Debreceni Bárczi Gusztáv Egységes Gyógypedagógiai Módszertani Intézmény,
Általános Iskola, Készségfejlesztő Iskola és Kollégium
DTK Szervezeti egységkód: HA0101
✉ 4024 Debrecen, Budai Ézsaiás u. 2.
☎ 52/349-064, Tel/fax: 52/531-690
E-mail címünk: barczi@barczi-debr.sulinet.hu

Debreceni Bárczi Gusztáv EGYMI, Általános Iskola, Készségfejlesztő Iskola és Kollégium

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Debrecen, 2020.09.01.

Készítette: Kovács Anikó Gyöngyi
intézményvezető

Az Informatikai Biztonsági Szabályzat célja

Az Informatikai Biztonsági Szabályzat, továbbiakban 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,
- 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.

Az Informatikai Biztonsági Szabályzat hatálya

Személyi hatálya

Az IBSZ személyi hatálya kiterjed az intézmény minden alkalmazottjára

Tárgyi hatálya

- kiterjed a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed a rendszer- és felhasználói programokra,
- kiterjed az adatok felhasználására vonatkozó utasításokra,
- kiterjed az adathordozók tárolására, felhasználására.

Az IBSZ biztonsági fokozata

Az adatok különböző biztonsági fokozatba tartozhatnak. (hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas adatok)

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

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 az intézmény rendszergazdája.

Minden intézményi dolgozó, aki intézményi/pályázati úton kapott laptopot használ és birtokol, köteles a biztonsági szabályok betartására.(pld: jogtiszta programok használata, idegen adathordozó használata)
A jelen szabályzatban foglaltak szakszerű végrehajtásáról az intézmény vezetőjének kell gondoskodnia.

Adatvédelmi felelősök feladatai

Rendszergazda feladatai:

- 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 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
- ellenőrzi a rendszer adminisztrációját
- a kötelező adatszolgáltatásról gondoskodik
- heti rendszerességgel menti az intézményi adatokat

Az informatikai vezető jogai

Az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet.

Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére a vezető biztosítja.

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.

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

Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

- illetéktelen hozzáférés (adat, eszköz)
- adatok- eszközök eltulajdonítása
- rongálás (gép, adathordozó)

Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya)
- szakmai hozzá nem értés
- 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.

Az informatikai eszközök környezetének védelme

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 (CD, DVD) a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni

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 az informatikusok végzik.

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.

Adathordozók tárolása

Az adathordozók tárolása zárt szekrényben biztosított.

Selejtezés, sokszorosítás, másolás

A selejtezés a selejtezési szabályzata alapján kell lefolytatni.

Leltározás

A szoftvereket és adathordozókat a Leltározási Szabályzatban foglaltaknak megfelelően 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 felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban az informatikus segítséget nyújt.
A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért a rendszergazda a felelős.

13. Ellenőrzés

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki.