INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

Az Információbiztonsági Szabályzat célja 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:

1. ♣ a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
2. ♣ az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
3. ♣ az üzembiztonságot szolgáló karbantartás és fenntartás,
4. ♣ az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
5. ♣ az adatállományok tartalmi és formai épségének megőrzése,
6. ♣ az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
7. ♣ a munkaállomásokon lekérdezhető adatok körének meghatározása,
8. ♣ az adatállományok biztonságos mentése,
9. ♣ az informatikai rendszerek zavartalan üzemeltetése,
10. ♣ a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
11. ♣ az adatvédelem és adatbiztonság feltételeinek megteremtése.

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;

**2 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 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), 7 • 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.