A Lackó Dezső Múzeum

INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

A Laczkó Dezső Múzeum Informatikai Biztonsági Szabályzatát (továbbiakban IBSZ) a *Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény* rendelkezése alapján a következők szerint határozom meg:

1. Az Informatikai Biztonsági Szabályzat célja

Az IBSZ alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az IBSZ célja továbbá:

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

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzembe helyezésen keresztül az üzemeltetésig.

A jelen IBSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

2. A szabályzat hatálya

Tevékenységek, amelyek a szabályzat hatálya alá tartoznak:

- Informatikai eszközök beszerzése és használata,
- Szoftverek telepítése és használata,

- A számítástechnikai adathordozók védelme,
- Az adathordozókon tárolt adatok védelme és elérhetőségének biztosítása,
- A belső és külső hálózatok használata.

Személyi hatálya kiterjed

Az intézmény valamennyi fő- és másodállású, mellék- illetve részfoglalkozású dolgozójára,

Az intézmény számára számítástechnikai feladatokat bármilyen megállapodás alapján az intézmény területén végzőkre. Bárki más számára az intézmény területén és számítástechnikai eszközein dolgozó külső személyekre.

Tárgyi hatálya kiterjed

Az intézmény tulajdonában vagy használatában lévő valamennyi számítástechnikai eszközre,

Az intézmény területén használatban levő idegen tulajdonú számítástechnikai eszközre a tulajdonjogból eredő korlátokkal,

Az intézmény eszközein (ld.: 1-2. pont) használt rendszer- és felhasználói programokra,

A számítástechnikai munkához kapcsolódó dokumentációkra,

Az adatok számítógépre vitelére, tárolására és megjelenítésére, nyomtatására,

Az adathordozók tárolására, felhasználására.

3. Kapcsolódó szabályozások

A Laczkó Dezső Múzeum nyilvántartó adatbázisainak üzemeltetési szabályzata.

4. Az IBSZ alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére a rendszergazda biztosítja az intraneten való közzététel formájában. A szabályzat tudomásul vételéről a dolgozók a Megismerési záradékban aláírásukkal nyilatkoznak.

5. Az *IBSZ* karbantartása

Az IBSZ-t a számítástechnikában – valamint az intézménynél – a fejlődés során bekövetkezett változások miatt időközönként aktualizálni kell. Ez az informatikai vezető és a rendszergazda feladata.

6. A védelem felelősei

A védelem felelőse a mindenkori informatikai vezető és a rendszergazda.

A jelen szabályzatban foglaltak szakszerű végrehajtásáról az intézmény vezetőjének kell gondoskodnia.

Adatvédelmi felelősök feladatai

a) Informatikai vezető feladatai:

- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- a digitális nyilvántartási adatbázisok felügyelete,
- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására.
- ellátja az adatkezelés és adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- ellenőrzi a szoftverek használatának jogszerűségét.

b) Rendszergazda feladatai:

- a rendszergazda a hálózat működőképességét felügyeli,
- felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének folyamatos ellenőrzése,
- felelős az intézmény informatikai rendszer hardver eszközeinek karbantartásáért,
- együttműködik a gazdasági osztállyal a beszerzett, illetve üzemeltetett hardver és szoftver eszközök nyilvántartásában,
- gondoskodik a folyamatos vírusvédelemről
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer adminisztrációját.

7. Az adatvédelem alapelve

Az adatvédelem alapelve, hogy kívülről csak a publikus adatokhoz lehet hozzáférni (honlap). Az intézményen belül mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

8. A használat általános szabályai

Számítógépek és egyéb eszközök

Kiszolgálók (szerverek)

Annak a helyiségnek, ahol hálózati szerver működik (a továbbiakban: gépterem), biztonságosan zárhatónak kell lennie. A gépteremben az ott illetékes dolgozókon kívül mások csak a géptermi dolgozók felügyeletével tartózkodhatnak. A gépterem a "D" tűzveszélyességi osztályba tartozik. Az erre vonatkozó részletes előírásokat a *Tűzvédelmi utasítás* tartalmazza.

