A Hit Gyülekezete Informatikai Biztonsági Szabályzata

2013

Tartalom

Az IBSZ célja és hatálya

A Hit Gyülekezete Informatikai Biztonsági Szabályzata (a továbbiakban: IBSZ) az információs önrendelkezési jogról és az információszabadságról szóló többször módosított 2011. évi CXII. törvény alapján készült.

Az IBSZ alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem alkotmányos 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 üzemeltetésükön keresztül a felhasználásig.

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

Az IBSZ személyi hatálya kiterjed a Hit Gyülekezete (továbbiakban: HGY) Informatikai rendszereinek (továbbiakban: IRSZ) valamennyi felhasználójára és üzemeltetőjére.

Az IBSZ tárgyi hatálya

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

A Hit Gyülekezete alapbiztonsági fokozatba tartozik. Ez a személyes adatok, üzleti titkok, pénzügyi adatok, illetve belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.

A Hit Gyülekezete általános informatikai adatkezelést végez.

Az adatkezelés során használt fontosabb fogalmak

Érintett: bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy.

Személyes adat: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés.

Különleges adat:

- a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,
- az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.

Bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.

Közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

Hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez.

Tiltakozás: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.

Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.

Adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen 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 (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.

Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele.

Adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.

Adatmegjelölés: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából.

Adatzárolás: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából.

Adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.

Adatfelelős: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett.

Adatközlő: az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatait honlapon közzéteszi.

Adatállomány: az egy nyilvántartásban kezelt adatok összessége.

Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval.

Adatközlő: az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatait honlapon közzéteszi.

Adatállomány: az egy nyilvántartásban kezelt adatok összessége.

Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval.

A Védelem tárgya és eszközei

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 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.

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 felelősei és feladataik

A védelem felelőse a Hit Gyülekezete Informatikai Csoport (a továbbiakban IT) vezetője, az egységvezetők és a rendszergazdák.

A jelen szabályzatban foglaltak szakszerű végrehajtásáról az egységvezetőknek kell gondoskodnia.

- Egységvezetőnek minősül ezen szabályzat keretein belül a szervezeti felosztásban az IT rendszer szolgáltatásait használó egységek vezetői

IT csoportvezetőjének minősül azon személy, akit az Országos Hivatal vezetője bíz meg ezzel a feladattal.

IT csoportvezető feladatai:

- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására,
- felelős az informatikai rendszer hardver eszközeinek karbantartásáért,
- ellátja az adatkezelés és adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- az adatvédelmi feladatok ismertetése,
- a felhasználók számítógépén ellenőrzi a szoftverek használatának jogszerűségét,
- ellenőri tevékenységét adminisztrálja,
- ellenőri tevékenységéről rendszeresen, de legalább évente beszámol az Országos Hivatal vezetője előtt.

Egységvezetők feladatai:

- 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.

Rendszergazda feladatai:

- a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli,
- gondoskodik a rendszer kritikus részeinek újraindíthatóságáról, illetve az újraindításhoz szükséges paraméterek reprodukálhatóságáról,
- gondoskodik a folyamatos vírusvédelemről,
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
- felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
- feladata a védelmi eszközök működésének folyamatos ellenőrzése,
- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer önadminisztrációját.

Felhasználó feladatai

- az általa létrehozott adatok mentésének biztosítása,
- hozzáférési azonosítóinak és a hozzájuk tartozó jelszavainak titkosságának megőrzése.

Az IT csoportvezető ellenőrzési 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.

Az IT csoportvezető jogai:

- az előírások ellen vétőkkel szemben szabálytalanságkezelési eljárás kezdeményezésére tehet javaslatot a Országos Hivatal vezetője felé,
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,
- betekinthet valamennyi iratba, amely az informatikai feldolgozásokkal kapcsolatos,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

Az IBSZ megismerését az érintett dolgozók részére az egységvezetők oktatás formájában biztosítják, melyről nyilvántartást vezetnek.

Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában, valamint a HGY-ben a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell.

Az IBSZ folyamatos karbantartása az IT csoportvezető 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,
- bizalmas, személyes adatok,
- minősített, titkos adatok.

Az informatikai kezelés során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik, illetve a központi rendszerekhez kapcsolódóan az informatikai egység biztonsági felelőse minősíti. A minősítést a meghatározott definíciók alapján kell végezni.

Különös védelmi utasítások és szabályozások nem mondhatnak ellent a törvények és a jogszabályok mindenkori előírásainak.

A kijelölt dolgozók előtt a titokvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell, szóbeli tájékoztatás útján, a munkába lépésük napján.

Alapelv, hogy mindenki csak ahhoz az adathoz juthasson hozzá, amire a munkájához szüksége van.

