SAVARIA
MÚZEUM

5-6/2023/ALAPDOK2023

Savaria Múzeum és tagintézményei
(Továbbiakban: Múzeum)

Székhely: Szombathely, Kisfaludy Sándor utca 9.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Érvényes: 2023. 02. 15-től

Jóváhagyta: .....

Csapláros Andrea
múzeumigazgató

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

A Múzeum Informatikai Biztonsági Szabályzatát (továbbiakban IBSZ) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII.törvény, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló többször módosított 1992. évi LXVI. törvény, valamint az 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 Informatikai Biztonsági Szabályzat alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az intézménynél az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek az érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az Informatikai Biztonsági Szabályzat célja továbbá:

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

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

2. Az Informatikai Biztonsági Szabályzat hatálya

Személyi hatálya
Az IBSZ személyi hatálya az intézmény valamennyi fő- és részfoglalkozású dolgozójára, illetve az informatikai eljárásban résztvevő más szervezetek dolgozóira egyaránt kiterjed.

Tárgyi hatálya

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

3. Az adatkezelés során használt fontosabb fogalmak

Személyes adat:
A meghatározott természetes személlyel kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható;

Különleges adat:
a) a faji eredetre, a nemzeti, nemzetiségi és etnikai hovatartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más meggyőződésre,

b) az egészségi állapotra, a kóros szenvedélyre, a büntetett előéletre vonatkozó személyes adat;

Közérdekű adat:
Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, a személyes adat fogalma alá nem eső adat;

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

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

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

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

Adatfeldolgozó:

Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely az adatkezelő megbízásából személyes adatok feldolgozását végzi.

Nyilvánosságra hozatal:
Ha az adatot bárki számára hozzáférhetővé teszik;

Adatbiztonság:
Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

4. Az IBSZ biztonsági fokozata

Intézményünk alapbiztonsági fokozatba tartozik.
Intézményünk általános informatikai feldolgozást végez.

5. Kapcsolódó szabályozások

Az Informatikai Biztonsági Szabályzatot az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:
- Szervezeti és Működési Szabályzat,
- Bizonylati rend,
- Leltárkészítési és leltározási szabályzat,
- Felesleges vagyontárgyak hasznosításának és selejtezésének szabályzata,
- Belső ellenőrzési kézikönyv.
- Közbeszerzési Szabályzat

6. Védelmet igénylő, az informatikai rendszerre ható elemek

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.
Az informatikai rendszerre az alábbi tényezők hatnak:
- a környezeti infrastruktúra,
- a hardver elemek,
- az adathordozók,
- a dokumentumok,
- a szoftver elemek,
- az adatok,
- a rendszerelemekkel kapcsolatba kerülő személyek.

A védelem tárgya

A védelmi intézkedések kiterjednek:

- a rendszer elemeinek elhelyezésére szolgáló helyiségekre,
- az alkalmazott hardver eszközökre és azok működési biztonságára,
- az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
- az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerekre, valamint a feldolgozást
- támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,
- a személyhez fűződő és vagyoni jogokra.

A védelem eszközei

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

7. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az Informatikai Biztonsági Szabályzat megismerését az érintett dolgozók részére biztosítani kell.

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

Az Informatikai Biztonsági Szabályzat karbantartása

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

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

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

- közlésre szánt, bárki által megismerhető adatok,
- minősített, titkos adatok.

Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik.

Különös védelmi utasítások és szabályozások nem mondhatnak ellent a törvények és a jogszabályok mindenkori előírásainak.

A hivatali titoknak minősülő adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot.

A kijelölt dolgozók előtt a titokvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.

Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

Minden dolgozóval, aki az adatok gyűjtése, felvétele, tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése során információkhoz jut adatkezelési nyilatkozatot kell aláíratni. (1. sz. melléklet)

A titkot képező adatok védelmét, a feldolgozás - az adattovábbítás, a tárolás - során az operációs

rendszerben és a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal az adott lehetőségekhez mérten is biztosítani kell (szoftver, hardver adatvédelem).

8. Az informatikai eszközbázist veszélyeztető helyzetek

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

Környezeti infrastruktúra okozta ártalmak

- Elemi csapás:
  - földrengés,
  - árvíz,
  - tűz,
  - villámcsapás, stb.
- Környezeti kár:
  - légszennyezettség,
  - nagy teljesítményű elektromágneses térerő,
  - elektrosztatikus feltöltődés,
  - a levegő nedvességtartalmának felszökése vagy leesése,
  - piszkolódás (pl. por).
- Közüzemi szolgáltatásba bekövetkező zavarok:
  - feszültség-kimaradás,
  - feszültségingadozás,
  - elektromos zárlat,
  - csőtörés.

Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a megváltozott körülmények figyelmen kívül hagyása,
- illegális másolattal vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

9. A szükséges biztonsági-, jelző és riasztó berendezések

karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

10. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

Tervezés és előkészítés során előforduló veszélyforrások

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

A rendszerek megvalósítása során előforduló veszélyforrások

- hibás adatállomány működése,
- helytelen adatkezelés,
- programtesztelés elhagyása.

A működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság,
- szervezetlenség,
- képzetlenség,
- szándékosan elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

Az intézmény székhelyén és telephelyein üzemelő biztonsági kamerarendszer rögzítő egységén tárolt felvételek csak hatósági felhívásra adhatóak ki és kiadásához, felhasználásához az intézmény adatgazdájának engedélye is szükséges.
Intézményünknél az adatgazda az igazgató. A felvételekhez való illetéktelen hozzáférés elleni védelmet, adminisztrátori (adatgazda) jelszó megadásával kell biztosítani.
A használó a készülék használata során köteles betartani az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben foglaltakat, illetve figyelembe venni az adatvédelmi biztos 415/K/2009-3 ügyiratszámú állásfoglalását.

A biztonsági kamerarendszer meglétéről, a vonatkozó rendeletben meghatározott tájékoztatótáblákat kell kihelyezni az intézmény bejáratánál.

11. Az informatikai eszközök környezetének védelme

Vagyonvédelmi előírások

- A számítógéppel ellátott irodák külső és belső helyiségeit zárakkal kell felszerelni,
- a számítógéppel ellátott irodákba való be- és kilépés rendjét szabályozni kell,
-számítógéppel ellátott irodákban, mások, csak az ott illetékes dolgozók jelenlétében tartózkodhatnak
- munkaidőn túl a számítógéppel ellátott irodákban csak engedéllyel lehet tartózkodni,
- a számítógép monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- a számítógéppel ellátott irodákba történő illetéktelen behatolás tényét az intézmény vezetőjének azonnal jelenteni kell,
- az informatikai eszközöket csak a kijelölt dolgozók használhatják,
- az informatikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

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 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 más szervezetnek átadni csak engedéllyel szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

Tűzvédelem

A számítógéppel ellátott irodák a "D" tűzveszélyességi osztályba tartoznak, amely mérsékelt tűzveszélyes üzemet jelent.

A tűzvédelem feladatait, sajátos előírásokat a számítógéppel ellátott irodákra vonatkozóan az intézmény Tűzvédelmi szabályzata tartalmazza.

A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell. Külön tűzszakaszt kell képezni a gépterem és az adatállomány-tároló helyiség között.

Az intézmény azon helyiségeiben, ahol informatikai eszközöket használnak vagy tárolnak, a főbejárat mellett 1-1 db 2-5 kg-os poroltó tűzoltó készüléket kell elhelyezni.

Az informatikai eszköz elhelyezésére szolgáló helyiségben elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.

A számítógéppel ellátott irodákban csak a napi munkavégzéshez szükséges mennyiségű gyúlékony anyagot szabad tárolni (pl. leporellót).
A számítógéppel ellátott irodákban dohányozni tilos!

A nagy fontosságú, pl. törzs adat-állományokat 2 példányban kell őrizni és
a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni.

12. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

A használat általános szabályai

Kiszolgáló (szerverek)
Annak a helyiségnek, ahol hálózati szerver működik biztonságosan zárhatónak kell lennie. A szerverteremben az ott illetékes dolgozókon kívül mások, csak az informatikai csoport dolgozóinak felügyeletével tartózkodhatnak. A szerveretem „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.
Hálózati szerver elindítására és leállítására, a szerveren könyvtár nyitására, csak az informatikai csoport munkatársai jogosultak.
Havonta egy napon, előre bejelentés után, a szerverek hálózati szolgáltatásai karbantartás céljából szünetelhetnek.

Hálózati háttértárolók (NAS-ok)
Annak a helyiségnek, ahol NAS működik biztonságosan zárhatónak kell lennie. A NAS-ok merevlemezeit RAID5 tárolási technikával kell üzembe helyezni. Meghibásodott lemezt azonnal cserélni kell. A teremben az ott illetékes dolgozókon kívül mások, csak az ott illetékes dolgozók felügyeletével tartózkodhatnak. A NAS-on hálózati könyvtár nyitására csak az informatikai csoport munkatársai jogosultak. A hálózati könyvtáron belül, a rendszergazda által hozzáadott felhasználók jogosultak könyvtár és fájlműveletekre. A NAS-on legalább egy hálózati könyvtárt, a hálózaton mindenki számára elérhetővé kell tenni.

Munkaállomások
Az asztali és mobil számítástechnikai eszközök nagy része személyi használatú, azokon az arra kijelölt személy végezhet munkát, épségükért és rendeltetés szerű használatukért felelős. Más személy az eszközt, csak a kijelölt személy jelenlétében és engedélyével használhat. A munkaállomás merevlemezének tartalmát a hálózaton megosztani tilos.

A számítógépeken a rendszergazdák névre szóló felhasználói bejelentkezést, ha a rendszer lehetőséget ad rá, akkor hálózati bejelentkezést kötelesek beállítani.

Az számítógéppel ellátott irodák védelme

Elemi csapás *(vagy más ok)* esetén a számítógéppel ellátott irodákban bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:
- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- új adatfeldolgozás, helyiségek kialakítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell.
A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.
A karbantartási munkákat tervezetten, körültekintően és gondosan kell elvégezni.
A munkák szervezésénél figyelembe kell venni:
- a gyártó előírásait, ajánlatait,
- a tapasztalatokat,

- a hardver tesztek által feltárt hibákat.

Alapgép szétbontását (kivéve a garanciális gépeket) csak a rendszergazda, vagy ennek hiányában megfelelő műszaki végzettséggel rendelkező a feladat ellátására kijelölt szakember végezheti el.

Vírus és kártevő védelem

Minden szerveren és munkaállomáson telepíteni kell a Múzeum által licencelt vírusvédelmi szoftver legfrissebb verziójú végponti verzióját. A végpontokat összekötő lokális vagy felhő alapú szervert, valamint az azon futó vírusvédelmi csoportházirendeket a rendszergazdák üzemeltetik.

Az informatikai feldolgozás folyamatának védelme

Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- tesztelt adathordozóra lehet adatállományt rögzíteni,
- a bizonylatokat és mágneses és optikai adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
- az adatrögzítés szoftver védelme. A programokat ellenőrző funkciókkal kell ellátni, ellenőrző számok, kontrollösszegek használatát biztosítani kell. Biztosítani kell továbbá a rögzített tételek visszakeresésének és javításának lehetőségét is.
  hozzáférési lehetőség:

a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (Alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá).

A központi szerveren (//server), és a központi számítógépen létrehozott osztott mappák felhasználói jogosultsághoz kötöttek. A jogosultságok a csoportvezetők és a szakmai felettesek által kerülnek meghatározásra, akik ezt írásban engedélyezik a 4. számú melléklet alapján. Az engedélyt a informatikai csoportvezető hagyja jóvá és ezután a rendszergazda állítja be a szerveren.

- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

A szerver(ek) rendszergazda jelszavát és az operációs rendszerek rendszergazda jelszavát zárható szekrényben kell tárolni.

Adathordozók védelme

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

Az informatikai eszközök üzemeltetését a rendszergazda vagy ennek hiányában megfelelő műszaki végzettséggel rendelkező a feladat ellátására kijelölt szakember látja el.

