991-1/2018 (3)

VÖRÖSMARTY MIHÁLY KÖNYVTÁR

INFORMATIKAI ÉS BIZTONSÁGI SZABÁLYZAT

Jóváhagyta:

Vasné B. Bíró Ilona

igazgató

VÖRÖSMARTY MIHÁLY KÖNYVTÁR * SZÉKESFEHÉRVÁR * 1.

Hatályba lépés: 2018. augusztus 1.

Tartalomjegyzék

INFORMATIKAI ÉS BIZTONSÁGI SZABÁLYZAT 4

1. AZ IBSZ CÉLJA 4
2. AZ IBSZ HATÁLYA 5
   - 2.1. *Személyi hatálya* 5
   - 2.2. *Tárgyi hatálya* 5
3. KAPCSOLÓDÓ SZABÁLYOZÁSOK 5
4. VÉDELMET IGÉNYLŐ, AZ INFORMATIKAI RENDSZERRE HATÓ ELEMEK 5
   - 4.1. *A védelem tárgya* 6
   - 4.2. *A védelem eszközei* 6
   - 4.3. *A védelem felelőse* 6
   - 4.4. *Rendszergazdák feladatai* 6
   - 4.5. *A rendszergazdák ellenőri feladatai* 7
   - 4.6. *A rendszergazdák jogai* 7
5. AZ IBSZ ALKALMAZÁSÁNAK MÓDJA 7
   - 5.1. *Az IBSZ karbantartása* 8
   - 5.2. *A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság* 8
6. AZ INFORMATIKAI ESZKÖZBÁZIST VESZÉLYEZTETŐ HELYZETEK 8
   - 6.1. *Környezeti infrastruktúra okozta ártalmak* 8
   - 6.2. *Emberi tényezőre visszavezethető veszélyek* 9
7. AZ ADATOK TARTALMÁT ÉS A FELDOLGOZÁS FOLYAMATÁT ÉRINTŐ VESZÉLYEK 10
   - 7.1. *A működés és fejlesztés során előforduló veszélyforrások* 10
8. AZ INFORMATIKAI ESZKÖZÖK KÖRNYEZETE, AZOK VÉDELME 10
   - 8.1. *A szerverszoba minimális igénye* 10
   - 8.2. *Vírusvédelem* 10
     - 8.2.1 Bevezetés 10
     - 8.2.2 A szabályzat hatálya 10
     - 8.2.3 Vírusfertőzés gyanús helyzetek 11
     - 8.2.4 Vírusvédelmi teendők 11
     - 8.2.5 Teendők vírusfertőzés esetén 12
   - 8.3. *Levelezési szabályzat* 12
     - 8.3.1 Bevezetés 12
     - 8.3.2 A szabályzat hatálya 12
     - 8.3.3 Alapelvek 12
     - 8.3.4 Szabályok 13
9. AZ INFORMATIKAI RENDSZER ALKALMAZÁSÁNÁL FELHASZNÁLHATÓ VÉDELMI ESZKÖZÖK ÉS

MÓDSZEREK 13
9.1. *A gépterem (szerverszoba) védelme* *13*
9.2. *Hardvervédelem* *13*
9.3. *Az informatikai feldolgozás folyamatának védelme* *14*
9.3.1. Az adatrögzítés védelme 14
9.3.2. Adathordozók védelme 14
9.3.3 Selejtezés, sokszorosítás, másolás 14
9.4. *Szoftvervédelem* *14*
9.4.1. Rendszerszoftver védelem 14
9.4.2. Felhasználói programok védelme 15
10. A KÖZPONTI SZÁMÍTÓGÉPEK ÉS A HÁLÓZAT MUNKAÁLLOMÁSAINAK MŰKÖDÉSBIZTONSÁGA 15
10.1. *Központi gépek (Szerver)* *15*
10.2. *Munkaállomások (felhasználók)* *15*
11. INTERNET-HOZZÁFÉRÉSSEL KAPCSOLATOS INTÉZKEDÉSEK 15
12. MENTÉSI ÉS ARCHIVÁLÁSI FELADATOK 16
12.1. *Általános rendelkezések* *16*
12.2. *Üzemeltetői feladatok* *16*
12.3. *Szerver és munkaállomások adatainak mentése* *17*
13. KÖNYVÁR HONLAPJA 17
14. KÖNYVTÁRELLÁTÁSI SZOLGÁLTATÓ RENDSZER (KSZR) 17
SZÁMÍTÓGÉP-HASZNÁLATI SZABÁLYZAT KÖNYVTÁRHASZNÁLÓK SZÁMÁRA 19
A BELSŐ HÁLÓZAT LEÍRÁSA 22

