AASZC 8-26/2022.

ALFÖLDI AGRÁRSZAKKÉPZÉSI CENTRUM
6640 Csongrád Kis-Tisza u. 4/a.-6/a.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

1. számú módosítása

Jóváhagyja és hatályba lépteti:

Dr. Horváth József
főigazgató

Vári László
kancellár

2022.

Tartalomjegyzék

I. ÁLTALÁNOS RENDELKEZÉSEK

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.

2.3. A Szabályzat jogi háttere és kapcsolódó belső irányítási eszközök

Az IBSZ jogi alapját az alábbi jogszabályok, közjogi szervezetszabályozó eszközök és belső irányítási eszközök képezik:

a) 2013. évi L. törvény (a továbbiakban: Ibtv.) az állami és önkormányzati szervek elektronikus információbiztonságáról,
b) 2015. évi CXXX. törvény az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról,
c) 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú információs rendszerek meghatározásáról,
d) 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról,
g) a Centrum Szervezeti és Működési Szabályzata.

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.
- **Adatállomány**: egy nyilvántartásban kezelt adatok összessége.
- **Adatátvitel:** elektronikus adatok informatikai rendszerek közötti továbbítása, amely lehet párbeszédre épülő (online) vagy nem párbeszédre épülő (offline) elektronikus kapcsolat.
- ***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.
- **Adatgazda:** annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik.
- ***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

- **Autentikáció (azonosítás):** informatikai eljárás, amelynek során a felhasználó az informatikai rendszerben az autorizáció megszerzése érdekében igazolja személyazonosságát. Lehet tudás alapú (pl. jelszavas), birtoklás alapú (pl. tokenes) vagy tulajdonság alapú (pl. biometrikus), illetve ezek kombinációi.
- **Autorizáció (feljogosítás):** azonosításra épülő informatikai eljárás, amelynek eredményeként egyértelműen azonosított személy (eszköz) a feladatai ellátásához meghatározott hozzáférési, eljárási vagy egyéb jogosultságokat kap.
- **Belső felhasználó:** Az AASzC központi szerve és a ASzC Szakképző Intézményei valamennyi foglalkoztatottja.
- **Belső hálózat (intranet):** az AASzC saját, védett hálózata, mely belső telefonkönyvet szolgáltat, emellett, az itt található menükből strukturáltan, kereshető formában teszi elérhetővé az AASzC feladataival összefüggő adatbázisokat, az AASzC belső utasításokat és nyomtatványokat.
- **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.
- **Biztonság:** egy adott infrastruktúra, infrastruktúra elem, vagy elemek olyan – az érintett számára kielégítő mértékű – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Részei a fizikai, környezeti, személyi, szervezeti, valamint az információbiztonság, az infokommunikációs infrastruktúrákban kezelt elektronikus adatok és információk biztonsága
- **Biztonsági esemény:** nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.
- **Biztonsági intézkedések:** illetéktelen személyek információs infrastruktúrához, vagy információkhoz való szándékos, vagy véletlen fizikai hozzáférése elleni eszközök használatát szabályozó, valamint az illetékes személyek jogosulatlan tevékenységével szemben fellépő előírások, tervek és útmutatások összessége.

- **Biztonsági kockázat:** az informatikai rendszerrel szembeni fenyegetés, amely a rendszer rendeltetésszerű működését és/vagy a rendszerben kezelt adatok bizalmasságát, rendelkezésre állását, sértetlenségét veszélyezteti vagy veszélyeztetheti.

- **Biztonsági követelmények:** a kockázatelemzés eredményeként megállapított, elfogadhatatlan mértékű veszély mérséklésére, vagy megszüntetésére irányuló szükségletek együttese.
- **Biztonsági megfelelőség:** az informatikai rendszer mennyiben, milyen mértékben felel meg az informatikai biztonsági követelményeknek.
- **Biztonsági osztály:** az elektronikus információs rendszer védelmének elvárt erőssége. Biztonsági szint: az elektronikus információs rendszerek felhasználásának a módja határozza meg egy szervezet biztonsági szintjét. A szervezeten kívül a következő szervezeti egységeket is biztonsági szintbe kell sorolni. A besorolási útmutatót a technológiai vhr. tartalmazza.
- **Demilitarizált zóna (továbbiakban: DMZ):** összekapcsolt hálózatok megbízhatatlan külső és megbízható belső részei között elhelyezkedő terület. A DMZ a benne elhelyezkedő hálózati eszközökhöz mind a megbízható belső, mind pedig a megbízhatatlan külső területről szabályozott mértékben engedélyezi a hozzáférést, de megakadályozza, hogy a külső területről bármilyen hozzáférési kísérlet eljusson a belső hálózatra.
- **Elektronikus információs rendszer:**
  a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;
  b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy
  c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok
- **Értékelés:** az infokommunikációs rendszerekkel kapcsolatos biztonsági intézkedések, eljárásrendek, Magyarországon elfogadott technológiai értékelési szabványok, követelményrendszerek és ajánlások, illetve jogszabályok szerinti megfelelőségi vizsgálata.
- **Fejlesztői rendszer:** olyan informatikai rendszer vagy alkalmazás, amelynek felhasználói informatikusok. Célja felhasználói programok vagy alkalmazások kifejlesztésének támogatása.
- **Felhasználók**: Általános felhasználók a Centrum foglalkoztatottjai (ideértve a gyakornokokat is).
- **Fizikai biztonság:** illetéktelen személyek információs infrastruktúrához, vagy információkhoz való szándékos, vagy véletlen fizikai hozzáférése elleni intézkedések összessége, valamint az illetéktelen személyek, vagy illetékes személyek jogosulatlan tevékenységével szemben az adott struktúrák ellenálló képességét növelő tervek és útmutatások összessége.
- **Folytonos védelem:** az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem.

- **Funkcionális rendszer:** az ASzC működését támogató informatikai rendszer vagy alkalmazás.
- **Hardver:** az informatikai rendszer vagy számítógép fizikai elemei
- **Hálózat:** számítógépek és hozzájuk kapcsolódó eszközök meghatározott szabályok szerinti összekapcsolása, amely adat- és információcserét tesz lehetővé.
- **Helyreállítás:** valamilyen behatás következtében megsérült, eredeti funkcióját ellátni képtelen, vagy ellátni csak részben képes infrastruktúra-elem eredeti állapotának és működőképességének biztosítása, eredeti helyen.
- **Hitelesítés:** a rendszerbe kerülő, ott lévő és onnan kikerülő adatok forrásának (az adat közlőjének), megbízható azonosítása.
- **Hitelesség:** annak biztosítása, hogy a rendszerbe kerülő adatok és információk eredetiek, a megadott forrásból az abban tárolttal azonos, változatlan tartalommal származnak.
- **Hozzáférés:** az infokommunikációs rendszer, vagy rendszerelem használója számára a rendszer szolgáltatásainak, vagy a szolgáltatások egy részének ellenőrzött és szabályozott biztosítása.
- **Illetéktelen személy:** olyan személy, aki az adathoz, információhoz, az informatikai infrastruktúrához való hozzáférésre nem jogosult.
- **Infokommunikáció:** az informatika és a telekommunikáció, mint konvergáló területek együttes neve.
- **Informatikai alkalmazás:** számítógépen, illetve egyéb informatikai eszközön futó program.
- **Informatikai biztonság:** az informatikai rendszer olyan állapota, amikor a rendszer rendeltetésszerűen működik és a rendszerben kezelt adatok bizalmassága, rendelkezésre állása, sértetlensége biztosított.
- **Informatikai biztonsági incidens:** az informatikai rendszerrel szemben olyan külső, vagy belső előre tervezett, szándékos károkozású, vagy nem szándékos cselekmény, melynek célja az AASzC kezelésében lévő adatok, dokumentumok és egyéb információk jogosulatlan megismerése, megszerzése, módosítása valamint további károkozással kapcsolatos felhasználása.
- **Informatikai biztonsági követelmények:** az informatikai rendszer használatával, üzemeltetésével és fejlesztésével kapcsolatos elvárások. Részterületei: a számítógépes biztonság, a kommunikációs biztonság, a kisugárzás biztonság és a rejtjelbiztonság. Informatikai biztonsági politika: a biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása meghatározott biztonsági feladatok irányítására és támogatására.
- **Informatikai biztonsági stratégia:** az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere.
- **Informatikai infrastruktúra:** az AASzC-hez kapcsolódó feladatokat ellátó, illetve a AASzC működését biztosító hálózatba kapcsolt hardverelemek, az azokon futó szoftverek és a rajtuk megtalálható adatok együttese, amely jól körülhatárolható, önmagában is működőképes, önálló szolgáltatás nyújtására képes infrastruktúra elemekből áll.

