Állambiztonsági Szolgálatok
Történeti Levéltára
H-1067. Budapest, Eötvös u. 7
Pf: H-1369. Bp. 367
Tel:(06-1)478-6020
Fax:(06-1)478-6036
e-mail: info@abtl.hu
Internet:www.abtl.hu

1. számú példány

Az Állambiztonsági Szolgálatok Történeti Levéltára Főigazgatójának

13/2013. utasítása

a Történeti Levéltár Informatikai Biztonsági Szabályzat kiadásáról

1. §

Az Állambiztonsági Szolgálatok Történeti Levéltára informatikai rendszerének a Szervezeti és Működési Szabályzat szerinti biztonságos és megbízható működtetése érdekében a mellékelt Informatikai Biztonsági Szabályzatot adom ki.

2. §

Előírásokat a Levéltár valamennyi munkatársával ismertetni kell és a Levéltár belső honlapján el kell helyezni. Az utasítás megismerését, a munkatársak az Informatikai, Adatrögzítő és Állományvédelmi Osztály által készített névjegyzéken sajátkezű aláírásukkal igazolják.

3. §

Ez az utasítás 2013. július 15-én lép hatályba. Ezzel egyidejűleg a 33/2012. számú szabályzat hatályát veszti.

Budapest. 2013. április 09.

ÁLLAMBIZTONSÁGI SZOLGÁLATOK TÖRTÉNETI LEVÉLTÁRA

Dr. Gyarmati György
főigazgató

Készült: 1 példányban
Egy példány: 1 + 15 + 16 lap
Készítette: Cseh Gergő Bendegúz
Itsz: 28/T/NS
Kapja: Irattár

Állambiztonsági Szolgálatok
Történeti Levéltára
H-1067. Budapest, Eötvös u.7
Pf: H-1369. Bp. 367
Tel:(06-1)478-6020
Fax:(06-1)478-6036
e-mail: info@abtl.hu
Internet:www.abtl.hu

melléklet a 13/2013 számú utasításhoz

ÁLLAMBIZTONSÁGI SZOLGÁLATOK TÖRTÉNET LEVÉLTÁRÁNAK INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Tartalomjegyzék

Vezetői elkötelezettség 3
1. Az Informatikai Biztonsági Szabályzat célja 3
1. Az Informatikai Biztonsági Szabályzat hatálya 4
2. Az adatkezelés során használt fontosabb fogalmak 4
3. Az IBSZ biztonsági fokozata 5
4. Kapcsolódó szabályozások 5
5. Védelmet igénylő, az informatikai rendszerre ható elemek 5
5.3. A tesztelés során elért adatok védelme 6
6. A védelem felelőse 6
7. Az Informatikai Biztonsági Szabályzat alkalmazásának módja 7
8. Az informatikai eszközbázist veszélyeztető helyzetek 9
9. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek 10
10. Az informatikai eszközök környezetének védelme 10
11. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek.. 11
12. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága 14
13. Ellenőrzés 15
14. Függelék 15

Vezetői elkötelezettség

Az Állambiztonsági Szolgálatok Történeti Levéltára (továbbiakban Intézmény) vezetésének szilárd meggyőződése, hogy a Levéltárban tárolt információ az Intézmény és az állampolgárok olyan vagyona, amelyet védeni kell a különböző fenyegetések ellen, a bizalmasság, a sértetlenség és a rendelkezésre állás, illetve az üzletmenet folytonosságának biztosítása érdekében. Ennek érdekében az Intézmény vezetése a levéltár mindenkori informatikai biztonsági stratégiáját szem előtt tartva a Informatikai Biztonsági Szabályzatban (a továbbiakban IBSZ) meghatározott egyetemleges alapelvek és belső biztonsági alapkövetelmények maradéktalan teljesítését várja el a vezetőségtől, valamennyi munkatársától és minden egyéb érdekelt féltől. Az Intézmény informatikai biztonságpolitikája kivétel nélkül kiterjed az Intézmény által végzett valamennyi folyamatra és valamennyi szervezeti egységre. A legfelső vezetés biztosítja a teljesítéshez alapvetően szükséges erőforrásokat.