INFORMATIKAI ÉS BIZTONSÁGI SZABÁLYZAT

A Vörösmarty Mihály Könyvtár Informatikai Biztonsági Szabályzatát (továbbiakban IBSZ) az Európai Parlament és Tanács 2016/679. számú általános adatvédelmi rendelete (GDPR), az információs önrendelkezési jogról és az információszabadságról szóló a 2011. évi CXII. törvény (Info tv.), a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény, 1997. évi CXL. törvény a muzeális intézményekről, a nyilvános könyvtári ellátásról és a közművelődésről 55. §-a, valamint az államtitok és szolgálati titok számítástechnikai védelméről szóló 3/1988. (XI.22.) KSH rendelkezés alapján a következők szerint határozom meg:

1. Az IBSZ célja

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

Az IBSZ célja továbbá:

- a titok-, munka, 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,
- az adatfeldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

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

2. Az IBSZ hatálya

2.1. *Személyi hatálya*

Az IBSZ személyi hatálya az intézmény valamennyi munkavállalójára, kulturális közfoglalkoztatottjára, önkéntesére, a könyvtár olvasóira, illetve az informatikai eljárásban résztvevő más szervezetek dolgozóira egyaránt kiterjed.

2.2. *Tárgyi hatálya*

- Kiterjed a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- az intézmény tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre, valamint a gépek műszaki dokumentációira is,
- a rendszer- és felhasználói programokra,
- az adathordozók tárolására, felhasználására.

3. Kapcsolódó szabályozások

Az IBSZ-t az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:

- Szervezeti és Működési Szabályzat,
- Leltárkészítési és leltározási szabályzat,
- Könyvtárhasználati szabályzat,
- Adatkezelési tájékoztató.

4. 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:

- környezeti infrastruktúra,
- hardver elemek,
- adathordozók,
- dokumentumok,
- szoftver elemek,
- adatok,
- rendszerelemekkel kapcsolatba kerülő személyek.

4.1. *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 rendszerszoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára.

4.2. *A védelem eszközei*

Az intézmény lehetőségeihez mérten mindent elkövet annak érdekében, hogy a védelem tárgyának - különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítse, illetve biztosítsa.

4.3. *A védelem felelőse*

A védelem felelősei a rendszergazdák, akik gondoskodnak a jelen szabályzatban foglaltak szakszerű végrehajtásáról. Adatvédelmi felelősök: a rendszergazdák.

A rendszergazdák az intézmény vezetőjének van közvetlenül alárendelve.

4.4. *Rendszergazdák feladatai*

- ellenőrzik a védelmi előírások betartását,
- kialakítják a védelmi eszközök alkalmazására vonatkozó döntés elkészítése érdekében a szakterületek bevonásával a biztonságot növelő intézkedéseket,
- felelősek az informatikai rendszerek üzembiztonságáért, biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodnak a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- folyamatosan ellenőrzik a védelmi eszközök működését, szervizellátás biztosítását,
- a Szervezeti és Működési Szabályzatot adatvédelmi szempontból véleményezik,
- az adatvédelmi feladatokat ismertetik, oktatják,
- a védelmi rendszer érvényesülését ellenőrzik,

- felelősek az intézmény informatikai rendszer hardver eszközeinek karbantartásáért, és időszakos hardver tesztjeiért,
- ellenőrzik a vásárolt szoftverek helyes működését, vírusmentességét, a használat jogszerűségét,
- a vírusvédelemmel foglalkozó szervezetekkel kapcsolatot tartanak,
- a vírusfertőzés gyanúja esetén gondoskodnak a fertőzött rendszerek izolálásáról,
- folyamatosan figyelemmel kísérik és vizsgálják a rendszer működése és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzik a rendszer önadminisztrációját,
- javaslatot tesznek a rendszer szűk keresztmetszeteinek felszámolására,
- tevékenységükről rendszeresen beszámolnak az intézmény vezetőjének.

4.5. *A rendszergazdák ellenőri feladatai*

- évente egy alkalommal részletesen ellenőrzik az IBSZ előírásainak betartását,
- rendszeresen ellenőrzik a védelmi eszközökkel való ellátottságot,
- előzetes bejelentési kötelezettség nélkül ellenőrzik az informatikai munkafolyamat bármely részét.

4.6. *A rendszergazdák jogai*

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhetnek az intézmény vezetőjénél,
- bármely érintett szervezeti egységnél jogosultak ellenőrzésre,
- betekinthetnek valamennyi iratba, ami az informatikai feldolgozásokkal kapcsolatos,
- javaslatot tesznek az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezik.