Köteles gondoskodni a feldolgozások igényeinek megfelelő adathordozók biztosításáról, beleértve a biztonsági másolatok eszközigényeit, illetve az üzemeltetés biztonságát növelő generációs adatállományok alkalmazását is.
Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval kell ellátni. Az azonosítókat mind emberi, mind informatikai olvasásra alkalmas formába kell feltüntetni. Az azonosító felépítése a következő legyen:
Programnév_verziószám_dátum_alszám,

Az operációs rendszer adta lehetőségek figyelembevételével biztosítani kell a külső és belső címek azonosságát.

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

Adathordozók tárolása

Az adathordozók tárolására a géptermen kívüli műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

Adathordozót a részlegből ki-, illetve oda bevinni csak a *informatikai csoportvezető* engedélye alapján lehet.
Az adathordozók szállítása csak megfelelő módon kialakított fémdobozban történhet.

Az adathordozók megőrzése

Az adathordozók megőrzési idejét a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló többször módosított 1995. évi LXVI. törvényben foglaltak, továbbá intézményünk Bizonylati rendjében és Iratkezelési szabályzatában foglaltak alapján az adatkezelő határozza meg.

Selejtezés, sokszorosítás, másolás

Olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért selejtezni kell.

Selejtezni kell:

- a fizikailag sérült, javíthatatlan, a gyári, raktározási hibából követően felhasználásra alkalmatlan, CD-t, pendrive-t, külső HDD-t ha a kapacitás a névleges érték 90 %-ánál kevesebb,
- véglegesen elhasználódott anyagot *(pl. leporelló).*

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni.

Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adathordozókról, törlő programokkal kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni.

(Az üzemi másolás nem minősül másolásnak.)
Biztonsági illetve archív adatállomány előállítása másolásnak számít.

Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését. A mentést meghatározott időszakonként el kell végezni.

A munkák során a helyi gépeken, munkaállomásokon létrehozott és tárolt word és excel dokumentumok mentése az azt létrehozó munkatársak *(felhasználók)* feladata, illetve azt az adott program kezelésével megbízott dolgozó végzi el.

A szerveren elhelyezkedő osztott könyvtárban tárolt közösen használt dokumentumok mentését kéthavi gyakorisággal a rendszergazda végzi el egy külső merevlemezes adathordozóra.

Felelős rendszergazdák:
Iformatikai Csoport munkatársai.

Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak. A fontosabb file-okat tartalmazó adathordozókról másolatot kell időnként készíteni.
A másolt lemezek csak az illetékes vezető engedélyével adhatók ki.

Szoftver védelem
Rendszerszoftver védelem

A munkaállomások rendszerszoftvereit naprakész állapotban kell tartani, ami az automatikus frissítési szolgáltatás beállításával érhető el.
A szerverek és NAS-ok rendszerszoftvereinek naprakészen tartása a rendszergazdák feladata, mely manuális úton, legfeljebb két heti gyakorisággal, illetve ismert biztonsági fenyegetések tükrében azonnal történik.

Teendők a következők:

- Ki kell kijelölni azokat a személyeket, akik a rendszerszoftverben módosításokat végezhetnek:

Kijelölt személyek a rendszergazdák.

A kijelölt személyek nevét az 1/a mellékletű dokumentum tartalmazza.

Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem
A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni. Gondoskodni kell arról, hogy a tárolt programok, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek.

Lokális gépekre programot csak a rendszergazda telepíthet.

A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt.

A programokról nyilvántartást kell vezetni, amelynek. legalább az alábbi adatokat kell tartalmaznia:
- a program azonosítója,
- a program készítőjének neve,
- a program megnevezése.

A program dokumentáció a rendszerdokumentációnak része.

Programok megőrzése, nyilvántartása

- a programokról naprakész nyilvántartást kell vezetni,

- a nyilvántartásból egyértelműen megállapítható legyen a program azonosítására és kezelésére vonatkozó adatok.

Programok fizikai védelme

A védelem érdekében a felhasználás helyétől elkülönítetten, behatolástól védetten egy-egy duplikált példányt kell tárolni a programkönyvtárba elhelyezett programokról.

