KERTÉSZ LÁSZLÓ
VÁROSI KÖNYVTÁR

A Kertész László Városi Könyvtár

INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Készítette: Síki Szilárd rendszergazda

Jóváhagyta: Bakó Ildikó könyvtárigazgató

Dátum: 2024. 09. 10.

Tartalomjegyzék

1. Az Informatikai Biztonsági Szabályzat célja

A Kertész László Városi Könyvtár 4220 Hajdúböszörmény, Bocskai István tér 2. ***Informatikai Biztonsági Szabályzatának (továbbiakban: IBSZ)*** alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, mentését karbantartását és hogy megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az IBSZ célja továbbá:

- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- 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 üzembehelyezésen keresztül az üzemeltetésig.

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

Meghatározó rendelkezések:

Európai Parlament és Tanács 2016/679. számú általános adatvédelmi rendelete (GDPR), az információs önrendelkezési jogról és az információszabadságról szóló a 2011. évi CXIL törvény (Info tv.), a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVL 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

2. Az Informatikai Biztonsági Szabályzat hatálya

2.1. Személyi hatálya

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

2.2. Tárgyi hatálya

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

3. Az adatkezelés során használt fontosabb fogalmak

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, 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, aki vagy amely az adatkezelő megbízásából 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

Az intézmény adatai különböző biztonsági fokozatba tartozhatnak. (üzleti titkok, pénzügyi adatok, illetve a vállalkozás belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas adatok.

5. Kapcsolódó szabályozások

- Szervezeti és Működési Szabályzat,
- Leltározási és Leltárkészítési Szabályzat,
- Állományellenőrzési Szabályzat,
- Könyvtárhasználati szabályzat,
- Adatkezelési 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.

6.1. A védelem tárgya

A védelmi intézkedések kiterjednek:

- 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 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, reprodukálhatóságát.

6.2. 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. A védelem felelőse és feladatai

A védelem felelőse az intézmény informatikai szakembere. A jelen szabályzatban foglaltak szakszerű végrehajtásáról az **intézményvezetőnek** kell gondoskodnia. A rendszergazda az intézmény vezetőjének van közvetlenül alárendelve.

7.1 A rendszergazda:

- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására.
- meghatározza a védett adatok körét,
- ellátja az adatkezelés és adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- az adatvédelmi feladatok ismertetése,
- ellenőri tevékenységét adminisztrálja.
- ellenőrzi a szoftverek használatának jogszerűség ét
- a saját feladatkörébe tartozó rendszert felügyeli,
- felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének folyamatos ellenőrzése,
- felelős az intézmény informatikai rendszer hardver eszközeinek karbantartásáért,
- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- gondoskodik a folyamatos vírusvédelemről
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer adminisztrációját,

7.2. A rendszergazda ellenőri feladatai

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

7.3. A rendszergazda jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet az intézmény vezetőjénél,
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,
- betekinthet valamennyi iratba, ami az informatikai feldolgozásokkal kapcsolatos,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

8. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére a vezető és a rendszergazda oktatás formájában biztosítják. Erről nyilvántartást kötelesek vezetni.

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

8.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában - valamint az intézménynél - történt változások miatt időközönként aktualizálni kell. Az IBSZ folyamatos karbantartása a rendszergazda feladata.

8.2. 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.

Az 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).

9. 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.

9.1. 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, feszültségingadozás, elektromos zárlat, csőtörés.

9.2. 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,
- 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.

10. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

10.1. A működés és fejlesztés során előforduló veszélyforrások

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

11. Az informatikai eszközök környezetének védelme

11.1 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.

11.2 Vírusvédelem

11.2.1. 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.

11.2.2. A szabályzat hatálya

Minden a könyvtár hálózatába kötött személyi számítógépre, laptopra és szerverre/szerverekre vonatkozik.

11.2.3. 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.

11.2.4. 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 az intézmény 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.

11.2.5. 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.

11.3. 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 másnak átadni csak engedéllyel szabad, a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

11.4. Tűzvédelem

A gépterem illetve kiszolgáló helyiség a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent. A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell. Az intézmény géptermeibe, szerverszobáiba minimum 1-1 db tűzoltó készüléket kell elhelyezni. Az intézmény géptermeiben, szerverszobáiban elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.

12. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

12.1. A számítógépek és szerverek védelme

Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

12.2. Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell. A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése. Az üzemeltetést, karbantartást és szervizelést az informatikus végzi. A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlatait,
- a tapasztalatokat.

Alapgép megbontását (kivéve a garanciális gépeket) csak informatikus végezheti el.

