és azok 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 alkalmazott programok és adatállományok dokumentációinak nyilvántartása,

g) a munkaállomásokon lekérdezhető adatok körének meghatározása,

h) az adatállományok biztonságos mentése,

i) az informatikai rendszerek zavartalan üzemeltetése,

j) a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,

k) az adatvédelem és adatbiztonság feltételeinek megteremtése.

A szabályzat hatálya

2. § (1) Az IBSZ személyi hatálya kiterjed az Intézet valamennyi közalkalmazotti és munkavállalói jogviszonyban foglalkoztatott munkatársára és az Intézet tulajdonában vagy használatában álló informatikai eszközt, az Intézet által üzemeltetett rendszert használó további személyekre.

(2) Az IBSZ tárgyi hatálya kiterjed

a) az Intézet tulajdonában lévő, illetve az általa bérelt valamennyi informatikai eszközre, valamint azok műszaki dokumentációira,

b) az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési stb.),

c) az a) pont szerinti eszközökön található valamennyi rendszer- és felhasználói programra,

d) az adatok felhasználására vonatkozó utasításra,

e) az elektronikus adathordozókra, azok tárolására, felhasználására, beleértve a feldolgozásra beérkezés és a felhasználókhoz eljuttatás folyamatát.

(3) A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt, ide értve a tervezést, az üzemeltetést és a felhasználást. Ha valamely esetben időlegesen egyes rendszerek, programok IBSZ-től eltérő alkalmazása szükséges, azt az igazgató engedélyezheti.

Az adatkezelés során használt fontosabb fogalmak

3. § (1) Adat: az információ hordozója, megjelenési formája, értelmezhető (észlelhető, érzékelhető, felfogható és megérthető) jelsorozat. Olyan jelsorozat, amelyből információ nyerhető ki.

(2) Adatállomány: adathordozón tárolt, jelképes névvel ellátott adathalmaz.

(3) Adatbázis: a megfelelő kezelőszoftverrel rendszerbe szervezett egy vagy több adatállomány.

(4) Adathalmaz: valamilyen feldolgozás részére rendelkezésre álló adatok összessége.

(5) Adatbiztonság: az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és a szervezési intézkedések és eljárások együttes rendszere.

(6) 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.

(7) Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi.

(8) Adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása, vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése.

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

(10) Adattovábbítás: az adat harmadik személy számára történő hozzáférhetővé tétele.

(11) Adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.
(12) Adatvédelem: az adatok jogosulatlan megszerzésének, illetve manipulálásának megakadályozására irányuló intézkedések összessége.
(13) Adatzárolás: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából.
(14) Érintett: bármely, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy.
(15) Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval.
(16) Hozzáférés: olyan eljárás, amely a felhasználó számára, jogosultsága függvényében elérhetővé teszi az informatikai rendszer erőforrásait.
(17) Informatikai biztonság: az informatikai rendszer olyan állapota, amelyben az adatokhoz minden felhasználó kizárólag jogosultsága mértékében képes hozzáférni. Az adatok egyéb (nem szabályozott) módon nem változnak s hitelességük megállapítható. A rendszer rendelkezésre állása kielégíti a megadott követelményeket.
(18) Informatikai eszköz: minden olyan hardver és szoftver elem, amely az informatikai és számítástechnikai rendszerek működésében részt vesz.
(19) Informatikai rendszer: az adat- illetve információkezelés különböző feladatainak és folyamatainak teljesítésére alkalmazott, hardverek és szoftverek kombinációjából álló rendszer.
(20) Informatikai rendszerek működtetéséért és fejlesztéséért felelős szervezeti egység: az Intézet Igazgatói Titkársága.
(21) Működőképesség: a rendszernek és elemeinek, az elvárt s igényelt üzemeltetési állapotban való fennmaradása.
(22) Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele.
(23) Program: eljárási leírás, amely valamely informatikai rendszer által közvetlenül vagy átalakítást követően végrehajtható.
(24) Rendelkezésre állás: az a tényleges állapot, amikor információk vagy adatok elérhetősége és a rendszer működőképessége az arra jogosultak számára sem átmenetileg, sem pedig tartósan nincs akadályozva.
(25) Személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés.
(26) Szoftver: valamely informatikai rendszer olyan logikai része, amely a működtetés vezérléséhez szükséges.
(27) Vírus: olyan programtörzs, amely önállóan vagy a felhasználói programba épülve annak normál működését akadályozza.

Biztonsági osztály

4. § Az Intézet által használt informatikai rendszerek alapbiztonsági osztályba tartoznak. Ez a személyes adatok, üzleti titkok, pénzügyi adatok, illetve az Intézet belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.

Védelmet igénylő, az informatikai rendszerre ható elemek

5. § (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.

A védelem tárgya

6. § (1) A védelmi intézkedések kiterjednek:
a) az informatikai rendszer elhelyezésének környezetére,
b) az alkalmazott hardver eszközökre és azok működési biztonságára,
c) az informatikai eszközök üzemeltetéséhez szükséges dokumentációra,
d) az adatokra a keletkezésüktől a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
e) az adathordozókra az érvénytelenítésükig és selejtezésükig,
f) az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszerszoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,
g) a személyhez fűződő és a vagyoni jogokra.

A védelem eszközei

7. § 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.

A védelem felelőse

8. § (1) A védelem felelőse az igazgató, az Intézet informatikai rendszerek működtetéséért és fejlesztéséért felelős szervezeti egységének vezetője, továbbá a rendszergazda és (amennyiben van ilyen) az alkalmazásgazda.
(2) A jelen szabályzatba foglalt felhasználói feladatok betartásáról és ellenőrzéséről a szervezeti egységek vezetői gondoskodnak.

Az adatok védelemért felelős személyek feladatai

9. § Az igazgató irányítja az informatikai rendszerek működtetéséért és fejlesztéséért felelős szervezeti egység tevékenységét, jóváhagyja az IBSZ-t és a kapcsolódó szabályzatokat, stratégiákat, továbbá dönt beruházások, fejlesztések engedélyezéséről; ha kötelezettséget vállalni egyéb szabály alapján nem jogosult, az informatikai rendszerek működtetéséért és fejlesztéséért felelős szervezeti egység vezetőjének kezdeményezésére javaslatot tesz beruházásra, fejlesztésre.

10. § Az informatikai rendszerek működtetéséért és fejlesztéséért felelős szervezeti egység vezetőjének feladatai:

a) felügyeli az Intézet informatikai rendszerének folyamatos és egységes működtetését, amelynek keretében
  aa) az üzemeltetést végző külső cégek, megbízottak munkáját koordinálja, ellenőrzi,
  ab) az informatikai eszközökkel kapcsolatos javítási, karbantartási szerződéseket megkötésre előkészíti,
  ac) nyomon követi az informatikai tárgyú szerződéseket, azok teljesítését ellenőrzi és igazolja,
  ad) nyomon követi az Intézet által üzemeltetett informatikai eszközök és a felhasználók jogosultsági beállításait,
  ae) kivizsgálja az informatikai biztonsági eseményeket,
  af) javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére;
b) az informatikai biztonságot meghatározó, befolyásoló területek, tevékenységek összehangolása;
c) az IBSZ előkészítése, naprakészen tartása, módosítása kezdeményezése;
d) az Intézet Szervezeti és Működési Szabályzatának és egyéb szabályzatainak informatikai biztonsági szempontból való véleményeztetése;
e) felelős az Intézet informatikai rendszere hardver eszközeinek karbantartásáért;
f) az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása;
g) ellenőrzi a védelmi előírások betartását, a felhasználók számítógépén a szoftverek használatának jogszerűségét, a védelmi eszközökkel való ellátottságot;

h) nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket
i) figyelemmel kíséri az Intézetnél az IBSZ betartását, előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét;
j) betekinthet valamennyi iratba, amely az informatikai feldolgozásokkal kapcsolatos.

11. § (1) A rendszergazda irányítja és végzi a szerverek és a kliens gépek rendszerszoftver üzemeltetési feladatait.
(2) A rendszergazda feladatai:
a) az informatikai rendszerek felügyelete,
b) gondoskodik az informatikai rendszerek kritikus részeinek újraindíthatóságáról, illetve az újraindításhoz szükséges paraméterek reprodukálhatóságáról,
c) gondoskodik a folyamatos vírusvédelemről,
d) vírusfertőzés gyanúja esetén gondoskodik a fertőzött informatikai rendszer vírusmentesítéséről,
e) felelős az informatikai rendszerek üzembiztonságáért, a szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
f) a védelmi eszközök működésének folyamatos ellenőrzése,
g) folyamatosan figyelemmel kíséri és vizsgálja az informatikai rendszerek működése és biztonsága szempontjából a lényeges paraméterek alakulását,
h) ellenőrzi az informatikai rendszerek önadminisztrációját,
i) az arra jogosultak kezdeményezése alapján a jogosultsági szintek beállítása és gondozása,
j) a felügyelete alá tartozó teljes rendszer komplex biztonságával összefüggésben minden üzemeltető és felhasználó felé jogosult intézkedni, tevékenységüket jogosult korlátozni.

12. § (1) Az igazgató a kritikus fontosságúnak minősített informatikai rendszerhez alkalmazásgazdát nevez meg. Az alkalmazásgazda feladata a rábízott rendszer olyan mélységű ismerete, hogy zavartalan működését szakmai oldalról ellenőrizni tudja, illetve szükség esetén intézkedni tudjon a biztonságos működés érdekében.
(2) A szakmai rendszerek közvetlen felügyelője:
a) feladatának ellátásához szükséges hozzáféréssel rendelkezik, a megfelelő szoftverrendszer vonatkozásában;
b) az adott szoftverrendszer által biztosított lehetőségek alapján, a jogosultsági struktúra szerint gondoskodik az adott szakmai rendszerben a felhasználói jogosultságok beállításáról; a jogosultsági beállításokat dokumentálja (ez automatikus is lehet, amennyiben a rendszer rendelkezik ilyen lehetőségekkel);
c) szakmai támogatást nyújt a felhasználóknak a szoftverrendszer használatát illetően;
d) az adott szakmai rendszert illetően meghatározhatja az adatmentéseket, archiválásokat;
e) hiba esetén közreműködik a szakmai rendszer helyreállításában, tesztelésében.

13. § (1) Az Intézet informatikai rendszereinek összes felhasználója mindenben köteles a vonatkozó informatikai-szakmai és biztonsági szabályokat betartani, illetve ezek betartásában az informatikai rendszer használatát irányító személyekkel együttműködni.

(2) A felhasználó feladatai:

a) az adatok elvárható és a vonatkozó szabályzásoknak megfelelő gondossággal való kezelése;

b) a rendelkezésre bocsátott számítástechnikai eszközök megóvása;

c) a belépési jelszavának (jelszavainak) az előírt vagy javasolt időben történő megváltoztatása, titkosságának megőrzése;

d) a gépen tárolt információk védelme; ha elhagyja a munkaállomást, köteles azt olyan állapotban hagyni (például a számítógép zárolása funkcióval), hogy más ne használhassa, segítségével semmilyen információhoz hozzá ne férhessen, azokat ne módosíthassa, illetve a rendszerbe semmilyen információt be ne juttathasson;

e) felelős adatállományai biztonságáért, ezért köteles a munkaállomásukon létrehozott adatait, dokumentumait a hálózati meghajtókra menteni (amelyek nagyobb megbízhatóságúak, mint a helyi merevlemezek illetve napi rendszeres mentésük biztosított);

f) az általa felügyelt külső szakértők informatikai igényeinek közvetítése az informatikai rendszerek működtetéséért és fejlesztéséért felelős szervezeti egység felé;

g) az üzemeltető személyzettel való együttműködés;

h) az esetlegesen felfedezett biztonsági vagy működési problémák jelentése az illetékes üzemeltető személyzetnek;

i) a számára szervezett informatikai oktatásokon való részvétel;

j) a feladatainak elvégzéséhez szükséges eszközök, alkalmazói programok kezelésének megfelelő szintű ismerete.

(3) A felhasználónak a biztonságos munkavégzés érdekében tilos:

a) az informatikai eszközök megbontása, a hardver konfigurációk megváltoztatása;

b) más felhasználók munkájának akadályozása, dokumentumainak illetéktelen megtekintése, másolása;

c) a hálózat megbontása, átstrukturálása, számítógépek, eszközök engedély nélküli csatlakoztatása, áthelyezése;

d) az Intézet informatikai rendszerében nem alkalmazott vagy tiltott szoftver installálása;

e) engedély nélkül telekommunikációs eszköz beszerelése és használata.