5. Az IBSZ alkalmazásának módja

Az IBSZ-t az érintett dolgozókkal az adatvédelmi felelősök megismertetik. Erről nyilvántartást vezetnek.

Az IBSZ-ben érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

5.1. *Az IBSZ karbantartása*

Az IBSZ-t az informatikában - valamint az intézménynél - történt változások miatt időközönként aktualizálni kell.

Az IBSZ folyamatos karbantartása a rendszergazdák feladata.

5.2. *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.

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

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 is biztosítani kell (szoftver, hardver adatvédelem).

6. Az informatikai eszközbázist veszélyeztető helyzetek

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

6.1. *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,
- feszültség-ingadozás,
- elektromos zárlat,
- csőtörés.

6.2. *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.

A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

7. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

7.1. *A működés és fejlesztés során előforduló veszélyforrások*

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

8. Az informatikai eszközök környezete, azok védelme

8.1. *A szerverszoba minimális igénye*

- a szerverszobát a legbiztonságosabb, legvédettebb területre kell telepíteni,
- a lehető legkevesebb nyílászáróval kell rendelkeznie,
- váratlan áramkimaradás esetén a szervek(eket) intelligens UPS-sel kell ellátni (szünetmentes tápegység), mellyel az áramkimaradás folyamatosságát biztosítani lehet.

8.2. *Vírusvédelem*

8.2.1 Bevezetés

A számítógépes vírusok a számítógépen tárolt adatok és programok kártevői. A vírus a megfertőzött program futása közben másolja, többszörözi önmagát. Rendszerbe kerülésük történhet fertőzött lemeztől történő rendszerindítási kísérlet (bootvírusok), egy fertőzött program elindítása (fájlvírusok), egy vírusos makrókat tartalmazó dokumentum megnyitása (makrovírusok), Internethasználat közben (etikailag nem javasolt tartalmak látogatása), vagy e-mailben csatolt állományként terjedő makró- illetve script vírusok, férgek megnyitásának eredményeként. A vírusok gépről gépre terjednek, többnyire észrevehetetlenek, amíg nem aktivizálódnak. Ekkor azonban nagy kárt okozhatnak pótolhatatlan adatok megsemmisítésével, a rendszer bénításával, bizonyos esetekben hardveres károkozással.

A víruskeresők, vírusirtók használata elengedhetetlen, de ezek is csak a már ismert vírusok ellen jelentenek igazi védelmet.

8.2.2 A szabályzat hatálya

A vírusvédelmi szabályzat minden a könyvtár hálózatába kötött személyi számítógépre, laptopra és szerverre/szerverekre vonatkozik.

8.2.3 Vírusfertőzés gyanús helyzetek

Sok jele lehet vírus jelenlétének, azonban ezek nagy része normál tevékenység eredményeként is előállhat. Mivel a vírusok írói általában igyekeznek elkerülni a feltűnő viselkedést, a felhasználó nem feltétlenül találkozik az alább felsorolt – vírusfertőzésre utaló – jelenségekkel:

- A víruskereső program névvel azonosított vírust jelez.
- Fájl másolása esetén az újonnan keletkezett és az eredeti példány hossza eltérő.
- Szokatlan és váratlan képernyő-tevékenység (szokatlan üzenetek, ablakok megjelenése).
- Szokatlan számítógép- vagy programviselkedés (pl. programok maguktól elindulnak).
- A rendszer működése többszöri újraindítás után is egyértelműen lassabb a megszokottnál.

8.2.4 Vírusvédelmi teendők

Az alábbi utasítások betartása erősen ajánlott a vírusfertőzések megelőzése, illetve azok kockázatának csökkentése érdekében:

- Vírusvédelmi szoftverrel biztosítani kell a szerverek, a munkaállomások vírusvédelmét. Ehhez a könyvtár a Panda Endpoint Security Plus és a Panda Adaptive Defense 360 vírusvédelmi szoftvert alkalmazza, amely a webszűrést is ellátja.
- A vírusvédelmi programnak rezidens módban kell futnia, így az minden egyes rendszerindításkor aktivizálódik és állandó háttérvédelmet biztosít. A felhasználóknak nem szabad kikapcsolni ezt a védelmet.
- Ne fusson egyszerre két vírusölő program.
- Havonta minden gépen teljes vírusellenőrzést kell végrehajtani (a vírusvédelmi szoftver támogatja az időzített keresési funkciót).
- A vírusvédelmi program vírusdefiníciós adatbázisát a lehető leggyakrabban frissíteni kell. Ha erre lehetőség van, az automatikus frissítést kell választani, így az új elemek rögtön megjelenésük után felkerülhetnek a rendszerre.
- Soha nem szabad ismeretlen vagy gyanús helyről fájlokat letölteni.
- Ismeretlen, megbízhatatlan forrásból származó furcsa, gyakran vicces e-mailek csatolt fájljait nem szabad megnyitni, azonnal törölni kell őket. Az e-mailben küldött vírusok, férgek rendszeresen operálnak valamilyen különös megjegyzéssel a levél tárgya mezőben.