A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.

Hálózati szerver elindítására és leállítására, a szerveren könyvtárak nyitására, könyvtárak és fájlok módosítására vagy törlésére a rendszergazda, szükség esetén kijelölt helyettese.

Havonta egy napon, lehetőleg a hónap első csütörtökjén a szerver(ek) hálózati szolgáltatásai karbantartási céllal szünetelhetnek.

A belső file-szerveren (Adatszolga) személyes könyvtár hozható létre a hálózat valamennyi felhasználója számára, ezek esetében minden felhasználó a saját könyvtárában korlátlan (olvasási, írási, törlési) jogokkal rendelkezik, más könyvtárához azonban nem férhet hozzá.

A személyes könyvtárakban a maximális tárhely nagyságát a szerver erőforrásainak függvényében a rendszergazda állítja be.

Munkaállomások

Az asztali és mobil számítástechnikai eszközök nagy része személyi használatú, ezeket a használó leltárilag átveszi, épségükért, rendeltetésszerű használatukért felelős. Más személy az eszközt csak a leltárilag felelős használó tudtával és belegyezésével használhatja.

A számítógépeken megosztott erőforrások lehetnek, amelyeket a hálózat segítségével mások is elérhetnek, ilyen:

legalább egy megosztott alkönyvtár, amelyet bárki elérhet,

CD-meghajtó, nyomtató, stb., amelyhez személyre szabott jogosultságok tartoznak.

A munkaállomás teljes merevlemezét egyben megosztani, a hálózaton bárki számára elérhetővé tenni nem szabad.

A számítógépeken a rendszergazda felhasználónkénti bejelentkezést – ha az operációs rendszer lehetőséget ad rá, akkor hálózati bejelentkezést – köteles beállítani. A hálózati jelszavak minimális hossza 6 karakter, tartalmazhatják az angol ABC kis- és nagybetűit, valamint számokat. Jelszavát – szükség esetén a rendszergazda segítségével – bármely felhasználó módosíthatja.

Közös használatú eszközök

Egyes feladatokra (pl. szkennelés, stb.) közös használatú asztali számítógépek is lehetnek üzembe állítva. Ezekhez az illetékes munkahelyi vezető jelöli ki azt a felhasználót, aki a gépet felügyeli, szükség esetén a rendszergazdának jelzi, ha szakszerű beavatkozásra van szükség. Az ilyen közös használatú gépeken minden felhasználó köteles a felhasználónevével elkülönített könyvtárba helyezni saját állományait, és a lehető leghamarabb gondoskodni a hely felszabadításáról (pl. a fájlok saját használatú számítógépre illetve CD-re, DVD-re történő mentésével).

Közös használatú számítógépen bizalmasan kezelt adatokat tárolni nem szabad!

Mobil számítógépek és eszközök

A mobil eszközök (notebook, digitális fényképezőgép, stb.) átadásáról és átvételéről az eszközért leltárilag felelős személy nyilvántartást köteles vezetni, amelyben szerepel az eszköz sorozatszáma, a tartozékok felsorolása, az átadás és visszavétel dátuma aláírásokkal.

Fájl- és könyvtárnevek használata

Fájlok (állományok) és könyvárak (mappák) nevében ékezetes (nemzeti) karakterek használatát a későbbi esetleges adatvesztések elkerülése érdekében kerülni kell. Hasonlóképpen kerülendő a szóköz használata, helyette az aláhúzás-karakter (_) javasolt. Ez a két szabály a szerveren tárolt központi adatbázisok és képek esetében, valamint az archiválásra leadott CD könyvtárszerkezetében kötelező, betartásáról a rendszergazda gondoskodik.

9. Számítógépes nyilvántartások

A műtárgyak számítógépes nyilvántartásáról és az adatvédelmi feladatokról az üzemeltetési szabályzat rendelkezik.

Digitális fényképek kezelése

A digitális fényképezőgépekkel készült képek tárolása három módon lehetséges:

Belső adatbázis-kiszolgálón:

Web-alapú programmal kezelendők a múzeum szempontjából lényeges, megőrzendő, de a leltári rendszerben nem szereplő képek. A jelenlegi program („DigiTár") az alábbi jellemzőkkel rendelkezik:

- a képeket egyedi fájlnévvel azonosítja
- a képek kisebb változatát a szerveren tárolja, az eredetit minimum 30 napig ugyanitt, majd a továbbiakban CD-re mentve tárolja
- minden képhez kötelezően adattartalmakat rendel.

A program részletes specifikációját a „DigiTár kézikönyv" és a „DigiTár rendszeradminisztrációs kézikönyv" tartalmazza. A program által készített mentéseket 2 példányban kell lemezre írni, amelyből az egyik példányt az intézményi adattárban kell tárolni.

A készítő illetve használó saját használatú számítógépén:

Így az ideiglenes jellegű, munkaanyagnak tekinthető képek és másolatok tárolhatók. Ebben az esetben a mentések készítése a használó felelőssége.

Számítógépes nyilvántartó programmal:

A leltárba vett tárgyak illetve dokumentumok kisméretű tárgyfotóit, valamint a beleltározott képek digitális másolatait a múzeum számítógépes nyilvántartó adatbázisaiban tároljuk (Monari).

10. Hálózat és Internet

Az intézmény belső számítógépes hálózatán a felhasználók név és jelszó megadásával vehetik igénybe a hálózati erőforrásokat. A jelszó minimális hossza 6 karakter. Az intézményi hálózaton érvényes név-jelszó párt egyéb helyeken használni nem szabad. (Ld. még *A károk megelőzésének és minimalizálásának módja / Felhasználók*).

A LDM belső hálózatának összes felhasználója rendelkezik e-mail postafiókkal.

Az egyes telephelyeket a nyilvános hálózat (internet) felhasználásával titkosított adatcsatorna – úgynevezett VPN – köti össze. Ennek integritásáról a rendszergazda gondoskodik. A VPN által összekötött részhálózatok biztonsági szempontból egységes belső hálózatnak számítanak.

11. Az eszközöket és adatokat veszélyeztető helyzetek

Az alábbi helyzetek kezelésére kell védelmi intézkedéseket tenni, ezek részleteit *A károk megelőzésének és minimalizálásának módja* című fejezet tartalmazza:

- Elemi csapások
- Környezeti ártalmak
- Közüzemi szolgáltatás zavarai
- Feszültség-kimaradás, -ingadozás
- Emberi tényezőkre visszavezethető veszélyek
- Szándékos károkozás
- Illetéktelen behatolás a számítástechnikai rendszerbe

- Illetéktelen adathozzáférés
- Eltulajdonítás, rongálás
- Megtévesztő adatok bevitele
- Nem szándékos, illetve gondatlan károkozás
- Számítástechnikai képzettség és gyakorlat hiánya
- Vírusfertőzés
- Adathordozók rongálódása

12. A károk megelőzésének és minimalizálásának módja

- Dokumentálás
- Számítógéphálózat dokumentációja

A rendszergazda köteles a hálózathoz kapcsolt számítógépekről naprakész dokumentációt vezetni gépenként az alábbi adatokkal:

- gép neve, leltári száma és/vagy gyári száma,
- a hardver konfiguráció legfontosabb elemei (processzor, memória, merevlemez mérete, busz, hálózati csatoló),
- operációs rendszer(ek),
- felhasználó(k).

A rendszergazda köteles a hálózat felhasználóiról az alábbi adatokkal naprakész nyilvántartást vezetni:

- teljes név,
- felhasználói név a hálózatban, e-mail cím,
- esetleges bejelentkezési korlátozások.