Az elektronikusan tárolt adatok folyamatosan ki vannak téve a hardver meghibásodásának lehetőségének, ezért a biztonság növelése és a károk csökkentése érdekében szükség van rendszeres mentésekre. Míg a mentések fő feladata a biztonsághoz kapcsolódik, addig az archiválás egy korábbi állapot eltárolását szolgálja. Ez utóbbinak biztonsági incidensek bekövetkezése esetén lehet fontos szerepe, a napló és log fájlokban, valamint egyéb adatok között értékes információkat, nyomokat lehet találni a biztonsági esemény bekövetkezésével kapcsolatban.

12.3. Az informatikai feldolgozás folyamatának védelme

12.3.1. Az adatrögzítés védelme

Az adatbevitel hibátlan műszaki állapotú berendezésen történjen. Tesztelt adathordozóra lehet adatállományt rögzíteni. A bizonylatokat, adminisztrációs dokumentumokat és adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani.

Az adatrögzítő szoftver védelme: Lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített rekordok visszakeresésének és javításának lehetőségét is.

Hozzáférési lehetőség: a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz a Huntéka integrált könyvtári rendszerben és a NAS szerveren. Alapelv: a tárolt adatokhoz csak az illetékes személyek férjenek hozzá. A szerverek rendszergazda jelszavát a rendszergazda kezeli.

12.3.2. Az adathordozók nyilvántartása

Az adathordozókról az egységeknek nyilvántartást kell vezetni. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval (sorszámmal) kell ellátni.

12.3.3. Adathordozók tárolása

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

12.3.5. Az adathordozók megőrzése

Az adathordozók megőrzési idejét az intézmény adatvédelmi szabályzatában meghatározott őrzési kötelezettségnek megfelelően kell kialakítani.

12.3.6. Selejtezés, másolás

A selejtezést az intézmény selejtezésének szabályzata alapján kell lefolytatni. Biztonsági illetve archív adatállomány előállítása másolásnak számít.

12.3.8. Leltározás

A szoftvereket és adathordozókat a Leltározási és Leltárkészítési Szabályzatban foglaltaknak megfelelően kell leltározni.

12.3.9. Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését.

A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata.

A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban a rendszergazda segítséget nyújt.

A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért a rendszergazda a felelős negyedévente egyszer.

A mentési és visszaállítási eljárásokat úgy kell kialakítani, hogy a Kertész László Városi Könyvtár által üzemeltetett rendszerek előre nem látható esemény bekövetkezte után szükség esetén helyreállíthatók legyenek, ezáltal ne sérüljenek az információk, adatok, rendszerek rendelkezésre állásának kritériumai.

A mentéseket mindig biztos helyen kell tárolni. A biztonsági mentés nem ér semmit, ha csőtörés, tűz vagy lopás során az eredeti rendszerrel együtt megsemmisül!

12.4. Szoftver védelem

12.4.1. Rendszerszoftver védelem

A rendszergazdának biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

12.4.2. Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni. A felhasználói gépek jelszavakkal védettek. Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

Programok megőrzése, nyilvántartása

A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni.

12.4.3. Kiskorúak védelme

Az intézmény a kiskorúak által is használható, internethozzáféréssel rendelkező számítógépek használatát a kiskorúak védelmét lehetővé tevő, könnyen telepíthető, magyar nyelvű szoftverrel biztosítja a kiskorúak lelki, testi és értelmi fejlődésének védelmét.

13. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

13.1. Központi gépek

Szünetmentes áramforrást használva, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől. A központi gépek háttértárairól folyamatosan biztonsági mentést kell készíteni.

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

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!

Ezt a funkciót könyvtárunkban a NAS szerver védi, melyben kialakított a RAID MIRROR, mely két HDD segítségével tükrözi az adatokat. Évente ezeket be kell vizsgálnunk.

13.2. Munkaállomások

Az Intézmény által a munkavállaló részére munkavégzés céljára rendelkezésre bocsátott számítógépet, laptopot és a hozzá tartozó eszközöket, perifériákat a munkavállaló kizárólag munkaköri feladata ellátására használhatja.

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.

Vírusfertőzés gyanúja esetén a rendszergazdát azonnal értesíteni kell.

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 csak az eszköz leltárfelelőse tudtával és engedélyével szabad.

14. Ellenőrzés

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

A munkafolyamatba épített ellenőrzés során az IBSZ rendelkezéseinek betartását a rendszergazda és a könyvtárvezető folyamatosan ellenőrzik.

15. Záró rendelkezések

Az IBSZ a Kertész László Városi Könyvtár Adatvédelmi Szabályzatában lefektetett elvek, eljárások és biztonsági szabályok figyelembe vételével érvényes, amelyek betartásáért az intézmény minden munkatársa felelős.

Az Informatikai Biztonsági Szabályzat 2024.. év 10 hó 01 nap lép hatályba.

.....

informatikus/rendszergazda

Kertész László Városi Könyvtár Hajdúböszörmény

.....

könyvtárigazgató