AASzC 8-4/2022.

ALFÖLDI AGRÁRSZAKKÉPZÉSI CENTRUM

Informatikai Biztonsági Szabályzat

Jóváhagyja és hatályba lépteti:

Dr. Horváth József
főigazgató

Alföldi Agrárszakképzési Centrum 1.

Vári László
kancellár

2022.

Tartalomjegyzék

1. Az IBSZ célja

Az IBSZ alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, 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,
- 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.

2. IBSZ hatálya

2.1. Személyi hatálya

Az IBSZ végrehajtását a hatályba lépésnek megfelelően, kihirdetéstől kezdődően meg kell kezdeni. Az IBSZ a biztonságos információ ellátás érdekében utasításokat tartalmaz, amelyek hatálya kiterjed az Alföldi ASzC informatikai rendszereinek teljes életciklusára (tervezés, fejlesztés, beszerzés, bevezetés, üzemeltetés, kivonás).
Az IBSZ személyi hatálya kiterjed a Centrum valamennyi alkalmazottjára.

2.2. Tárgyi hatálya

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

Az informatikai biztonsági rendszer működtetése

Megfelelés a jogszabályoknak és a belső szabályzatoknak:

- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013.évi L.törvény
- az információ önrendelkezési jogról és az információszabadságról 2011.évi CXII.törvény
- Alföldi ASzC Szervezeti és Működési Szabályzata

Helyesbítő-megelőző intézkedések rendszere
Azokra a fenyegetettségekre, amelyekre szabályzatban nem rögzített eljárások, előírások, illetve a technikai eszközök nem adnak megoldást, az alábbi eljárásrend érvényes:
Az IT biztonsági rendszerrel kapcsolatos nem megfelelő működésekről, észrevételekről, javaslatokról az Alföldi ASzC bármely dolgozója köteles tájékoztatni az informatikust. Az informatikus az igényeket, bejelentéseket megvizsgálja, azokra intézkedési terveket dolgoz ki, amelyeket az Alföldi ASzC kancellárja elé terjeszt jóváhagyásra. Jóváhagyás esetén az IT biztonsági rendszer fejlesztése, módosítása a műszaki csoportvezető mellett történik.

3. Az adatkezelés során használt fontosabb fogalmak

- ***Adat:*** az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.
- ***Adatátvitel:*** elektronikus adatok informatikai rendszerek közötti továbbítása, amely lehet párbeszédre épülő (online) vagy nem párbeszédre épülő (offline) elektronikus kapcsolat
- ***Adatbázis:*** azonos minőségű (jellemzőjű), többnyire strukturált adatok összessége, amelyet a tárolására, lekérdezésére és szerkesztésére alkalmas szoftvereszköz kezel.
- ***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.
- ***Adatfeldolgozás:*** az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.
- ***Adatfeldolgozó:*** az a természetes vagy jogi személy, aki vagy amely az adatkezelő megbízásából az adatok feldolgozását végzi.
- ***Adathordozó:*** az elektronikus adatkezelő rendszerhez csatlakoztatható vagy abba beépített olyan eszköz, amelynek segítségével az elektronikus adatok tárolása, terjesztése megvalósítható. Pl. CD, DAT, DVD, floppy, merevlemez, USB-memória, cloud (felhő).
- ***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.