Dokumentálás

Kiemelkedő szerepe van a megfelelő szintű és részletezettségű dokumentálásnak.

13. A központi számítógépek és a hálózat munkaállomásainak működésbiztonsága

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

A vásárolt szoftver eszközökről biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag el kell különíteni.

Munkaállomások (USER-ek)

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

- Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
- Vírusfertőzés gyanúja esetén a rendszergazdát azonnal értesíteni kell.
- Vírusmentesítő programot futtatni csak a rendszergazda felügyelete mellett szabad.
- Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.
- Az intézmény informatikai eszközeiről programot, illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.
- A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.
- Az informatikai eszközt és tartozékait helyéről elvinni a rendszergazda tudta és engedélye nélkül nem szabad.

14. Hálózat és internet

Az intézmény belső számítógépes hálózatán a felhasználók név és jelszó megadásával vehetik igénybe a hálózati erőforrásokat. A jelszavak minimális hossza 8 karakter, melynek kis és nagy betűket, valamint számot kell tartalmaznia. Az intézményi hálózaton érvényes felhasználó név jelszó kombinációt egyéb helyen nem szabad alkalmazni. A jelszavak szabadon módosíthatóak.

15. Ellenőrzés

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszerben meglévő veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése, illetve annak megakadályozása, hogy azok megismétlődjenek.

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

Az Informatikai Biztonsági Szabályzat

2023. év 02. hó 15. napjával lép hatályba.

1./a. *melléklet*

Savaria Múzeum és tagintézményei
Székhely: Szombathely, Kisfaludy S. u. 9.

Hozzáférési, adatgazdai jogosultságok és jogkörök

Jogkörök:

1. Adatgazda: Múzeumigazgató

2. Rendszergazda: Az intézmény tulajdonában lévő számítógépek és szerver(ek) operációs rendszerében és a rajta futtatott alkalmazásokon az alábbi rendszergazdai jogosultsággal rendelkező személyek végezhetnek módosításokat:

- Kiss Tamás informatikai csoportvezető
- Milos László műszaki ügyintéző munkatárs

3. Gyűjteményi adatbázist töltő felhasználó: A gyűjteménnyel rendelkező osztályok munkatársai, akiknek feladata az adatbázis töltése.

4. Gyűjteményi adatbázisba betekintő felhasználó: A gyűjteménnyel rendelkező osztályok minden munkatársa és az osztályvezetők.

5. Általános jogú felhasználó: A saját számítógépén található munkájának ellátásához szükséges programok futtatása, adatállományok kezelése.

Jogosultsági szabályok:
Minden gyűjteményi adatbázissal rendelkező osztály munkatársa a saját adatbázisához férhet hozzám más osztályéhoz nem.
Az összes adatbázishoz csak a rendszergazda jogkörrel rendelkező felhasználók férhetnek hozzá biztonsági mentés céljából.

1./b. *melléklet*

Savaria Múzeum és tagintézményei
Székhely: Szombathely, Kisfaludy S. u. 9.

ADATKEZELÉSI NYILATKOZAT

Alulírott.....
(név ,lakcím)
nyilatkozom, hogy a feladatellátás során tudomásomra jutott információkat megőrzöm, azt illetéktelen személyek részére nem adom át.

A munkavégzés során csak a részemre hozzáférhető, a munkavégzéshez szükséges adatokkal dolgozom, más adatok hozzáférésére kísérletet sem teszek.

A számítógépek háttértárolóján csak a munkavégzéshez szükséges adatok, fájlok programok tárolhatók, különös tekintettel tilos bármilyen illegális tartalom, médiatartalom letöltése, tárolása és felhasználása.
Az adatbiztonság, és jogszerű adattárolás megtartásáért a mindenkori számítógép kezelője, a felelős személy.

A fentieket megértettem, büntetőjogi felelősségem tudatában magamra nézve kötelezőnek tartom.

Dátum: 202.....

.....
aláírás

2. *sz. melléklet*
Számítógéppel ellátott irodák rendje

1. A Számítógéppel ellátott irodákban és tantermekben az oda munkavégzésre beosztottakon kívül csak az alábbi személyek tartózkodhatnak:

- az intézmény igazgatója, helyettesei
- csoportvezetők
- az igazgató által kijelölt személyek
- rendszergazda

Más személyek benntartózkodását csak az igazgató engedélyezheti.

2. Üzemeltetés alatt az ajtókat állandóan becsukva, üzemidőn kívül pedig zárva kell tartani. Munkaidőn, kívül idegen személy csak az intézmény igazgatójának (távollétében helyettesének) engedélyével tartózkodhat számítógéppel ellátott irodákban. A számítógéppel ellátott irodák áramtalanításáért a számítógép kezelő a felelős. A munkaidő végén, az irodát utoljára elhagyó dolgozó köteles ellenőrizni az áramtalanítást, ellenőrizni az ablakok zárt állapotát, köteles a riasztóberendezést élesíteni és az ajtókat kulcsra zárni.

3. Az számítógéppel ellátott irodákban az esztétikus, higiénikus, folyamatos munkavégzés feltételeit meg kell őrizni.

4. A számítógépek közvetlen közelében ételt, italt fogyasztani TILOS!

5. SZIGORÚAN TILOS számítógéppel ellátott irodákba égő cigarettával belépni, illetve ott dohányozni!

6. A számítógéppel ellátott irodák takarítását csak az arra előzőleg kioktatott személyek végezhetik.

7. A berendezések belsejébe nyúlni TILOS! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak a rendszergazda vagy egy megfelelő műszaki végzettséggel rendelkező a feladat ellátására kijelölt dolgozó végezhet. Ez alól csak a megbízott szervizek szakemberei kivételek – a megbízást írásos megrendelővel kell alátámasztani, amit a műszaki csoportvezető vagy az igazgatóhelyettes írhat alá.

8. Az informatikai eszközöket csak rendeltetésszerűen és kizárólag az üzemszerű munkák elvégzésére lehet használni.

9. Az számítógéppel ellátott irodákban elhelyezett adathordozókhoz *a adatkezelő dolgozókon* kívül, illetve azok engedélye vagy jelenléte nélkül senki nem nyúlhat.

10.Optikai lemezeket, pendrive-okat, memoriakártyákat egyéb adathordozókat valamint leporellókat, nyomtatványokat, dokumentumokat csak az adatkezelő engedélyével lehet kihozni, illetve bevinni a számítógéppel ellátott irodába.

11. Az elektromos hálózatba más - nem a rendszerekhez, illetve azok kiszolgálásához tartozó - berendezéseket csatlakoztatni nem lehet!

12. A javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetmentes használat, a szakszerűség, a vonatkozó érintésvédelmi szabványok és az esztétikai követelményeket. Nem végezhető olyan javítás, szerelés, átalakítás vagy bármilyen beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat.

3. sz. melléklet

Informatikai biztonsági útmutató

Az intézmény informatikai szoftver-hardver védelmének eszközeit az Informatikai Biztonsági Szabályzat (IBSZ) foglalja magában. Ez minden dolgozó számára kötelező érvényű. Az IBSZ hozzáférhető az igazgatói irodában, illetve elektronikus formában a szerver számítógép osztott könyvtárában. Az „Informatikai biztonsági útmutató" az IBSZ mellékletét képezi.

Az informatikai rendszer biztonsága érdekében a következő veszélyforrásokra kell különösen ügyelni:

1. **Külső adathordozókról történő adatátvitel** a számítógép háttértárolójára. (CD-ről, pendriveról, stb.)
Minden esetben az állomány megnyitás, másolás előtt kötelező a víruskeresés.

2. **Internet weboldalak megnyitása:** Csak a biztonságos adattartalommal rendelkező. illetve a munkavégzéshez kapcsolódó, vagy belső hálózaton tárolt intézményi weboldalakat szabad megnyitni. Szigorúan tilos az illegális fájlcserélő, tiltott tartalommal rendelkező weblapok megnyitása, különös tekintettel a médiatartalmakra (mp3, filmek, képek)
- audio: MP3, WAV, stb.
- video: AVI, MPG, MP4, WMV, MKV, stb.
- kép: JPG, PNG, BMP, stb.