Az IBSZ az Intézmény vezetésének akaratnyilvánítása a szervezet informatikai rendszerei által kezelt információvagyon bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzésére és fenntartására irányuló intézkedések bevezetésére. Az IBSZ alapul szolgál továbbá az alacsonyabb szintű szabályozási eszközök, kialakítására és bevezetésére.
Az információ védelem megvalósítása érdekében tervezni és biztosítani kell azokat az anyagi feltételeket, amelyek lehetővé teszik a megfelelő színvonalú technika, valamint a speciális felkészültséget igénylő személyi feltételek megteremtését és folyamatos fenntartását.

1. Az Informatikai Biztonsági Szabályzat célja

Az *Állambiztonsági Szolgálatok Történeti Levéltárának (továbbiakban: Levéltár) 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,
- 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 tesztfolyamatok során elért adatok védelme.

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzembe-helyezésen keresztül az üzemeltetésig.
A jelen IBSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

1. Az Informatikai Biztonsági Szabályzat hatálya

1.1. Személyi hatálya

Az IBSZ személyi hatálya kiterjed a Levéltár összes munkatársára.

1.2. Tárgyi hatálya

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

2. 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;

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.

3. Az IBSZ biztonsági fokozata

A Levéltár adatai különböző biztonsági fokozatba tartoznak. (pénzügyi adatok, illetve a Levéltár belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas adatok)

4. Kapcsolódó szabályozások

Az IBSZ előírásai összhangban vannak:
- Leltározási és értékelési szabályzattal,
- Számviteli politikával

5. 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.

5.1. 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 és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,

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 tesztelés során elért adatok védelme

Az informatikai fejlesztések során bevezetésre kerülő új szoftververziók tesztelése kizárólag a levéltár zárt, belső hálózatán belül, kizárólag erre dedikált speciális szervereken történhet.

6. A védelem felelőse

A védelem felelőse a mindenkori informatikai vezető és rendszergazdák.
A jelen szabályzatban foglaltak szakszerű végrehajtásáról a Levéltár vezetőinek kell gondoskodnia.

6.1. Adatvédelmi felelősök feladatai

a) Informatikai vezető feladatai:

- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására.
- 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, rendellenesség esetén írásos jelentést készít,
- ellenőrzi a szoftverek használatának jogszerűségét.

b) 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, rendkívüli esemény esetén írásos jelentés készítése,
- felelős a Levéltár informatikai rendszer hardver eszközeinek karbantartásáért,
- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- 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,

6.2. Az informatikai vezető ellenőri 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,
- rendkívüli esemény bekövetkezése esetén írásos feljegyzést, szükség esetén intézkedési tervet is készít.

6.3. Az informatikai vezető jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a Levéltár vezetőjénél,
- bármely érintett szervezeti egységnél 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.

7. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az érintett munkatársak részére a vezetők és a rendszergazdák oktatás formájában biztosítják. Erről nyilvántartást kötelesek vezetni.
Az Informatikai Biztonsági Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

7.1. Az Informatikai Biztonsági Szabályzat karbantartása

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

7.2. 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,
- minősített, titkos adatok.

Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik.
Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot. A kijelölt munkatársak 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. El kell különíteni a külső és a belső számítógépen elérhető adatok körét.
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. Az ORCALE adatbázis közvetlen elérésének naplózását és auditálását (ORACLE Audit Trail) is meg kell oldani.
Az alkalmazás minden adatváltozást (beszúrás, módosítás, törlés) naplóz. Ehhez az Oracle adatbázis specifikus elemeket úgynevezett tiggereket használ. Ezek a logikák érzékelik az adatváltozást és készítik el a naplósorokat. Mivel az adatbázis szerves része, nem szükséges hozzá az alkalmazás használata (mivel ha valaki közvetlenül az adatbázisba csatlakozik és módosítja az adatokat akkor ezek a logikák ugyanúgy naplózzák a változtatást, mintha azok az alkalmazáson keresztül következnének be). Így az Oracle adatbázisban az audit trailben elegendő csak a tiggerek aktiválásával, inaktiválásával és törlésével kapcsolatos műveletek naplózása.
A naplófájlokat rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét a Levéltár vezetőjének jelenteni kell, illetőleg azonnal intézkedni kell a jogosulatlan hozzáférési lehetőség megszűntetéséről.

A naplófájlok áttekintéséért, értékeléséért az informatikai vezető és a rendszergazdák a felelősek.

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 is biztosítani kell (szoftver, hardver adatvédelem).

8. 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.

8.1. 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.

8.2. Emberi tényezőre visszavezethető veszélyek

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).

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. Ezen rendszerek műszaki állapotát ezért rendszeresen ellenőrizni kell, rendellenesség esetén írásos feljegyzést, szükség esetén intézkedési tervet kell készíteni, sürgős esetben pedig azonnal intézkedni kell az fenyegető veszélyhelyzet elhárításáról.

9. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

9.1. Tervezés és előkészítés során előforduló veszélyforrások

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

9.2. A rendszerek megvalósítása során előforduló veszélyforrások

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

9.3. A működés és fejlesztés során előforduló veszélyforrások

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

10. Az informatikai eszközök környezetének védelme

10.1. Vagyonvédelmi előírások

- a géptermek külső és belső helyiségeit biztonsági zárakkal kell felszerelni,
- a gépterembe való belépés kártyás beléptetőrendszerrel történik,
- a gépterembe, szerverterembe történő illetéktelen behatolás tényét a Levéltár vezetőjének azonnal jelenteni kell,
- az informatikai eszközöket csak a Levéltár arra felhatalmazott alkalmazottai használhatják,

- az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

10.2. 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, merevlemez) 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 másnak átadni csak engedéllyel szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

10.3. Tűzvédelem

A gépterem illetve kiszolgáló helyiség a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.
A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.
A Levéltár géptermébe, szerverszobába minimum 1 db tűzoltó készüléket kell elhelyezni.
A Levéltár géptermében, szerverszobában elektromos vagy más munkát csak a tűzvédelmi felelős tudtával, ill. engedélyével szabad végezni.
A nagy fontosságú, pl. törzsadat-állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni. (Ezen adatállományok kijelölése az informatikai vezető feladata.)

11. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

Az informatikai rendszer védelmének biztosításához a rendszerbe csak letesztelt hardver illetve szoftver elemek illeszthetőek.
A szoftver-változásokról nyilvántartást kell vezetni, melynek ki kell terjednie a beszerzett szoftver nyilvántartására, telepített verzió változásának rögzítésére.
Az informatikai rendszer hardver-elemeiről folyamatosan karbantartott nyilvántartást kell vezetni, melynek ki kell terjednie az adott eszközön végrehajtott esetleges alkatrész-cserékre, bővítésekre vagy egyéb módosításokra is.

11.1. 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.

11.2. 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.
A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlatait,
- a tapasztalatokat.

Alapgép megbontását (kivéve a garanciális gépeket) csak informatikus végezheti el.

11.3. Az informatikai feldolgozás folyamatának védelme

11.3.1. 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.
- A szerverek rendszergazda jelszavát az informatikai vezető kezeli.

11.3.2. Adathordozók tárolása

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

11.3.3. Az adathordozók megőrzése

A levéltári anyag digitális másolatát tartalmazó adathordozók nem selejtezhetők.

A pénzügyi vonatkozású adathordozók megőrzési idejét a törvényekben meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani.

11.3.4. Selejtezés, sokszorosítás, másolás

A selejtezést a Levéltár selejtezésének szabályzata alapján kell lefolytatni.
Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni.
Biztonsági illetve archív adatállomány előállítása másolásnak számít.