8.2.5 Teendők vírusfertőzés esetén

- Tájékoztatni kell a rendszergazdát a fertőzésről vagy annak gyanújáról.
- A számítógépet újra kell indítani egy előkészített, vírusmentes, a használt operációs rendszert és a vírusvédelmi program legfrissebb változatát tartalmazó lemezről. Ha ez nem lehetséges, akkor védett módban kell újraindítani a gépet csak a legszükségesebb szolgáltatásokkal (lehetőleg hálózati kapcsolat nélkül).
- A vírusvédelmi szoftvert elindítjuk, és megszüntetjük a vírusfertőzést. Ez történhet elsődlegesen a fertőzött állomány javításával (a vírus eltávolítása), ha erre lehetőség van, egyébként a fertőzött állomány törlésével. Ez utóbbi esetben ügyelni kell arra, hogy nem rendszerállományról van-e szó.
- A víruskeresést addig kell végezni, amíg el nem éri a rendszerfelelős, hogy a víruskereső program úgy fusson végig az összes állományon, hogy fertőzött állományt már nem talál.

8.3. *Levelezési szabályzat*

8.3.1 Bevezetés

A szabályzat célja, hogy biztosítsa az elektronikus levelezés zavartalanságát. Minden könyvtári alkalmazottnak kötelező <felhasznalonev>@vmk.hu formájú postafiókot igényelni. A könyvtár nem monitorozza a hálózatából küldött, illetve ide érkező levelek tartalmát.

A Könyvtár hálózatán átmenő leveleken központilag vírusellenőrzés történik, ami különböző védelmi és szűrési funkciókkal egészül ki.

A megnövekedett SPAM-ek (levélszemetek) miatt a Könyvtár kétlépcsős biztonsági rendszert vezetett be. Első lépcsőben egy spamszűrő szerverre érkeznek be a levelek (spamzabalo.hu), ahol a beérkezett levelek szűrése után érkeznek a könyvtár levelezőszerverére. Ott a Panda levélszemétszűréje is átvizsgálja a leveleket, amik ezután érkeznek meg a postaládákba. Ezek a folyamatok időbeni kiesést nem okoznak a levélforgalomban.

8.3.2 A szabályzat hatálya

A szabályzat érvényes minden levélre, amit a vmk.hu tartományba eső e-mailcímről küldtek.

8.3.3 Alapelvek

- A levelek nem képviselhetnek a hatályos magyar jogszabályokba ütköző magatartásformát.
- A levelek tartalma nem sérthet meg szerzői és kapcsolódó jogokat.
- A levelezés nem veszélyeztetheti a hálózati infrastruktúra működését.

8.3.4 Szabályok

- Tilos kéretlen leveleket, hirdetéseket küldeni.
- Tilos a levélbombák, levelezési láncok küldése, illetve továbbküldése.
- Tilos a levelezési címet olyan kereskedelmi listára feltenni, amelyről a könyvtári levelező rendszert e-mail szeméttel (SPAM) terhelhetik meg.
- A könyvtár hálózatán maximum 20 Mb méretű levelek küldhetők, ez a korlát az egyes helyi (igazgatóság, titkárság) szerverek levelező rendszerei esetében pozitív irányban módosulhat.
- A felhasználó postafiókja maximum 2 GB. Indokolt esetben ennek mérete eltérhet, megváltoztatásához igazgatói engedély szükséges. A felhasználó köteles gondoskodni arról, hogy ezt a korlátot ne lépje túl (régi, nem fontos, nagyméretű levelek törlése, törölt levelek végleges eltávolítása, elküldött levelek törlése).

9. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

9.1. *A gépterem (szerverszoba) védelme*

Elemi csapás (vagy egyéb ok) esetén a gépteremben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- a még használható anyag mentése,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- új adatfeldolgozás, helyiségek kialakítása,
- archivált anyagok (ill. eszközök) használatával feldolgozás folytatása.

9.2. *Hardvervédelem*

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 hardvertesztek által feltárt hibákat.

Alapgép szétbontását (kivéve a garanciális gépeket) csak a rendszergazda végezheti el.

9.3. *Az informatikai feldolgozás folyamatának védelme*

9.3.1. Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- tesztelt adathordozóra lehet adatállományt rögzíteni,
- hozzáférési lehetőség
    - o a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (Alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek dolgozói férjenek hozzá).
    - o az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
    - o a mappák hozzáférési jogosultságairól a rendszergazda nyilvántartást vezet.

9.3.2. Adathordozók védelme

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

Az informatikai eszközök üzemeltetéséért a rendszergazdák felelnek.

9.3.3 Selejtezés, sokszorosítás, másolás

Selejtezés menete

- A rendszergazda köteles meggyőződni arról, hogy az adathordozó fizikailag sérült, javíthatatlan, a tárolt adatok, szoftverek elavultak, további megőrzésük szükségtelen.
- Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adathordozókról, törlő programokkal kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.
- Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni.
- Gondoskodni kell veszélyes hulladékként való elszállításukról.

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

9.4. *Szoftvervédelem*

9.4.1. Rendszerszoftver védelem

Az üzemeltetésért felelős vezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

Teendők a következők:

- a rendszerszoftverben módosításokat a rendszergazdák végezhetnek,
- a módosítással egy időben, a dokumentációban is át kell vezetni a változásokat.

9.4.2. Felhasználói programok védelme

- 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.
- A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a programdokumentációt.

10. A központi számítógépek és a hálózat munkaállomásainak működésbiztonsága

10.1. *Központi gépek (Szerver)*

- Szünetmentes áramforrást kötelező használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.

10.2. *Munkaállomások (felhasználók)*

- A hálózatra idegen programot, adatot másolni csak a rendszergazdákkal történt egyeztetés után lehet.
- Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
- Vírusfertőzés gyanúja esetén a rendszergazdákat azonnal értesíteni kell.
- 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 rendszergazdák tudta és engedélye nélkül nem szabad.

11. Internet-hozzáféréssel kapcsolatos intézkedések

- Az internetes gépen minden esetben működtetni kell a vírusvédelmet.
- A vírusok és az illetéktelen hozzáférések miatt tűzfalat kell konfigurálni.

12. Mentési és archiválási feladatok

12.1. *Általános rendelkezések*

- A mentési és visszaállítási eljárásokat úgy kell kialakítani, hogy a könyvtár által üzemeltetett rendszerek előre nem látható esemény bekövetkezte után szükség esetén helyreállíthatók legyenek, ezáltal ne sérüljenek az információk, adatok, rendszerek rendelkezésre állásának kritériumai.
- Az adatmentésnek és archiválásnak mindig a lehető legfrissebbnek kell lennie.
- Egy rendszerösszeomlásnál annyi adatot fogunk elveszíteni, amennyi a legutóbbi mentés óta keletkezett. A mentés gyakoriságát ennek megfelelően kell meghatározni.
- A mentett adatoknak mindig visszaolvashatónak kell lennie. Célszerű időnként próba visszatöltést tartani.
- A mentéseket mindig biztos helyen kell tárolni.
- A biztonsági mentés nem ér semmit, ha csőtörés, tűz vagy lopás során az eredeti rendszerrel együtt megsemmisül! Tartsuk más helyiségben, vagy távoli helyen (Budai úti Tagkönyvtár).
- Ne keverjük össze a rendelkezésre állást a biztonsági mentéssel. Az olyan megoldások, mint pl. a lemezegységek tükrözése, RAID alrendszerek, stb. növelik a rendelkezésre állás nagyságát és az adatbiztonságot, mert pl. egy lemezegység meghibásodása esetén is működőképes marad a rendszer, de nem helyettesítik a biztonsági mentést. Egy teljes RAID lemezegység is teljesen tönkre tud menni, pl. tűz, villámcsapás stb. esetén, ekkor a rajta tárolt adatok elvesznek, vagyis mentésre ekkor is szükség van!
- Az adattárolásra szolgáló adathordozók meg kell, hogy feleljenek az adatok, információk biztonsági osztályba sorolási modellben meghatározott időn belüli működőképesség követelményeinek.

12.2. *Üzemeltetői feladatok*

- Teljes biztonsági mentést és archiválást kell végezni a munkaállomásokon és szervereken található elektronikus adatokról.
- Félévente, évente teljes rendszerarchiválást kell készíteni, és ezeket megőrizni. Ehhez biztosítani kell a megfelelő számú adathordozó egységet.
- A mentéseket lehetőleg úgy kell elvégezni, hogy azzal a felhasználók munkáját ne akadályozzák.
- Legalább évente visszatöltési kísérletet kell végezni a technika megfelelőségének ellenőrzése érdekében.

