8360 Keszthely
Zeppelin tér 3.
Tel.: 83/312-446
Fax: 83/312-446

Fejér György Városi Könyvtár

2019

SZMSZ 6. sz. melléklet
Informatikai és adatvédelmi szabályzat

Készült: 2019. február 1.

.....
Pappné Beke Judit
igazgató

A Fejér György Városi Könyvtár (továbbiakban: intézmény) Informatikai és Adatvédelmi Szabályzata a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló 2016/679/EU rendelet, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény, valamint a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény alapján került összeállításra.

1. Az Informatikai és Adatvédelmi Szabályzat célja

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

Az informatikai és adatvédelmi szabályzat célja továbbá:

- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználás megelőzése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése,
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

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

2. Az informatikai és adatvédelmi szabályzat hatálya

2.1. Személyi hatálya

Kiterjed az intézmény valamennyi fő- és részfoglalkozású dolgozójára, illetve a számítástechnikai eljárásban résztvevő más szervezetek dolgozóira egyaránt.

2.2. Tárgyi hatálya

- kiterjed a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed az intézmény tulajdonában lévő valamennyi informatikai berendezésre, valamint a gépek műszaki dokumentációira is,
- kiterjed az informatikai folyamatban szereplő összes dokumentációra (szervezési, programozási, üzemeltetési),
- kiterjed a rendszer- és felhasználói programokra,

- kiterjed az adatok felhasználására vonatkozó utasításokra,
- kiterjed az adathordozók tárolására, felhasználására.

3. Az informatikai és adatvédelmi szabályzat biztonsági fokozata

Az intézmény alapbiztonsági fokozatba tartozik, általános informatikai feldolgozást végez.

4. Kapcsolódó szabályozások

Az informatikai és adatvédelmi szabályzatot az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:

- Szervezeti és Működési Szabályzat,
- Ügyrend,
- Iratkezelési szabályzat
- Belső ellenőrzési szabályzat
- Felesleges vagyontárgyak hasznosításának, selejtezésének szabályzata
- Leltárkészítési és leltározási szabályzata
- Munkavédelmi szabályzat
- Tűzvédelmi szabályzat

5. Védelmet igénylő informatikai rendszer

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.

5.1. Védelmi területek

- Vagyonvédelem:
  - Az informatikai eszközöket csak a kijelölt személyek használhatják.
  - Az informatikai eszközök rendeltetésszerű működéséért a felhasználó a felelős.
- A hardver és szoftver elemek: elsődleges védelme ezen eszközök és programok nyilvántartásba vétele a pénzkezelési szabályzatban lefektetett iránymutatás szerint. A hardverek és szoftverek telepítő lemezei, a szoftverek licencei és kódjai az informatikai iroda zárható szekrényében kerülnek elhelyezésre. A számítógépek hardver felépítéséről és szoftver tartalmáról nyilvántartást kell vezetni (gépenként), melyet változás esetén módosítani kell. A nyilvántartás elhelyezése az informatikai irodában, aktualizálása a rendszergazda feladata.
  Ezen eszközök és dokumentumok segítségével szükség esetén lehetővé válik a számítógépek gyors újratelepítése az eredeti állapot szerint.
- Az adathordozók (háttértárak): használatba vételéről, felhasználásáról, nyilvántartás készül, mely az eszközökkel együtt az informatikai iroda zárható szekrényében kerül elhelyezésre. A nyilvántartásnak naprakészen követnie kell az adathordozók fizikai mozgását, vezetéséért a rendszergazda a felelős.
  A használni kívánt adathordozót a tárolásra kijelölt helyről kell kivenni, és oda kell visszahelyezni is. Adathordozót más szervezetnek átadni csak igazgatói engedéllyel szabad.
  Olyan adathordozót amelyet javíthatatlan fizikai károsodás ért, vagy megőrzési ideje lejárt, selejtezni kell. A selejtezést az intézmény Felesleges

vagyontárgyak hasznosításának és selejtezésének szabályzata, valamint Iratkezelési szabályzata alapján kell lefolytatni.
Ezen adathordozókat selejtezés után fizikai roncsolással használhatatlanná kell tenni.