A fenti dokumentációk – vagy azok egy része – számítógépes adatbázis formájában is lehet.
Internetes szerveren az alábbi adatokat kell naplózni:

- E-mail (SMTP és POP3) bejelentkezések
- Külső web-elérések

A szerver operációs rendszerét tartalmazó lemezegységen az operációs rendszer és az intranet könyvtáraihoz törlési jogot csak a rendszergazda és a szerver-operátorok kaphatnak.

13. Mentések dokumentációja

Munkaállomásokon

Ha a munkaállomáson intézményi adatokat tárolunk, a munkaállomást használó köteles mentéseket végezni és a mentéseket a felhasználó köteles dokumentálni, az *Adatkezelés / Adatok mentése, adathordozók tárolása* pontban meghatározott szabályok szerint.

Szerveren

A szerveren tárolt adatok mentését a mentést végző feladata dokumentálni –a mentési naplók megőrzésével – az alábbi adatokkal:

- dátum,
- adatbázis,
- adathordozó (HDD, CD, stb.),
- címke.

Felhasználók

Új és távozó munkatársak

A munkájukhoz számítógépet használó dolgozóknak ki- és belépéskor fel kell keresniük a rendszergazdát

- a rendszergazda által nekik kiadott illetve kiadandó számítástechnikai eszközök,
- a felhasználónév létrehozása, törlése vagy megtartása,
- az e-mail cím létrehozása, törlése vagy megtartása

tárgyában.

Távozó dolgozó esetén az e-mail cím meghatározott ideig – maximum fél évig – megtartható az ide érkező levelek új címre irányításával. Főállásból távozó, de az intézmény számára más jogviszony keretében továbbra is munkát végző személy esetén a felhasználónév (és vele együtt a jelszó, valamint az e-mail cím) határidő nélkül megtartható, amennyiben erre a munkavégzéshez szükség van.

A gazdasági illetve munkaügyi feladatokat végzők ki- és belépéskor a rendszergazdához is el kell, hogy irányítsák a dolgozót. Ennek betartásáról a gazdasági vezető gondoskodik.

14. A felhasználók azonosítása

A hálózathoz csatlakozó számítógépeket felhasználói név és jelszó megadásával lehet igénybe venni. A felhasználói névre (úgynevezett login-névre) vonatkozó szabályok:

- a nevet a felhasználóval történt egyeztetés után a rendszergazda adja,
- a hálózaton a rendszergazda köteles közzé tenni (mindenki által elérhető módon tárolni) a nevek aktuális listáját,
- a név minimális hossza 3, maximális hossza 16 karakter,
- ez a név képezi az e-mail cím első (privát) részét is.

A jelszóra vonatkozó szabályok:

- a jelszó minimum 6, maximum 16 karakter lehet,
- a hálózat felhasználói adatbázisába történő felvételkor a rendszergazda ad jelszót,
- a felhasználónak bármikor joga van jelszavát megváltoztatni,
- minden felhasználó kötelessége jelszava titkosságát megőrizni, ha kétség vagy gyanú merül fel, a jelszót haladéktalanul meg kell változtatnia,
- ha a rendszergazda tapasztal a jelszóval való visszaélést, köteles ezt a múzeum vezetőjének jelenteni, és a szóban forgó név-jelszó párt törölni.

15. A felhasználók képzettségével kapcsolatos feladatok

Az intézményben számítógépet használó dolgozóknak ismerniük kell a használathoz szükséges legfontosabb alapfogalmakat, ilyenek:

- lemezegységek, könyvtárak, fájlok fogalma, elnevezése illetve a név szabályai,
- operációs rendszer és felhasználói program viszonya,
- az operációs rendszerbe illetve a hálózatba való bejelentkezés és az abból való kilépés,
- könyvtárak (mappák) létrehozása, átnevezése, törlése, fájlok másolása, törlése,
- mentés, biztonsági mentések tudnivalói,
- a vírusvédelem és a hálózati munka legfontosabb tudnivalói (jelen szabályzat alapján).

A fentiek elsajátítását külső képzéseken való részvétellel vagy belső továbbképzéssel lehet megoldani. Belső továbbképzésére az igazgató évente legalább egy számítástechnikai szakmai napot jelöl ki, ennek programjáról a rendszergazda gondoskodik a felmerülő igények alapján. Minden számítógép-használó kétévente legalább egy belső továbbképzési napon köteles részt venni.

A rendszergazda és a könyvtáros közösen gondoskodik arról, hogy a számítógép-használattal kapcsolatos alapvető szakirodalom betekintésre vagy kölcsönzésre a dolgozók rendelkezésére álljon – ehhez az intézmény gazdasági vezetése könyvvásárlási keretet biztosít.

A rendszergazda – illetve ha van külön webmester, akkor ő – köteles gondoskodni arról, hogy az intraneten legyen a számítógép-használattal kapcsolatos – mindenek előtt az előzőekben felsorolt alapfogalmakra vonatkozó – tananyag és információs anyag.

16. Adatkezelés

Adatbevitel

A számítógépes feldolgozásnak csak megbízható adatok esetén van értelme, ezért minden adatot beíró munkatárs a beírás után köteles a bevitt adat helyességét ellenőrizni.

A nyilvántartó programok esetében fontos szempont, hogy a téves adatbevitelt minél inkább szűrjék ki (pl. adatmaszk, megfelelő mezőhosszak és adattípusok, ellenőrzőszámok illetve dupla adatrögzítés alkalmazásával). Ezt a szempontot a programok beszerzésénél a rendszergazda feladata érvényesíteni.

Ha megtévesztő adatok bevitelére, adatfeldolgozások programmal történő zavarására utaló jeleket tapasztal bármely felhasználó, illetve a rendszergazda, köteles azonnal írásbeli feljegyzésben jelezni az intézmény vezetőjének, aki a rendszergazdával történő egyeztetés és az eset kivizsgálása után intézkedik a szükséges fegyelmi vagy jogi eljárásról.

Adatok mentése, adathordozók tárolása

A munkaállomásokon tárolt múzeumi adatokat és a hivatali munkához tartozó dokumentumokat a felhasználó (adatfelvivő) kötelessége rendszeresen menteni. A mentéshez külső adathordozót (HDD, DVD) lehet igénybe venni. A mentésekhez a rendszergazda ad szakmai segítséget.

A mentéseket erre a célra szolgáló lapon vagy füzetben a mentést végző felhasználó köteles dokumentálni az alábbi adatokkal:

- dátum,
- adatbázis, könyvtár, vagy a program, amelynek állományairól a mentés készült,
- címke (név, amely utal arra, hogy milyen mentésről van szó).

A mentésre használt adathordozón fel kell tüntetni a címkét. A mentéseket és a róluk szóló dokumentációt a felhasználó az egyéb hivatali iratokkal és eszközökkel azonos módon köteles megőrizni és munkaviszonya megszűnése esetén átadni.

A szervereken található adatbázisok mentéséről a rendszergazda gondoskodik adatmentés-kiszolgáló üzemben tartásával illetve DVD/hordozható HDD lemezre történő mentésekkel.

A gondatlanságból vagy figyelmetlenségből adódó rongálódásért mindenki a károkozásra vonatkozó általános szabályok szerint felel. Amennyiben ez adatok elvesztését is okozza, a kárt a rendszergazdának is köteles a kárt észlelő jelezni. A rendszergazda az adatvesztésről akkor tájékoztatja az intézmény vezetőjét, ha saját hatáskörében a mentésekből az adatokat nem tudja visszaállítani.

A szerverek mentési, archiválási rendje

rendszer megnevezése	mentő/archivál ó eszköz	mentés gyakorisága	adathordozó tárolási helye	megjegyzés
Monari, Digi-tár	HDD	napi, heti	rendszergazda iroda, külső	növekményes és teljes
felhasználói munkakönyvtárak	HDD	heti	rendszergazda iroda	
internetes adatok	HDD	heti	rendszergazda iroda	üzemeltetett WEB oldalak adatai
szerverkonfigurációs adatok	HDD	heti	rendszergazda iroda, külső	
levelezési adatok	HDD	heti	rendszergazda iroda	

Hozzáférés az adatokhoz

Munkaállomások

Az intézményben az asztali számítógépeken tárolt adatokért a gépet leltárilag is átvevő használó felelős. Tudta és hozzájárulása nélkül más az eszközt és az azon tárolt adatokat nem használhatja.