11.3.5. Leltározás

A szoftvereket és adathordozókat a Leltározási Szabályzatban foglaltaknak megfelelően kell leltározni.

11.3.6. 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 informatikusok segítséget nyújtanak.
A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért az informatikai vezető illetve a rendszergazdák a felelősek.

11.4. Szoftver védelem

11.4.1. Rendszerszoftver védelem

Az informatikai vezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

11.4.2. Felhasználói programok védelme

11.4.2.1. 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.

11.4.2.2. Programok megőrzése, nyilvántartása

A programokról naprakész nyilvántartást kell vezetni.
A számvitelről szóló többször módosított 2000. évi C. törvény, valamint az államháztartás szervezetei beszámolási és könyvvezetési kötelezettségének sajátosságairól szóló 249/2000 (XII.24.) Korm. rendelet értelmében a vállalkozásoknak 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 és működőképes állapotban való tartásáért a vezetők a felelősek.

12. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

12.1. Központi gépek

Szünetmentes áramforrás használata, 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 központi szerverek működésében legfeljebb 24 órás leállás engedhető meg, az esetleges műszaki meghibásodásokat ezen idő alatt kell elhárítani és a rendszert ismét működőképessé tenni. A levéltár alapfeladatainak ellátásához szükséges informatikai támogatás működésében legfeljebb 24 órás leállás, illetve ugyanezen időszak alatt keletkezett adatmennyiség elvesztése tolerálható.
A szerverek és háttértárolók megsemmisülése (tűzkár, csőtörés stb.) esetén a teljes hardver- és szoftverinfrastruktúrát, valamint a biztonsági másolatokon tárolt adategyütteseket – a beszerzések adminisztrációs időkorlátai, valamint az intézmény anyagi erőforrásainak függvényében – lehetőleg 30 napon belül helyre kell állítani.

12.2. Munkaállomások

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell.
Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.
A Levéltár 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 eszköz leltárfelelőse tudtával és engedélyével szabad.

13. 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 adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

Az IT biztonsági rendszert, illetve annak egyes elemeit rendszeresen, esemény hatására, azon kívül kell felülvizsgálni.

A szükséges felülvizsgálatok az alábbiak:

A felülvizsgálat tárgya	A felülvizsgálat ciklussága
Kockázatfelmérés	2 évente
IT biztonsági utasítás	2 évente
IT biztonsági folyamatok	2 évente
Vírusvédelem	2 évente
Mentési, archiválási rend	2 évente
IT biztonsági oktatás	1 évente

14. Függelék

1. Jogosultságok eljárásrendje
2. Jelszó és napló házirend
3. Hardver leltár
4. Szoftver leltár
5. Munkatárs jogosultság nyilvántartás
6. Adatmentési ügymenet
7. Informatikai biztonsági kockázatelemzés

Jogosultságok eljárásrendje

Az eljárásrend szabályozza a Levéltár munkatársi állományába belépő, illetve az onnan távozó munkatárs hozzáféréseit, jogosultságait a Levéltár informatikai rendszeréhez.

Az egyes munkakörökhöz tartozó jogosultsági szinteket a Levéltár főigazgatója határozza meg

- A Intézményhez érkező új munkatárs felvételekor a Humánpolitikai Osztálytól kapott információ alapján a Felhasználó rögzítése a rendszerben.
- Hozzáférések és a felhasználói fiók beállítása a Levéltár tartományi rendszerében.
- Szükséges eszközök biztosítása, számítógép felhasználói fiók beállítása.
- Hozzáadás a belső levelezési szolgáltatáshoz, szükség esetén internetes e-mail cím igénylése, beállítása.
- A Levéltárból kifelé irányuló telefonhálózat használatához szükséges kód generálása, átadása a Titkársági Főosztály részére.
- A jogosultságok felfüggesztésre kerülnek az intézménytől távozás esetén (munkaviszony megszűnése, kilépés) illetve vezetői utasításra. A felhasználó felfüggesztett jogosultsága záros határidőn belül megszüntetésre kerül. Az általa hátrahagyott levéltári munkájával összefüggésben készült dokumentumokat a felettes vezető részére hozzáférhetővé kell tenni, és az Ő utasítására lehet a rendszerből eltávolítani.