Az információhoz való hozzáférést lehetőség szerint a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység - adatbázisokhoz való hozzáférés, a fájlba vagy mágneslemezre történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet - utólag visszakereshető.

A naplófájlokat rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét az egységek vezetőjének azonnal jelenteni kell.

A naplófájlok áttekintéséért, értékeléséért a rendszergazdák a felelősek.

Minden dolgozóval, aki az adatok gyűjtése, felvétele, tárolása, kezelése, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt), valamint törlése során információkhoz jut, adatkezelési nyilatkozatot kell aláíratni. Ennek aláírásáig a dolgozó kizárható az informatikai szolgáltatások igénybevételéből.

Az adatkezelési nyilatkozat naprakészen tartásáért az egységvezetők a felelősek.

A titkot képező adatok védelmét a feldolgozás - adattovábbítás, 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).

Az informatikai rendszerekhez hozzáférési jogosultságot igényelni vagy jogosultság változást kérni az IT-nál, külön erre a célra rendszeresített igénylőlapon lehet.

A hozzáférési jogosultsági igényt az igénylő személy szervezeti egységének vezetője bírálja el, az igény jogosságát az igénylőlapon aláírásával igazolja.

Az igénylőlapon található információk alapján a hozzáférési jogosultságok kiosztását, illetve módosítását az egységvezetők által adott útmutatás szerint a rendszergazdák végzik.

Környezeti infrastruktúra okozta ártalmak és emberi tényezőre visszavezethető veszélyek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatok legyenek.

Elemi csapás:

- földrengés,
- árvíz,
- tűz,
- villámcsapás, egyéb vis major.

Környezeti kár:

- légszennyezettség,
- nagy teljesítményű elektromágneses térerő,
- elektrosztatikus feltöltődés,
- a levegő nedvességtartalmának felszökése vagy leesése,
- piszkolódás (pl. por).

Közüzemi szolgáltatásban bekövetkező zavarok:

- feszültség-kimaradás,
- feszültségingadozás,
- elektromos zárlat,
- csőtörés.

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, hálózati forgalom).

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.

Károkozás esetén belső vizsgálatot kell végezni az IT csoportvezető és az érintett egységvezető közreműködésével.

Szándékos károkozás esetén azonnal minden további hozzáférés megakadályozása szükséges. Ezt az IT csoportvezető javaslata alapján az Országos Hivatal vezetője rendeli el.

A Büntető törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 386. §-a szerinti „Védelmet biztosító műszaki intézkedés kijátszása", vagy a Btk. 422. §-a szerinti „Tiltott adatszerzés", vagy a Btk. 423. §-a szerinti „Információs rendszer vagy adat megsértése", vagy a Btk. 424. §-a szerinti „Információs rendszer védelmét biztosító technikai intézkedés kijátszása" bűncselekmény gyanúja felmerülésének alapján az illetékes hatóság felé feljelentést kell tenni.

A szándékos károkozás tényéről és a tett intézkedésről írásban kell tájékoztatni az Országos Hivatal vezetőjét.

Nem szándékos károkozás esetén meg kell határozni a kárt okozó felelősségének mértékét, és annak függvényében kell lefolytatni a szükséges fegyelmi eljárást.

Az adatok tartalmát és a kezelésük folyamatát érintő veszélyek

Tervezés és előkészítés során előforduló veszélyforrások

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

A rendszerek megvalósítása során előforduló veszélyforrások

- hibás adatállomány működése,
- helytelen adatkezelés,
- programtesztelés elhagyása.

A működés és fejlesztés során előforduló veszélyforrások

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

Vagyonvédelmi előírások:

- a géptermek külső és belső helyiségeit biztonsági zárakkal kell felszerelni,
- a gépterembe való be- és kilépés rendjét szabályozni kell,
- a számítógép monitorát lehetőleg úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- a gépterembe, szerverterembe történő illetéktelen behatolás tényét a Országos Hivatal vezetőjenak azonnal jelenteni kell,

- az informatikai eszközöket csak az HGY alkalmazottjai, ill. a munkavégzésre irányuló jogviszonnyal rendelkező személyek használhatják,
- az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

Külső 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 külső 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 más, külső szervezetnek átadni csak az Országos Hivatal vezetője engedélyével szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

Elektronikus adattovábbítás:

- Az HGY hálózatára csak felhasználói azonosító birtokában szabad csatlakozni,
- a levelezésben és elektronikus adattovábbításban felhasználói azonosító használata kötelező,
- a felhasználói azonosítókat, digitális aláírásokat központilag az IT kezeli, és tartja nyilván,
- hivatalos dokumentumot interneten közzétenni, harmadik fél felé továbbítani csak nem szerkeszthető formátumban szabad.

Tűzvédelem:

- A gépterem, illetve kiszolgáló helyiség a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.
- A tűzvédelem feladatait, a sajátos előírásokat a gépteremre, szerverszobára vonatkozóan a Tűzvédelmi Szabályzata tartalmazza.
- A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.
- A gépteremben és szerverszobában minimum 1-1 db tűzoltó készüléket kell elhelyezni.
- A szerverszobában elektromos vagy más munkát csak a tűzvédelmi szakreferens tudtával engedélyével szabad végezni.
- A nagy fontosságú, pl. törzsadat-állományokat, adatbázisokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni.(Ezen adatállományok kijelölése az egységvezetők feladata.)

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 eszközöket, berendezéseket és adatokat
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- archivált anyagok (III. 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 IT Informatikusai végezik.
- A munkák szervezésénél figyelembe kell venni:
    - a gyártó előírásait, ajánlatait,
    - a tapasztalatokat.
- Bármely számítógép, vagy számítástechnikai eszköz szétbontását (kivéve a garanciális gépeket) csak az IT informatikusai végezhetik el.

Az IT folyamat védelme

Az informatikai folyamat védelme:

- Az adatrögzítés védelme:
    - adatbevitel hibátlan műszaki állapotú berendezésen történjen,
    - csak tesztelt adathordozóra lehet adatállományt rögzíteni,
    - a külső adathordozókat csak az e célra kialakított és megfelelő tároló helyeken szabad tartani,
    - az adatrögzítés szoftveres védelme: lehetőség szerint olyan szoftvereket kell vásárolni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is.
    - hozzáférési lehetőség:
    - a felhasználói azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (Alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá).
    - az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
    - a szerverek rendszergazda jelszavait az IT rendszergazdái kezelik.
    - az adatrögzítés folyamatához kapcsolódó dokumentációk:
    - adatrögzítési utasítások,
    - ellenőrző rögzítési utasítások,
    - tesztelő és törlő programok kezelési utasításai,
    - megőrzési utasítások,
    - gépkezelési leírások.

A külső adathordozók nyilvántartása:

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

Külső adathordozók tárolása :

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

Az adathordozók megőrzése:

Az adathordozók megőrzési idejét a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló többször módosított 1995. évi LXVI. törvényben foglaltak alapján az adatkezelő határozza meg.

Selejtezés, sokszorosítás, másolós:

Selejtezéskor biztonsági intézkedésekkel kell megakadályozni, hogy a hibás informatikai eszközök adathordozói ellenőrizetlenül kerüljenek ki a szervezeten kívülre. Szintén alapvető követelmény, hogy a selejtezés az egységvezetők engedélyéhez kötött és megfelelően dokumentált legyen. A selejtezési jegyzőkönyvben a későbbi félreértések elkerülése végett, érdemes feltüntetni a selejtezendő alkatrész gyári számát, típusát, valamint a benne lévő adathordozók törléséről szóló nyilatkozatot, a felelős munkatárs aláírásával.

A kényes információk kiszivárgásának megelőzése érdekében a selejtezendő adathordozók esetében a sikeres törlés tényét ellenőrizni kell.

Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni. Biztonsági, illetve archív adatállomány előállítása másolásnak számít.

Mentések, file-ok védelme:

- Az adatfeldolgozás után biztosítani kell az adatok mentését.
- A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése és a mentés biztonságos tárolása az azt létrehozó munkatársak (felhasználók) feladata.
- A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban az informatikusok segítséget nyújtanak.
- A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért az egységvezetők, illetve a rendszergazdák a felelősek.

Szoftver védelem

Rendszerszoftver védelem:

Az egységeknek az IT-n keresztül biztosítani kell, hogy a rendszerszoftverek naprakész állapotban legyenek és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

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.

Programok megőrzése, nyilvántartása:

A programokról a rendszergazdáknak naprakész nyilvántartást kell vezetni

A programok nyilvántartásáért és működőképes állapotban való tartásáért az egységvezetők a felelősek.

A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

Központi gépek:

- Szünetmentes áramforrást kell használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén az 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:

- A külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
- Vírusfertőzés gyanúja esetén az rendszergazdákat azonnal értesíteni kell.
- Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal kell ellenőrizni működésüket.
- Az informatikai eszközökről 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.
- A hálózatra hálózati eszközt csak az IT vezetőjének engedélyével szabad csatlakoztatni. Az engedély nélkül csatlakoztatott eszköz hálózati hozzáférését az észlelést követően azonnal meg kell szüntetni, az eszközt csatlakoztató személy ellen az eljárást le kell folytatni.

Az IBSZ ellenőrzése

Évente egy alkalommal részletesen ellenőrzi szükséges az IBSZ előírásainak betartását.

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 adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

Budapest, 2013. december 1.

Petrőcz László

az Országos Hivatal vezetője