Adatbázis-szerver és Internet

A szervereken tárolt adatbázisokhoz felhasználónkénti jogosultságokat kell beállítani. Ennek felügyelete az informatikai vezető feladata. Egy-egy tematikus adatbázishoz szintén beállítandó a szakterület (adott téma) felelőse és az adatfelvivők elérési joga. A további jogosultságokat a téma felelőse határozza meg. Ha az adatbázis-kezelő program lehetővé teszi, beállítható egyes rekordokra vagy mezőkre az összes – vagy egy felhasználói csoporthoz tartozó összes – munkatárs, vagy a "vendég" felhasználó olvasási joga is. Az Internetes publikálás esetén a jogok kiegészülhetnek értelemszerűen továbbiakkal (pl. szakmai partnerek, bizonyos intézmények vagy azonosított felhasználók), a vendég jogállás ebben az esetben azt jelenti, hogy nyilvánosan, bárki számára elérhető.

A gyűjtemények számítógépes adatbázisaihoz tartozó felhasználói jogosultságokról az üzemeltetési szabályzat rendelkezik.

Adatok mozgatása

A hálózatra (a hálózathoz kapcsolt bármely munkaállomásra) idegen programot, adatot másolni csak a rendszergazdával történt egyeztetés után szabad. A másolás előtt vírusellenőrzést kell végezni (ld.: *Vírusvédelem*).

Az illegálisan másolt, illetve az informatikai biztonság szempontjából veszélyes adatokat, programokat a rendszergazda bármely számítógépről eltávolíthatja.

Az intézményben levő számítógépekről külső igénylőnek, partnernek adatot – ha egyébként az adat kiadható – számítástechnikai adathordozón (CD, dvd, pendrive, stb.) csak vírusellenőrzés után lehet kiadni. Ezért minden esetben az adatot szolgáltató munkatárs felelős.

17. Az eszközök környezetének védelme

Számítástechnikai eszközt erősen poros, nyirkos, nagy hőingadozásnak kitett, az emberi tartózkodásra alkalmas hőmérséklettől tartósan eltérő hőmérsékletű helyen üzemeltetni nem szabad. Ez alól értelemszerűen kivételt képeznek a kifejezetten ilyen célokra készített eszközök (pl. időjárásálló digitális fényképezőgép).

A számítástechnikai adathordozókat (beleértve a számítógépek merevlemezét is) tároló helyiségek zárhatóságát biztosítani kell.

Elemi csapás, katasztrófa esetére a teendőket jelen szabályzat katasztrófaterve tartalmazza.

Az intézmény azon helyiségeiben, ahol fontos adatokat tartalmazó számítástechnikai eszközöket használnak vagy tárolnak, a bejárat előtt széndioxiddal oltó tűzoltó készüléket kell elhelyezni.

Vagyonvédelmi előírások

- a géptermek külső és belső helyiségeit biztonsági zárakkal kell felszerelni,
- a gépterembe való be- és kilépés rendjét szabályozni kell,
- a gépterembe, szerverterembe történő illetéktelen behatolás tényét a vállalkozás vezetőjének azonnal jelenteni kell.

Adathordozók

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

- a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,
- adathordozót másnak átadni csak engedéllyel szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

Hardvervédelem

A hálózati szerver(ek)re illetve a hálózat legértékesebb elemeire biztosítást kell kötni.

Erősen szennyezett levegőjű, fokozottan tűz- és robbanásveszélyes vagy erős elektromágneses terű helyiségben csak ipari PC üzemeltethető.

A hálózat fájl-szervere és Internet-szervere kizárólag szünetmentes tápegységgel üzemeltethető. A szünetmentes tápegység áthidalási ideje az adott gépkonfigurációt tekintetbe véve legalább 15-20 perc kell legyen .