- ***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.
- ***Adattovábbítás:*** ha az adatot meghatározott harmadik fél számára hozzáférhetővé teszik.
- ***Adminisztratív biztonsági követelmények:*** az informatikai rendszer használata, üzemeltetése vagy fejlesztése során az adatok és a munkafolyamatok nyilvántartását, nyomon követhetőségét, továbbá az ezzel kapcsolatos feladatok ellátásának ellenőrzését lehetővé tevő segédletek és eljárásrendek meglétére, alkalmazására vonatkozó elvárások. Pl. naplók, nyilvántartások vezetése, ellenőrzése, ennek rendje.
- ***Archiválás:*** a ritkán használt, meghaladottá vált, de nem selejtezhető adatok, adatbázisrészek változatlan tartalmi formában történő hosszú távú megőrzése.
- ***Bizalmasság:*** az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
- ***Nyilvánosságra hozatal:*** ha az adatot bárki számára hozzáférhetővé teszik.
- ***Elektronikus információs rendszer:*** Az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese. (Informatikai rendszer) Az elektronikus információs rendszerekhez tartoznak:
    - a számítástechnikai rendszerek és hálózatok, ide értve az internet szolgáltatást is;
    - helyhez kötött, mobil és egyéb rádiófrekvenciás, valamint műholdas elektronikus hírközlési hálózatok, szolgáltatások;
    - a vezetékes, a rádiófrekvenciás és műholdas műsorszórás;
    - a rádiós vagy műholdas navigáció;
    - az automatizálási, vezérlési és ellenőrzési rendszerek (SCADA, távmérő, távérzékelő és telemetriai rendszerek, stb.);
    - valamint a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek

4. Az IBSZ biztonsági fokozata

A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében az elektronikus információs rendszereket – ideértve a rendszer által kezelt adatokat – biztonsági osztályba kell sorolni, a bizalmasságuk, a sértetlenségük, valamint a rendelkezésre állásuk szempontjából.

Osztályozási szintek	**Bizalmasság**	**Sértetlenség**	**Rendelkezésre állás**
1.Nyilvános	Nyilvános	Nem védett	Általános
2. Bizalmas	Belső használatra vagy Bizalmas	Védett	Fontos
3.Titkos	Titkos	Fokozottan védett	Kritikus

Az elektronikus információs rendszerek biztonsági osztályba sorolását az alábbi alapkövetelmények figyelembe vételével kell végrehajtani:

- a biztonsági osztályokhoz tartozó védelmi követelményeket jogszabály rögzíti,
- a nemzeti adatvagyont kezelő rendszerek esetében a jogszabályi előírásoknak megfelelően,
- a biztonsági osztályokat a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából erősödő védelmi követelményeket meghatározó, 1-5 fokozatú skála szerint kell meghatározni.

A Centrum biztonsági szintbe történő sorolása az elektronikus információs rendszerek védelmére való felkészültsége alapján történik, jogszabályban meghatározott szempontok szerint.

A biztonsági szintbe és osztályba való sorolást a Centrum vagy az elektronikus információs rendszer – illetve az abban kezelt adatok – jelentős megváltozása esetén, de legalább 3 évente felül kell vizsgálni.

A Centrum elvárt biztonsági szintbe, valamint az elektronikus információs rendszerek elvárt biztonsági osztályba sorolását az 1. sz. melléklet tartalmazza.

Cselekvési terv készítése

Amennyiben a vizsgálat – vagy felülvizsgálat – alapján meghatározott biztonsági szint alacsonyabb, mint a szervezet jogszabályban meghatározott biztonsági szint, vagy ha a szervezet az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, akkor a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie a számára előírt biztonsági szint elérésére vagy hiányosságok megszüntetésére.
A cselekvési terv elkészítése és folyamatos nyomon követése az informatikai biztonsági felelős, a cselekvési terv elfogadása pedig a kancellár feladata.

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:

- 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 rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,
- 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.

6. A védelem felelőse

A védelem felelősei az informatikai biztonsági felelős, valamint a rendszergazdák.

A jelen szabályzatban foglaltak szakszerű végrehajtásáról a Centrum központ és szakképző intézményei vezetőinek kell gondoskodnia.

6.1. Adatvédelmi felelősök feladatai

A) Informatikai biztonsági felelős feladatai:
- IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- javaslatot tesz a rendszer szűk keresztmetszeteinek a 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,
- 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 újraindíthatóságáról, illetve az újraindításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének folyamatos ellenőrzése,
- felelős az intézmény 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 biztonsági felelős 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 folyamat bármely részét.

6.3. Az informatikai biztonsági felelős jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet az intézményvezetőnél,
- 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 véleményezni.

6.4. Felhasználók feladatai

- Minden felhasználó felelős az általa használt IT-eszközök rendeltetésszerű használatáért, azok megóvásáért.
- Minden felhasználó, a reá vonatkozó szabályok - szerint, felelős az általa elkövetett szabálytalanságért, valamint a keletkező károkért és hátrányért.
- Minden felhasználó köteles: az IBSZ-ben megfogalmazott szabályokat megismerni és betartani, illetve ezek betartásában az informatikai rendszer használatát irányító és üzemeltető személyekkel együttműködni.
- Minden felhasználó köteles az általa használt jelszavakat megőrizni, azokat másnak nem adhatja át és más felhasználó jelszavát nem használhatja.
- Köteles az észlelt rendellenességekről közvetlen felettesét és/vagy a rendszergazdát értesíteni.
- Köteles részt venni a számára szervezett informatikai továbbképzésen.

7. Az IBSZ alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére az informatikai biztonsági felelős 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 IBSZ karbantartása

Az IBSZ-t az informatikában – valamint az intézménynél – a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. Az IBSZ folyamatos karbantartása a rendszergazda 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.

A hivatali titoknak minősülő adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot. A kijelölt dolgozók 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.

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.

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 be- és kilépés rendjét szabályozni kell, ezt telephelyenként melléklet szabályozza,
- a gépterembe, szerverterembe történő illetéktelen behatolás tényét a tagintézmény vezetőjének azonnal jelenteni kell,
- 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 (floppy, CD, DVD) a tárolásra kijelölt helyről kell kivenni, és oda kell visszahelyezni,
- 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. Kézi tűzoltó-berendezések elhelyezése a bejárat közvetlen közelében.
A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.
Az intézmény géptermeibe, szerverszobáiba tűzoltó készüléket kell elhelyezni.
Az intézmény géptermeiben, szerverszobáiban elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.
A helyiség elhelyezését úgy kell megválasztani, hogy a felette elhelyezkedő helyiségekben ne legyen vizes blokk (mosdó, WC, Konyha, stb.). Ellenkező esetben a födém vízzárásának kialakítása szükséges.
Ha szerverszoba szintjén vízkár veszélye forog fenn (árvíz, belvíz, csőtörés, stb.). akkor az alábbi védőmechanizmusok bevezetése szükséges:

- álpadló, a berendezések mennyezetről való táplálása
- falak, nyílászárók vízbehatolás elleni védelme
- Ún. védőtálcák alkalmazása a berendezések elhelyezésére

11. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

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.
Alapgép megbontását (kivéve a garanciális gépeket) csak a rendszergazdák végezhetik el.

11.3. Az informatikai feldolgozás folyamatának védelme

Az adatrögzítés védelme:

- Az adatbevitel hibátlan műszaki állapotú berendezésen történjen.
- Az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
- 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 szabályozása: 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 adathordozók nyilvántartása:
Az adathordozókról nyilvántartást kell vezetni. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval (sorszámmal) kell ellátni.

Adathordozók tárolása:
Az adathordozók tárolására műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.
Figyelembe kell venni a gyártó által meghatározott tárolási környezetre vonatkozó paramétereket.
Két példányban való tárolás esetében a tároló helyet úgy kell kiválasztani, hogy szükség esetén az arra jogosult akadálytalanul viszonylag gyorsan hozzáférhessen, de célszerűen, viszonylag távol. Ezzel megakadályozva mindkét példány egyidejű megsemmisülését természeti katasztrófa esetén.

Az adathordozók megőrzése:
Az adathordozók megőrzési idejét a jogszabályokban meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani.

Selejtezés, sokszorosítás, másolás:
A selejtezést az intézmény selejtezésének szabályzata alapján kell lefolytatni.
Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni. Biztonsági illetve archív adatállomány előállítása másolásnak számít. Másolás után meg kell győződni, hogy a másolt adatok egyeznek-e az eredetivel.

Leltározás:
A szoftvereket és adathordozókat a leltározási szabályzatban foglaltaknak megfelelően kell leltározni. Az eredeti szoftvereket használat előtt 2 példányban le kell másolni, feliratozni, és az eredetit, valamint egy másolt példányt külön-külön helyen őrizni. A megvásárolt szoftverek adathordozóját lehetőleg eltávolíthatatlan módon fel kell címkézni.

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 adatmentés kell végeznie a munkafolyamatokról és az online munkafelületekről. Az archiválásban az informatikusok segítséget nyújtanak. A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért a rendszergazdák a felelősek.
A dokumentum célja, hogy meghatározza az Alföldi ASzC informatikai rendszerén elektronikusan tárolt adatok mentési és archiválási rend alapelveit. A mentési rend alapelveinek célja, hogy kialakítsa azokat az eljárásokat, feladatokat és felelősségeket, amelyekkel biztosítani lehet az üzleti szempontból „fontos", vagy annál magasabb adatosztályba sorolt adatok előírt rendelkezésre állását.
Felelősségek a helyi informatikus elektronikusan tárolt adatok mentésével kapcsolatos feladati és felelőssége:

- felelős az Alföldi Aszc mentési, archiválási rendjének kidolgozásáért
- felelős a mentési, archiválási rend rendszeres ellenőrzéséért.

- felelős a mentési rendet érintő változások követéséért, illetve a mentési rendről szóló dokumentációk felülvizsgálatáért.
- felelős a mentési feladatokkal megbízott rendszergazda által jelentett incidensek kezelésére vonatkozó intézkedések foganatosításáért, illetve szükség esetén a kezeléséhez szükséges erőforrások biztosításáért.
- A mentésért felelős rendszergazda felelőssége:
- felelős a kezelésére bízott informatikai rendszerben tárolt elektronikus adatok mentésének, archiválásának rendszeres, előírásszerű végrehajtásáért,
- felelős a mentések visszatöltéssel történő ellenőrzések végrehajtásáért,
- felelős az archívumban elhelyezett médiák rendszeres ellenőrzéséért, időszakonként történő átcsévéléséért, vagy átmásolásáért,
- felelős a mentéssel, archiválással, illetve visszatöltéssel kapcsolatos dokumentálások elvégzéséért.

Mentések irányelvei

A mentések megtervezésekor az alábbi szempontokat kell figyelembe venni:

- Minden olyan adat mentésre kerüljön, amely az adatosztályozás során „fontos", vagy annál magasabb besorolást kapott.
- Minden mentésnek biztosítani kell az adatok kezeléséhez szükséges szoftverkörnyezet következetes helyreállíthatóságát (operációs rendszer, adatbázis kezelő, stb).
- Minden olyan adat mentésre kerüljön, amely az auditálás, ellenőrzés eszköze lehet (naplófájlok, riportok, stb.).
- Minden olyan eszköz konfigurációja mentésre kerüljön, amely részt vesz „fontos", vagy annál magasabb besorolású adat kezelésében (tárolásában, továbbításában, stb. pl.: hálózati aktív eszközök.)
- Minden mentés alkalmas legyen olyan környezet helyreállítására, mely lehetővé teszi valamely igazolható állapothoz való visszatérést.
- A kritikus rendszerek mentése legalább két példányban készüljön, a két példányt elkülönítetten kell tárolni.

A mentések tartalma

Az adatkommunikációs eszközök mentését az alábbi esetekben kell elvégezni:

- Új eszköz rendszerbeállítása esetén,
- Az adatkommunikációs eszközök konfigurációjában történő bármilyen változás esetén.
- Félévente egy alkalommal
- Mentendő állományok:
    - Router, tűzfal, switch esetében: az NVRAM-ban található startup-config file.
    - Az adatkommunikációs eszközök konfigurációit a kijelölt szerveren a rendszergazdai könyvtárban kell lementeni, valamint a lementett konfigurációs fájlok archiválását legalább 6 havonta, a gyors visszaállíthatóság érdekében CD-re is kell elvégezni.

11.4.Szoftver védelem

Rendszerszoftver védelem:
A rendszergazdáknak biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

Felhasználói programok védelme

- **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 leltárfelelősöknek naprakész nyilvántartást kell vezetni, 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.

