Arany János Közösségi Ház és Városi Könyvtár
2360 Gyál, Kőrösi út 118-120. www.gyalikozhaz.hu

Arany János Közösségi Ház és Városi Könyvtár
INFORMATIKA BIZTONSÁGI SZABÁLYZAT

Hatályos:
2019. április 10 napjától,
kiegészítve:
2020. augusztus 17.

Jóváhagyta:

B

Bretus Imre
igazgató

Bevzetés

Jogszabályi környezet

1. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
2. 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról
3. 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről
4. 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről
5. Az Intézmény a GDPR keretszabályokat külön szabályozza.

1. Az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) célja

Az Arany János Közösségi Ház és Városi Könyvtár(továbbiakban: Intézmény) részére az elektronikus információbiztonsággal kapcsolatos elveket, szabályokat, az elvárt és betartandó magatartásformákat és gyakorlatokat az alábbi szabályzat szerint határozza meg.

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

Az IBSZ célja továbbá:

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

2. Az IBSZ hatálya

Személyi hatálya

Az IBSZ személyi hatálya kiterjed az Intézmény alkalmazottaira, függetlenül attól, hogy alkalmazására milyen jogviszonyban kerül sor.

- Tárgyi hatálya
- kiterjed a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed az Intézmény tulajdonában lévő, illetve az általa használt 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.

Az adatkezelés során használt fontosabb fogalmak

Az Intézmény a GDPR keretszabályokat külön szabályozza.

Adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen az adatok 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 rögzítése;

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;

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, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - 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.

Az IBSZ biztonsági fokozata

Az Intézmény adatai különböző biztonsági fokozatba tartozhatnak. Annak érdekében, hogy az a törvény hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából.

A biztonsági osztályba sorolás alkalmával - az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján - 1-től 5-ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt.

Kapcsolódó szabályozások

Az IBSZ előírásai összhangban vannak:

- Eszközök és források leltározási és leltárkészítési szabályzatával,
- Számviteli politikával
- Adatvédelmi szabályzattal
- A közérdekű adatok megismerésének és a kötelezően közzéteendő adatok nyilvánosságra hozatalának szabályzatával

- 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:

- 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, logikaiegységére, előírásszerű felhasználására, reprodukálhatóságára

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.

A védelem felelőse

A védelem felelőse a mindenkori rendszergazda.

A jelen szabályzatban foglaltak szakszerű végrehajtásáról az intézményvezetőnek kell gondoskodnia.

Adatvédelmi felelős feladatai

- az IBSZ kezelése,
- ellátja az adatkezelés és adatfeldolgozás elvárható felügyeletét,
- ellátja a védelmi előírások betartását,
- az adatvédelmi feladatok ismertetése,
- ellenőrzi a szoftverek használatának jogszerűségét
- a rendszergazda 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,
- 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

Az IBSZ alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére az igazgató és a rendszergazda oktatás formájában biztosítják.

Az IBSZ karbantartása

Az IBSZ-t az informatikában - valamint az Intézménynél - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. Az IBSZ folyamatos karbantartása a rendszergazda feladata.

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,
- megkeresésre kiadható közérdekű adatok
- belső ügyintézéshez szükséges dolgozói adatok
- az Intézmény gazdálkodására vonatkozó adatok, dolgozói szenzitív adatok
- minősített, titkos adatok.

Az informatikai feldolgozás során keletkező adatok minősítője az igazgató

Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot. A kijelölt dolgozók előtt az adatvédelmi 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. 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 biztosítani kell (szoftver, hardver adatvédelem). Ennek biztosítása a rendszergazda feladata.

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.

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

Az informatikai eszközöket csak közalkalmazott munkavállalók használhatják.

Az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

Tűzvédelem

Az Intézmény Tűzvédelmi Szabályzata szerint.

Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

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.

Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell. A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése. Az üzemeltetést, karbantartást és szervizelést a rendszergazda végzi. A munkák szervezésénél figyelembe kell venni: a gyártó előírásait, ajánlatait, a tapasztalatokat. Alapgép megbontását (kivéve a garanciális gépeket) csak a rendszergazda végezheti el.

Az informatikai feldolgozás folyamatának védelme

Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- tesztelt adathordozóra lehet adatállományt rögzíteni,
- a bizonylatokat és mágneses 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 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 személyek férjenek hozzá).
- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
- Az adatrögzítés folyamatához kapcsolódó dokumentációk: adatrögzítési utasítások, ellenőrző rögzítési utasítások, tesztelő és törő programok kezelési utasításai, megőrzési utasítások, gépkezelési leírások.

Adattárolók tárolása

Az adattárolók tárolására műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget lehet csak használni (pl.: szerverszoba, Intézményi széf).

Az adattárolók megőrzése

Az adattárolók megőrzési idejét a törvényekben meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani.

Selejtezés, sokszorosítás, másolás

A selejtezést az Intézmény Felesleges vagyontárgyak hasznosításának szabályzata alapján kell lefolytatni. Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni. Biztonsági illetve archív adatállomány előállítása másolásnak számít.