3. A nem beazonosítható úgynevezett **hivatkozás (link)** megnyitása nagy veszélyt rejt magában, mivel olyan káros tartalmú internetes oldalra irányíthat, ami vírust, kártevőt tartalmaz. Ezek a hivatkozások lehetnek weblapokon, megkaphatók e-mailben, chat site-okon vagy akár skype-on, messenger-en és más üzenetküldőn.

4. Csak olyan **e-mailt** nyissunk meg, amely feladóját ismerjük, viszont ebben az esetben is óvatosan kell eljárni. mert egyes esetekben adathalász weboldalak, „cégek" saját ismerősünk által küldött üzenetként megjelenő e-mailjei is előfordulnak a postafiókunkban. Az ilyen e-mailek a gyanútlan felhasználót a bennük található linkre, vagy gombra kattintásra utasítják, amit követően azonnal indul a vírus, kémprogram telepítése a számítógépre.
Amennyiben gyanús levelet kapunk azonnal töröljük és a törölt elemek közül is távolítsuk el. E-mail-ben kapott csatolt állományt semmiképpen ne nyissuk meg közvetlenül. Először a Fájl mentése lehetőséggel mentsük a számítógép háttértárolójára egy külön mappába, majd a megnyitása előtt víruskeresést kell rajta végrehajtani.

Összefoglalva a veszélyforrások:
- nem biztonságos weblap
- külső adathordozók
- veszélyes hivatkozások !!!
- e-mail-ek, különös tekintettel a csatolt állományokra

A számítógépek háttértárolóján csak a munkavégzéshez szükséges adatok, fájlok programok tárolhatók, különös tekintettel tilos bármilyen illegális tartalom, médiatartalom letöltése, tárolása és felhasználása.
Az adatbiztonság, és jogszerű adattárolás megtartásáért a mindenkori számítógép kezelője, a felelős személy.

Megismerési záradék:

Aláírásommal igazolom, hogy a Savaria Múzeum Informatikai Biztonsági Szabályzatában foglaltakat és a hozzátartozó dokumentumok előírásait megismertem, betartását rám nézve kötelezőnek ismerem el. Intézmény-, osztály- és csoportvezetőként gondoskodom róla, hogy az általam irányított dolgozók a szabályzat tartalmát megismerjék.

Név	Képviselt szerv/Beosztás	Dátum	Aláírás
CSAPLÁROS ANDREA	SAVARIA MÚZEUM MÚZEUMIGAZGATÓ	2023. 02. 15.	
Dr. Vig Károly	Savaria Múzeum Tud. ig. helyettes	2023. 02. 15.	
CZENKI ZSUZSANNA	SAVARIA MÚZEUM AM. IGH.	2023. 02. 15.	
PÉTER BENCE	SAVARIA MÚZEUM pályázati munkatárs	2023. 02. 15.	
MILOS László	SAVARIA Múzeum Informatika	2023.02.15	
KISS ERNŐ CSABA	SAVARIA MÚZEUM Botanikus	2023.02.15.	
MÉSZÁROS IRÉN	SAVARIA MÚZEUM TÖRTÉNETTUD. OSZT.	2023. 02. 15.	
Dankovics Róbert	Savaria Múzeum tem. tud. osztály	2023. 02. 15.	
KÁLMÁN GYÖRGY	SAVARIA M. MŰV. CSOP.	2023. 02. 15	
CEBULA ANNA	Szombathelyi Képtár igazgató	2023. 02. 15.	
Dr. Balogh Lajos	Savaria Múzeum történeti osztályvez.	2023. II. 15.	
PÁRTZI PIROSKA	Savaria Múzeum gazdasági ü.	2023. 02. 15.	
KISS TAMÁS	Sav. Múz. inf. csop.	2023. 02. 15	
TÁNCZ BALÁZS	SAVARIA MÚZEUM - INTÉZMÉNYVEZETŐI MEGBÍZOTT	2023. 02. 15.	
ANDREA KOVÁCS	SAVARIA MÚZEUM RÉGÉSZETI OSZT.	2023 02 15	
SOLTÁSZ GÁBOR	INTV H SAVARIA MÚZEUM	2023.02.15	