- **Informatikai rendszer:** a számítógépek és a hozzájuk kapcsolódó eszközök (hálózat), a számítógépeken futó programok, valamint a számítógépeken kezelt, feldolgozott adatok együttese.
- **Informatikai vészhelyzet:** az AASzC információs infrastruktúrájának leállása, szolgáltatások megszakadása, elérhetetlensége, az AASzC nemzeti információs vagyonának jelentős mértékű sérülése, illetve az ezekkel fenyegető rendellenes működés.
- **Információ:** bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti.
- **Információbiztonság:** az adatok és információk szándékosan, vagy gondatlanul történő jogosulatlan gyűjtése, károsítása, közlése, manipulálása, módosítása, elvesztése, felhasználása, illetve természeti vagy technológiai katasztrófák elleni védelmének koncepciói, technikái, technikai, illetve adminisztratív intézkedései. Az információbiztonság része az informatikai biztonság is, melynek alapelvei a bizalmasság, sértetlenség, rendelkezésre állás.
- **Információvédelem:** szervezeti, személyi, fizikai, informatikai és adminisztratív előírások kidolgozása és intézkedések végrehajtása az információbiztonság érdekében.
- **Jogosultság:** az arra felhatalmazott által adott hozzáférési lehetőség valamely információs infrastruktúrához.
- **Kockázat:** a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.
- **Kockázatelemzés:** az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.
- **Kockázattal arányos védelem:** az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.
- **Következmény:** valamely esemény, baleset, beavatkozás, vagy támadás hatása, amely tükrözi a belőle eredő veszteséget, valamint a hatás jellegét, szintjét és időtartamát. Külső felhasználó: az AASzC -vel szerződéses jogviszonyban álló magánszemélyek, jogi személyek és jogi személyiséggel nem rendelkező egyéb szervezetek és ezek alkalmazottai.
- **Mentés (biztonsági mentés):** biztonsági másolat készítése az informatikai rendszerben tárolt adatokról, adatállományokról, illetve az informatikai rendszerben használt alkalmazásokról. A másolat célja az elsődleges adattároló megsérülése esetén az adatok helyreállíthatóságának biztosítása.
- **Mobil eszköz:** asztali munkaállomásnak nem minősülő egyes informatikai és kommunikációs feladatok ellátására használható, operációs rendszerrel, kommunikációs szolgáltatásokkal rendelkező, hordozható elektronikus eszköz. Ide tartoznak: laptopok, notebookok, táblagépek, mobiltelefonok és okos telefonok.

- **Munkaállomás:** a felhasználó számára biztosított számítógép; lehet asztali vagy hordozható (laptop, notebook).
- **Napló:** az informatikai rendszerben bekövetkező eseményeket, felhasználói tevékenységeket és ezek időpontját rögzítő, a rendszer által automatikusan kezelt adatállomány, amely a változások észlelését és a számon kérhetőséget biztosítja.
- **Naplózás:** az informatikai rendszerben bekövetkező események, felhasználói tevékenységek és ezek időpontjának automatikus rögzítése a változások észlelése és a számon kérhetőség biztosítása érdekében.
- **Osztályozás:** adatok, információk, információs infrastruktúra elemek, információs infrastruktúrák biztonsági szempontból való osztályainak kialakítása és ez alapján osztályokba sorolása.
- **Program:** számítógépes nyelven megírt utasítássorozat. Állhat egyetlen programmodulból vagy programmodulok halmazából.
- **Rendelkezésre állás:** annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.
- **Rendszerelem:** információs infrastruktúra elem.
- **Sebezhetőség:** olyan fizikai tulajdonság, vagy működési jellemző, amely az adott információs infrastrukturális elemet egy adott veszéllyel szemben érzékennyé vagy kihasználhatóvá teszi.
- **Személyi biztonság:** az adott rendszerrel/erőforrással kapcsolatba kerülő személyekre vonatkozó, alapvetően a hozzáférést, annak lehetőségeit és módjait szabályozó biztonsági szabályok és intézkedések összessége a kapcsolat felvétel tervezésétől, annak kivitelezésén keresztül a kapcsolat befejezéséig, valamint a kapcsolat folyamán a személy birtokába került információk vonatkozásában.
- **Szervezeti biztonság:** egy adott szervezet strukturális felépítéséből adódó biztonsága és bevezetett biztonsági szabályainak és intézkedéseinek összessége a védendő rendszerhez/erőforráshoz való hozzáférés védelme érdekében.
- **Sértetlenség:** az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.
- **Szoftver:** a számítógép, az informatikai rendszer logikai elemei; a működtető programok (rendszerprogramok, operációs rendszerek) és a felhasználói programok (alkalmazások) összefoglaló neve.
- **Teljes körű védelem:** azon bármilyen típusú aktív, vagy passzív védelmi intézkedések, melyek a rendszer összes elemére kiterjednek.
- **Tesztrendszer:** olyan informatikai rendszer (környezet), amelynek célja a fejlesztés vagy bevezetés alatt álló program kipróbálásának, oktatásának támogatása.
- **Titkosítás:** az informatikai rendszerben kezelt adatok bizalmasságának biztosítására szolgáló, nem a minősített adat elektronikus biztonságának, valamint a

rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet hatálya alá tartozó olyan tevékenység vagy eljárás, amelynek során az adatot úgy alakítják át, hogy annak eredeti állapota a megismerésére illetéktelenek számára rejtve maradjon, de a megismerésre jogosultak számára az adat az eredeti formájába visszaállítható legyen.

- **Veszély (fenyegetés):** természeti vagy mesterséges esemény, személy, szervezet vagy tevékenység, amely potenciálisan káros a jelen szabályzatban védett tárgyakra.
- **Védelem:** a biztonság megteremtésére fenntartására, fejlesztésére tett intézkedések, amelyek lehetnek elhárító, megelőző, ellenálló képességet fokozó tevékenységek, vagy támadás, veszély, fenyegetés által bekövetkező kár kockázatának csökkentésére tett intézkedések.
- **Visszaállítás:** az eredeti infokommunikációs rendszer kiesése esetén a szolgáltatások további biztosítása, korábbi mentésből való visszaállítása.
- **Zárt védelem:** az összes számításba vehető fenyegetést figyelembe vevő védelem.

4. AZ INFORMÁCIÓBIZTONSÁG SZERVEZETI STRUKTÚRÁJA, FELELŐSSÉGI KÖRÖK

4.1. A kancellár feladatai

- Felügyeli az informatikai biztonsági feladatok ellátását, felelős azok betartásáért.
- Felelős a Centrum informatikai tevékenységének jogszerűségéért, beleértve az informatikai biztonsági tevékenységet is.
- Kivizsgáltatja az ellenőrzések során feltárt hiányosságokat, gondoskodik a jogszabálysértő körülmények megszüntetéséről.

5. 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 rendszerek osztályba sorolása ötfokozatú skálán történik, a rendszer funkciói és a kezelt adatok fajtájától függően kell a bizalmasság, a sértetlenség és a rendelkezésre állás szerinti követelményeket súlyozni. Az 1-től 5-ig terjedő fokozatokhoz emelkedő irányban egyre szigorodó védelmi intézkedések tartoznak, amiket az adott elektronikus információs rendszerre vonatkozóan meg kell valósítani.

A **bizalmasság** az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak és csak a jogosultságuk mértékéig ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról. A bizalmasság elsődlegesen a (különleges) személyes-, és üzleti adatokat kezelő rendszereknél lehet fontos, tehát minden olyan esetben, ahol nem szeretnénk, ha az információ illetéktelen kezekbe kerülne.

A **sértetlenség** az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanság) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható. A sértetlenség olyan rendszereknél lehet vezető szempont, ahol fontos, hogy a kezelt adatokat illetéktelenül senki ne változtathassa meg, pl. közhiteles nyilvántartások, de termelési környezetből is említhetők a különböző mérő-, érzékelő rendszerek.

A **rendelkezésre állás** az adat, illetve az elektronikus információs rendszer elemeinek olyan állapota, amelyben az az arra jogosultak által a szükséges időben és időtartamra használható. Azoknál a rendszereknél, ahol alapvető igény a működés fenntartása, pl. a létfontosságú termelő, szolgáltató rendszerek, a rendelkezésre állás esik nagy súllyal latba.
A rendszerek osztályba sorolása két részből áll, az első fázisban azt kell megállapítani, hogy az adott elektronikus információs rendszer a kockázatelemzés alapján melyik biztonsági osztályba tartozik (elvárt/tervezett biztonsági osztály). A biztonsági osztályok megállapítása a káresemények szempontjából8 a rendszer által kezelt adatok sérülésének és az ebből fakadó következmények, a szervezettel szembeni bizalomvesztés, illetve a közvetlen- és közvetett anyagi kár mértékének szintezésével történik. A jogszabályban megadott elvek szerinti besorolás alkalmazása nem kötelező, de más módszer használatánál is fel kell tüntetni az értékelési szempontokat.

A jogszabály lehetőséget ad a hiányosságok fokozatos megszüntetésére10, a teljesített biztonsági osztálytól a tervezett eléréséig minden egyes szint (biztonsági osztály) követelményeinek teljesítésére két év áll rendelkezésre. (A gyakorlatban: ha a rendszer elvárt biztonsági osztálya 4-es, de jelenleg csak a 2-es osztályhoz tartozó követelményeket teljesíti, úgy két éven belül kell elérnie a 3-as szintet, és újabb két éve van a 4-es szinthez tartozó követelmények kivitelezésére.)

A rendszerek osztályba sorolásának elvégzéséhez a **Nemzeti Kibervédelmi Intézet [OKFovi4602] Osztályba sorolás és védelmi intézkedés űrlap** alatti excel fájlban kell elvégezni.

Miután meghatároztuk a rendszer biztonsági osztályát, a **41/2015. BM rendelet védelmi intézkedések katalógusában alkalmazott 2.melléklet alapján** munkalapokon jelölni kell, hogy a rendszer teljesíti-e az adott részkövetelményt. A táblázat automatikusan jelzi, hogy a meghatározott osztálynál kötelező-e az adott követelmény teljesítése (0, N: nem kötelező, X, K: kötelező). Az itt felvitt adatok alapján az „Összegzés" munkalapra automatikusan átvezetődik, hogy a rendszer teljesíti-e a meghatározott osztályhoz tartozó követelményeket.

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.**

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.

6. 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.

6.1. 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.

6.2. 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.

7. 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.

7.1. 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.

7.2. 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.
- Amennyiben az IBSZ rendkívüli módosítása szükséges – a szükséges módosítás jellegétől vagy terjedelmétől függetlenül – az információs rendszer biztonságáért felelős személy közvetlenül jelzi ezt a Centrum vezetőjének.

7.3. 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.

7.4. Felhasználók feladatai

Általános felhasználók a Centrum foglalkoztatottjai (ideértve a gyakornokokat is).

A kiemelt felhasználók rendelkeznek az általános felhasználókhoz kapcsolódó jogokkal, valamint azon túlmenően a feladatkörüktől és a szakmai területtől függő további egyedi jogosultságokkal is. A kiemelt felhasználókat – az elektronikus információs rendszer biztonságáért felelős személy tájékoztatása mellett – a munkáltató jogokat gyakorló vezető, a szerződéskötést kezdeményező szervezeti egység vezetője jelöli ki.

A Centrumban valamennyi felhasználó – jogosultságtól és állományba tartozástól függetlenül –:

a) felelős az általa használt, az IBSZ hatálya alá eső eszközök rendeltetésszerű használatáért,
b) a rá vonatkozó szabályok szerint felelős az általa elkövetett informatikai vonatkozású szabálytalanságokért, valamint a keletkező károkért és hátrányért, különös tekintettel az informatikai biztonsági incidens fogalomkörébe tartozó cselekményekért,
c) köteles az IBSZ-ben megfogalmazott szabályokat megismerni és betartani, illetve ezek betartásában az informatikai rendszer használatát irányító személyekkel együttműködni,
d) köteles a számára szervezett informatikai biztonsági oktatáson részt venni, az ismeretanyag elsajátításáról számot adni,
e) köteles a rendelkezésére bocsátott számítástechnikai eszközöket megóvni,
f) köteles a belépési jelszavát (jelszavait) az előírt időben megváltoztatni, biztonságosan kezelni,
g) felügyelet nélkül a munkahelyen (munkaállomáson) személyes adatot vagy minősített adatot tartalmazó dokumentumot, adathordozót nem hagyhat,

h) információ biztonságot érintő esemény gyanúja esetén az észlelt rendellenességekről köteles tájékoztatni a közvetlen felettesét és elektronikus információs rendszer biztonságáért felelős személyt,
i) köteles a folyó munka során nem használt hivatalos adatokat, dokumentumokat, nem nyilvános anyagokat, adathordozókat elzárni,
j) köteles a munkahelyről történő eltávozáskor az addig használt – kivéve, ha ez a rendszer(ek) más által történő használatát, vagy a karbantartást akadályozza – eszközt szabályszerűen leállítani,
k) az elektronikus levelezés és az internet használat során tartózkodik a biztonság szempontjából kockázatos tevékenységektől.

7.5. A Centrum informatikai rendszerét használó valamennyi felhasználónak tilos:

a) az általa használt eszközök biztonsági beállításait megváltoztatni,
b) a saját használatra kapott számítógép rendszerszintű beállításait módosítani (ide nem értve az irodai programok felhasználói beállításait),
c) a munkaállomására telepített aktív vírusvédelmet kikapcsolni,
d) belépési jelszavát (jelszavait), hardveres azonosító eszközét más személy rendelkezésére bocsátani, hozzáférhetővé tenni,
e) a számítógép-hálózatot fizikailag megbontani, számítástechnikai eszközöket lecsatlakoztatni, illetve bármilyen számítástechnikai eszközt rácsatlakoztatni a hálózatra az informatikai rendszert üzemeltetők jóváhagyása nélkül,
f) a számítástechnikai eszközökből összeállított konfigurációkat megbontani, átalakítani,
g) bármilyen (kivéve rendszergazda által engedélyezett, oktatási célra használt) szoftvert installálni, internetről letölteni, külső adathordozóról merevlemezre másolni az elektronikus információs rendszer biztonságáért felelős személy engedélye, illetve az üzemeltető közreműködése nélkül, a munkaállomásokon nem a Centrumban rendszeresített, vagy engedélyezett szoftvereket (szórakoztató szoftverek, játékok, egyéb segédprogramok) installálni és futtatni,
h) online játékokat használni,
i) bármilyen eszközt számítástechnikai eszközökbe szerelni és használni,
j) az általa használt adathordozó (pl. CD, DVD, pendrive stb.) eszköz számítógépben hagyni a munkaállomásáról való távozás esetén,
k) ellenőrizetlen forrásból származó adatokat tartalmazó adathordozót az eszközökbe helyezni,
l) más szerzői, iparjogvédelmi, egyéb szellemi tulajdonhoz fűződő, vagy egyéb személyhez fűződő jogát vagy jogos érdekét sértő dokumentumokat, tartalmakat (zenéket, filmeket, stb.) az eszközökön tárolni, oda le-, illetve onnan a hálózatra feltölteni,
m) láncleveleket továbbítani, levélszemetet, továbbá azok mellékleteit, vagy linkjeit megnyitni,
n) rendszer biztonságáért felelős személy külön engedélye nélkül – feliratkozni, kivéve a munkavégzéshez szükséges:
    I. a Centrum által megrendelt, működtetett, vagy előfizetett szolgáltatásokat,
    II. belső információs rendszereket,
    III. közigazgatási, illetve nemzetközi, vagy uniós szervek/szervezetek által biztosított szolgáltatásokat,

IV. közigazgatási szervek által felügyelt szervek, vagy szervezetek által biztosított szolgáltatások levelező listáit.

A munkaállomás illetéktelen hozzáférés elleni védettségéért, a munkaállomáson végzett minden tranzakcióért a bejelentkezéstől a kijelentkezésig a bejelentkezett felhasználó a felelős. Ez a felelősség akkor is fennáll, ha a tranzakciókat harmadik személy hajtotta végre, amennyiben erre az IBSZ előírásainak felhasználó általi be nem tartása miatt kerülhetett sor.

Amennyiben a munkaállomást több személy is használhatja, a felhasználó a munkaállomást csak akkor hagyhatja el, ha minden futó programból, azonosított kapcsolatból és abban az esetben, ha nem egyedi felhasználói fiókos rendszer üzemel a számítógépen, az operációs rendszerből is kijelentkezett.

A felhasználó dokumentum nyomtatásakor köteles biztosítani, hogy az általa kinyomtatott irathoz illetéktelen személy ne férjen hozzá. Közös használatú hálózati nyomtató esetében a kinyomtatott iratot köteles a nyomtatóból eltávolítani, sikertelen nyomtatás esetén köteles meggyőződni – amennyiben szükséges, informatikus munkatárs segítségével – arról, hogy a nyomtató memóriájában nem maradt nyomtatandó dokumentum.

A felhasználó a rendelkezésére bocsátott, hordozható informatikai, irodatechnikai, multimédiás eszközt vagy adathordozót köteles megőrizni, az illetéktelen hozzáféréstől személyes felügyelettel vagy az eszköz, adathordozó elzárásával megvédeni.

8. 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.

A Centrum információbiztonsági fenyegetettségének elemzését és a kockázatok meghatározását évente el kell végezni. Az IBSZ-nek megfelelő működést igény szerint, de legalább évente teljes körűen ellenőrizni kell.

Az Informatikai Biztonsági Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

8.1. 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.

8.2. 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.

9. INFORMÁCIÓBIZTONSÁGI KÖVETELMÉNYEK TELJESÜLÉSE

9.1. Szervezeti biztonsági követelmények:

Az egyes informatikai rendszerekkel és adathordozókkal kapcsolatos fejlesztési, üzemeltetési és biztonsági tevékenységet úgy kell megtervezni és végrehajtani, a fejlesztési, működtetési és védelmi terveket, dokumentumokat, előírásokat úgy kell elkészíteni, hogy azok a biztonsági osztályozási előírások figyelembevételével garantálják az információbiztonság szükséges és elégséges szintjét. Ezen elvek alapján kockázatarányos, differenciált, többszintű informatikai védelmi rendszert kell kialakítani és működtetni.

9.2. Fizikai biztonsági követelmények:

Az informatikai eszközöket úgy kell telepíteni és tárolni, hogy azokhoz a foglalkoztatottakon kívüli más személy hozzáférése kizárt legyen.
A Centrum tulajdonát képező vagy az általa használt informatikai, irodatechnikai, multimédiás eszközt vagy adathordozót a Centrum objektumaiból kivinni csak hivatali feladat ellátására, a közvetlen vezető elektronikus írásbeli engedélyével (e-mail) lehet.

9.3. Informatikai biztonsági követelmények:

Az informatikai rendszerekben csak jogtiszta szoftver telepíthető. A hivatali feladatok ellátásához szükséges felhasználáson kívül informatikai, irodatechnikai, multimédiás eszközt vagy adathordozót az informatikai rendszerekhez csatlakoztatni tilos. Nem a Centrum tulajdonát képező informatikai, irodatechnikai, multimédiás eszközt az informatikai rendszerekhez vagy azok elemeihez csatlakoztatni tilos. Kivételt képeznek a Centrum alap- vagy funkcionális tevékenységével összefüggésben az együttműködő partnerektől hivatalos tevékenységük során átvett eszközök. A Centrum területén a Centrum által kezelt adatok védelmére vonatkozó rendelkezéseket vagy személyiségi jogokat sértő, továbbá a Centrum működésére vonatkozó magáncélú adatrögzítés – beleértve a hang- és képfelvétel készítését is – tilos. Az informatikai rendszerekben végrehajtott műveleteket a felhasználó azonosítását lehetővé tevő módon naplózni kell.

10. Az informatikai biztonsági események felismerése, jelentése

Minden felhasználó kötelessége – amennyiben kellő gondossággal eljárva azt felismerhette – a lehetséges legrövidebb időn belül közvetlen vezetőjének bejelenteni minden olyan

veszélyforrást, amely az elektronikus információbiztonságra nézve érdemi fenyegetést jelent vagy jelenthet.

10.1. A felhasználó részéről különösen a következő veszélyforrások jelzése kötelező:

a) az IBSZ-ben, a vonatkozó jogszabályokban előírt elektronikus információbiztonsági rendszabályok lényeges megszegése, illetve ennek gyanúja,
b) a felismert vagy felismerni vélt, az elektronikus információbiztonságot lényegesen veszélyeztető esemény, ezen belül különösen:
   I. nem nyilvános adat illetéktelen személy általi megismerése,
   II. informatikai rendszerekben tárolt adatok illetéktelen személyek általi megváltoztatása, törlése vagy hozzáférhetetlenné tétele,
   III. informatikai rendszer működésének, használatának jogosulatlan akadályozása,
   IV. nem engedélyezett vagy licenc-szel nem rendelkező szoftver telepítése, V. felhasználói jelszavak egymás közötti megosztása, hozzáférhetővé tétele, VI. vírusfertőzés, kémprogramok, billentyűzetleütést figyelő alkalmazások megjelenése,
   VII. mobil eszköz elvesztése, ellopása esetén,
   VIII. fentiek bármelyikére tett kísérlet (a továbbiakban együtt: biztonsági események).

Nem számít informatikai biztonsági eseménynek az informatikai hiba, meghibásodás vagy rendszeresemény, amely nem érinti az informatikai szolgáltatások minőségét és azt az üzemeltetők, képesek megoldani.

10.2. A bejelentés során minimálisan megadandó információk:

a) az informatikai biztonsági esemény pontos leírása,
b) érintett informatikai szolgáltatás pontos megnevezése,
c) érintett informatikai eszköz gyári száma, leltári száma, típusa,
d) tagintézmény neve, pontos címe (emelet, ajtó),
e) észlelő neve, elérhetősége (opcionális),
f) A vezető által kijelölt helyszíni kapcsolattartó neve, elérhetősége.

11. Biztonsági események kivizsgálása

A biztonsági eseményeket soron kívül ki kell vizsgálni. A vizsgálatot az elektronikus információs rendszer biztonságáért felelős személy folytatja le, szükség szerinti mértékben bevonva a Centrum központi szervezetét.

A vizsgálat eredményét az elektronikus információs rendszer biztonságáért felelős személy írásban dokumentálja, amelyből 1-1 példányt kap az elektronikus információs rendszer biztonságáért felelős személy, illetve a biztonsági eseményben közvetlenül érintett(ek).

12. Biztonsági események nyilvántartása

A biztonsági események kapcsán tett bejelentések, a lefolytatott vizsgálatok, valamint a végrehajtott intézkedések adatait külön nyilvántartás, a Biztonsági Nyilvántartás tartalmazza, amelyet az elektronikus információs rendszer biztonságáért felelős személy és a biztonsági vezető közösen vezet.

12.1. A Biztonsági Nyilvántartás adatait fel kell használni:

a) a bekövetkezett biztonsági esemény következményeinek enyhítésére,
b) a jövőben várható hasonló biztonsági események megelőzésére, bekövetkezési gyakoriságának csökkentésére

13. A biztonsági szabályok megszegésének következményei

Az informatikai biztonsággal kapcsolatos szabályok megszegése esetén a szabályszegőkkel szemben érvényesítendő jogkövetkezmények tekintetében elsősorban annak súlyosságára tekintettel vagy etikai, vagy munkáltatói fegyelmi jogkörben kell eljárni.

14. Azonosítás és feljogosítás az informatikai rendszer használatára

A felhasználó az informatikai rendszert csak egyértelmű azonosítást követően, a számára meghatározott és biztosított jogosultságok keretei között használhatja.

Az informatikai rendszer használata során a felhasználók egyértelmű azonosítását folyamatosan biztosítani kell.

Minden felhasználót kizárólagos személyi használatú egyedi azonosítóval kell ellátni, amelyhez minimálisan egyedi jelszót kell rendelni. További azonosítási lehetőségek is elfogadottak, melyek az elektronikus információs rendszer biztonságáért felelős személy engedélyével vezethetők be.

A felhasználók azonosítójának a felhasználói nevet tartalmaznia kell. Kivételt képeznek az operációs rendszerek különleges, előre rögzített azonosítói és a különleges informatikai feladatkört ellátók által használt speciális és teszt felhasználói nevek. A felhasználói névben törekedni kell a családi és utónév használatára, névazonosság esetén a felhasználónevek megkülönböztetésére.

14.1. A felhasználói jelszónak legalább az alábbi követelményeket teljesítenie kell:

a) legalább 6 karakter hosszú,
b) kis- és nagybetűket és számokat vegyesen tartalmaz,
c) nem tartalmazhat könnyen kitalálható, ismétlődő karaktersorozatot,
d) nem utalhat a felhasználó személyére,
e) érvényességi ideje legfeljebb 90 nap,

14.2. A jelszó megváltoztatása kötelező:

a) a felhasználói azonosító informatikai rendszerbe történt felvételét követő első bejelentkezéskor,
b) az informatikai üzemeltető szervezeti egység munkatársa általi újbóli jelszóbeállítást, felülírást követően,
c) ha a jelszó illetéktelen személy tudomására juthatott vagy bármilyen módon nyilvánosságra kerülhetett,
d) az érvényességi idő lejártakor.

A felhasználó köteles a jelszót bizalmasan őrizni, illetéktelenek általi megismerését kizárni.

Tilos a jelszót más által megismerhető módon feljegyezni, azt mással bármilyen formában közölni.

15. Szoftverek telepítése, internethasználat

A hálózathoz csatlakozó munkaállomásra csak a munkavégzéshez szükséges adatállományok, programok tölthetők le, illetve telepíthetők.

A hálózathoz csatlakozó munkaállomásra nem telepíthető, nem másolható – ideiglenesen sem –, illetve a belső hálózaton nem tehető közzé olyan adatállomány, információ, amely

a) jogszabályt sért, így különösen adatvédelmi, szerzői jogvédelmi, személyiségvédelmi előírásba ütközik,

b) a hálózat rendeltetésszerű működését, biztonságát veszélyezteti vagy veszélyeztetheti, így különösen annak erőforrásait indokolatlanul, vagy szándékosan túlzott mértékben, pazarló módon veszi igénybe.

Az internet felhasználása csak a Centrum ügymenete érdekének megfelelően kialakított és betartott szabályok alapján történhet.

Az internet-szolgáltatás minőségének szinten tartása és a Centrum érdekeinek biztosítása céljából a Centrum – az elektronikus információs rendszer biztonságáért felelős személy javaslatára vagy engedélyével – korlátozásokkal élhet. A korlátozások a következőkre terjedhetnek ki:

a) bizonyos fájl-típusok letöltésének korlátozása,
b) az alapvető etikai normákat sértő oldalak látogatásának tiltása,
c) a látogatható weboldalak körének behatárolása és a maximális fájl-letöltési méret korlátozása.

15.1. Felhasználók internet használatára vonatkozó általános szabályok:

a) csak a munkavégzéshez, szakmai tájékozottság bővítéséhez szükséges vagy általános tájékozottságot biztosító információt, segítséget nyújtó oldalak látogathatók,
b) tilos a jó ízlést, közerkölcsöt sértő, rasszista, uszító és más, a véleménynyilvánítás kereteit meghaladó oldalak szándékos látogatása, online játékok, fogadási oldalak

felkeresése, bármely tartalommal kapcsolatos magánvélemény kinyilvánítása (pl. privát blog és chat),
c) a felhasználók nem tölthetnek fel egyénileg – a felelős jóváhagyása nélkül – a Centrummal kapcsolatos adatot az internetre,
d) az internetről csak a munkavégzéshez szükséges adatállományok, táblázatok, tölthetők le, alkalmazások, programok nem,
e) a látogatott oldal nem szokványos működése (pl.: folyamatos újratöltődés, kilépés megtagadása, ismeretlen oldalak látogatására történő kényszerítés, ismeretlen program futásának észlelése, stb.) esetén a közvetlen technikai támogató segítségét kell kérni.

16. Elektronikus levelezőrendszer használata a központi munkaegységben

A Centrum foglalkoztatottai központi feladatainak végrehajtásához alkalmazott elektronikus levelezésben kizárólag az aaszc.hu végződésű, hivatali levelezési cím használható. Magán e-mail címről hivatali információt továbbítani tilos. A Centrum tevékenységével össze nem függő célra a hivatali postafiók, levelezési cím nem használható.

A levelezőrendszerek használata során a vírusvédelmi előírásokat folyamatosan érvényesíteni kell.

A hivatali levelezőrendszeren kizárólag hivatali célú üzenetek továbbíthatók. Magáncélú üzenetet nem nevesített felhasználóknak (pl. csoport, mindenki) küldeni tilos.

17. INFORMÁCIÓBIZTONSÁGI ELJÁRÁSOK

17.1. Általános irányelvek

Az egyes felhasználói azonosítókhoz rendelt jogosultságok minden esetben csak az adott munkakör, feladat ellátásához szükséges minimális funkcióelérést biztosíthatják.

A hozzáférési jogosultságok kezelését, a jogosultságigénylés folyamatának részleteit – annak kiadását követően – a jogosultságkezelési szabályzat tartalmazza.

A felhasználók a hozzáférésüket megalapozó jogviszonyuk létrejöttét követően (a lehető legrövidebb időn belül) megkapják felhasználói azonosítójukat.

17.2. Munkaállomások hozzáférésére vonatkozó minimális előírások

A számítógépes munkaállomások képernyőit (monitor) úgy kell elhelyezni, hogy az azon megjelenő információkat illetéktelen személy ne láthassa.

A munkaállomás beállításait adminisztrátori jelszóval kell védeni módosítás ellen.

Szenzitív adatbázisokat és programokat – amennyiben megoldható – hardveres azonosítást biztosító eszközzel kell védeni.

17.3. Szoftvereszközök használatának szabályozása

Az informatikai biztonság teljes körű megvalósításához hozzájárul a jogtiszta szoftverek és a szoftvereszközök jogszerű használata, valamint a szoftverek biztonságos kezelése.

A Centrum által használt szoftvereket az elektronikus információs rendszer biztonságáért felelős személy ellenőrizheti.

A rendszeres szoftvervizsgálat során ellenőrizni kell:

a) a használatban lévő szoftverek rendelkeznek-e licence-szel (ide nem értve az engedélyezett freeware szoftvereket),
b) a megvásárolt licencek száma arányos-e a használt szoftverek mennyiségével,
c) a használt szoftverek verziószámát,
d) a ténylegesen használt szoftverek megegyeznek-e az engedélyezett szoftverek listájával.

A szoftvereszközök telepítésére és használatára vonatkozó általános szabályok:

a) a Centrum munkaállomásaira csak eredményesen tesztelt szoftverek telepíthetők,
b) tilos a munkaállomásokra licence-szel nem rendelkező vagy a kereskedelmi forgalomban beszerezhető nem engedélyezett vagy nem a Centrum által fejlesztett szoftvert telepíteni,
c) a Centrum által vásárolt és kifejlesztett szoftverek (és a hozzájuk tartozó dokumentumok) másolása és átadása harmadik fél részére tilos, kivéve, ha a licencszerződés ezt külön szabályozza és lehetővé teszi,
d) a felhasználók csak a Centrum által telepített szoftvereket, ide értve az engedélyezett freeware szoftvereket is használhatják
e) a felhasználók rendelkezésére bocsátott hardver és szoftver eszközök ellenőrzését az elektronikus információs rendszer biztonságáért felelős személy bejelentés nélkül bármikor kezdeményezheti.

17.4. Mobil IT tevékenység, hordozható informatikai eszközök használata

A mobil eszközök használatával kapcsolatban a következő biztonsági eljárásokat kell alkalmazni:

a) a mobil eszközök átvételéhez átadás-átvételi dokumentumokat kell készíteni; (3.sz. melléklet)
b) valamennyi hordozható személyi számítógépet rendszeres szoftver-, adat- és biztonsági ellenőrzéseknek kell alávetni. Rendszeres időközönként (lehetőleg fél évente) a munkahelyi hálózatához kell csatlakoztatni az eszközt. Biztonsági másolatot kell készíteni, ezeket felkell jegyezni és nyilván kell tartani.

Rendszer biztonsági és vírusvédelmi frissítéseinek végrehajtása érdekében. A mobil eszközt szállító felhasználók:

I. kötelesek azt a szállítás idejére lehetőleg minél kevésbé szem előtt lévő módon elhelyezni,
II. nem hagyhatják őrizetlenül gépjárműben,
II. repülés vagy vonatút, valamint autóbuszon történő utazás ideje alatt kézipoggyászként kötelesek szállítani.

Azokban az esetekben, amikor az eszközök nem a Centrum épületeiben (szálloda, lakás) találhatók, fokozott figyelmet kell szentelni a jogosulatlan hozzáférés, az adatok esetleges módosítása, megrongálása vagy ellopása elleni védelemnek.

Tilos a mobil eszközök:
a) engedély nélküli átruházása vagy adatainak közlése, lementése,
b) megfelelő védelem nélkül nem biztonságos hálózathoz csatlakoztatása, (pl. nyílt WIFI)
c) bármilyen indokolatlan veszélynek történő kitétele vagy nem rendeltetésszerű használata.

A Centrum adataiból csak azon adatokat szabad mobil eszközön tárolni:

a) amely adatokról központi biztonsági mentés készül,

b) amelyekkel kapcsolatban biztosítani lehet a jogszabályban vagy belső szabályban előírt adatbiztonságot és adatvédelmet.

18. 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.

18.1. 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.

18.2. 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.

19. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

19.1. Tervezés és előkészítés során előforduló veszélyforrások

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

19.2. A rendszerek megvalósítása során előforduló veszélyforrások

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

19.3. A működés és fejlesztés során előforduló veszélyforrások

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

20. Az informatikai eszközök környezetének védelme

20.1. 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.

20.2. 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.

20.3. 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

21. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

21.1. 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.

21.2. 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.

21.3. 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.

Az adathordozók biztonságos kezelése: Az adathordozók biztonságos kezelésének kialakításával megakadályozható az Alföldi ASzC magasabb szintű adatbiztonsági kategóriákba besorolt adatainak illetéktelen kézbe való kerülése.
Az alföldi ASzC tulajdonában lévő, magasabb szintű adatbiztonsági kategóriákba besorolt adatok tárolására használt adathordozókat egyedi azonosítóval kel ellátni. Az adathordozóra tett címkén, az adattal dolgozó Alföldi ASzC alkalmazottnak fel kell tüntetnie az adott tartalomra vonatkozó bizalmassági kategóriákat. Kezelését ennek megfelelően kell megvalósítani.