Felhasználó jogosultság nyilvántartás

		Belső hálózat																																												Internetes hálózat		
			tartományi csoport															TH Info													Saldo	Savtalanítás									Hálózati nyilvántartás	Adatlapok	E-archivum	BM	Munkaidőny. belépt.	Név	sajátgép	munkacsoport
	NÉV	Sajátgép	Domain Users	Adatrögzítő	Államp.adatszolg.o.	Iratfeldolg.o.	Kutatást elő.o.	Rendszergazda	Domain Admins	Ügyfélszolgálat	Ügyfélszolgálati o.	Informatika	Humánpol.o.	Gazdasági főo.	Referensek	Levéltárosok	Tudományos főo.	Adatrögzítők	Adatszolgáltatók	Dosszié admin.	Felhasználók	Fotódokumentátor	Kutatáselőkészítők	Lev.nyilv.rendsz.felhaszn.	Mindent látók	Rendszergazdák	Tud.Főoszt.munkatársai	Ügyfélszolgálat	Ügyfelek	Kutatók		Raktárosok	Előkészítők	Digitalizálók	Restaurátorok	Savtalanítók	Ellenőrzők	Adminisztrátorok	Keresők	Vendégek								
1																																															
2																																															
3																																															
4																																															
5																																															
6																																															
7																																															
8																																															
9																																															
10																																															
11																																															
12																																															
13																																															
14																																															
15																																															

IBSZ 2.sz függelék a 13/2013. sz. utasításhoz

Jelszó és napló házirend

A munkaállomásokon történő feladatvégzés megfelelő felhasználónévvel és jelszóval lehetséges.
A felhasználónév képzése a dolgozó vezetéknevéből történik. A hozzákapcsolódó jelszónak minimum 6 karakter hosszúnak kell lennie.
Első bejelentkezés után a felhasználónak lehetősége van jelszavának módosítására.
Hibás felhasználó illetve jelszó használata esetén a rendszer 5 sikertelen bejelentkezés után letiltja a felhasználói fiókot 30 percre.
Amennyiben a felhasználó elfelejti felhasználónevét, vagy jelszavát, a rendszergazdához fordulhat segítségért.
A szervereken, munkaállomásokon végzett tevékenységek a naplózással követhetőek. Bármilyen a rendszert érintő probléma jelentkezésekor a naplók visszanézésével lehet következtetni a kialakult problémára, az elhárítás, javítás lehetőségére.
A visszakövethetőség érdekében az eseménynaplót, annak méretének biztosításával úgy kell beállítani, hogy az események csak szükség esetén kerüljenek felülírásra.
A munkaállomásokon a helyi házirendben, azon belül a naplórend beállításakor tekintettel kell lenni fentiekre.

Hardver leltár (nyilvántartás)

Tartalmazza az Állambiztonsági Szolgálatok Történeti Levéltárában (Levéltár) használt informatikai berendezések nyilvántartását.

A lista a Levéltár belső szerverén meghatározott helyen (\\Abtl-server\InformSzabalyzatAg\IBSZ\Függelék\HardverLelt.xls) kerül tárolásra.

Frissítése, aktualizálása minden hardver eszközt érintő változás esetén szükséges.

ABTL hardver leltár

Sorszám	Megnevezés	Gyáriszám	Leltáriszám	Használó	Megjegyzés
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

Szoftver leltár (nyilvántartás)

Tartalmazza az Állambiztonsági Szolgálatok Történeti Levéltárában (Levéltár) használt jogdíjas szoftverek nyilvántartását, hozzáférésüket, verzió számát.
A lista a Levéltár belső szerverén meghatározott helyen (\\Abtl-server\InformSzabalyzatAg\IBSZ\Függelék\SzoftverLelt) kerül tárolásra.
Frissítése, aktualizálása minden jogdíjas szoftvert érintő változás esetén szükséges.