11.5 Vírusvédelmi események

A fertőzés nagyságától függően az alábbi területeket különböztetjük meg;

- Elszigetelt: ha az Alföldi ASzC területén, 24 órán belül legfeljebb 2-3 intézményben legfeljebb 1-2 fertőzés fordul elő, és egy védendő eszközön sem ismétlődött meg a fertőzés
- Ismétlődő: ha egy bizonyos eszköz egy nap többször, vagy több egymás utáni napon, hasonló módon megfertőződik.
- Sorozatos: ha 24 órán belül az Alföldi ASzC területén 10-20, egy intézményen belül 5-10 fertőzés történt.
- Tömeges: fentieknél nagyobb 24 órán belüli fertőzésszám.

Fertőzés az is, amit nem a vírusvédelmi eszközök jeleznek, hanem ami a felhasználók és rendszergazdák jelzései alapján valószínűsíthető.

Események szintjei:

1. szintű vírusvédelmi eseménynek minősül, ha a víruskereső elszigetelt fertőzést észlelt, és az előírt vírusmentesítést elvégezte.
2. szintű vírusvédelmi eseménynek minősülnek a következők:

- A vírusvédelem elszigetelt fertőzést észlel, de nem tudja a vírusmentesítést elvégezni.
- A vírusvédelem sorozatos vagy ismétlődő vírust észlelt, és a vírusmentesítést elvégezte.
- A vírusvédelmi menedzsment alkalmazás azt észleli, hogy valamelyik kiemelt eszközön nem fut a vírusvédelem.
- A vírusvédelmi menedzsment alkalmazás azt észleli, hogy valamelyik munkaállomáson 2 napja nem fut a vírusvédelem.
- A vírusvédelmi eszköz jelzi, hogy egy számítógépen 5 napnál régebbi a szignatúra. Kivételt képez az az eset, amikor a menedzsmentfelület a saját adatbázisa alapján azért mutat régi

szignatúrákat, mert az adott számítógép több apja nincs bekapcsolva vagy nem elérhető, illetve már nem a hálózat része.

- A központi vírusvédelmi eszközök valamelyikének 1 napnál hosszabb üzemképtelensége.
- Itt fel nem sorolt egyéb esetek, amikor a vírusvédelmi rendszerbe bármi okból illetéktelenül beavatkoznak.

3. szintű vírusvédelmi eseménynek (vírusriadó) minősül:

- Tömeges vírusfertőzés
- Sikertelen vírusmentesítés sorozatos vagy ismétlődő fertőzés esetén.

11.6 A valósidejű védelem kialakítása

Az Alföldi ASzC-nél a védendő eszközök hatékony védelmének érdekében valósidejű védelmet kell kialakítani. A szervereken és munkaállomásokon a valósidejű védelemnek folyamatosan bekapcsolva kell lennie, hogy biztosítsa a felhasználói munka során igénybevett állományok (adatok, programok) használat előtti vírusellenőrzését. Olyan központi kliens szerver megoldáson alapuló megoldást kell alkalmazni, mely automatikusan ellenőrzi:

- A teljes lokális és távoli fájlrendszert,
- A hálózati (vezetékes és vezeték nélküli) kapcsolatokat,
- Az adatbeviteli perifériákat (floppy, USB tárolók, CD és DVD meghajtók),
- Levelezési rendszer.

Biztosítani kell, hogy a munkaállomásokon a valósidejű védelmet a felhasználók ne tudják kikapcsolni.
Amennyiben a valósidejű védelem a detektált vírus eltávolítására nem képes, a vírusvédelmi rendszer automatikus értesítést küld a felhasználó és az IT rendszergazda számára, és a fertőzés gyanús állományt a rendszer automatikusan karanténba helyezi. A vírusfertőzésről vagy annak gyanújáról a felhasználó köteles értesíteni a helyi IT rendszergazdát.

11.7 A vírusveszély csökkentésének hardveres és szoftveres lehetőségei

Az Alföldi ASzC a vírusfertőzés veszélyének csökkentése érdekében ki kell használni azokat a rendelkezésre álló technikai eszközöket, amelyek nem vírusvédelmi feladatokat látnak el, de egyes funkcióik alkalmas a vírusok elleni védekezésre, mint pl:

- A hálózati aktív eszközök nem használt –fizikai és szoftveres – portok letiltása
- A tartalomszűrő eszközökkel letöltések vagy levélben való küldésének blokkolása
- A határvédelmi tűzfalakon a nem használt illetve nem támogatott protokollok és szoftver portok letiltása.
- A szervereken a nem használt applikációk és szervizek leállítása, eltávolítása.
- A szervereken kizárólag a működésükhöz és üzemeltetésükhöz szükséges programok telepítése.

11.8 Levelezés biztonsága

Tilos megnyitni ismeretlen forrásból származó elektronikus levelet. A levél fertőzöttségének elbírálásához az alábbiakat kell figyelembe venni:

- A levél feladója ismert személy-e, illetve várható-e a levél a feladótól? (Fertőzött levél ismert személytől, vagy ismerősnek tűnő forrásból is származhat.)

- A levél tárgya: gyanús a levél, ha az nem munkaköri feladatokkal vagy várt információval kapcsolatos.
- A levél címzettje: fertőzött lehet, ha szokatlanul sok a címzettje.
- A levél nyelvezete: fertőzött lehet a levél, ha idegen nyelven, vagy nem a szokásos kommunikációs nyelven íródott.
- A levél csatolmánya: gyanús lehet a levél, ha az alábbi kiterjesztésű csatolt állományt például: bat, .com, .exe, .dll, .sys, bit, .pif, hlp . txt, vagy beágyazott linket (ÚR) tartalmaz.
- A fertőzöttnek ítélt elektronikus levelet a mellékletek megnyitása nélkül törölni kell, még a törölt levelek mappájából is.

11.9 Internetezés biztonsága

Az Alföldi ASzC-nál tilos a fájlletöltő oldalak, Internetes játékoldalak, ún. csevegő oldalak, valamint szexuális szolgáltatásokat kínáló oldalak látogatása.
Tilos az ügyvitellel és az oktatási, kutatási feladatokkal össze nem függő fájlok megnyitása, letöltése az internetről. A letöltéseket átmeneti mappába (külön létrehozandó) kell elhelyezni.

12 A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

Központi gépek

Szünetmentes áramforrást célszerű használni, amely 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 vásárolt szoftverekről biztonsági másolatot kell készíteni.

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.
Az intézmény 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 IT biztonság szempontjából kritikus pontokon mérési és ellenőrzési rendszert kell bevezetni.
A mérések eredményéről az informatikus félévente számol be az Alföldi ASzC Kancellárjának, annak érdekében, hogy a központi rendszereket érintő esetlegesen felmerült kockázatok

kezelése időben megtörténjen. A mérési rendszer kontroll pontjait összefoglaló táblázat a 2. számú mellékletben található.
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 ellenőrzések során elsősorban az alábbiakat kell vizsgálni:

- Az IT biztonsági rendszer működése megfelel-e a törvényi előírásoknak
- Az IT biztonsági szabályok érvényesítve vannak-e folyamatokban
- Az IT biztonsági rendszer előírt dokumentumai léteznek-e, illetve naprakészek-e
- Az IT személyzet, illetve a felhasználók rendelkeznek-e a megfelelő IT biztonsági ismeretekkel.
- Az adatokra és rendszerekre vonatkozó kezelési szabályok betartását.
- A naplózási rendszer megfelelő alkalmazását. A biztonsági események kezelésének, a szükséges mértékű felelősségre vonás gyakorlatát.
- A mentési rendszer üzemeltetők, és felhasználók informatikai biztonsággal kapcsolatos ismereteit.
- A hozzáférési jogosultságok nyilvántartásának naprakészségét, a kiadott jogosultságok szükségességét.
- Az alkalmazott szoftverek jogtisztaságát.
- A szerződések megfelelőségét.
- A fizikai biztonsági előírások betartását.

Az IT biztonsági rendszer, illetve annak egyes elemeit rendszeresen felülvizsgálatra kerülnek. A biztonsági rendszerek felülvizsgálati idejét összefoglaló táblázat a 3. számú mellékletében található.

14 Záró rendelkezések

Jelen szabályzat 2022. február 21.napján lép hatályba.