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.

21.4. 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.

21.5. 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.

A vírusvédelmi eljárásokat, a vírusvédelemre vonatkozó szabályozást, beleértve az intézkedési rendet, úgy kell kialakítani, hogy az

a) a folyamatos vírusvédelmi felügyelet ellátását lehetővé tegye,
b) támogassa a valós riasztások kiszűrését,
c) alkalmas legyen a súlyos gondatlanságot, szándékosságot jelentő esetek felismerésére,
d) tegye lehetővé az általános vírusbiztonsági helyzet értékelését,
e) biztosítsa az új fenyegetések időben történő felismerését.

A hálózat esetében a vírusvédelem központilag biztosított.

A vírusvédelmi előírások súlyos, szándékos vagy sorozatos megsértése rendkívüli információbiztonsági eseménynek (incidens) minősül.

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.

Incidensek priorizálása: a magas prioritású incidesnek kivizsgálását és elhárítását azonnal meg kell kezdeni.

- Határsértés, és illegális tevékenység észlelése (behatolás).
- Vírus-vészhelyzet (tömeges fertőzés), vagy központi vírusvédelmi eszköz kiesése.
- Adminisztrátori jogosultságok sérülése.
- Kritikus rendszer, vagy rendszer elemek kiesése.
- „Titkos" információk bizalmasságának, sértetlenségének elvesztése.

Közepes prioritású incidensek: Az incidensek kivizsgálását azonnal meg kell kezdeni, ha az egy magas prioritású incidens elhárítása nem akadályozza.

- Ismétlődő vírusfertőzés, vagy vírusdefiníciós állomány nem frissülése.
- Felhasználói jogosultságok sérülése.
- Kiemelten fontos rendszer, vagy rendszer elemek kiesése.
- „Bizalmas" információk bizalmasságának, sértetlenségének elvesztése.

Alacsony prioritású incidensek: Az incidensek kivizsgálását két órán belül meg kell kezdeni, ha az egy magasabb prioritású incidens elhárítása nem akadályozza.

- Egyszeri vírusfertőzés, vagy helyi vírusvédelmi eszköz kiesése.
- Fontos rendszer, vagy rendszer elem kiesése.
- Kisebb jogosultsági incidensek (felhasználó elfelejtette a jelszavát, vagy az lejárt, stb).

- Vírusvédelmi menedzsment eszközök kiesése.
- Törvénysértések.

Egyéb incidensek: Az incidensek kivizsgálását lehetőleg még a bejelentés vagy az észlelés napján, a folyamatban levő magasabb prioritású incidensektől függően kell megkezdeni.

- Nem fontos rendszer, vagy rendszer elem kiesése.
- Munkaállomás működésével kapcsolatos működési hibák.
- Szabály-, és eljárássértések.
- Felhasználói hibák.

Biztonsági incidensek kezelésének folyamata:
Incidens bejelentés bármely Alföldi ASzC informatikai eszközt használó, vagy üzemeltető Alföldi ASzC munkatársától illetve tanulótól érkezhet munkaidőben.

- A bejelentett incidensről szükséges minden rendelkezésre álló információt elkérni a felhasználótól/bejelentőtől. Minden vonatkozó információt rögzíteni kell. A bejelentéseket (pl. e-mail vagy telefon) minden esetben, a prioritásától függően minél hamarabb vissza kell igazolni
- Amennyiben az IT biztonsági rendszergazda vagy az általános rendszergazda saját hatáskörben meg tudja oldani a bejelentett incidenst, és a megoldódott incidenssel kapcsolatban a bejelentő 5 napon belül nem jelzett vissza az incidens megoldottnak tekinthető. A megoldódott incidensről a felhasználót/bejelentőt értesíteni kell.
- Amennyiben az IT biztonsági rendszergazda vagy az általános rendszergazda saját hatáskörben nem tudja megoldani a bejelentett incidenst, prioritástól függően azonnal értesíteni kell a helyi IT biztonsági felelőst. Ebben az esetben a probléma megoldására az adott helyi rendszergazdával együttműködve, megpróbálja a megfelelő megoldást kidolgozni.
- Amennyiben a probléma továbbra sem oldódik meg, a probléma szélesebb eszkalálása szükséges. Ebben az esetben a probléma további megoldására az IT biztonsági és az általános rendszergazdákkal együttműködve, külső szakértő vagy a rendszer szállítójának bevonásával megpróbálja a megfelelő megoldást kidolgozni.
- Ha eddig a pontig eljutva nem sikerül megoldást találni a problémára, akkor az IT biztonsági felelőse javaslatot tesz az Alföldi ASzC Kancellárja részére.

22. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

22.1. 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.

22.2. 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.
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.

23. 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.

24. Záró rendelkezések

Jelen szabályzat 2022. 07. 06. lép hatályba. A tárgyra vonatkozó minden szabályozás hatályát veszti.

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

Csongrád, 2022.07.06.

Dr. Horváth József
főigazgató

Vári László
kancellár

1. 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 **Dokumentálási követelmények**	A belépések naplózása	A kulcs felvételénél kell dokumentálni.	A felügyeleti eszközök jelentéseit naplózni kell.

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.melléklet:Átadás-átvételi jegyzőkönyv

ALFÖLDI AGRÁRSZAKKÉPZÉSI CENTRUM

Átadás-átvételi jegyzőkönyv

Informatikai eszköz, telefonkészülék átadásáról

Amely létrejött egyrészről:

Szervezeti egység neve: .....

Felhasználó / rendszerüzemeltető neve.....

mint átadó, másrészről:

Alulírott.....(név):

sz.ig.szám:.....

Születési év:..... lakcím:.....

e-mail cím, tel.szám:.....

mint átvevő között.

A mai napon átadásra került(ek) az alábbi informatikai eszköz(ök), telefonkészülék(ek):

Megnevezés: .....

Típus: .....

Eszköz leltári száma: .....

Indoklás: .....
.....

Csongrád, ...

_____ _____

átadó átvevő

Megjegyzés:

.....

Felelősségvállalási nyilatkozat

Kijelentem, hogy teljes anyagi felelősséget vállalok az általam kizárólagosan, visszaszolgáltatási kötelezettséggel használatba vett átadás-átvételi jegyzőkönyvben feltüntetett megnevezésű és leltári számú eszközökért.

Amennyiben tőlem fenti eszközök valamelyikét eltulajdonítják vagy az balesetben, illetve egyéb káreseményben megsemmisül, vagy abban ilyen események következtében bármilyen hiány vagy károsodás keletkezik,

- megsemmisülés esetén az eszköz megsemmisülés időpontjában érvényes, az eszköz avulására tekintettel megállapított piaci árával-,

- károsodás esetén az eszköz kijavítására fordított kiadásnak –figyelembe véve a kijavítás ellenére még fennmaradó esetleges értékcsökkenés mértékét is –megfelelő összeggel,

Az Alföldi Agrárszakképzési Centrum felé teljes anyagi felelősséggel tartozom –leszámítva a kárnak azt a részét, amely az Alföldi ASzC esetleges közrehatása következtében állt elő -, kivéve, ha a kár elhárítása érdekében mindent megtettem, és az esemény elháríthatatlan volt.

Saját felelősségemre rendeltetésszerűen használom. Használat után az eszközöket sértetlen állapotban visszaszolgáltatom az Alföldi ASzC részére.

Ezen kötelezettség vállalás az eredeti átvétel időpontjától érvényes.

Dátum:

.....

aláírás

Készült 2 példányban:
1 pld. Kötelezettség vállaló
1 pld. Tárgyi eszköz nyilvántartó

4.számú melléklet: Üzemeltetési és munka napló 20..

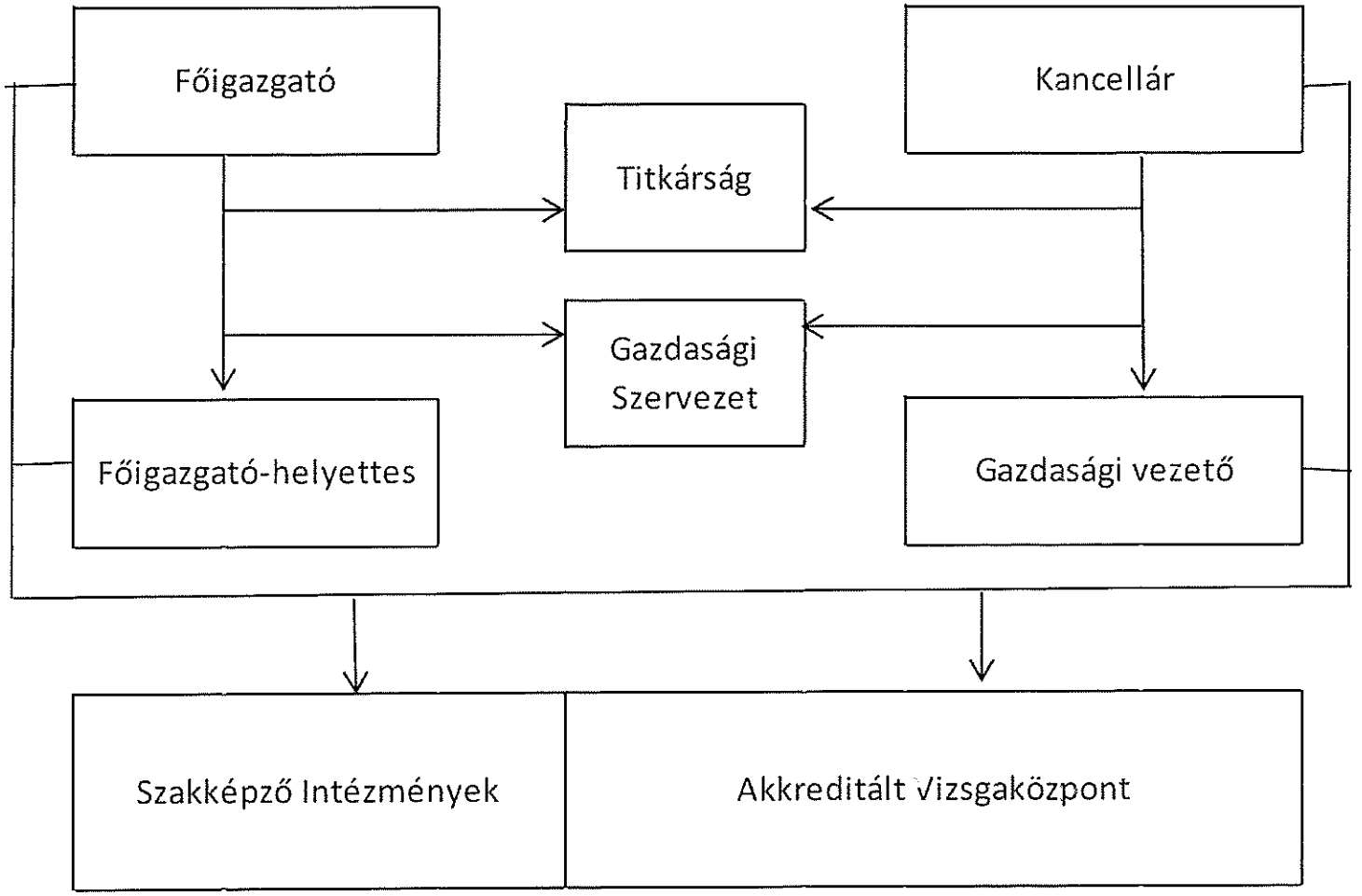
Üzemeltetési és munka napló 20

Ssz.	tól	ig	típus	feladatvégzés hely feladat megnevezése	jellege	érintett eszköz	felhasznált kellék vagy alkatré résztvevők	megjegyzés
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								
11.								
12.								
13.								
14.								
15.								
16.								
17.								
18.								
19.								
20.								
21.								
22.								
23.								

5.számú melléklet: Kockázatok felmérése

Típus	Fenyegetések	Fenyegetettség szintje	Előfordulás valószínűsége	Kockázati érték	Elfogadható minimum	Intézkedési terv	Megvalósítás kompetenciája
Funkciók veszélyeztetése	MINTA	6	10	60	25	MINTA	helyi
Kompromittálódás	MINTA	7	8	56	25	MINTA	központi
Engedély nélküli müveletek	MINTA	7	8	56	25	MINTA	helyi
Technikai meghibásodás	MINTA					MINTA	központi
Kritikus szolgáltatások kimaradása	MINTA					MINTA	helyi
Természeti csapás	MINTA					MINTA	központi
Fizikai kár	MINTA					MINTA	helyi
Sugárzás okozta károk	MINTA					MINTA	központi

6.számú melléklet: Szervezet topologikus ábrája:



7.számú melléklet: Biztonsági incidensek bejelentése:

Az Alföldi ASzC alkalmazottainak és tanulóinak az általuk észlelt, az Alföldi ASzC informatikai rendszerében keletkező biztonsági incidenseket be kell jelenteniük a helyi informatikai rendszergazdának.
A bejelentésre az alábbi információs csatornák állnak rendelkezésre:

Alföldi ASzC Intézménye	**Telefon**	**Email**
Központ		
Alföldi Agrár Vizsgaközpont		
Alföldi ASzC Bársony István Mezőgazdasági Technikum, Szakképző Iskola és Kollégium		
Alföldi ASzC Kenderesi Mezőgazdasági Technikum, Szakképző Iskola és Kollégium		
Alföldi ASzC Bethlen Gábor Mezőgazdasági és Élelmiszeripari Technikum, Szakképző Iskola és Kollégium		
Alföldi ASzC Kétegyházai Mezőgazdasági Technikum, Szakképző Iskola és Kollégium		
Alföldi ASzC Bedő Albert Erdészeti Technikum, Szakképző Iskola és Kollégium		
Alföldi ASzC Kiss Ferenc Erdészeti Technikum		
Alföldi ASzC Fodor József Élelmiszeripari Technikum és Szakképző Iskola		
Alföldi ASzC Bartha János Kertészeti Technikum és Szakképző Iskola		
Alföldi ASzC Gregus Máté Mezőgazdasági Technikum és Szakképző Iskola		
Alföldi ASzC Galamb József Mezőgazdasági Technikum és Szakképző Iskola		