- A rendszergazda feladata ellenőrizni, hogy a meghatározott mentési rend alapján az adatminősítésnek megfelelően a visszaállítási eljárások során is csak az arra jogosult személyek férhessenek hozzá a visszaállítandó adatokhoz

12.3. *Szerver és munkaállomások adatainak mentése*

- Minden felhasználó a bejelentkezés után kapcsolódik a szerverhez. A megosztott mappák közül mindenki csak a jogokat kapott könyvtárakra tud belépni. A jogosultságokról a rendszergazda nyilvántartást vezet.
- Minden felhasználó rendelkezik a szerveren egy saját mappával, ami a munkavégzéshez biztosított. Itt csak a könyvtári dokumentumokat tárolhatja. Minden más, a munkavégzéshez nem szükséges dokumentumokat a számítógépén levő mappában tárolhatja.
- A megosztott mappák közül csak a könyvtár működéséhez szükséges könyvtárak kerülnek mentésre.
- A felhasználó feladata saját dokumentumairól biztonsági mentést végezni.
- A felhasználó felelős a saját munkaállomásán bekövetkezett adatvesztésekért és az adatok sérüléséből keletkezett károkért.
- A rendszergazda felelős azért, hogy
    - a mentésből visszaállíthatók legyenek az adatok,
    - a mentések mindig a leírt módon és időben történjenek. (lásd xx melléklet a biztonsági mentésekről)

13. Könyvár Honlapja

A könyvtár weboldalának tartalma, adatai a Neosoft Kft. szerverén van tárolva. Ezek védelméről, biztonsági mentéséről az üzemeltető gondoskodik a saját szabályzata szerint.

14. Könyvtárellátási Szolgáltató Rendszer (KSZR)

A könyvtár rendszergazdája látja el az alábbi feladatokat azon településeken, ahol nem látnak el rendszerfelügyeletet

- a KSZR-hez csatlakozott településeknek könyvtári szolgáltatásokhoz szükséges informatikai eszközök, szoftverek beszerzése,
- azok karbantartása, felügyelete,
- a felhasználók által jelzett hibák kijavítása,

- a rendszergazda távfelügyelettel (Teamviewer) bármikor ellenőrizheti a gépek állapotát, szoftverek jogtisztaságát,
- a számítógépeket a Panda Endpoint Protection Plus telepített szoftverrel adja át, ami gondoskodik a vírus és kiskorúak védelméről.
- A Könyvtár a vele együttműködő KSZR települések könyvtárosainak hivatali e-mail címet biztosít <felhasználónév>@fejerkeszr.hu domain névvel.

Felhasználó kötelességei

- A számítógépekre idegen programot telepíteni csak a rendszergazdákkal történt egyeztetés után lehet.
- Csak jogtiszta programokat lehet telepíteni, illegális szoftvereket szigorúan tilos.
- Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
- Vírusfertőzés gyanúja esetén a rendszergazdákat azonnal értesíteni kell.
- A felhasználó feladata saját dokumentumairól biztonsági mentést végezni.
- A felhasználó felelős a saját munkaállomásán bekövetkezett adatvesztésekért és az adatok sérüléséből keletkezett károkért.

ZÁRADÉK

Jelen szabályzat 2018. augusztus 1-jétől lép hatályba, ezzel egyidejűleg a 2015.08.01-jén kelt szabályzat hatályát veszti.

VÖRÖSMARTY MIHÁLY KÖNYVTÁR * SZÉKESFEHÉRVÁR * 1.

Székesfehérvár, 2018. augusztus 1.

Vasné Borsos Beáta Bíborka
igazgató

1. számú melléklet

SZÁMÍTÓGÉP-HASZNÁLATI SZABÁLYZAT KÖNYVTÁRHASZNÁLÓK SZÁMÁRA

VÖRÖSMARTY MIHÁLY KÖNYVTÁR

A Vörösmarty Mihály Könyvtárban **összesen 41 db számítógép áll a látogatók rendelkezésére**. A Központi Könyvtárban 22 db, a Pedagógiai Szakkönyvtárban: 2db, a Budai úti Tagkönyvtárban 4db; a Széna téri Tagkönyvtárban 5db; a Tolnai utcai Tagkönyvtárban 2db; a Mészöly Géza utcai Tagkönyvtárban 3db; a Zsolt utcai Tagkönyvtárban 3db számítógépet biztosítunk Olvasóinknak.

1. A használat lehetőségei a Központi Könyvtárban

A számítógépeket beiratkozott (kölcsönzési joggal rendelkező) vagy regisztrált olvasóink használhatják.

A számítógép használat díja: **minden megkezdett félóra 100,- Ft.** Kölcsönzési joggal rendelkező olvasóink **naponta 60 percig ingyen** használhatják gépeinket. A kedvezmény a kölcsönzési joggal nem rendelkező olvasóinkra nem vonatkozik!

Az olvasójegyet a használat idejére le kell adni az adminisztrációt végző könyvtárosnak, aki a használat kezdetét és befejezését regisztrálja.

A számítógéphasználat után minden adat, Internet böngészési előzmény, letöltött anyag törlődik.

Adatbázisok és WiFi ingyenes használatára minden részlegben lehetőséget biztosítunk.

A **Zenei és számítógépes részlegben** az alábbi **számítógépes szolgáltatások** vehetők igénybe:

- Internethasználat,
- Windows Office irodai programcsomag,
- szkennelés,
- nyomtatás.

A részleg **NAVA-pont**ként működik.

2. A használat lehetőségei a Pedagógiai Szakkönyvtárban és a Tagkönyvtárakban

A számítógépeket beiratkozott (kölcsönzési joggal rendelkező) vagy regisztrált olvasóink használhatják.

A számítógép használat díja: **minden megkezdett félóra 100,- Ft.** Kölcsönzési joggal rendelkező olvasóink **naponta 30 percig ingyen** használhatják a gépeket. A kedvezmény a kölcsönzési joggal nem rendelkező olvasóinkra nem vonatkozik!

Az olvasójegyet a használat idejére le kell adni az adminisztrációt végző könyvtárosnak, aki a használat kezdetét és befejezését regisztrálja.

A számítógéphasználat után minden adat, Internet böngészési előzmény, letöltött anyag törlődik.

Adatbázisok ingyenes használatára a szakkönyvtárban és minden tagkönyvtárban lehetőséget biztosítunk.

A szakkönyvtárban és a tagkönyvtárakban az alábbi **számítógépes szolgáltatások** vehetők igénybe:

- Internethasználat,
- MS Office irodai programcsomag,
- Szkennelés,
- Nyomtatás.

NAVA-pontként működik a Budai úti Tagkönyvtár, a Széna téri Tagkönyvtár és a Zsolt utcai Tagkönyvtár.

3. A számítógép-használat a könyvtár minden területén érvényes szabályai

A számítógép-használat **elsősorban önálló használatot jelent**, de szükség esetén a könyvtáros segítségét lehet kérni.

A számítógépet használók tevékenységükkel, **viselkedésükkel nem zavarhatják a könyvtár használóit és a könyvtárban folyó munkát.**

A számítógép hardver és szoftver beállításai nem módosíthatók.
A felhasználó nem telepíthet letöltött vagy hozott számítógépes programokat.

A szükséges anyagok saját tároló eszközre letölthetők. Saját anyagok megőrzését nem vállaljuk.

Saját eszközöket a számítógépből kivezetett USB porton keresztül csatlakoztathat.

A hálózat használata során **tilosak az érvényes magyar törvényekbe ütköző cselekmények, ideértve a következőket**, de nem korlátozva ezekre:

- a számítógépek beállításainak megváltoztatása,
- mások személyiségi jogainak megsértése,
- másokra nézve sértő, mások vallási, etnikai, politikai vagy más jellegű érzékenységét sértő, másokat zaklató tevékenység, (pl. pornográf anyagok használata, közzététele; kéretlen levelek),
- fájlmegosztók használata, mp3, filmek, jogvédett anyagok letöltése,
- software szándékos és tudatos illegális terjesztése,
- profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése,
- a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, módosítása, megrongálása, megsemmisítésére irányuló tevékenység,
- a hálózat biztonságos működését zavaró vagy veszélyeztető információk, programok terjesztése (pl. vírusok).

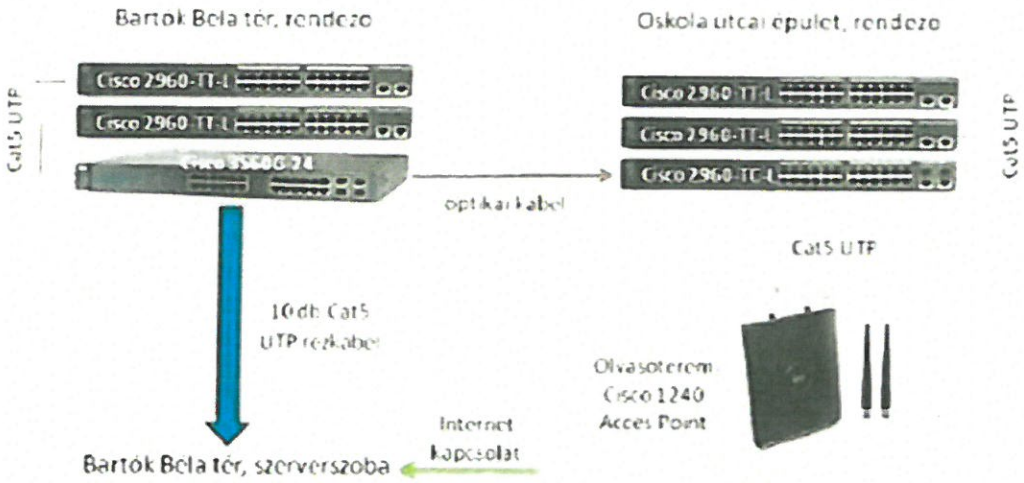
A Vörösmarty Mihály Könyvtár, mint üzemeltető fenntartja magának a jogot, hogy amennyiben kétség merül fel a dokumentum szabad terjesztésének lehetőségét illetően, akkor annak használatát megtiltja. **Könyvtárunk az illegálisan letöltött tartalmakért felelősséget nem vállal.**

A könyvtárnak okozott károkból eredő költség a könyvtárhasználót terheli.

2. számú melléklet

A BELSŐ HÁLÓZAT LEÍRÁSA

1. Központi Könyvtár



A központi két épület rendezőszekrényébe bekerült eszközök

Bartók Béla tér, Igazgatóság		
Eszköz	Gyári szám	IP cím
Cisco Catalyst 2960/2* 1000BT	FOC1342X49S	192.168.1.93
Cisco Catalyst 2960/2* 1000BT	FOC1429Y6H7	192.168.1.92
Cisco Catalyst 3560	FOC1408Z4Y7	192.168.1.91
Oskola utca		
Cisco Catalyst 2960/2* 1000BT	FOC1351Z6A6	192.168.1.96
Cisco Catalyst2960/2* 1000BT	FOC1351YSP7	192.168.1.95
Cisco Catalyst 2960 2T SFP	FOC1424X4U6	192.168.1.94

Wifi		
Eszköz	Gyári szám	IP cím
Olvasóterem	FCZ144582WJ	192.168.1.29
Gyermekrészleg		192.168.1.2
Zenei és Számítógépes részleg		192.168.1.3
Felnőtt Kölcsönző		192.168.1.4

Bartók Béla tér szerverszoba		
Szerverek		
Eszköz	Gyári szám	IP cím
Windows 2016 szerver		192.168.1.14
Exchange 2016 szerver		192.168.1.15 192.168.1.16
Portal szerver		192.168.1.17
Textlib szerver		192.168.1.11
VPN szerver		192.168.1.10
NAS Backup Helyismeret		192.168.1.42
NAS Backup Titkárság		192.168.1.40
NAS Backup Központi Szerver		192.168.1.41
Router		
Mikrotik RB450G		192.168.1.1

IP cím tartomány

192.168.1.0/24	Központ

Hálózati eszköz publikus IP címe

78.131.58.101	Központ

2. Pedagógiai Szakkönyvtár

IP cím tartomány

192.168.1.0/24	Pedagógia

Hálózati eszköz publikus IP címe

78.131.56.195	Pedagógia

3. Állományalakító és feldolgozó csoport valamint tagkönyvtárak

A szervezeti egységek **saját internet kapcsolattal rendelkezik, ezen keresztül kapcsolódnak a Könyvtár szerveréhez Open VPN segítségével.**

A feldolgozó csoport és a tagkönyvtárak **belső hálózatai a 192.168.X.0/24 C osztályú IP cím tartományokat használják** úgy, hogy ne legyen az egyes fiókok között sem ütközés.

A **hálózati kliensek DHCP segítségével kapnak IP címet**, ezeken a helyeken az IPv6 nem elérhető.

IP cím tartományok

192.168.2.0/24	Budai
192.168.3.0/24	Széna
192.168.5.0/24	Tolnai
192.168.6.0/24	Mészöly
192.168.7.0/24	Zsolt
192.168.9.0/24	Feldolgozó

Hálózati eszközök belső IP címei

192.168.2.1	Budai router
192.168.2.2	Budai HP szerver
192.168.3.1	Széna router
192.168.5.1	Tolnai router
192.168.6.1	Mészöly router
192.168.7.1	Zsolt router
192.168.9.1	Feldolgozó router

Hálózati eszközök publikus IP címei

78.131.58.98	Budai router
78.131.56.128	Mészöly router
78.131.58.99	Széna router
78.131.58.209	Tolnai router
100.73.154.241	Feldolgozó router
212.40.112.4	Zsolt router