ABTL szoftver leltár

Sorszám	Beszerzés időpontja	Megnevezés	Medium	Medium mennyisége	Licensz száma
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

IBSZ 5.sz függelék a 13/2013. sz. utasításhoz

Munkatárs jogosultság nyilvántartás

Tartalmazza az Állambiztonsági Szolgálatok Történeti Levéltárában (Levéltár) dolgozók informatikai rendszerhez történő hozzáférésének jogosultságait.
A lista a Levéltár belső szerverén meghatározott helyen, az arra illetékesek által tekinthető meg (\\Abtl-server\InfSzabAg\Eljárásrendek\Hozzáférések.xls) kerül tárolásra.
Frissítése, aktualizálása minden munkaügyi változás, belépő és kilépő munkatárs, áthelyezés esetén szükséges.

IBSZ 6.sz függelék a 13/2013. sz. utasításhoz

A Történeti Levéltár informatikai rendszerének adatmentési ügymenete

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.

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.

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 adatbiztonsági mentés

Az informatikai rendszerben tárolt adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

Az adatkezelés során keletkezett adatokról biztonsági mentést kell készíteni.

Az adatmentési folyamatot az adatkezelő határozza meg. Az adatkezelő utasítása alapján végzi az adatmentést egy adatfeldolgozó, akit a munkaköri leírásában az adatmentéssel bíztak meg.

Az adatkezelő utasítása alapján az adatmentéssel megbízott adatfeldolgozó végzi az adatbiztonsági mentést.

Az adatkezelő feladatai az informatikai rendszerben tárolt adatok mentése során

1. Maghatározza az informatikai rendszerben tárolt adatállományok biztonsági kockázatait és ennek megfelelően kialakítja az adatmentés és visszaállítás biztonságos rendjét.
2. Egy erre a feladatra alkalmas, megfelelő képzettségű munkatársat bíz meg az adatmentések végrehajtásával.
3. Rendszeresen ellenőrzi az adatmentések megtörténtét és ezt a mentési napló aláírásával igazolja.
4. Rendszeresen ellenőrzi a mentett állományokból történő kísérleti adat-visszaállítások megtörténtét.
5. Az informatikai rendszerben történt rendkívüli esemény (üzemzavar, hardver-meghibásodás, felhasználói adatvesztés stb.) esetén gondoskodik a mentett állományokból történő mielőbbi adatvisszaállításról.

Az adatbiztonsági mentéssel megbízott adatfeldolgozó feladata

1. A Levéltárban működő, ORACLE alapú adatbázis napi rendszerességgel történő mentése, mely az ügyfelek és kutatók kiszolgálásának alapjául szolgáló ABTLInfo adatbázisát tartalmazza, beleértve a Történeti Levéltár feldolgozott iratainak adatait, az ügyfél- és kutatószolgálati nyilvántartásokat, valamint magukat a digitalizált iratokat is;
2. az ABTL integrált moduláris számviteli rendszerének, a SALDO Creatornak az adatfeldolgozása során keletkezett MSSQL adatbázis (MSDE) napi mentése;
3. az ABTL egyéb működéséhez szükséges adatállományainak (telefon díjrögzítő, beléptető rendszer, páramérő rendszer, e-Archívum, savtalanító adatbázis, hálózati nyilvántartó adatbázis, BM-dolgozók adatbázisa), illetve a felhasználók által készített és az abtl-szerveren tárolt dokumentumainak heti mentése,
4. az ABTL által üzemeltetett webszerveren működő www.abtl.hu. www.betekinto.hu, www.abparancsok.hu, www.munkataborok.hu honlapok heti mentése,
5. az ABTL internetes hálózatán használt munkaállomások felhasználóinak fájlszintű mentése, heti rendszerességgel.

Az adatmentéssel megbízott adatfeldolgozónak a mentések elvégzését a mentési naplóban rögzíteni kell, melyet az adatkezelő aláírásával igazol. A mentési napló tartalmazza a mentés időpontját, a mentést végző dolgozó nevét, valamint a mentés eredményét.

A mentett állományok kezelése

A belső hálózat adatbiztonsági mentéseit szalagos mentőegységre kell menteni, melyeket a következő mentésig az erre a célra telepített tűzálló páncélszekrényben kell tárolni.

Az internetes hálózat mentéseit az erre a célra üzemeltetett NAS típusú berendezésen kell tárolni.

A mentett adatok visszaállítása

Az adatbiztonsági mentéseket az adatkezelő utasítása alapján, de legalább negyedévente egy tesztüzem során vissza kell állítani és meggyőződni arról, hogy az adatbiztonsági mentésekből használható és a mentési időpontnak megfelelő adatokat lehet visszaállítani.

Az adatbiztonsági mentések visszaállításáról visszaállítási naplót kell vezetni, mely tartalmazza a visszaállítás idejét, a visszaállítást végző adatfeldolgozó nevét és a visszaállítás eredményét. A visszaállítási naplóban a mentés visszaállítását az adatkezelő aláírásával igazolja.

Informatikai Biztonsági Kockázatelemzés

2013

Tartalomjegyzék

Bevezető 3
A kockázat számítás 4
Az alkalmazott számítási módszer 4
Kártípusok 4
Kárérték osztályozás 5

Bevezető

Az informatikai kockázatelemzés célja, hogy megállapítsa az intézményben alkalmazott informatikai rendszerek és az általuk kezelt adatokat érintő lehetséges káreseményeket, majd ezek minősítésével a károsszegeket. Mindezt azért, hogy az intézmény fenyegetettség mértékével arányos védelmi (megelőzési) intézkedéseket hozhasson, illetve ennek alapján a szabályzásban meghatározott időnként ezt felülvizsgálhassa, módosíthassa.

A dokumentum tartalmazza a kockázat számításához alkalmazott számítási módszert, a megállapítható kártípusok felsorolását, illetve a kárérték osztályozásához használandó értékeket.

Jelen dokumentum a hivatkozott leírásokban található módszerek egyszerűsített kivonata. A kidolgozásához az Irodalom jegyzékben található leírások, értekezések szolgáltak alapul.

A Levéltárban használt informatikai rendszerek, kockázatelemzés szempontjából a következő csoportokra bonthatóak. Minden csoport alatt felsorolásra kerül az azonosított kockázat:

- **ABTL (külső, internetről publikusan és kutatók számára elérhető változata)**
  - Szolgáltatás akadályoztatása (DDoS)
  - Kutatók számára elérhető adatok illetéktelen megszerzése
  - Adatok megrongálása
- **ABTL (belső, védett adatokat tartalmazó belső változata)**
  - Védett adatok megszerzése
  - Védett adatok rongálása
  - Adatok megrongálása
- **Saldo Creator**
  - Könyvelési adatok megszerzése
  - Adatok megrongálása
- **Minden egyéb ami az ABTL működtetéséhez szükséges**
  - Működési adatok megszerzése
  - Működési adatok megrongálása

A kockázat számítás

A kockázatszámítás első lépése a fenyegetett informatikai rendszerek, azok adatcsoportjainak összegyűjtése.

Ezt követi a kártípusok megállapítása. (Amennyiben egy informatikai rendszer biztonsági szempontból külön vizsgálandó eleméhez több kártípus is megállapítható akkor azok külön sorban kerülnek felsorolásra, hogy a kárérték kártípusonként külön kerüljön megállapításra.)

Ezután következik a kárérték osztályozása és a költségek (C1-C5) tételes megállapítása.

Végezetül a súlyosság (W) és bekövetkezési valószínűség (P) megállapítása majd a kockázathoz tartozó kárérték kiszámítása.

Az alkalmazott számítási módszer

A szakirodalmakban található módszerek gyakorlatba átültetett módja:

$$K = (C1 + C2 + C3 + C4 + C5) \cdot W \cdot P$$

- **K** a kockázat;
- **C1** az eredeti állapot helyreállításának költsége;
- **C2** a rendelkezésre-állás költsége;
- **C3** a követelmények összehangolásának költsége;
- **C4** az információ kiáramlás költsége;
- **C5** a büntetések vagy biztosítások költsége;
- **W** súlyosság, nem anyagi érték, pl. a jó hír elvesztése;
- **P** a kár bekövetkezésének valószínűsége.

Kártípusok

Kódja	Megnevezése
KNA	Közvetlen anyagi
KTA	Közvetett anyagi
TPH	Társadalmi-politikai, humán
SZE	Személyi sérülés, haláleset
JOG	Jogszabály által védett adatokkal történő visszaélés vagy azok sérülése

árérték osztályozás

Kódja	Megnevezése
0	Jelentéktelen kár
1	Csekély kár
2	Közepes kár
3	Nagy kár (magas)
4	Kiemelkedően nagy kár
4+	Katasztrofális kár

Kárérték 1.000 e Ft-ig csekély a kockázat

Kárérték 2.000 e Ft-ig közepes a kockázat

Kárérték 2.000 e Ft- felett magas a kockázat

Kockázat/Kárérték táblázat

K	KT	KO	C1	C2	C3	C4	C5	W	P	SZK
ABTL (külső, internetről publikusan és kutatók számára elérhető változata)										
Szolgáltatás akadályoztatása	THP		eFt	eFt	eFt	eFt	eFt			eFt
Kutatók számára elérhető adatok illetéktelen megszerzése	JOG, KTA		eFt	eFt	eFt	eFt	eFt			eFt
Adatok megrongálása	KNA		eFt	eFt	eFt	eFt	eFt			e Ft
Kárérték összesen										
ABTL (belső, védett adatokat tartalmazó belső változata)										
Védett adatok megszerzése	JOG, KTA		eFt	eFt	eFt	eFt	eFt			eFt
Védett adatok rongálása	JOG,KNA		eFt	eFt	eFt	eFt	eFt			eFt
Kárérték összesen										e Ft
Saldo Creator										
Könyvelési adatok megszerzése	KTA		eFt	eFt	eFt	eFt	0 eFt			eFt
Adatok megrongálása	KNA, KTA		eFt	eFt	eFt	eFt	eFt			eFt
Kárérték összesen										e Ft
Minden egyéb ami az ABTL működtetéséhez szükséges										
Működési adatok megszerzése	KTA		eFt	eFt	eFt	eFt	eFt			eFt
Működési adatok megrongálása	KTA		eFt	eFt	eFt	eFt	eFt			eFt
Kárérték összesen										e Ft

- **K** a kockázat;
- **KT** kár típus;
- **KO** kár érték osztály;
- **C1** az eredeti állapot helyreállításának költsége;
- **C2** a rendelkezésre-állás költsége;
- **C3** a követelmények összehangolásának költsége;
- **C4** az információ kiáramlás költsége;
- **C5** a büntettetések vagy biztosítások költsége;
- **W** súlyosság, nem anyagi érték, pl. a jó hír elvesztése;
- **P** a kár bekövetkezésének valószínűsége, 0-1.0 közötti érték lehet. (0 a 0%, 0.5 az 50%, 1.0 a 100%)
- **SZK** a számított kárérték, **SZK = (C1 + C2 + C3 + C4 + C5) · W · P**

Az értékelés eredménye alapján kell a megfelelő intézkedéseket megtenni az alacsonyabb kockázat elérése céljából.
A kockázat elemzés felülvizsgálatát legalább 3 évente kell elvégezni.