Leltározás

A szoftvereket, adattárolókat és adathordozókat az Eszközök és források leltározási és leltárkészítési szabályzatban foglaltaknak megfelelóen kell leltározni.

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 munkavégzés során készített valamennyi állományt a szerveren a felhasználó nevére létrehozott mappába kell menteni. Kizárólag a munkavégzésre használt gép merevlemezén adatokat tárolni tilos. A gépen lévő valamennyi adatnak a szerveren is elérhetőnek kell lennie. A felhasználó által létrehozott adatok szerverre történő mentéséért az adatot létrehozó felhasználó a felelős. A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért a rendszergazda a felelős.

Szoftver védelem

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

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, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

Eljárásrend informatikai támadás esetén

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) hatálya nem terjed ki a helyi önkormányzatok által fenntartott költségvetési szervekre, az Intézmény ennek ellenére van IBSZ-e. Mivel az Ibtv. rendelkezési nem vonatkoznak az Intézményre így informatikai incidens esetén az „eseménykezelő központ" felé sem szükséges bejelentést tenni, azonban az incidens dokumentálása kötelező. Személyes adatokat nem érintő informatikai incidens esetén az Infotv. 25/J. § alapján *Az adatvédelmi incidenst nem kell bejelenteni, ha valószínűsíthető, hogy az nem jár kockázattal az érintettek jogainak érvényesülésére."* Az azonnali támadás elhárítását követően IT biztonsági Incidens Jegyzőkönyv felvétele haladéktalanul, legkésőbb a támadást követő 72órán belül kötelező. Az incidens esetén legkésőbb a támadást követő 72 órán belül kötelező.az Intézményfenntartót is értesíteni. A jegyzőkönyveknek tartalmaznia kell az incidens kezelése, kivizsgálása, fenntartó értesítése pontokat. Személyes adatokat is érintő támadás esetén a hatályos jogszabályok alapján kell eljárni, miszerint *25/J. § (1) Az adatkezelő az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt adatokkal összefüggésben felmerült adatvédelmi incidens kapcsán rögzíti az (5) bekezdés a), c) és d) pontja szerinti adatokat, valamint az adatvédelmi incidenst haladéktalanul, de legfeljebb az adatvédelmi incidensről való tudomásszerzését követő hetvenkét órán belül bejelenti a Hatóságnak*. A bejelentést az Intézményvezető, akadályoztatása esetén az Intézményvezető-helyettes köteles megtenni. Továbbá az Intézményvezető, akadályoztatása esetén az Intézményvezető-helyettes a

Btk. 423-424. § értelmében az elektronikus információs rendszerrel való visszaélés bűncselekmény kapcsán köteles 72 órán belül feljelentést tenni.

Programok megőrzése, nyilvántartása

A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni. A számvitelről szóló többször módosított 2000. évi C. törvény értelmében az Intézménynek az üzleti évről készített beszámolót, valamint az azt alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá más, a számviteli törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 10 évig meg kell őrizni.
A bizonylat elektronikus formában is megőrizhető, ha az alkalmazott módszer biztosítja az eredeti bizonylat összes adatának késedelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az utólagos módosítás lehetőségét.
A programok nyilvántartásáért Katona Krisztina a felelős.

A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

Szünetmentes áramforrást célszerű használni, 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.
A vásárolt szoftverekről biztonsági másolatot kell készíteni.
Munkaállomások
Külső eszközről csak az előzetesen engedélyezett adatok érhetőek el. Munkavégzéshez a megfelelő eszközöket az Intézmény biztosítja, más eszközről belépés csak előzetes engedélyezés után lehetséges. Kívülről behozott hálózati csatlakozásra képes eszközök csak a külön erre fenntartott WI-FI hálózatra csatlakoztathatóak. 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 intézményvezető tudtával és engedélyével szabad. Az informatikai eszközöknek az Intézmény területéről való kivitele csak megfelelő jogosultság mellett, indokolt esetben lehetséges, jegyzőkönyvbe vétel után.

Belső hálózat használata

A lehetséges jogosultságok:
- vezetői jogosultság
- közalkalmazotti jogosultság

Az egyes jogosultságokhoz kapcsolódó lehetőségek

Közalkalmazotti jogosultság
- munkaértekezletek dokumentumai
- szabályzatok, eljárásrendek, teremnyilvántartás
- mindenki számára elérhető, vezetett és ellenőrzött feladatlisták
- közös naptár
- orientációs csomagok
- belső adatbázisok, dokumentációk K meghajtó használata
- Vezetői jogosultság látja a személyes, a szervezeti, a közalkalmazotti, vezetői mappát is.

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 az igazgató ellenőrzi.

Felelősség

Az Intézmény alkalmazottai kötelesek betartani a jelen Szabályzatban leírtakat, az abban foglaltak szándékos megszegése felelősségre vonást eredményez.

Gyál, 2019. április 04

Bretus Imre
igazgató