

Viski Károly Múzeum Kalocsa

6300 Kalocsa, Szent István király út 25.

**ADATVÉDELMI ÉS SZÁMÍTÁSTECHNIKAI
VÉDELMI SZABÁLYZAT**

Érvényes: 2017. január 1-től

TARTALOMJEGYZÉK

I. ÁLTALÁNOS ADATVÉDELMI SZABÁLYOK.....	3
1. A szabályzat célja, hatálya	3
2. Az adatkezelés során használt fontosabb fogalmak.....	4
3. A keletkezett adatok besorolási rendje.....	6
4. Személyes adatok védelme	7
II. SZÁMÍTÁSTECHNIKAI VÉDELMI SZABÁLYOK.....	8
1. Adatok és programok védelme	8
2. Számítógépek, eszközök és dokumentációk védelme.....	9
3. Mágneses adathordozók védelme	10
4. Az adathordozók selejtezése	10
5. Vírusvédelmi eljárások	11
6. A vírusvédelem szabályai a felhasználó részéről.....	11
7. Az elektronikus levelezés vírusvédelme	12
III. ZÁRÓ RENDELKEZÉS.....	12

AZ ÁLTALÁNOS ÉS A POLGÁROK SZEMÉLYES ADATAIVAL KAPCSOLATOS ELJÁRÁSOK RENDJÉRE VONATKOZÓ ADATVÉDELMI, VALAMINT SZÁMÍTÁSTECHNIKAI VÉDELMI SZABÁLYZAT

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény, a kutatás és a közvetlen üzletszerzés célját szolgáló név és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvényben foglaltak alapján, az 1992. évi LXVI. törvény. 30. § (1) bekezdésében kapott felhatalmazás alapján a múzeum adatvédelemmel összefüggő feladatait és eljárási rendjét a következők szerint szabályozom.

I. ÁLTALÁNOS ADATVÉDELMI SZABÁLYOK

1. A szabályzat célja, hatálya

A szabályzat célja, hogy a rendelkezéseink figyelembevételével meghatározza a szervezetnek a személyes adatok védelmével kapcsolatos általános feladatait és az eljárás rendjét, továbbá az adatbiztonság követelményeinek érvényesülését.

A szabályzat *személyi hatálya* kiterjed a Viski Károly Múzeummal közalkalmazotti jogviszonyban álló vezetőkre, valamint a munkajogviszony keretében foglalkoztatott ügyviteli és fizikai alkalmazottakra. Kiterjed továbbá azokra a személyekre, akik a múzeumtól kapott megbízásuk alapján az Adatvédelmi és Számítástechnikai Védelmi szabályzat előírt rendelkezéseivel kapcsolatba kerülnek.

A szabályzat *tárgyi hatálya* kiterjed a Viski Károly Múzeum tulajdonát képező, továbbá az épület(ek)ben lévő és használt:

- valamennyi használatban lévő, vagy tárolt informatikai berendezésre és azok műszaki dokumentációjára függetlenül attól, hogy az személyi használatra vagy szervezeti egység használatába került kiadásra;
- a Viski Károly Múzeumnál keletkezett minden elektronikus adatra, annak keletkezésének, felhasználásának és feldolgozásának helyétől és megjelenési formájától függetlenül;
- valamennyi adathordozóra, azok tárolására és felhasználására, illetve a beérkezés és a feldolgozás közötti időszakra;
- a Viski Károly Múzeum által használt felhasználói programokra és rendszerprogramokra;

- az informatikai rendszerben megjelenő valamennyi dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési).

A szabályzat az informatikai rendszerrel kapcsolatos, biztonságos adatkezelési és adatvédelmi eljárásokat és feladatokat rögzít. A számítástechnikai eszközök beszerzésének és használatának, a saját készítésű és vásárolt szoftverek alkalmazásának a folyamatát, továbbá egyes személyek informatikai biztonságot érintő feladatait.

A személyes adatok védelméért, az adatkezelés jogszerűségéért a múzeumigazgató felelős.

A múzeum által vezetett személyes adatokat tartalmazó, illetve a személyes adatokat nem tartalmazó nyilvántartásokat, valamint az azokból történt adattovábbításokat, továbbá a múzeum által elérhető személyes adatokat tartalmazó, nem saját nyilvántartásokat jelen szabályzat **1-6. számú melléklete** tartalmazza.

A múzeumnál nyilvántartott adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, illetve a sérülés, törlés, vagy megsemmisülés ellen.

Iratot munkaköri feladat ellátásán kívül a munkahelyről kivinni, valamint munkahelyen kívül feldolgozni, tárolni csak a múzeumigazgató egyetértésével lehet, azzal a feltétellel, hogy az irat tartalmát illetéktelen személy ne ismerje meg.

Az iratok kezelése, tárolása során ki kell zárni annak a lehetőségét, hogy illetéktelen személy az iratok tartalmába betekintést nyerjen. Az iratokat a múzeum zárható helyiségében, elkülönítetten kell tárolni. A munkavégzés céljára szolgáló irodákat a közalkalmazott munkavállaló távozásakor kulcsra kell zárni.

Az irodahelyiségek nyitva tartása miatti iratokhoz történő illetéktelen hozzáférés esetén az érintett fegyelmi és kártérítési felelősséggel tartozik.

2. Az adatkezelés során használt fontosabb fogalmak

Adat: az adatok osztályozása szempontjából adatnak tekintjük azokat a dokumentumokat, jelentéseket, információkat, leveleket stb., amelyek az informatikai rendszerben elektronikusan tárolódnak.

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 általa megbízott adatfeldolgozóval végrehajtatja.

Adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a 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, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.

Adatgazda: az a személy, akinél a rendszerben tárolásra kerülő elektronikus adat keletkezik.

Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Adathordozó: adathordozónak nevezzük az informatikai rendszertől elválasztható adattároló eszközöket.

Adatfelelős: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett.

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.

Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelővel kötött szerződése alapján - beleértve a jogszabály rendelkezése alapján történő szerződéskötést is - adatok feldolgozását végzi.

Adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.

Adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.

Adatzárolás: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából.

Dokumentum: számítástechnikai eszközökkel készített irat vagy fájl (például Word szövegszerkesztővel vagy Excel táblázatkezelővel készített állomány, stb).

Felhasználó: minden dolgozó, aki az informatikai szolgáltatásokat használja.

Hozzáférés: olyan eljárás, amely lehetővé teszi valamely informatikai rendszer használója számára, hogy a rendszerben lévő adatokat elérje (írás, olvasás, módosítás, törlés, stb.).

Hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez.

Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

Közzététel: közérdekű és közérdekből nyilvános adatoknak internetes honlapon, digitális formában, bárki számára, személyazonosítás nélkül, korlátozástól mentesen, díjmentesen történő hozzáférhetővé tétele.

Különleges adat:

a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,

b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.

Közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és

tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

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.

3. A keletkezett adatok besorolási rendje

A múzeumban az informatikai biztonsággal összefüggésben az adatok besorolási rendje a következő:

- Bizalmasság: az információt csak az legyen képes elolvasni, aki arra jogosult.
- Sértetlenség: az információt csak az módosíthassa vagy törölhesse, aki arra jogosult, továbbá az adat hiteles forrása bizonyítható legyen.
- Rendelkezésre állás: az arra jogosult felhasználó a szükséges információhoz a megfelelő helyen és időben hozzáférhessen.

A keletkezett információk besorolási kategóriái a következők:

- Nyilvános: Minden olyan személyes és közérdekű adat, amelynek nyilvánosságra kerülése az érintett személyek, illetve szervezetek számára erkölcsi, anyagi és jogi következményekkel nem jár.
- Belső információ: Minden olyan adat, amely a szervezeten belül minden alkalmazottnak és szerződéses munkatársnak korlátozás nélkül rendelkezésre áll, ugyanakkor szervezeten kívül nem kerül kihirdetésre.
- Bizalmas: Olyan nem minősített adat, amelynek nyilvánosságra kerülése az érintett személyek vagy szervezetek számára hátrányos erkölcsi, jogi és anyagi következményeket von maga után.
- Szigorúan bizalmas: a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 2011. évi CXII. törvényben meghatározott adatok, különös tekintettel a személyes és azon belül a különleges adatokra.

Ha a rögzíteni vagy létrehozni kívánt adat egyértelműen egyik adatscsoportba sem sorolható be, abban az esetben az adatgazda köteles az adat besorolási eljárását írásban kérni a múzeumigazgatótól.

A múzeum informatikai rendszerének minden felhasználója köteles az általa tárolt, kezelt vagy létrehozott adatot annak besorolása szerint a szabályzatban meghatározott módon kezelni és tárolni. Az egyes adatokra vonatkozó előírások betartásáért az adatgazda felelős. A

múzeum informatikai rendszerében tárolt és kezelt adatok adatgazdája az a felhasználó, aki azt a rendszerben rögzítette, illetve létrehozta.

4. Személyes adatok védelme

A múzeumigazgató a személyes adatkezelést végző személy munkaköri leírásában határozza meg az általa kezelhető és elérhető személyes nyilvántartások körét.

A személyes adatkezelést végző személy felelőséggel tartozik azért, hogy tevékenységét az adatkezelésre és az adatok védelmére vonatkozó jogszabályoknak, az adatkezelést elrendelő jogszabály hiányában pedig az érintett hozzájárulásának megfelelően végezze. Az adatgazda a nyilvánvalóan jogsértő adatkezelési utasítást köteles megtagadni és erről a múzeumigazgatót haladéktalanul írásban tájékoztatni.

Az adatkezelési tevékenységet végző személyek kötelesek az adatvédelmi és az adatbiztonsági szabályokat betartani.

Az adatgazda azokat a személyes adatokat veheti fel, illetve veheti át harmadik személytől, amelyek kezelésére törvény vagy az érintett felhatalmazza.

Az érintett hozzájárulásán alapuló adatkezelésnél az adat felvételekor az érintettet előzetesen tájékoztatni kell az adatszolgáltatás önkéntességéről és kérésére a hozzájárulás megadásának vagy megtagadásának az adatkezelő tevékenységi körébe eső következményeiről.

Az adatok tárolási módját úgy kell megválasztani, hogy törlésük az adattörlési határidő lejártakor, illetve ha az más okból szükséges, elvégezhető legyen.

Az adatok a jogszabályban és a besorolási kategóriában elfoglalt helyük szerint a meghatározott célra használhatók fel.

A múzeum számítógépes hálózatán lévő nyilvántartásokba történő belépés a múzeumigazgató döntése alapján – a személyes jelszón kívül – a hálózati szoftverben egyedileg beállított hozzáféréssel engedélyezhető. A belépés csak a legszükségesebb körben, az ügyintéző munkaköri feladatai ellátásához kapcsolódóan engedélyezhető a következők szerint:

Megnevezés	Hozzáférési jogosultság
Ügyirat nyilvántartás	gyűjteménykezelők
Illetmény átutalás	pénzügyi ügyintéző /gyűjteménykezelő
Gyarapodási napló	múzeológusok, gyűjteménykezelők
Szakleltárkönyvek	múzeológusok, gyűjteménykezelők

(A hozzáférési jogosultság általánosságban a hálózaton levő adatok feldolgozását jelenti, melyet az adott munkakör ellátására feljogosított ügyintéző végez.)

A múzeum által elérhető nem saját személyes adatokat tartalmazó nyilvántartásokból történő adatkezelés esetén az alábbiak szerint kell eljárni:

- Az adatkezelésre jogosultak névsorának jóváhagyása a múzeumigazgató feladatkörébe tartozik. A belépésre vonatkozó személyi javaslat csak a munkavégzéshez feltétlenül szükséges, lehető legszűkebb körre vonatkozhat.
- A nyilvántartási rendszerekhez hozzáférési jogosultsággal rendelkezők névsorát a *pénzügyi ügyintéző/gyűjteménykezelő* köteles naprakészen vezetni.
- Hozzáférési jogosultsággal rendelkező adatkezelő az adatlekérdezésekről e szabályzat mellékletét képező „Adatszolgáltatási nyilvántartást” köteles vezetni.

II.

SZÁMÍTÁSTECHNIKAI VÉDELMI SZABÁLYOK

1. Adatok és programok védelme

A múzeum számítógépes adat-feldolgozási folyamatába kerülő információkat és programokat fokozott biztonsági szabályok szerint kell kezelni. Ennek oka, hogy a számítógépen titoknak minősített adatokat nem tárolnak, illetve a feldolgozás során keletkező adatok sem minősülnek titkosnak. Ezen fokozatba sorolás független az adatok megjelenési formájától. Ettől eltérő esetben a titkos ügykezelés szabályai szerint kell eljárni.

A múzeumban működő számítógépeken csak előzetesen ellenőrzött programot szabad futtatni. Az ellenőrzésnek ki kell terjednie a vásárolt vagy átvett program tesztelésére, esetleges működést akadályozó hibák felderítésére. A feltárt hiányosságokról jegyzőkönyvet kell felvenni, melyet a programot szállító szervhez haladéktalanul el kell juttatni. Hibás programot üzembe helyezni tilos.

Tilos vírusellenőrzés nélkül floppyt, CD-t, DVD-t vagy más adathordozót a számítógépbe helyezni, arról programot vagy adatot a rendszerbe tölteni!

A tesztelést a felhasználóval közösen az informatikai feladatot ellátó szervezet végzi.

Vásárolt, vagy átvett floppy, CD, DVD lemezen tárolt program esetén minden esetben biztonsági másolatot kell készíteni, majd az eredeti lemezt írásvédetté kell tenni.

A programok felhasználói dokumentációját a felhasználás helyén kell elhelyezni.

Feldolgozásra kerülő adatok előkészítése

- a) Számítástechnikai feldolgozásra csak tartalmilag és formailag ellenőrzött adatok kerülhetnek.
- b) Az ellenőrzésért az adatfelelősség elve szerint adatlapos rögzítés esetén az adatlapot kiállító, adatlap nélküli rögzítés esetén feldolgozást végző kijelölt közalkalmazott felelős. Lehetőség szerint biztosítani kell, hogy az adatok a keletkezés helyén kerüljenek rögzítésre.

Feldolgozás folyamata

- a) Az adatállományok módosítását kizárólag csak a feldolgozásra készült programmal lehet elvégezni.
- b) Az adatfeldolgozás során a számítógép- vagy programhibából adódó adatvesztés fordulhat elő. Ilyenkor az adatrögzítést azonnal be kell fejezni és a további adatvesztés elkerülésére az informatikai felelőst haladéktalanul értesíteni kell.

Mentés

- a) A számítógépeken tárolt információk biztonságos megőrzése céljából az adatokat szükséges rendszerességgel legalább két egyező példányban menteni kell.
- b) Hetente mentést kell végezni a hálózati működést biztosító központi gépen történt adatváltozásokról.
- c) Egyedi gépek vagy programok esetén a mentés gyakoriságát a múzeumigazgató határozza meg.
- d) Az egyedi gépekről a mentést az egyedi gép használója, a múzeum központi szervergépéről a mentést a kijelölt munkatárs végzi el.

Másolás

A számítógépes programok a szerzői jog szerint védelmet élveznek, ezért másolásuk, harmadik fél számára történő továbbadásuk tilos.

Törlés

Mágneses adathordozókon tárolt adatok és programok törlését csak a múzeumigazgató írásbeli engedélye alapján lehet elvégezni. Külön figyelmet kell fordítani az irattározási és selejtezési szabályok betartására.

Archiválás

Az informatikai eszközökön tárolt adatok archiválását az adatok biztonságos kezelése érdekében a múzeumnál évente egyszer (december 31-ig) kell elvégezni. Az archív adatok tárolásánál figyelembe kell venni a biztonsági előírásokat (zárható, tűzbiztos tárolóeszköz), és biztosítani kell a tárolási körülményeket (hőmérséklet, páratartalom).

Visszatöltés

Az adathordozókon tárolt adatok visszatöltését, visszaállítását a múzeumigazgató engedélyezheti. Ez alól kivételt képeznek az egyedi felhasználók, akik a mentésekből saját munkakönyvtárak adatait engedély nélkül is visszatöltetik.

Hálózati alkalmazások esetében az adatvesztés elkerülésére és az adatbiztonság fokozására személyre lebontott hozzáférési jogosultságot kell meghatározni. (**8. számú melléklet**).

2. Számítógépek, eszközök és dokumentációk védelme

A számítógépek és eszközök rendeltetésszerű használatáért a személyi leltár szerint a használatra kijelölt közalkalmazott felelős.

A hálózati működő számítógépeken kizárólag az erre kiképzett szakemberek dolgozhatnak.

Meghibásodás megelőzéséről folyamatos karbantartással kell gondoskodni, üzemzavar esetén a javítást csak arra kiképzett szakember végezheti.

Fizikai sérülések megelőzésére (pl.: hálózati vezetékszakadás) a számítógépet telepítési helyéről elmozdítani, vagy áthelyezni nem szabad.

Vagyonvédelmi megfontolásból azokat a szobákat, ahol számítógép üzemel, biztonsági felszereléssel kell ellátni. A közalkalmazott köteles a munkaidő végeztével a számítógépet kikapcsolni, az azok elhelyezésére szolgáló irodahelyiséget bezárni és a kulcsot az időpont dokumentálásával elzárt helyen letenni. A múzeumtól javításra, vagy más célból elszállítani eszközöket csak bizonylatolás után lehet.

Elektromos érintésvédelmi szempontból a számítástechnikai eszközöket csak védőföldeléses, minden számítógéphez leltár szerint tartozó biztonsági kapcsolóval ellátott dugaszoló aljzatba lehet csatlakoztatni. Annak sérülését minden esetben jelezni kell. ***A berendezéseket vízzel oltani vagy tisztítani tilos!***

A tűz elleni védekezés rendjét és elhárítása érdekében szükséges intézkedéseket a szervezet Tűzvédelmi Szabályzata tartalmazza.

3. Mágneses adathordozók védelme

A mágneses adathordozók védelmére és azonosítására az adathordozókat azonosítóval (címkével) kell ellátni és azokról nyilvántartást kell vezetni.

A mentést tartalmazó adathordozók megőrzési idejét úgy kell meghatározni, hogy azokról az aktuális adatállomány sérülés esetén visszaállítható legyen.

Vírust tartalmazó, nem mentesíthető adathordozót használatban tartani nem lehet.

Az adathordozót óvni kell a szennyeződésektől és a fizikai sérüléstől, ezért használat közben óvakodni kell a mágnesezhető réteg megérintésétől, használat után pedig zárható dobozban, vagy a gyári csomagolásban elektromos erőterektől távol (monitor, televízió, hangszóró, ventilátor, telefon, rádió, stb.) kell tartani.

Külső szervnek átadott adathordozókról bizonylatot (az átadás, átvétel időpontját, az átadás célját, az átadott adathordozó számát, tartalmát az átvevő szerv megnevezését és címét, az átadás idejét, (ideiglenesen vagy véglegesen) az átvevő szerv őrzéssel megbízott felelősének megnevezését, valamint az átadó és átvevő szerv erre feljogosított képviselőjének aláírását tartalmazó jegyzéket) kell készíteni.

4. Az adathordozók selejtezése

A múzeum által vásárolt és a dolgozó(k) részére kiadott adathordozót abban az esetben kell selejtezni, ha:

- fizikailag megsérült,
- gyári, gyártási hibából következően felhasználásra alkalmatlan,
- a tároló kapacitás a megengedhető érték alá csökken,

- véglegesen elhasználódott.

A felhasználók felelőssége, hogy a használhatatlanná vált adathordozókat (floppy, CD, DVD, stb.) a múzeumigazgató felé jelezze, aki gondoskodik azok közös helyen történő összegyűjtéséről. A selejtezés előtt biztosítani kell az adathordozón tárolt adatok biztonságos törlését (fizikai törléssel, formattálással). Ha a tárolt adatok biztonságosan nem törölhetők, akkor az adathordozót úgy kell megsemmisíteni, hogy további felhasználásra már alkalmatlan legyen, azaz fizikai roncsolással kell használhatatlanná tenni.

A megsemmisítés során a felesleges vagyontárgyak hasznosításának és selejtezésének szabályzatában előírtak szerint kell eljárni, annak tényét megsemmisítési jegyzőkönyvben kell rögzíteni.

5. Vírusvédelmi eljárások

A múzeumnál alkalmazott vírusvédelmi rendszernek meg kell felelnie a következő elvárásnak:

- a vírus védelmi szoftvernek jó minőségűnek és kellő gyakorisággal aktualizáltnak (frissítettnek) kell lennie, hogy felismerési hatékonysága maximális legyen;
- a vírus védelmi szoftvernek minden támadási ponton aktívan üzemelnie kell.

A múzeum egészére kiterjedően a vírusfertőzések megelőzése, kiszűrése és megszüntetése céljából az *ESET NOD32 Antivirus* elnevezésű vírusvédelmi szoftvert alkalmazza. A szoftver teljes számítástechnikai gépparkot lefedő (beleértve a mobil eszközöket is) telepítéséért, naprakész és folyamatos üzemeltetéséért, frissítéséért, a vírustámadások elleni védekezés megszervezéséért a múzeumigazgató a felelős. Az újonnan vásárolt számítógépekre azok rendszerbe állítása során telepíteni kell a víruskereső programot.

A számítógépes munkaállomásokon a víruskereső programot úgy kell beállítani, hogy naponta egyszer (az első bejelentkezéskor) megtörténjen az automatikus vírusesztt futtatása. A rendszerbe kívülről bekerülő adatokat (floppylemez, USB portról csatlakoztatható eszközök, CD-ROM, Internet stb.) felhasználás előtt vírusellenőrzésnek kell alávetni. A víruskereső program munkaállomásokon történő lefuttatása a felhasználó feladata és felelőssége.

A víruskereső szoftvernek minden lehetséges bejutási pontot (floppylemez, USB portról csatlakoztatható eszközök, CD-ROM, hálózat, e-mail, stb.) ellenőriznie kell, így az elsődleges támadási felületnek minősülő munkaállomásokat, és a másodlagos támadási felületnek minősülő tűzfalakat, alkalmazás és levelező szervereket.

A vírusadatbázisok frissítése a rendszer hatékony működésének szempontjából fontos, mivel az új vírusok megjelenése és elterjedése között rövid idő (esetenként néhány óra) telik el.

6. A vírusvédelem szabályai a felhasználó részéről

A múzeumnál alkalmazott *ESET NOD32 Antivirus* elnevezésű vírusvédelmi rendszer a számítógépek működése közben folyamatosan dolgozik, így a felhasználói munka során igénybe vett állományok (programok, adatok, dokumentumok) közvetlenül már a használat előtt vírusellenőrzésre kerülnek. A számítástechnikai eszközökön beállított aktív védelmi rendszer kikapcsolása tilos. A rendszer kikapcsolásából adódó károkért (adatvesztés, illetéktelen hozzáférés stb.) a szabályt megszegő teljes körű felelősséggel tartozik.

Amennyiben a felhasználó a víruskereső program „*futtatása*” során víruszt észlel, azonnal jelentenie kell a pénzügyi ügyintéző/gyűjteménykezelő felé, aki feljegyezi a vírus és a

fertőzött file nevét, továbbá a munkaállomás számát (helyét). pénzügyi ügyintéző/gyűjteménykezelő gondoskodik a vírus további terjedésének megakadályozásáról, és – amennyiben a felhasználói gépen futó program automatikusan nem törölte – a vírus szakszerű kiirtásáról.

7. Az elektronikus levelezés vírusvédelme

Ha a múzeum elektronikus levelezési rendszerén keresztül fertőzött levél, vagy csatolt állomány érkezik, arról az *ESET NOD32 Antivirus* víruskereső szoftver értesíti a felhasználót (és amennyiben van a rendszergazdát). Ha az aktív védelem a fertőzött állományt eltávolítja, akkor a munka megkezdhető vagy tovább folytatható, amennyiben nem képes a fertőzés eltávolítására, akkor a víruskereső rendszer a fertőzött állományt törli.

Ha a felhasználó levelezési rendszerébe indokolatlan vagy váratlan e-mail érkezik annak tartalmát személyesen (pl. telefonon, e-mailben) ellenőrizni szükséges. Ha a küldő nem szándékosan mellékelte az e-mailhez állományt, akkor nem szabad megnyitni.

III. ZÁRÓ RENDELKEZÉS

Ez a szabályzat 2017. január 1-én napján lép hatályba.

A múzeumnál a múzeumigazgatónak kell gondoskodni arról, hogy e szabályzatot valamennyi munkatárs megismerje, és ennek tényét a szabályzathoz csatolt íven aláírásával igazolja a hatálybalépés napjával egyidejűleg.

Mellékletek: 7 db

A szabályzat kiadásra került és megtalálható:

- 1) Viski Károly Múzeum Kalocsa
- 2) Kalocsai Polgármesteri Hivatal

Kalocsa, 2016. október 21.

.....
Romsics Imre
múzeumigazgató

A Szabályzattal egyetértek:

.....
Dr. Bálint József Miklós
polgármester

HOZZÁFÉRÉSI JOGOSULTSÁG

Sor- szám	Adatfeldolgozás megnevezése	Ügyiratszám	Név	Munkahely
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				

7. sz. melléklet

Lapszám:

ADATSZOLGÁLTATÁSI NYILVÁNTARTÁS

Ügyintéző neve:

.....adatbázisból

Sor-szám	Dátum	Ügyirat szám	Érintett személy neve, szül. ideje	Igénylő megnevezése	Lekérdezés célja, jogalapja	Lekérdező neve	Megjegyzés
1.							
2.							
3.							
4.							
5.							
6.							

HOZZÁFÉRÉSI JOGOSULTSÁG

Módosítva: 2018. szeptember 18.

Adatvédelmi felelős: Szabóné Lantos Andrea régész

Sor-szám	Adatfeldolgozás megnevezése	Név	Beosztás
1.	Ügyirat nyilvántartás	Takács Hajnalka gyűjteménykezelő Réz Ildikó gyűjteménykezelő	gyűjteménykezelők
3.	Illetmény átutalás	Réz Ildikó gyűjteménykezelő	pénzügyi ügyintéző/gyűjteménykezelő
	Gyarapodási napló	Romsics Imre etnográfus múzeumigazgató Szabóné Lantos Andrea régész Mácsainé Iván Éva segédmuzeológus	múzeológusok, gyűjteménykezelők
	Szakleltárkönyvek	Romsics Imre etnográfus múzeumigazgató Szabóné Lantos Andrea régész Mácsainé Iván Éva segédmuzeológus Istella Tímea gyűjtemény- és raktárkezelő Takács Hajnalka gyűjteménykezelő Réz Ildikó gyűjteménykezelő	múzeológusok, gyűjteménykezelők