A munkaállomások közül mindazokat, amelyek az intézmény számára fontos adatokat tartalmazhatnak, illetve ilyen adatok bevitelére, feldolgozására használatosak, szünetmentes tápegységgel kell védeni, melynek áthidalási ideje legalább 10 perc legyen az adott konfigurációra.

Túlfeszültség elleni védőeszközt kell alkalmazni:

A hálózati szerver és az adathálózat kábelei között.

Bármilyen külső adatvonal (telefon, TV-kábel, stb.) és az intézmény számítógépe között,

Nagy értékű, szünetmentes tápegységgel nem védett berendezések (pl. szkenner) tápellátásánál.

Olyan számítástechnikai eszközt (hardvert, szoftvert), amely nem rendelkezik dokumentációval, használati és hibaelhárítási útmutatóval, valamint pontos műszaki specifikációval, csak különleges, rendkívül indokolt esetben lehet használatba venni. Törekedni kell a forráskóddal is dokumentált szoftverek használatára. A beszerzésnél előnyben kell részesíteni a szakmailag megfelelő és emellett megbízható termékeket, valamint az ilyen termékeket műszaki és felhasználói információkkal, támogatással együtt adó szállítókat. A beszerzéseknél figyelembe veendők a garanciális feltételek, az esetleges későbbi javítások során kieső idő és felmerülő költségek is. E szempontok érvényesítése a rendszergazda feladata.

Szoftverek

Szoftverhasználat

Az intézmény területén csak jogtiszta szoftvereket szabad használni, ezek lehetnek:

- vásárlás útján szerzett,
- díjmentesen használható (freeware, GPL licenc, stb.),

- a szerzőtől illetve a jogok tulajdonosától díjmentes használatra átengedett programok.

Az intézményben hivatalosan használt programok jogtisztaságát az informatikai vezető és a rendszergazda figyeli, szoftvervásárlás esetén gondoskodik arról, hogy a fenti feltételeknek megfeleljen a beszerzés. A jogtisztasággal kapcsolatos teendőkről az igazgatónak tesz javaslatot.

Az egyes munkaállomások felhasználói is csak a fentiek betartásával és a rendszergazdával egyeztetve telepíthetnek gépükre programot, az általuk telepített programok jogtisztaságáért fegyelmileg és büntetőjogilag is felelősek.

A nagy értékű szoftverekről biztonsági másolatot kell készíteni CD-re vagy más adathordozóra, ennek felelőse a rendszergazda. E szoftverek eredeti példányát illetve telepítő lemezét lehetőleg lemezszekrényben vagy páncélszekrényben kell tárolni. A tároló szekrény a használat helyétől elkülönült helyen kell legyen (más iroda, épületrész).

Vírusvédelem

A munkaállomásokon a vírusvédelmi programot az állandó védelem bekapcsolásával kell használni. Ha ez valamilyen okból nem lehetséges, a felhasználó köteles vírusellenőrzést végezni

- az intézménybe általa vagy ügyfele által hozott – programot vagy dokumentumot tartalmazó – mágneses vagy optikai lemezen, illetve más adathordozón (pl. pendrive),
- az általa e-mail mellékleteként kapott állományokon.

Amennyiben a felhasználó munkaállomásán a víruskereső program nem működik a javítást a rendszergazdától kell haladéktalanul kérnie.

E-mail mellékletét csak abban az esetben szabad megnyitni, ha a címzett meggyőződött arról, hogy nem vírusról van szó. Ennek érdekében az általunk küldött e-mail esetén a levél szövegében csatolt mellékletek esetén szerepeltetni kell a fájl(ok) nevét és hosszát.

A rendszergazda köteles gondoskodni arról – és a megfelelő időben a szükséges licencvásárlásra javaslatot tenni –, hogy valamennyi munkaállomáson és a felhasználói fájlokat tartalmazó kiszolgálón állandó vírusvédelem működjön. Minden felhasználó köteles a gépén a vírusvédelem állapotát rendszeresen figyelni és hiba, probléma esetén a rendszergazdát értesíteni.

18. Katasztrófaterv

A katasztrófa-elhárítási terv, illetve az abban foglalt eljárási szabályok feladata, hogy elvárható mértékben biztosítsa egy esetlegesen bekövetkező katasztrófaesemény megelőzését, illetve az abból eredő károk minimalizálását, a következmények minél hamarabbi elhárítását.

Az informatikai rendszer katasztrófája egy olyan esemény, amely a rendszer adatfeldolgozó képességének részleges vagy teljes elvesztését okozza hosszabb időre. A katasztrófa-elhárítási terv definíciószerűen meghatározva eljárások vagy tevékenység-lépések sorozata, annak biztosítására, hogy a szervezet kritikus információ-feldolgozó képességeit helyre lehessen állítani elfogadhatóan rövid idő alatt, a szükséges aktuális adatokkal, egy katasztrófa bekövetkezése után.

A múzeum alapvető központi informatikai erőforrásai egy helyen, a szerverszobában kerültek elhelyezésre. Ebből eredően tehát kiemelt kockázatot jelent a tűz, az áramszolgáltatás kimaradása/kiesése, a tudatos rombolás és/vagy eltulajdonítás. Egy, a szerverszobában bekövetkező tűzeset akár a teljes központi informatikai rendszer (beleértve a külső kommunikációs hálózathoz csatlakozó eszközöket, a tűzfalat, és a teljes szerverparkot is!) megsemmisülését is eredményezheti.

A katasztrófa bekövetkezte utáni helyreállítás szakaszai:

Azonnali reakció: válasz a katasztrófa-helyzetre, a veszteségek számbavétele, a megfelelő emberek értesítése és a katasztrófa-állapot megállapítása. Katasztrófa esetén haladéktalanul értesítendő: az intézmény igazgatója és az informatikai vezető.

Környezeti helyreállítás: Az adatfeldolgozó rendszer helyreállítása: operációs rendszer, program termékek és a távközlési hálózat. A helyreállítás első lépéseként a fizikai környezetet kell helyreállítani: a meghibásodott rendszerelemeket ki kell javítani, illetve szükség esetén pótolni kell. A javításhoz, illetve az eszközök pótlásához – a kár mértékétől függően – különböző eszközök beszerzésére van szükség. A múzeum teljes informatikai infrastruktúráját érintő katasztrófa esetén a szervereket tartalmazó alhálózat önálló hálózatként bárhol létrehozható, amennyiben a hálózati aktív eszközök, és a számítógép-park pótlása megtörténik.

1) A hálózat helyreállítása:

A kiválasztott helyszínhez mérten meg kell tervezni, és el kell végezni a hálózati kábelezést, majd a kábeleket csatlakoztatni kell az aktív eszközökhöz, illetve a számító-gépekhez.

2) A szerverek helyreállítása (operációs rendszerek).

Funkcionális helyreállítás: Az informatikai rendszer alkalmazásainak és adatainak helyreállítása, az adatok szinkronizálása a tranzakció naplóval.

Adathelyreállítás: Az elvesztett vagy késleltetett tranzakciók ismételt bevitele. Az üzemeltetők, a rendszeradminisztrátorok, az alkalmazók és a végfelhasználók együtt munkálkodnak azon, hogy helyreállítsák a normál feldolgozási rendet.

Adatintegritás-teszt.

Veszprém, 2015. június 8.

LACZKÓ DEZSŐ MÚZEUM * VESZPRÉM *

S. dr. Perémi Ágota
múzeumigazgató

MEGISMERÉSI ZÁRADÉK

Alulírott a Laczkó Dezső Múzeum dolgozója nyilatkozom, hogy az intézmény Informatikai biztonsági szabályzatában foglaltakat megismertem, az abban foglaltak betartásáról gondoskodom.

Sorszám	Név, beosztás	Aláírás	Dátum