(4) Amennyiben a felhasználó az IBSZ-ben foglaltakat szándékosan vagy gondatlanul megszegi, közvetlen felettese vagy az informatikai rendszerek működtetéséért és fejlesztéséért felelős szervezeti egység vezetője írásban tájékoztatja az igazgatót, aki saját hatáskörében dönt a szankciókról. A szankcionálás körében a felhasználó munkaviszonya vagy az Intézettel fennálló egyéb jogviszonya is megszüntethető,

amennyiben az elkövetett szabályszegés súlya ezt indokolja. A munkaviszony – vagy egyéb jogviszony – megszüntetését megalapozó súlyos szabályszegésnek minősül különösen, az adatlopás, adatvesztés előidézése, adatok illetéktelen harmadik személy részére hozzáférhetővé tétele.

A felhasználói kör karbantartása

14. § (1) A felhasználók informatikai igényei – eltekintve a hibaelhárításhoz szükséges eseti igényeket – a következő eseményekkor jelentkeznek:
a) belépéskor (új felhasználó);
b) felhasználó adatainak változása esetén (felhasználó módosítása);
c) kilépéskor, távozáskor (felhasználó megszüntetése).
(2) Gondoskodni kell a jogosultságok karbantartásáról, melyhez a szükséges információkat az Igazgatói Titkárság kezdeményezésére a rendszer- és az alkalmazásgazda biztosítja. A nem közalkalmazotti- vagy munkajogviszony keretében informatikai eszközt használó személyek vonatkozásában az igazgató adhat engedélyt a használatra, módosításra, illetve törlésre.
(3) Távozás esetén a felhasználó munkatárs a vezetőjével, más személy az igazgatóval közösen köteles rendelkezni az általa használt adatok további sorsáról.

Hozzáférési jogosultságok

15. § (1) A hozzáférési jogosultsági rendszer átfogó gondozása az informatikai rendszerek működtetéséért és fejlesztéséért felelős szervezeti egység feladata, beleértve ennek dokumentálását is, amennyiben a rendszer nem teszi lehetővé az automatikus dokumentálást. Az informatikai rendszerekhez hozzáférési jogosultságot igényelni vagy jogosultság változást kérni az Igazgatói Titkárságnál lehet az 1. számú függelékként csatolt nyomtatvány megfelelő kitöltésével és leadásával.
(2) A hozzáférési jogosultsági igényt az Igazgató bírálja el, az igény jogosságát aláírásával vagy elektronikus úton igazolja.
(3) A hozzáférési jogosultságok biztosításáról, illetve módosításáról – a rendszergazda, vagy üzemeltető megkeresése útján – az Igazgatói Titkárság gondoskodik.

16. § (1) A hozzáférési jogosultság szabályozásának alapelvei:
a) a hozzáférési jogosultságokat az üzemeltetésért felelős illetékes személynek, munkatársnak – a felhasználói névvel és az első jelszóval az operációs rendszer és adatbázis szintjén a rendszer-adminisztrátornak – kell beállítani;
b) a jogosultság beállítását követően az érintett felhasználó haladéktalanul köteles bejelentkezni a rendszerbe és jelszavát módosítani; ennek biztosítására az illetékes

munkatárs, személy a beállítást megelőzően kapcsolatba lép a felhasználóval, egyeztetve az adott időpontban annak rendelkezésre állását.

(2) A jelszavak legalább nyolc karakter hosszúak legyenek és lehetőség szerint vegyesen tartalmazzanak betűket és számokat, illetve speciális karaktert (írásjelet).

(3) Az Intézettel fennálló munkavégzésre irányuló vagy egyéb, felhasználást megalapozó jogviszony megszűnése esetén azonnal intézkedni kell a jogosultság megvonásáról. A felhasználó fiók törlésére csak a felhasználó által kezelt adatok sorsának rendezése után kerülhet sor.

(4) Az Intézettel fennálló munkavégzésre irányuló jogviszony megszűnése vagy a munkatárs más szervezeti egységbe történő áthelyezése esetén az illetékes vezető és a felhasználó rendezi az adatok, adathordozók stb. átadását vagy a vezető és az üzemeltetésért felelős végrehajtja a szükséges feladatokat. A felhasználói név törlését csak az adatok sorsának elrendezése után rendelheti el az informatikai rendszerek működtetéséért és fejlesztéséért felelős szervezeti egység vezetője.

(5) A hozzáférési jog megvonását (felfüggesztését) az illetékes vezető szóbeli utasítására is végre kell hajtani, ezt utólag írásban meg kell erősíteni, illetve a végrehajtást azonnal naplózni kell.

(6) Tartós távollét (egy hónapot meghaladó időtartam) esetén a munkatárs jogosultságait fel lehet függeszteni a távollét időtartamára. A jogosultság felfüggesztését, illetve visszavonását a munkatárs vezetője kezdeményezi az igazgatónál.

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

17. § Az Intézet adatállományait, szükség esetén adatcsoportonként, illetve felhasználói rendszerenként, külön törvény, valamint szabályzat alapján minősíteni kell.

(2) Alapelv, hogy mindenki csak ahhoz az adathoz juthasson hozzá, amire a munkájához szüksége van.

(3) Minősítéstől függően egyes információkhoz való hozzáférést a tevékenység naplózásával dokumentálni kell.

(4) A naplófájlokat rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét az igazgatónak azonnal jelenteni kell.

(5) A naplófájlok áttekintéséért, értékeléséért az informatikai rendszerek működtetéséért és fejlesztéséért felelős szervezeti egység vezetője által kijelölt személy és a rendszergazda a felelős.

(6) A jelen szabályzat hatálya alá tartozó személy, aki az adatok gyűjtése, felvétele, tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt), valamint törlése során információkhoz jut, adatkezelési nyilatkozatot tesz (2. *függelék*); a nyilatkozattételt megelőzően kizárható az informatikai szolgáltatások igénybevételéből.

(7) Az adatkezelési nyilatkozat kiállításáért a munkatárs vezetője, egyéb felhasználó esetén az engedélyezéssel egyidejűleg az igazgató, megőrzéséért az Igazgatói Titkárság a felelős.
(8) A minősített adat, titkot képező adat védelmét a feldolgozás – adattovábbítás, tárolás – során az operációs rendszerben és a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver adatvédelem).

Az informatikai eszközbázist veszélyeztető helyzetek

18. § (1) Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások – a környezeti infrastruktúra okozta ártalmak és az emberi tényezőre visszavezethető veszélyek – megelőző intézkedésekkel történő elhárítására törekedni kell.
(2) Környezeti infrastruktúra okozta ártalmak az elemi csapás, a környezeti kár, valamint a közüzemi szolgáltatásban bekövetkező zavarok.
(3) Elemi csapás:
a) földrengés,
b) árvíz,
c) tűz,
d) villámcsapás,
e) egyéb vis major.
(4) Környezeti kár:
a) légszennyezettség,
b) nagy teljesítményű elektromágneses térerő,
c) elektrosztatikus feltöltődés,
d) a levegő nedvességtartalmának felszökése vagy leesése,
e) piszkolódás (pl. por).
(5) Közüzemi szolgáltatásban bekövetkező zavarok:
a) feszültség-kimaradás,
b) feszültségingadozás,
c) elektromos zárlat,
d) csőtörés.
(5) Emberi tényezőre visszavezethető veszélyek: szándékos károkozás, valamint a nem szándékos, illetve gondatlan károkozás.
(6) 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, hálózati forgalom).
(7) 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.
(8) A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen, vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.
(9) Károkozás esetén belső vizsgálatot kell végezni az informatikai rendszerek működtetéséért és fejlesztéséért felelős szervezeti egység vezetőjének közreműködésével.
(10) Károkozás esetén ennek tényéről és a megtett, illetve javasolt intézkedésről írásban kell tájékoztatni a főtitkárt.
(11) Szándékos károkozás esetén azonnal minden további hozzáférés megakadályozása szükséges; erről az informatikai rendszerek működtetéséért és fejlesztéséért felelős szervezeti egység vezetője javaslata alapján az igazgató dönt.
(12) Bűncselekmény elkövetésének gyanúja esetén az Intézetnek az illetékes hatóság felé feljelentést kell tennie.

Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

19. § (1) Tervezés és előkészítés során előforduló veszélyforrások:
a) a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
b) hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.
(2) A rendszerek megvalósítása során előforduló veszélyforrások:
a) hibás adatállomány működése,
b) helytelen adatkezelés,
c) programtesztelés elhagyása.
(3) A működés és fejlesztés során előforduló veszélyforrások:
a) emberi gondatlanság,
b) szervezetlenség,
c) képzetlenség,
d) szándékosan elkövetett illetéktelen beavatkozás,
e) illetéktelen hozzáférés,
f) üzemeltetési dokumentáció hiánya.

Az informatikai eszközök környezetének védelme

20. § (1) Vagyonvédelmi előírások:

a) a számítógép monitorját lehetőleg úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,

b) az informatikai eszköz rendeltetésszerű használatáért a felhasználó felelős.

(2) Adathordozók:

a) könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,

b) az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni,

c) a használni kívánt külső adathordozót a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni,

d) a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,

e) adathordozót más, külső szervezetnek átadni csak az informatikai rendszerek működtetéséért és fejlesztéséért felelős szervezeti egység vezetőjének engedélyével szabad,

f) a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

(3) Elektronikus adattovábbítás:

a) a hálózatra csak hálózati azonosító birtokában szabad csatlakozni,

b) hivatalos dokumentumot harmadik személy felé továbbítani, nyilvánosságra hozni csak nem szerkeszthető formátumban szabad.

Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

21. § (1) A számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

a) a még használható anyag mentése;

b) a biztonsági mentésekről, a háttértárakról a megsérült adatok visszaállítása;

c) archivált anyagok, illetve 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 informatikusok végezik;

d) a munkák szervezésénél figyelembe kell venni a gyártó előírásait, ajánlatait, a tapasztalatokat;

e) bármely számítógép vagy számítástechnikai eszköz szétbontását (kivéve a garanciális gépeket) csak megbízott informatikai szakember végezheti el.

22. § (1) Az informatikai feldolgozás folyamatának védelme kiterjed:

a) az adatrögzítés védelmére,

b) az adathordozók tárolására,

c) az adathordozók megőrzésére,

d) a selejtezésre,

e) a sokszorosításra és a másolásra,

f) a leltározásra,

g) a mentésekre, a fájlok védelmére.

(2) Az adatrögzítés védelme:

a) az adatbevitel hibátlan műszaki állapotú berendezésen történjen;

b) csak tesztelt adathordozóra lehet adatállományt rögzíteni;

c) a bizonylatokat és adathordozókat csak az e célra kialakított és megfelelő tároló helyeken szabad tartani;

d) lehetőség szerint olyan szoftvereket kell vásárolni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is;

e) hozzáférési lehetőség:

ea) bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz; alapelv: a tárolt adatokhoz csak a felhasználás tekintetben illetékes személyek férjenek hozzá,

eb) az adatok bevitele során alapelv, hogy azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti,

ec) a szerverek rendszergazda jelszavát az informatikai rendszerek működtetéséért és fejlesztéséért felelős szervezeti egység vezetője biztosítja;

f) az adatrögzítés folyamatához kapcsolódó dokumentációk:

fa) az adatrögzítési utasítások,

fb) az ellenőrző rögzítési utasítások,

fc) a tesztelő és törlő programok kezelési utasításai,

fd) a megőrzési utasítások,

fe) a gépkezelési leírások.

(2) Az adathordozók tárolására műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

(3) Az adathordozók megőrzési idejét a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvényben, továbbá az Intézet iratkezelési szabályzatában foglaltak alapján az adatkezelő határozza meg.

(4) A selejtezést az Intézet felesleges vagyontárgyai feltárására, hasznosítására és selejtezésére irányadó külön szabály(ok), valamint az Intézet iratkezelési szabályzata és irattári terve alapján kell lefolytatni. Selejtezéskor biztonsági intézkedésekkel kell megakadályozni, hogy a hibás informatikai eszközök adathordozói ellenőrizetlenül kerüljenek ki a szervezeten kívülre. Szintén alapvető követelmény, hogy a selejtezés

vezetői engedélyhez kötött és megfelelően dokumentált legyen. A selejtezési jegyzőkönyvben fel kell tüntetni a selejtezendő alkatrész gyári számát, típusát, valamint a benne lévő adathordozók törléséről szóló nyilatkozatot, a felelős munkatárs aláírásával. A kényes információk kiszivárgásának megelőzése érdekében a selejtezendő adathordozók esetében a sikeres törlés tényét ellenőrizni kell.

(5) Sokszorosítást, másolást csak a vonatkozó előírások szerint szabad végezni. A biztonsági, illetve archív adatállomány előállítása másolásnak számít.

(6) A szoftvereket és adathordozókat a (4) bekezdésben hivatkozott, leltározásra és leltárkészítésre irányadó szabályokban foglaltaknak megfelelően kell leltározni.

(7) Mentések, fájlok védelme:

a) az adatfeldolgozás után biztosítani kell az adatok mentését.

b) a munkák során létrehozott általános (pl. word, excel) fájlok mentése és a mentés biztonságos tárolása az azt létrehozó munkatárs (felhasználó) feladata.

c) a felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie a központi szerver erre kijelölt területére. Az archiválásban szükség esetén informatikusok nyújtanak segítséget.

d) a szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért a rendszergazda felelős.

Szoftvervédelem

23. § Az Igazgatói Titkárság vezetőjének, vagy az általa kijelölt személynek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

24. § (1) A felhasználói programok védelme kiterjed:

a) a programhoz való hozzáférésre, a programvédelemre,

b) a programok megőrzésére, nyilvántartására.

(2) A programhoz való hozzáférés, programvédelem keretében

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

b) gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

(3) A programok megőrzése, nyilvántartása:

a) a programokról az Igazgatói Titkárságon nyilvántartást kell vezetni.

b) a nyilvántartás elektronikus formában is vezethető, ha az alkalmazott módszer biztosítja az eredeti nyilvántartás összes adatának késedelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az illetéktelen utólagos módosítás lehetőségét.

c) a programok működőképes állapotban való tartásáért a rendszergazda – ha szükséges, az üzemeltetővel együttműködve – felelős.

A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

25. § (1) Központi gépek esetében:

a) szünetmentes áramforrást kell használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén az adatvesztéstől.

b) a háttértárakról folyamatosan biztonsági mentést kell készíteni.

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

d) a vásárolt szoftverekről – amennyiben az indokolt – biztonsági másolatot kell készíteni.

(2) Munkaállomások esetében:

a) a külső helyről származó anyagokat ellenőrizni kell vírusellenőrző programmal.

b) vírusfertőzés gyanúja esetén a rendszergazdát azonnal értesíteni kell.

c) új rendszert a használatba vételt megelőzően szükség szerint adaptálni kell, és tesztadatokkal kell ellenőrizni a működését.

d) az Intézet informatikai eszközeiről programot, illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.

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

f) az informatikai eszközt és tartozékait helyéről eltávolítani csak engedéllyel szabad.

g) az Intézet hálózatára hálózati eszközt csak az Igazgatói Titkárság vezetőjének engedélyével szabad csatlakoztatni. Az engedély nélkül csatlakoztatott eszköz hálózati hozzáférését az észlelést követően azonnal meg kell szüntetni, és a 13.§ (4) bekezdés szerinti eljárásnak van helye.

Ellenőrzés

26. § (1) Az Intézet éves belső ellenőrzési tervében vagy munkatervében rögzíti az IBSZ-ben foglaltak betartása ellenőrzésének módját.

(2) Az ellenőrzésnek elő kell segítenie, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése, illetve annak megakadályozása, hogy az megismétlődjön.

(3) A munkafolyamatba épített ellenőrzés során az IBSZ rendelkezéseinek betartását a szervezeti egységek vezetői folyamatosan ellenőrzik.

Záró rendelkezések

27. § (1) A szabályzat az aláírást követő munkanapon lép hatályba.

(2) Jelen szabályzatot az Intézet munkatársai számára a helyben szokásos módon kell kihirdetni; az Intézet munkatársainak a szabályzat megismerését aláírásukkal igazolniuk kell.

Budapest, 2015. december

dr. Kocsis Miklós PhD
mb. igazgató

Informatikai jogosultság és eszköz igénylő lap

(A kívánt eljárást kérjük X –el jelölni !)

Név: .....

Beosztás: .....

Munkakör: .....

Szervezeti egység: .....

☐ ÚJ JOGOSULTSÁG IGÉNYLÉSE

☐ MEGLÉVŐ JOGOSULTSÁG(OK) TÖRLÉSE:

☐ MÁR MEGLÉVŐ JOGOSULTSÁG(OK) MÓDOSÍTÁSA:

LEVELEZÉS

Levelezési hozzáférés:

mma-mmki.hu-s email cím	☐ IGEN	☐ NEM	Email cím: .....
mindenki@mma-mmki.hu	☐ TAGJA	☐ NEM TAGJA	

További email címek:

.....	☐ ÍRHAT	☐ CSAK OLVASHAT	☐ ALIAS
.....	☐ ÍRHAT	☐ CSAK OLVASHAT	☐ ALIAS
.....	☐ ÍRHAT	☐ CSAK OLVASHAT	☐ ALIAS

FÁJLSZERVER

Megosztások hozzáférése:

K	MMKI-KÖZÖS	☐ IGEN	☐ NEM
T	TITKÁRSÁG	☐ IGEN	☐ NEM
V	VEZETŐSÉG	☐ IGEN	☐ NEM
...	.....	☐ IGEN	☐ NEM
...	.....	☐ IGEN	☐ NEM
...	.....	☐ IGEN	☐ NEM

ALKALMAZÁS

DMS	iktató hozzáférés	☐ IGEN	☐ NEM
INTRANET	MMA intranet.hozzáférés	☐ IGEN	☐ NEM
VPN	távoli fájlszerver elérés	☐ IGEN	☐ NEM
SCAN	scannelés lehetősége	☐ IGEN	☐ NEM
.....	.....	☐ IGEN	☐ NEM
.....	.....	☐ IGEN	☐ NEM

ESZKÖZ IGÉNY

Igényelt eszköz típusa:

☐ ASZTALI PC ☐ MONITOR ☐ LAPTOP ☐ DOKKOLÓ ☐MONITOR ☐ EGYÉB:.....

Jogosultsági szint: ☐ RENDSZERGAZDA ☐ FELHASZNÁLÓ ☐ VENDÉG

Igazgatói Titkársági aláírás:

Dátum: ..... Név: .....

Aláírás: .....

Igazgatói jóváhagyás:

☐ JÓVÁHAGYOM ☐ ELUTASÍTOM

Dátum: ..... Név: .....

Aláírás: .....

Rendszergazda

☐ HOZZÁFÉRÉSEK BEÁLLÍTÁSRA KERÜLTEK

Dátum: ..... Név: .....

Aláírás: .....

ÁTADOTT ESZKÖZÖK

Megnevezés	Típus	Serial number	Megjegyzés

ÁTADÁSI NYILATKOZAT

☐ A FELSOROLT ESZKÖZÖKET ÁTVETTEM.

Dátum: ..... Név: .....

Aláírás: .....

KILÉPÉSKORI VISSZAVÉTELI NYILATKOZAT

☐ A FELSOROLT ESZKÖZÖKET VISSZAADTAM.

Dátum: ..... Név: .....

Aláírás: .....

☐ RENDSZERGAZDA MEGERŐSÍTÉSE

Dátum: ..... Név: .....

Aláírás: .....

2. függelék

ADATKEZELÉSI NYILATKOZAT

Alulírott _____ (név) nyilatkozom, hogy a Magyar Művészeti Akadémia Művészetelméleti és Módszertani Kutatóintézet által biztosított informatikai eszközzel végzett feladataim ellátása során e tevékenységgel összefüggésben tudomásomra jutott információkat megőrzöm, azt illetéktelen személyek részére nem adom át.

A munkavégzés során csak a részemre hozzáférhető adatokkal dolgozom, más adatok hozzáférésére kísérletet sem teszek. A Magyar Művészeti Akadémia Művésztelméleti és Módszertani Kutatóintézet Informatikai Biztonsági Szabályzatában foglaltakat megismertem, megértettem, a munkavégzés során a szabályzatban foglaltaknak megfelelően járok el.

Dátum:

_____

Aláírás