- Dokumentációk: a hardver és szoftver elemek dokumentációja az informatikai irodában kerül elhelyezésre, rendszerezése, selejtezése a rendszergazda feladata.
- Biztonsági mentések:
  - TextLib szerver adatainak mentése: naponta.

    A szerver beállításai alapján 04.00-kor automatikusan kilép, mentést készít, majd újraindul. Minden munkanapon az informatikai és zenei részleg egyik munkatársa a gép által készített mentést átírja a rendszergazda által kijelölt számítógépre. A gépen visszamenőlegesen 1 hónapig kell megőrizni a kiírt mentéseket.
  - Egyéb számítógépek adatainak mentése: az olvasók által használt számítógépekről mentések nem készülnek. Az intézmény dolgozói által használt számítógépek adatainak mentése a dolgozók feladata, az általuk meghatározott időintervallumok szerint. A számítógépek újratelepítése előtt a rendszergazda köteles az adott gép adatairól teljes mentést készíteni, az adatvesztés elkerülése miatt.
- Katasztrófa elhárítás: A számítógépes hálózat túlfeszültség elleni védelme nem megoldott, ezért nyári időszakban, vihar előrejelzése esetén a Textlib szerver és az olvasószolgálati számítógépek kivételével munkaidő után a gépeket az informatikán dolgozó munkatársnak áramtalanítania kell.
  Egyéb esetben a munkavédelmi és tűzrendészeti szabályzat előírásai az irányadók.
- Az informatikai iroda védelme: elemi csapás (vagy más ok) esetén az informatikai irodában bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:
  - menteni a még használható anyagot,
  - biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
  - új adatfeldolgozás, helyiségek kialakítása,
  - archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

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,
- a személyhez fűződő és vagyoni jogokra.

5.2. 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.

5.3. A védelem felelőse

A védelem felelőse a rendszergazda.
A jelen szabályzatban foglaltak szakszerű végrehajtásáról az intézmény adatvédelmi felelősének kell gondoskodnia.

Az adatvédelmi felelős (rendszergazda) feladatai

- ellátja az adatfeldolgozás felügyeletét
- ellenőrzi a védelmi előírások betartását,
- ellátja az informatikai titokvédelmi munka szervezését és felügyeletét,
- felelős az informatikai rendszerek üzembiztonságáért, biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek (pl. TextLib szerver) újraindíthatóságáról, illetve az újraindításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének, szervízellátás biztosításának folyamatos ellenőrzése,
- az adatvédelmi feladatok ismertetése, oktatása,
- a védelmi rendszer érvényesülésének ellenőrzése,
- az informatikai és adatvédelmi szabályzat kezelése, naprakészen tartása, módosítások átvezetése,
- felelős az intézmény informatikai rendszere hardver eszközeinek karbantartásáért,
- ellenőrzi a vásárolt szoftverek helyes működését, vírusmentességét, a használat jogszerűségét,
- biztosítja a vírusvédelmet, vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek izolálásáról,
- ellenőrzi a rendszer önadminisztrációját,
- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására,
- tevékenységéről rendszeresen beszámol az intézmény vezetőjének.

5.4. Az adatvédelmi felelős (rendszergazda) ellenőri feladatai

- évente egy alkalommal részletesen ellenőrzi az informatikai és adatvédelmi szabályzat előírásainak betartását,
- előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

5.5. Az adatvédelmi felelős (rendszergazda) jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet az intézmény vezetőjénél,
- bármely érintett csoportnál 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.

Az adatvédelmi felelős megbízatása
Az adatvédelmi felelőst az igazgató bízza meg.
Az adatvédelmi felelős írásbeli meghatalmazás alapján jogosult ellátni a hatáskörébe tartozó feladatokat.

6. Az informatikai és adatvédelmi szabályzat alkalmazásának módja, karbantartása

A szabályzat megismerését az érintett dolgozók részére az adatvédelmi felelős oktatás formájában biztosítja, melyről jegyzőkönyv készül. A szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni a szabályzat előírásainak megfelelően.
A szabályzatot az informatikában – valamint az intézménynél – a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell, annak folyamatos karbantartása az adatvédelmi felelős feladata.

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

Az informatikai feldolgozás során két nagy területen keletkeznek védelmet igénylő adatok:

- TextLib Integrált Könyvtári Rendszer (továbbiakban: TextLib) működtetése során keletkező adatok.
- A könyvtár egyéb számítógépein keletkező adatok.

TextLib:
A szerver-kliens architektúrájú, az intézmény egyéb számítógépeitől független, önálló belső hálózatot alkotó, Linux (szerver) és Windows/Linux (munkaállomások) operációs rendszeren futó program védelme megoldott. A bejelentkezés felhasználóhoz kötött.

A program hozzáférési pontjai a következők:

Feldolgozó csoport:

A könyvtár dokumentum állományainak adatait a feldolgozó csoport munkatársai kezelik. Egyaránt jogosultak az adatok felvitelére, módosítására és törlésre jelölésére is. Ezen feladatok teljesítéséhez rendelkezniük kell a TextLib programhoz megfelelő jogosultságokkal (azonosítók, jelszavak, felhasználói felület, jogok), melyek biztosítása a rendszergazda feladata.
A felvitt, módosított, törlésre jelölt adatok ellenőrzése a feldolgozó csoport vezetőjének feladata.

Olvasószolgálat:

Az olvasószolgálat minden munkatársa, valamint azon személyek, akik a kölcsönzésben részt vesznek, rendelkeznek azonosítóval és jelszóval a TextLib olvasószolgálati moduljának használatához, melyben lehetőség van adatfelvitelre, módosításra, valamint törlésre jelölésre. Az olvasói tartozások részletben történő fizetésének engedélyezésére, csökkentésére, elengedésére indokolt esetben csak az igazgató jogosult.
Az előbb felsoroltak a következő adatcsoportokat érintik:

- Olvasók adatai
- Kölcsönzések adatai
- Előjegyzések adatai
- Felszólítások adatai

Az olvasószolgálati tevékenységek során létrejövő adatok titkosak, megtekintésükre, további felhasználásukra csak az érintett olvasók és az olvasószolgálat munkatársai jogosultak, harmadik fél részére tovább nem adhatók.

Könyvtárhasználók:

Azonosítóval és jelszóval csak a saját olvasói állapotuk (adataik, kölcsönzéseik adatai stb.) megtekintése céljából rendelkeznek. A könyvtár munkatársai nyitás előtt a könyvtárhasználók számára fenntartott OPAC számítógépeket bekapcsolják, a rendelkezésre álló azonosítóval és jelszóval belépnek.

Az olvasók adatfelvitelre, módosításra és törlésre alkalmatlan, lekérdező felülettel rendelkeznek.

Rendszergazda:

Azonosítóval és jelszóval rendelkezik. Jogosult a TextLib rendszer valamennyi funkciójának igénybevételére, bármely adatcsoportjának megtekintésére, adatok bevitelére, módosítására és szükség esetén törlésére. A munkavégzéshez szükséges felhasználói felületeket létrehozza. Előzetes egyeztetéssel elkészíti a belépéshez szükséges azonosítókat és jelszavakat. Minden dolgozó köteles a saját jelszavát kétévente megváltoztatni.

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

A könyvtár egyéb számítógépei:

A számítógépek Internetre kapcsolódását, valamint egymáshoz való viszonyát a router szabályozza. Az eszközök egy része az azonosításhoz fix IP címekkel rendelkezik, másik része DHCP segítségével bekapcsolás után kapja meg az IP címét.

Az olvasók rendelkezésére álló (Internettel rendelkező) számítógépek PC-védelmi szoftverrel, illetve beállításokkal rendelkeznek, melyek segítségével elkerülhető, hogy az illegális vagy egyéb szempontból veszélyt jelentő programok a gépekre tartósan települjenek.

Az olvasói számítógépek csak a számukra kijelölt hálózati nyomtató elérésére képesek.

A könyvtár dolgozói számára rendelkezésre álló számítógépek védelme a Windows/Linux operációs rendszerek által biztosított technikai megoldásokkal (jelszavas védelemmel), víruskereső és tűzfal programokkal, azok automatikus frissítésével megoldott.

Ezen gépek esetén nincs felhasználóhoz kötött bejelentkezés. Azonosítóval és jelszóval csak a rendszergazda rendelkezik. A jelszavakat zárható szekrényben kell tárolni.

7. Az informatikai eszközbázist veszélyeztető helyzetek

- elemi csapás (földrengés, árvíz, tűz, villámcsapás stb.),
- környezeti kár (légszennyezettség, nagy teljesítményű elektromágneses térerő, elektrosztatikus feltöltődés, a levegő nedvességtartalmának felszökése vagy leesése, piszkolódás),
- közüzemi szolgáltatásban bekövetkező zavarok (feszültség-kimaradás, feszültségingadozás, elektromos zárlat, csőtörés),
- illetéktelen hozzáférés (adat, eszköz),

- adatok és eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- ellenőrzés hiánya,
- a jelszó félévenkénti megváltoztatásának az elmulasztása,
- biztonsági követelmények és gyári előírások be nem tartása,
- a karbantartási műveletek elmulasztása.

8. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

9. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

Szünetmentes áramforrás használata a TextLib szerver esetén elengedhetetlen, a munkatársi munkaállomások esetén szükségszerű, mely megvédi a berendezést a kisebb feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.

A vásárolt szoftverekről amennyiben szükséges biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag el kell különíteni.

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

Vírusfertőzés gyanúja esetén a rendszergazdát azonnal értesíteni kell.

Az intézmény informatikai eszközeiről programot, illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.

Olyan háttértárakat, melyeken formatálás után az operációs rendszer rossz szektorokat mutat ki, tilos felhasználni.

A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.

Az informatikai eszközt és tartozékait helyéről elvinni a rendszergazda tudta és engedélye nélkül nem szabad.

10. Ellenőrzés

Az intézménynél munkafolyamatba épített belső ellenőrzés folyik, mely a betöltött munkakörökhöz tartozik. Az egyes munkakörökhöz tartozó konkrét ellenőrzési feladatokat az érvényes jogszabályok, az intézmény szabályzatai és a munkaköri leírások tartalmazzák.

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

11. Záró rendelkezések

Az Informatikai és Adatvédelmi Szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat.

TITOKTARTÁSI NYILATKOZAT

Alulírott……..……név……
munkakör, mint a Fejér György Városi Könyvtár munkavállalója az alábbi nyilatkozatot teszem:

Tudomással bírok arról, hogy a Fejér György Városi Könyvtár tevékenysége tekintetében az EU 2016/679. sz. általános adatvédelmi rendelet (GDPR) és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény alapján adatkezelőnek minősül. Ennek következtében biztosítania kell, hogy a személyes adatok kezelését végző személyek titoktartási kötelezettségvállalást tegyenek.

Kijelentem, hogy a „személyes adat" GDPR szerinti fogalmát megismertem.

Kijelentem, hogy a munkaviszonyommal/egyéb munkavégzésre irányuló jogviszonyommal összefüggésben a tudomásomra jutott személyes adatokat kizárólag a munkaköri feladataim teljesítése céljából kezelem és továbbítom, más célra nem használom, azokat illetéktelen személyekkel nem közlöm, nem adom át. A személyes adatokat nyilvánosságra nem hozom, azokhoz jogosulatlan hozzáférést nem engedek.

Tudomásul veszem, hogy a titoktartási kötelezettségem megszegése a munkaviszonyból eredő kötelezettség lényeges megsértésének minősül, amely kapcsán a munkáltató munkajogi jogkövetkezményeket alkalmazhat. Tudomásul veszem továbbá a Büntető Törvénykönyv személyes adattal való visszaélés bűncselekményére vonatkozó munkáltatói tájékoztatást. Tudomásul veszem továbbá, hogy az ilyen magatartásommal a társaságnak okozott kárt köteles vagyok megtéríteni.

Keszthely, ……..

…….
nyilatkozó munkavállaló aláírása