A Szabályzat betartásának ellenőrzése az informatikai biztonsági felelős közreműködése útján a kancellár feladata.

1.sz. melléklet: Informatikai biztonsági zónák

1. ZÓNÁK MEGHATÁROZÁS

Zóna követelmények	1.számú biztonsági zóna	2.számú biztonsági zóna	3.számú biztonsági zóna
Általános követelmények			
Természeti katasztrófák kockázatainak csökkentése			A zóna kialakításnál figyelembe kell venni az árvíz, belvíz, villámcsapás és egyéb természeti katasztrófák kockázatait.
Hozzáférési követelmények			
A belépés, beléptetés	Az irodákba történő belépés kulccsal történik.	Az irodákba történő belépés kulccsal történik.	A zónában történő belépés egyedi azonosítással történik.
A belépés engedélyeztetése	Külön engedély nem szükséges	A fogadó szervezet vezetőjének szóbeli engedélye szükséges.	Írásbeli engedély szükséges.
Környezeti követelmények			
Klimatizálás			Klimatizálás szükséges.
Páratartalom mérése			A páratartalom mérése szükséges.
Áramellátás szabályozása			Az áramellátás szabályozása, és redundanciája szükséges.
Biztonsági követelmények	Kézi tűzoltó készülékek kihelyezése szükséges a folyosón.	Kézi tűzoltó készülékek kihelyezése szükséges.	Tűzvédelmi füstérzékelő és a közelben kézi riasztó szükséges. A helységben vagy annak bejáratánál kézi tűzoltó készülék kihelyezése szükséges.
Tűzvédelem	Passzív behatolás védelmi eszközök szükségesek az alagsori, földszinti, és az 1.emeleti ablakokra.	Passzív behatolás védelmi eszközök szükségesek az alagsori, földszinti, és az 1. emelet ablakokra.	Passzív behatolás védelmi eszközök szükségesek az alagsori, földszinti, és 1. emeleti ablakokra, valamint aktív behatolás- védelmi eszközök felszerelése szükséges a helységbe vagy a folyosókra.

Behatolás-védelem			Felügyeleti (riasztó) eszközökkel kell ellátni.
Biztonsági események naplózása			A felügyeleti eszközök jelentéseit naplózni kell.
Dokumentálási követelmények	A belépések naplózása	A kulcs felvételénél kell dokumentálni.	

2.melléklet: Kontroll és felülvizsgálat

Mérendő terület	Mérendő mennyiség	Beszámolóban szerepel (- ; x)
IT tevékenység	Szerverszobába való belépések száma	
	Hozzáférések (logikai) naplózása	
Illegális IT tevékenységek	Észlelt behatolási kísérletek száma	
	Nem az Alföldi AszC dolgozó/hallgató által végzett tevékenység teljes körű naplózása	
Vírusvédelem	Beérkezett vírusok, SPAM-ek száma	
	Hatástalanított vírusok és blokkolt SPAM-ek száma	
	Nem Internetről beérkezett vírustámadások száma, ezek módja	
Mentési rendszer	A teszt visszatöltések eredményei	
Rendelkezésre állás	Rendszerek kieséseinek száma, ezek oka, időtartama, javítási költsége	
Kapacitás információk	Kritikus rendszerekre vonatkozó teljesítményadatok jelentős változása	
	Tárolási kapacitásokra vonatkozó információk	
Ellenőrzések eredményei	Feltárt hiányosságok, és azok megszüntetésére vonatkozó intézkedések	
Oktatás helyzete	IT biztonsági oktatásban részt vett személyek száma, a beszámoltatás eredményei	
IT biztonsággal kapcsolatos fegyelemsértések	IT biztonságot megsértő személyekre vonatkozó fegyelmi statisztikák	

Az IT biztonsági rendszer összesített értékelése	Az IT rendszer technikai és biztonsági szintjére vonatkozó megállapítások, javaslatok	
Javaslatok	Javaslatok kidolgozása a hiányosságok megszüntetésére, a biztonsági és rendelkezésre állási szint emelésére.	

3.sz. melléklet: Szervezet topologikus ábrája: