Ikt.: C/2753-1/ 2019.

CELLDÖMÖLKI KÖZÖS ÖNKORMÁNYZATI HIVATAL

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Alkalmazás: 2019. január 1-től érvényes: visszavonásig

Tartalomjegyzék

Dokumentum változások története

Verzió	Dátum	Változás leírása	Készítette/Módosította
1.0	2013.07.01.	1. verzió	Némethné Berki Veronika
2.0	2018.07.01.	2. verzió	Némethné Berki Veronika
3.0	2019.01.01	3. verzió	Némethné Berki Veronika

Bevezetés

A Celldömölki Közös Önkormányzati Hivatal (továbbiakban: Hivatal) Informatikai Biztonsági Szabályzatát (továbbiakban IBSZ) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, az információs önrendelkezési jogról és az információszabadságról szóló a 2011. évi CXII. törvény, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény, a közszolgálati tisztviselőkről szóló 2011. évi CXCIX törvény, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII.15.) BM rendelet, továbbá Az önkormányzati ASP rendszerről szóló 257/2016. (VIII.31.) Korm. rendelet, valamint az államtitok és szolgálati titok számítástechnikai védelméről szóló 3/1988. (XI. 22.) KSH rendelkezés alapján a következők szerint határozom meg:

A szabályzat célja

Az Informatikai Biztonsági Szabályzat alapvető célja, hogy az elektronikus információs rendszerek alkalmazása során biztosítsa a Hivatalnál az információbiztonság követelményeinek az érvényesülését bizalmasság, sértetlenség és rendelkezésre állás szempontjából. A kockázatelemzésben feltárt informatikai biztonsági kockázatok bekövetkezésének valószínűségét csökkentse és a lehető leghamarabb szüntesse meg a bekövetkező káros esemény hatását. Az Informatikai Biztonságpolitikában meghatározott védendő értékek megőrzése érdekében csökkentse minimálisra a jogosulatlan hozzáférések, az adatok megváltoztatásának, törlésének, jogosulatlan nyilvánosságra hozatalának kockázatát.

Az Informatikai Biztonsági Szabályzat célja továbbá:

- az adminisztratív, fizikai és logikai biztonsági követelmények megvalósítása,
- az elektronikus információbiztonsággal kapcsolatos szerepkörök meghatározása,
- a szerepkörökhöz rendelt tevékenységek és felelősségek meghatározása,
- a kockázatelemzés során feltárt kockázati tényezők minimálisra csökkentése, a védelmi intézkedések betartása,
- az elektronikus információs rendszerek rendeltetésszerű használatának meghatározása,

- az ügymenet folytonosságának biztosítása az elektronikus információs rendszerek karbantartásával,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adathordozók fizikai és logikai védelme,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása, a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatok biztonsági mentésének, archiválásának menete,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása, az információbiztonság feltételeinek megteremtése,
- elektronikus információs rendszer beszerzésekor követendő információbiztonsági eljárásrend meghatározása,
- a titok-, munka, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- biztonsági esemény bekövetkezésekor követendő eljárásrend
- az Önkormányzati ASP rendszerrel kapcsolatos biztonsági követelmények.

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül, a felhasználásig, sértetlenség és rendelkezésre állás szempontjából, valamint az elektronikus információs rendszerekben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának a biztosítása a teljes életciklus alatt.

A jelen Informatikai Biztonsági Szabályzat az információvédelem általános érvényű előírását tartalmazza, meghatározza az információbiztonság adminisztratív, fizikai és logikai feltétel- és eszközrendszerét.

Az IBSZ az Ibtv.-ben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről kiadott 41/2015. (VII. 15.) BM rendelete által meghatározott összes területre kiterjed, ugyanakkor egyes biztonsági témakörökkel kapcsolatban csak az általános elvárásokat fogalmazza meg, míg a részletes szabályozás további dokumentumokban találhatók meg.

I. Adminisztratív védelmi intézkedések

1. Az Informatikai Biztonsági Szabályzat hatálya

1.1. Szervezeti-személyi hatály

Az IBSZ szervezeti hatálya kiterjed a Hivatal minden olyan szervezeti egységére, és ezen szervezeti egységben dolgozó fő- és részfoglalkozású dolgozójára, akik a Hivatal elektronikus információs rendszereit használják, kezelik, üzemeltetik, karbantartják, továbbá ezekkel kapcsolatos fejlesztési tevékenységben, vagy új elektronikus információs rendszer bevezetési projektjében közreműködnek. Az IBSZ személyi hatálya kiterjed a Hivatallal munkavégzésre irányuló bármely jogviszonyban álló természetes és jogi személyre. Külső szolgáltató és szerződéses felek esetén az IBSZ-ben foglaltakat érvényesíteni kell a velük kötött szerződésekben.

1.2. Tárgyi hatály

Az IBSZ tárgyi hatálya kiterjed a Hivatal adataival és adatainak kezelésével összefüggésben használt bármilyen adatrögzítésre, tárolásra, feldolgozásra, továbbküldésre alkalmas informatikai eszközre, annak működési környezetére, az eszközön lévő szoftver(ek)re, illetve a benne tárolt, feldolgozott, kezelt adatokra, információkra, külső szolgáltatótól igénybevett elektronikus információs rendszerekre, az önkormányzati ASP rendszerre, annak összes szakrendszerére.

1.3. Területi hatály

Az IBSZ területi hatálya kiterjed a Celldömölki Közös Önkormányzati Hivatal székhelyére:

- 9500 Celldömölk, Városháza tér 1.

valamint a hozzá tartozó kirendeltségekre:

- Celldömölk-Alsóság, Sági u. 167.
- Celldömölk-Izsákfa, Izsákfa u. 37.
- Mesteri, Kossuth utca 49.
- Nemeskocs, Petőfi utca 42.
- Ostffyasszonyfa, Kossuth L. utca 40.
- Mersevát, Dózsa György utca 39.

1.4. Időbeli hatály

Jelen Informatikai Biztonsági Szabályzat a Celldömölki Közös Önkormányzati Hivatal Jegyzője által történő jóváhagyása napján lép hatályba, és mindaddig érvényesnek tekintendő, amíg annak egy új változatát a Jegyző jóvá nem hagyja.

1.5. Az IBSZ alkalmazása

Az IBSZ belső dokumentum, megismerését a Hivatal érintett dolgozói részére az elektronikus információ rendszer biztonságáért felelős személy oktatás formájában biztosítja. Erről nyilvántartást vezet. (2. melléklet). Illetékteleneknek továbbadni szigorúan tilos!

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

1.6. A kötelező felülvizsgálat rendje

Az IBSZ-t az informatikában, a szervezet életében, folyamataiban, az információbiztonságban bekövetkező változások miatt évente aktualizálni kell. Új elektronikus információs rendszer bevezetése vagy a régi rendszerek működését meghatározó jogszabályi környezetben való jelentős változások azonnali IBSZ módosítást igényelnek.

Az Informatikai Biztonsági Szabályzat folyamatos karbantartása az elektronikus információ rendszer biztonságáért felelős személy feladata. A módosítások engedélyezése és az újabb változat jóváhagyása a Jegyző hatásköre.

1.7. Kapcsolódó dokumentumok

1.7.1. Jogszabályok

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (továbbiakban: Ibtv.)
- 257/2016. (VIII. 31.) Korm. rendelet az önkormányzati ASP rendszerről
- 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 elektronikus információs rendszerek meghatározásáról

- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről (továbbiakban: technológiai vhr)
- 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 (továbbiakban: képzési rendelet)
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Info tv.)
- 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről
- 2012. évi I. törvény a munka törvénykönyvéről
- 2012. évi C. törvény a Büntető Törvénykönyvről
- 2013. évi V. törvény a Polgári Törvénykönyvről
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
- 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról
- 146/1993. (X. 26.) Korm. rendelet a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény végrehajtásáról
- 1995. évi LXVI. törvény a közokiratokról, a közlevéltárakról, és a magánlevéltári anyag védelméről
- 1999. évi LXXVI. törvény a szerzői jogról

1.7.2. Kapcsolódó szabványok, ajánlások

- MSZ ISO/IEC 27002:2011: Az információbiztonság irányítási gyakorlatának kézikönyve
- MSZ ISO/IEC 27001:2006: Az információbiztonság irányítási rendszerei. Követelmények
- A KIB 25. számú ajánlása: Magyar Információbiztonsági Ajánlások (MIBA) 1.0 verzió
- A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások
- A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár

- Szolgáltatási szabályzat a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz (HSZSZ-ESZIG) v1.3
- Hitelesítési rend a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz (HR-ESZIG) v1.3
- Időbélyegzés Szolgáltatási Rend (ISZR) v1.2
- Szolgáltatási szabályzat a minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz (HSZSZ-M) v1.6
- Tájékoztatás az önkormányzati ASP rendszerhez csatlakozáshoz megvalósítandó informatikai biztonsági követelményekről 1.0 (2018. november 19.)

1.7.3. Belső dokumentumok

Az Informatikai Biztonsági Szabályzatot az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:

- Szervezeti és Működési Szabályzat,
- Iratkezelési szabályzat
- Leltározási szabályzat,
- Adatvédelmi, adatbiztonsági szabályzat,
- Informatikai Biztonságpolitika,
- Informatikai Biztonsági Stratégia,
- Selejtezési szabályzat.

2. Az információbiztonság során használt fontosabb fogalmak [1]

érintett: bármely meghatározott, személyes adat alapján azonosított, vagy – közvetlenül vagy közvetve – azonosítható természetes személy;

adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;

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

különleges adat: a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

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

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

adatkezelő: az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az adatkezelést végzi;

adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása

[1] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról,
2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása;

adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;

adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;

adatmegjelölés: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

adatzárolás: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése;

adatfeldolgozás: az adatkezeléshez kapcsolódó technikai feladatok elvégzése;

adatfeldolgozó: az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az adatkezelő részére adatfeldolgozást végez;

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

adatközlő: az a közfeladatot ellátó szerv, amely – ha az adatfelelős nem maga teszi közzé az adatot – az adatfelelős által hozzá eljuttatott adatait honlapon közzéteszi;

adatállomány: az egy nyilvántartásban kezelt adatok összessége;

adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;

auditálás: előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;

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;

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 esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;

biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége;

biztonsági osztályba sorolás: a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;

biztonsági szint: a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

biztonsági szintbe sorolás: a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

elektronikus információs rendszer: elektronikus információs rendszernek kell tekinteni az azonos adatkezelő és adatfeldolgozó által, egymással kapcsolatban álló eszközökön (környezeti infrastruktúra, hardver, hálózat), egymással összefüggő eljárásokkal (szabályozás, szoftver és kapcsolódó folyamatok) azonos célból kezelt, kiszolgált, illetve felhasznált adatok, az ezek kezelésére használt eszközök, eljárások, valamint az ezeket kezelő, kiszolgáló és felhasználó személyek együttesét.

elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

életciklus: az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;

észlelés: a biztonsági esemény bekövetkezésének felismerése;

felhasználó: egy adott elektronikus információs rendszert igénybe vevők köre;

fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;

folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;

globális kibertér: a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese;

informatikai biztonságpolitika: a biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására;

informatikai biztonsági stratégia: az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere;

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;

kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez;

kibervédelem: a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését;

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;

kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;

kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;

korai figyelmeztetés: valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;

létfontosságú információs rendszerelem: az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné

válása vagy megsemmisülése az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené;

logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;

magyar kibertér: a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne;

megelőzés: a fenyegetés hatása bekövetkezésének elkerülése;

reagálás: a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;

rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

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;

sérülékenység: az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

sérülékenységvizsgálat: az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;

számítógépes incidenskezelő központ: az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)];

szervezet: az adatkezelést vagy adatfeldolgozást végző jogi személy, valamint egyéni vállalkozó;

teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;

üzemeltető: az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

védelmi feladatok: megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;
zárt célú elektronikus információs rendszer: jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer;
zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.

3. Az elektronikus információbiztonsággal kapcsolatos szerepkörök és felelősségek

3.1. Általános felelősségek meghatározása

A Hivatal minden munkatársa, valamint a szerződésben lévő külsős szolgáltatók, és természetes személyek felelősek az IBSZ betartásáért, betartatásáért, valamint a Hivatal minden munkatársa köteles elősegíteni és támogatni az IBSZ-ben előírt belső ellenőrzések sikeres megvalósítását, és tudomásul venni, hogy az elektronikus információ rendszer biztonságáért felelős személy bejelentés nélkül ellenőrizheti az információbiztonság megvalósulását, a kapcsolódó szabályzatok, eljárásrendek betartását.

3.2. Elektronikus információbiztonsággal kapcsolatos szerepkörök, felelősségek

Az állami és önkormányzati szervek elektronikus információbiztonságáról 2013. évi L. törvény alapján kötelezően meghatározott feladatkörök és felelősök a következők: jegyző, elektronikus információ rendszer biztonságáért felelős személy, informatikus, adatgazda, továbbá a szervezeti egység vezetője, munkavállalók.

3.2.1. A Jegyző feladatai, felelőssége

A Jegyző gondoskodik az elektronikus információs rendszerek védelméről a következők szerint:

- biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
- biztosítja a Hivatalra irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
- az elektronikus információs rendszer biztonsági osztálya és a Hivatal biztonsági szintje alapján előírt követelményeknek megfelelően az elektronikus információs rendszer

biztonságáért felelős személyt nevez ki vagy bíz meg, aki azonos lehet a minősített adat védelméről szóló 2009. évi CLV. törvény szerinti biztonsági vezetővel,

- kiadja a Hivatal elektronikus információs rendszereire vonatkozó informatikai biztonságpolitikáját,
- meghatározza a Hivatal elektronikus információs rendszereinek informatikai biztonsági stratégiáját,
- meghatározza a Hivatal elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,
- gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a Hivatal munkatársai információbiztonsági ismereteinek szinten tartásáról,
- rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a Hivatal elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
- gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
- biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,
- ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
- ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy a jelen IBSZ-ben foglaltak szerződéses kötelemként teljesüljenek,
- felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,
- megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.
- A Jegyző köteles együttműködni a jogszabályban meghatározott hatóságokkal. Ennek során
    - az elektronikus információ rendszer biztonságáért felelős személy személyéről tájékoztatást nyújt,
    - Hivatal informatikai biztonsági szabályzatát tájékoztatás céljából megküldi,

- biztosítja a jogszabályokban meghatározott hatóságok részére az ellenőrzés lefolytatásához és a biztonsági incidensek kivizsgálásához szükséges feltételeket.

A Jegyző felelőssége:

A Jegyző felelős a Hivatalban az Ibtv. által előírt biztonsági szintnek és biztonsági osztályoknak megfelelő információbiztonsági intézkedések megvalósulásáért, illetve az ezek végrehajtásához szükséges erőforrások biztosításáért.

3.2.2. Az Elektronikus információ rendszer biztonságáért felelős személy feladatai, felelőssége

A Jegyző egy, az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg, aki ellátja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (Ibtv) meghatározott feladatokat. Ezen személy, azaz az Elektronikus információ rendszer biztonságáért felelős személy információbiztonság ellenőrzésével és irányításával kapcsolatos feladatai a következők:

- gondoskodik a Hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
- elvégzi vagy irányítja az előző pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
- előkészíti a Hivatal elektronikus információs rendszereire vonatkozó informatikai biztonságpolitikát és az informatikai biztonsági szabályzatot,
- javaslatot tesz a Hivatal Informatikai Biztonsági Stratégiájának tartalmára,
- előkészíti a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,
- véleményezi az elektronikus információs rendszerek biztonsága szempontjából a Hivatal e tárgykört érintő szabályzatait és szerződéseit,
- kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.
- koordinálja a Hivatal valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködőket, ha a Hivatal adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők, az IBSZ hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

- évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását, rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,

Az Elektronikus információ rendszer biztonságáért felelős személy az IBSZ-ben foglaltak betartása/betartatása érdekében jogosult:

- külön engedély nélkül a Hivatal bármely helyiségébe belépni, amennyiben ott az információbiztonságot érintő munkavégzés folyik,
- bármelyik számítógép, adathordozó vagy számítógépes lista tartalmába betekinteni, függetlenül annak minősítésétől (a vonatkozó jogszabályok betartásával), amennyiben az adott ügyben, illetve témában vizsgálat folyik,
- a Jegyzőnek az információbiztonsággal kapcsolatos kérdésekben javaslatokat tenni.
- Információbiztonsági kérdésekben közvetlenül a Jegyzőnek tartozik beszámolási kötelezettséggel.

Az Elektronikus információ rendszer biztonságáért felelős személy felelőssége:

Az Elektronikus információ rendszer biztonságáért felelős személy felelős a Hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtésére és fenntartására.

3.2.3. Az informatikus feladatai, felelőssége

Az informatikusnak az információbiztonság megvalósításával kapcsolatos feladatai a következők:

- az elektronikus információs rendszerekről naprakész nyilvántartást vezet és karbantartja azt;
- gondoskodik a Hivatal elektronikus információs rendszereinek ügymenet-folytonos üzemeltetéséről,
- felelős az informatikai rendszerek üzembiztonságáért, biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újraindíthatóságáról,
- feladata az informatikai/védelmi eszközök működésének, szerviz ellátás biztosításának folyamatos ellenőrzése,
- gondoskodik a kellékanyagok, szükség esetén az alkatrészek beszerzéséről,
- felelős a Hivatal hardver eszközeinek karbantartásáért, az informatikai eszközök rendeltetésszerű üzemeltetéséért,

- köteles gondoskodni a feldolgozások igényeinek megfelelő adathordozók biztosításáról, beleértve a biztonsági másolatok eszközigényeit,
- ellenőrzi a vásárolt szoftverek helyes működését, vírusmentességét, a használat jogszerűségét,
- a vírusvédelemmel foglalkozó szervezetekkel kapcsolatot tart,
- rendszeres időközönként vírusellenőrzést tart a teljes rendszerben,
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött munkaállomások leválasztásáról, és vírusmentesítéséről,
- tevékenységéről rendszeresen beszámol a Jegyzőnek, az információbiztonságot érintő kérdésekben pedig az elektronikus információ rendszer biztonságáért felelős személynek,
- a Jegyzővel, az elektronikus információ rendszer biztonságáért felelős személyvel együttműködve kialakítja és működteti a hozzáférési jogok rendszerét.
- Az informatikus felelős az információbiztonság fenntartásáért a felügyeletére bízott elektronikus információs rendszerekben, a jelen Informatikai Biztonsági Szabályzatban leírtaknak megfelelően.

Az Informatikus felelőssége:

Az Informatikus felelőssége a jelen Informatikai Biztonsági Szabályzat elektronikus információs rendszereinek és a Hivatal hardver eszközeinek naprakész nyilvántartása, üzemeltetése, az Informatikai Biztonsági Szabályzatban foglaltak szerinti információbiztonság betartásával.

3.2.4. Az adatgazda feladatai, felelőssége

Az adatgazda annak az önálló szervezeti egységnek a vezetője, ahol az adat keletkezik, illetve amelyhez jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését vagy nyilvántartás vezetését elrendeli.

Az adatgazda információbiztonsággal kapcsolatos feladatai a következők:

- a jelen IBSZ 8. melléklete alapján biztonsági osztályba sorolja az általa kezelt adatokat, illetve elektronikus információs rendszereket; (9. melléklet)
- meghatározza az adatokhoz / tevékenységekhez hozzáférőket, a szükséges-elégséges hozzáférési elv alapján, azaz mindenki csak annyi jogot kapjon, amennyi a munkája elvégzéséhez feltétlenül szükséges;
- a Jegyzővel egyeztetve engedélyezi vagy megtiltja a hozzáféréseket a hatáskörébe tartozó adatokhoz, elektronikus információs rendszerekhez, amelyet a felhasználói jogosultság és változás nyilvántartó lapon átad az informatikusnak beállításra.

Az Adatgazda felelőssége:

Az Adatgazda felelős a hatáskörébe tartozó elektronikus információs rendszerek hozzáférési jogosultságainak – lehetőség szerint – a „szükséges, minimális jogosultságok" elve alapján történő engedélyezéséért.

3.2.5. A szervezeti egység vezetőjének feladatai, felelőssége

A szervezeti egység vezetőjének az információbiztonsággal kapcsolatos feladata és felelőssége a következő:

- gondoskodik arról, hogy az általa irányított szervezeti egység munkatársai megismerjék és betartsák a rájuk vonatkozó információbiztonsági előírásokat.

3.2.6. Munkavállalók felelőssége, feladatai

Eszközök, szoftverek védelme:

- A munkavállaló, azaz a felhasználó köteles az általa használt eszközöket és a szoftvereket rendeltetésüknek megfelelően használni. Köteles a tőle elvárható gondossággal eljárni az eszközök használata során, védeni azokat a rongálás vagy szándékos károkozástól.
- A felhasználó a rábízott eszközöket nem adhatja kölcsön harmadik személynek kockáztatva így az eszköz épségét, és az esetlegesen rajta lévő adatok bizalmasságát, sértetlenségét.
- A felhasználó bármilyen hibát vagy sérülést észlel, azonnal jelentenie kell az informatikusnak.
- A felhasználó a használatába adott eszközökön csak a munkavégzéséhez szükséges feladatokat végezheti, magán célokra nem használhatja azt. Tilos az eszközök személyes haszonszerzés, illetve nem a hivatal érdekében történő használata. Tilos a politikai (a hivatali feladatokon kívüli) vagy erkölcsi, vagy más törvénybe, vagy jó erkölcsbe ütköző anyagok készítése, tárolása, közlése, megjelenítése a hivatal eszközein. Az eszközöket a hivatal helyiségeiből csak külön engedéllyel szabad kivinni.
- Minden felhasználónak bizalmasan kell kezelnie valamennyi felhasználói azonosító, jelszó, eToken, kulcs, vagy bárminemű egyéb, a Hivatal erőforrásaihoz hozzáférést biztosító eszközt.
- A Hivatalban az alkalmazottak csak a Hivatal tulajdonát képező számítógépeket és engedélyezett szoftvereket használhatják. Ettől eltérni csak az elektronikus információ rendszer biztonságáért felelős személy vagy az informatikus engedélyével lehet.

- Az informatikust kivéve, tilos a Hivatal számítógépeire szoftvereket telepíteni, és azokat futtatni.
- Kizárólag a munkavégzéshez szükséges adathordozók használata engedélyezett.

Adatvédelem, információvédelem:

- Az eszközökön tárolt és használt adatok, információk védelmét bizalmasság, sértetlenség és rendelkezésre állás szempontjából azok keletkezésének, feldolgozásának, szétosztásának, tárolásának és selejtezésének teljes folyamata, életciklusa során biztosítani kell.
- Valamennyi felhasználó köteles azonnal értesíteni felettesét minden olyan körülményről, amely az informatikához kapcsolódó tevékenység fennakadásához, megszakadásához vezethet, vagy olyan adatokhoz fér hozzá, amelyek kezelésében nem illetékes, a hibát azonnal jeleznie kell az elektronikus információ rendszer biztonságáért felelős személynek.
- Valamennyi információbiztonsággal kapcsolatos észrevételt vagy szabályszegésre vonatkozó feltételezést haladéktalanul jelenteni kell az elektronikus információ rendszer biztonságáért felelős személynek.
- A személyi azonosító kódokat, jelszavakat szigorúan titokban kell tartani. Még a közeli munkakapcsolatban álló, egymást jól ismerő kollégák sem közölhetik ezeket egymással. A hozzáférési kódok az informatikusnak sem adhatók ki.
- Az információbiztonsági hiányosságok megelőzése céljából a felhasználók kötelesek rámutatni az információbiztonsági szint romlására, illetve annak lehetőségére, és a tapasztalatokat a további problémák elkerülésében felhasználni.
- Az információbiztonságot veszélyeztető események kivizsgálására irányuló felülvizsgálatokban a felhasználó köteles együttműködni a kivizsgálókkal.
- A felhasználó számára büntetőjogi, illetve munkajogi felelősségre vonás terhe mellett tilos illetéktelenül más felhasználó jogosultságainak használata, a hálózat monitorozása, felderítése, jelszavak kipróbálása, illetve ezek kísérlete is.

3.2.7. Külső szolgáltatók igénybevétele

- Külső szolgáltatók igénybevétele esetén a szolgáltatási megállapodásokban (szerződésekben) kell kikötni a szolgáltatásra érvényes biztonsági követelményeket és szabályozást. Biztosítani kell a feladatért felelős szervezet számára a mérés és ellenőrzés feltételeit.

- Az informatikai rendszerek, eszközök bevezetése, üzemeltetése során harmadik felek különféle személyes, illetőleg bizalmas adatokhoz férnek hozzá. Ezen adatok védelméről gondoskodni kell.
- Külső szolgáltató csak egyedi esetben, meghatározott időre és meghatározott feladat ellátásához látható el jogosultsággal, a „szükséges, minimális jogosultságok" elve alapján.
- A szolgáltatási megállapodásokban ki kell térni a külső szolgáltató titoktartási kötelezettségére a Hivatal rendszereinek üzemeltetésével, fejlesztésével kapcsolatos, illetve a rendszerekben tárolt, feldolgozott adatok, információk vonatkozásában.
- Minden harmadik féllel kötött megállapodás esetében elvárásként kell megfogalmazni a jelen Szabályzatban foglaltak betartását. Ennek teljesítése érdekében informatikai tárgyú szerződést a Hivatal kizárólag az Információbiztonsági vezető jóváhagyásával köthet.
- Külső szolgáltató a Hivatal adatait és az elektronikus információs rendszereit a hozzáférést rögzítő szerződés és a jelen Informatikai Biztonsági Szabályzat 12. mellékletében található titoktartási nyilatkozat aláírása előtt nem ismerheti meg.

3.2.8. Külső szolgáltató hozzáférési kockázatának azonosítása

A Hivatalnak fel kell mérnie, és meg kell határoznia, hogy mekkora a kockázata annak, ha a harmadik félnek hozzáférési joga van a Hivatal információs vagyonához.

A kockázatok felmérése a jelen Informatikai Biztonsági Szabályzat 13. melléklete szerint történik. A kockázatkezeléshez, a megfelelő óvintézkedések kialakításához és a hozzáférések engedélyezéséhez a hozzáférés igénylésben pontosan meg kell határozni a hozzáférések típusát és azt, hogy milyen okból történik a hozzáférés.

A kockázat meghatározásért a harmadik féllel kötött szerződés teljesítésében elsődlegesen érintett szervezeti egység vezetője a felelős, és a szerződés megkötése előtt köteles az Elektronikus információ rendszer biztonságáért felelős személyt bevonni a szerződéskészítés folyamatába.

3.2.9. Belső együttműködés

Az információbiztonság szervezetrendszerének belső együttműködését a Hivatal a Szervezeti és Működési Szabályzatában rögzíti.

4. A védendő értékek meghatározása, az elektronikus információs rendszerek osztályozása

A Hivatal számára elsődleges az ügyfelek elégedettsége, személyes adataik maximális védelme bizalmasság, sértetlenség és rendelkezésre állás szempontjából. Továbbá védendő érték a szervezet egésze, a folyamatok során keletkező információk, adatok, bizalmasság, sértetlenség és rendelkezésre állás szempontjából, az azokat kezelő elektronikus információs rendszerek fizikai, logikai és adminisztratív szinteken, a sértetlenségük és rendelkezésre állásuk biztosításával.

4.1. 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,
- a személyhez fűződő és vagyoni jogokra.

4.2. A védelem eszközei

A mindenkori technikai fejlettségnek megfelelő szervezeti, műszaki, jogi intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

4.3. Informatikai vagyonleltár

A Hivatal elkészítette az eszköz és adatvagyon leltárát, meghatározta azok jelentőségét és értékét, és megállapította a hozzájuk kapcsolódó biztonsági szinteket. Az alábbi főbb kategóriákban határozta meg ezeket:

- eszközök, fizikai vagyon: szerver, számítógépek, laptopok, monitorok, nyomtatók, multifunkciós készülékek, projektorok, hangosító berendezések, mikrofonok, hálózati

telefonok, faxok, adathordozók, egyéb műszaki berendezések (tápegységek, légkondicionáló készülékek, porszívók, kávéfőzők, ventillátorok)

- szoftver vagyon: rendszerszoftver, alkalmazói szoftverek, irodai szoftverek
- adatvagyon: ügyféladatokat és belső szabályzóval ellátott adatokat tartalmazó adatállományok, adatbázisok, és ezek mentései, felhasználói segédletek, oktatási anyagok, dokumentációk, szabályzatok, eljárásrendek
- szolgáltatások: külső szolgáltatókkal kötött, szerződés alapján végzett informatikai, távközlési szolgáltatások.

A továbbiakban ezeket együttesen vagyonleltárnak nevezzük.

A vagyontárgyak nyilvántartása az erre rendszeresített elektronikus nyilvántartásokban történik. A nyilvántartást az informatikus készíti és gondoskodik napra kész állapotban tartásáról.

Az informatikai vagyontárgyakról vezetett nyilvántartást naprakészen kell tartani a vagyontárgy beszerzésétől kezdve egészen annak leselejtezéséig.

4.4. Biztonsági osztályba sorolás

A vagyonleltár alapján az adatokat, információkat és az elektronikus információs rendszereket jelentőségük, bizalmassági fokozatuk, sértetlenségük és rendelkezésre állásuk szerint osztályozzuk:

Adatok és információk:

- közlésre szánt, bárki által megismerhető adatok,
- személyes adatok,
- minősített, titkos adatok.

Elektronikus információs rendszerek:

- az elektronikus információs rendszerek biztonsági osztályba sorolását a jelen szabályzat 9. melléklete tartalmazza.
- Az Önkormányzati ASP rendszer ASP Központ által kiadott biztonsági osztályba sorolását a 14. melléklet tartalmazza.

4.5. A Hivatal biztonsági szintje

A Celldömölki Közös Önkormányzati Hivatal a 2013. évi L törvény alapján a 2. biztonsági szintbe tartozik, általános informatikai feldolgozást végez. Az egyes elektronikus információs rendszerek biztonsági osztályba sorolását a 8. melléklet, az önkormányzati ASP rendszer biztonsági osztályba sorolását pedig és 14. melléklet tartalmazza.

5. Az elektronikus információs rendszerekkel és a kezelt adatokkal kapcsolatos eljárásrendek

5.1. Kockázatelemzési és kockázatkezelési eljárásrend

Az információbiztonsági kockázatelemzés célja, hogy feltárja a Hivatal elektronikus információs rendszereire és az azokban kezelt adatokra ható fenyegető tényezőket, veszélyforrásokat, vizsgálja az elektronikus információs rendszer gyenge pontjait, elemzi a bekövetkező sikeres támadások bekövetkezési valószínűségét és az okozott kár nagyságát, valamint kezeli a Hivatal által el nem fogadható kockázatokat.

A Hivatal kockázatelemzési és kezelési módszertanát a 13. melléklet tartalmazza.

Az elektronikus információs rendszerekre az alábbi tényezők hatnak fizikai, logikai és adminisztratív szinteken, amelyek a rendszerben kezelt adatokat veszélyeztetik:

- a fizikai, környezeti infrastruktúra,
- a kommunikáció, a hálózat, a hardver elemek, az adathordozók, a szoftver elemek,
- a dokumentumok, nyilvántartások
- az adatokkal, a rendszerelemekkel kapcsolatba kerülő személyek.

Ezek a fenyegetések lehetnek:

- A fizikai, környezeti infrastruktúra veszélyforrásai: földrengés, árvíz, tűz, villámcsapás, katasztrófa, környezeti kár, a biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása.
- Közüzemi szolgáltatásba bekövetkező zavarok: feszültség-kimaradás, feszültségingadozás, elektromos zárlat, csőtörés, üzemzavar.
- Emberi tényezőre visszavezethető veszélyek:
    - Szándékos károkozás: fizikai behatolás, illetéktelen hozzáférés (adat, eszköz), adatok-eszközök eltulajdonítása, rongálás (gép, adathordozó), bosszúállás, illetéktelen használat, másolás, zavarás (feldolgozások, munkafolyamatok), adathordozók megrongálása.
    - Nem szándékos, gondatlan károkozás: figyelmetlenség, szakmai hozzá nem értés, szakképzetlenség, a jelszó gyakori megváltoztatásának az elmulasztása, illegális adathordozóval, másolattal vírusfertőzött adathordozó behozatala, biztonsági követelmények és gyári előírások be nem tartása.

- Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek: szakszerűtlen tervezés, dokumentáció hiánya, szakszerűtlen üzemeltetés, karbantartás, hibás adatrögzítés, adatelőkészítés, az hiányos ellenőrzés.
- Új információs rendszer bevezetése, megvalósítása során előforduló veszélyforrások: hibás adatállomány tesztelés során, helytelen adatkezelés, programtesztelés elhagyása.
- A működés és fejlesztés során előforduló veszélyforrások: emberi gondatlanság, megvesztegetés, szervezetlenség, szabályozatlanság, szakképzetlenség, szándékosan elkövetett illetéktelen beavatkozás, illetéktelen hozzáférés, üzemeltetési dokumentáció hiánya, vírus, illetéktelen szoftverinstalláció.

5.2. Rendszer és szolgáltatás beszerzési eljárásrend

A fejlesztés vagy beszerzés kezdete előtt, az információs rendszerekre vonatkozó biztonsági kockázatokat elemezni kell, ez alapján meg kell határozni a vonatkozó biztonsági intézkedéseket. A biztonsági elvárásokat rögzíteni kell az ajánlatkérési dokumentációban, teljesítésük módját, megfelelőségét pedig értékelési szempontként kell meghatározni. A biztonsági követelmények elemzése és meghatározása a fejlesztés vagy beszerzés előtt az elektronikus információ rendszer biztonságáért felelős személy feladata. A berendezések megtervezésekor, kiválasztásakor és a beszerzése lebonyolításakor – összhangban a Hivatal hatályos szabályzataival, és az adott évre vonatkozó költségvetési tervével – a következő szempontokra kell figyelemmel lenni:

- technológiai elvárások (pl. biztonsági funkciók, terhelhetőség, skálázhatóság, kompatibilitás a meglévő infrastruktúrával, várható elavulás)
- funkcionális elvárások (jelenlegi felhasználói igények, jövőbeni növekedési
- installálás, üzembe-helyezés,
- bekerülési költség, elvárt haszon, üzemeltetési költség,
- garanciális, karbantartási és támogatási elvárások.

A szempontokat érvényesíteni kell – közbeszerzés esetén az ajánlati kiírásban és – a szállítóval kötött szerződésben is. A beszerzések lebonyolításakor törekedni kell az azonos, a piacon magas technikai színvonalat és megbízhatóságot jelentő, ismert gyártótól származó berendezések megvásárlására, mivel ez megkönnyíti az eszközök üzembe-helyezését, karbantartását és javítását. Csak olyan berendezéseket szabad megvásárolni, melyek karbantartása – a garanciális idő lejártát követően is – megoldható. A Hivatal az egyes berendezés típusokra (pl. számítógépek, nyomtatók, hálózati elemek)

karbantartási szerződést köthet, melyek garantálják, hogy a berendezés esetleges meghibásodása esetén azok javíthatósága biztosítható legyen.

5.2.1. Erőforrás igény felmérés

Az éves költségvetési tervezési folyamatban ki kell térni az elektronikus információs rendszerek biztonsági beruházásainak tervezésére, oly módon, hogy az a Hivatal költségvetésében elkülönítetten szerepeljen. A biztonsági beruházások tervezését az informatikai biztonsági stratégiai célok alapján kell elkészíteni. A tervezési dokumentumot az információbiztonsági felelős készíti el az informatikussal együttműködve. A tervezési dokumentumban legalább a következőket kell feltüntetni:

a) beruházás megnevezése;
b) beruházás indoka, célja, kezelt kockázat;
c) költség-hasznon elemzés;
d) a beruházás elhagyásának következményei (jogi, információbiztonsági kockázat).

Az információbiztonsági beruházások tervezését tartalmazó előterjesztést az információbiztonsági felelős terjeszti be a Jegyzőnek jóváhagyás céljából. A dokumentumot előzetesen ellen kell jegyeztetni az informatikussal.

A Jegyző a Hivatal költségvetési határozatába beépíti a beszerzés forrásait. Az eljárásrendet a beszerzési szabályzat tartalmazza, mely az elektronikus információs rendszer, és az ezekhez kapcsolódó szolgáltatások és információrendszer biztonsági eszközök beszerzésére vonatkozó szabályait fogalmazza meg.

5.2.2. Funkcionális biztonsági követelmények

A tervezés fázisában a Hivatalnak az információbiztonsági felelőssel együttműködve biztonsági osztályba kell sorolni a szállítandó rendszert.

Az információbiztonsági felelősnek a megállapított biztonsági osztály alapján meg kell határoznia a szállító felé a vonatkozó adminisztratív, fizikai és logikai védelmi intézkedéseket.

A szállító által teljesítendő védelmi intézkedéseket a szerződés mellékletévé kell tenni. A szállítónak dokumentált módon el kell készítenie a fentiekben meghatározott védelmi intézkedések alapján a szállítandó termék funkcionális biztonsági követelményeit, azaz ki kell fejtenie, hogy az adott

követelményt konkrétan hogyan, milyen módon teljesíti az általa szállítandó rendszer vonatkozásában.

Az információbiztonsági felelőssel el kell fogadtatni a funkcionális biztonsági követelményeket, anélkül a rendszer nem helyezhető éles üzembe.

A fentiek végrehajtása érdekében az információbiztonsági felelőst még a tervezés fázisában be kell vonni a projektbe.

5.2.3. Garanciális biztonsági követelmények

A biztonsági intézkedések fejtsék ki hatásukat, és teljesítsék a bennük közvetlenül megfogalmazott funkcionális követelményeket. A szállítóknak el kell készíteniük az intézkedések funkcionális leírását és tervét olyan részletességgel, amely lehetővé teszi az intézkedések elemzését és tesztelését (ideértve az intézkedést megvalósító összetevők közötti funkcionális interfészeket is). A szállítók az intézkedések szerves részeként szerepeltessék a kiosztott felelősségeket és speciális tevékenységeket annak érdekében, hogy amikor az intézkedéseket megvalósítják, azok folyamatosan és következetesen (azaz az informatikai célrendszer egészében) teljesítsék megkívánt feladatukat vagy céljukat, továbbá segítsék az intézkedések hatékonyságának javítását.

Az intézkedéseket oly módon dolgozzák ki, hogy nagy biztonsággal támogatni tudják azt, hogy az intézkedések összessége teljes, konzisztens és helyes.

5.2.4. Biztonsággal kapcsolatos dokumentációs követelmények

A szállítónak a következő dokumentumokat kell elkészítenie az átadás-átvétel előtt:

a) a szállítandó termék/fejlesztés biztonsági intézkedéseinek funkcionális biztonsági leírása;
b) adminisztrátori dokumentáció;
c) felhasználói dokumentáció.

Dokumentálás formai követelmények

Az elektronikus információ rendszer dokumentálása során az alábbi pontokban részletezett formai elemeket minden dokumentumban értelemszerűen kell szerepeltetni.

a) Dokumentum adatlap:
a. a Dokumentum címe,
b. tárgya,
c. fájl neve és verziója,
d. Dokumentum típusa,

e. Dokumentum verziószáma,
f. Dokumentum státusza,
g. Dátum,
h. Készítő, Ellenőr,
i. Verziószám,
j. Státusz,
k. Minősítés.

b) lapszámozás,
c) tartalomjegyzék,
d) tárgymutató.

Dokumentumok rendelkezésre állása

Az elektronikus információ rendszer dokumentációjának egy eredeti nyomtatott példányban és Microsoft Word vagy szerkeszthető és nyomtatható PDF formátumban elektronikus formában kell rendelkezésre állnia.

5.2.5. A biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelmények

Gondoskodni kell a biztonsággal kapcsolatos dokumentumok illetéktelenek elleni védelméről az elektronikus információ rendszer teljes életciklusa (létrehozás, módosítás, megsemmisítés) alatt.

A biztonsággal kapcsolatos dokumentumokat a következő szerepkörök ismerhetik meg:

a) fejlesztő;
b) informatikus;
c) az elektronikus információ rendszer biztonságáért felelős személy;
d) jegyző.

5.2.6. Fejlesztési szerződések biztonsági követelményei

A fejlesztést végző külső féllel megkötendő szerződésnek a következőket kell tartalmaznia:

Minden egyes, a Hivatal elektronikus információs rendszerével kapcsolatba kerülő fejlesztési vagy bővítési projektnél figyelembe kell venni a Hivatal érvényben lévő, vonatkozó szabályzatait, különös tekintettel az Informatikai Biztonsági Szabályzatra, annak tudomásul vételét és elfogadását a szerződésben rögzíteni kell.

Fejlesztett komponensek esetében a szerződésben rögzíteni kell, hogy a leszállított szoftver megfelelően biztonságos környezetben, auditálható körülmények között készült, így nem tartalmaz

kártékony kódot. Amennyiben mégis tartalmazna, és ebből adódóan a Hivatalnak bármilyen kára keletkezne, akkor azért a külső fél felelősséggel tartozik.

5.2.7. Rendszerkövetés (támogatás)

Az infokommunikációs rendszerhez a szállítónak szerződésben rögzített feltételek mellett az alábbi területeket magába foglaló támogatást kell nyújtania:

a) az infokommunikációs rendszerben felmerülő hibák javítása,
b) a Hivatal fejlesztési igényeinek ellátása,
c) az infokommunikációs rendszer futtató környezetének (operációs rendszer, adatbázis rendszerek) frissítése.

Minden egyes új verzióra kiterjedően a szoftver kód átadása a Társaság részére, vagy a kód letétbe helyezése közjegyzőnél olyan formában, hogy a támogató cég megszűnése esetén a kód a Hivatal számára hozzáférhető legyen.

A szerződésben rögzíteni kell a támogatás körülményeit (határidők, rendelkezésre állás, helyszíni vagy telefonos támogatás) is a megfelelő szolgáltatási szint biztosítására. A paraméterek pontos értékének meghatározása az infokommunikációs rendszer adatgazdájának és az informatikai üzemeltetésért felelős vezető feladata.

5.2.8. A védelem szempontjainak érvényesítése a beszerzés során

A fejlesztett termék csak a sikeres átadás-átvételt követően illeszthető be a Hivatal informatikai rendszerébe.

A sikeres átadás-átvétel feltétele

a) a jelen Informatikai Biztonsági Szabályzatban meghatározott dokumentációk Hivatal általi elfogadása,
b) a funkcionális biztonsági követelmények információbiztonsági felelős általi, tesztrendszerben történő ellenőrzése.

5.3. Üzletmenet folytonosságra vonatkozó eljárásrend

A Hivatal elektronikus információs rendszereinek folyamatos működése érdekében, valamint a rendkívüli helyzetek bekövetkezése során az alábbiakban leírtak szerint kell eljárni.

A Hivatal működésének folytonosságával kapcsolatos feladatok tervezése, irányítása, koordinálása, a szükséges erőforrások rendelkezésre állásának biztosítása a Jegyző feladata. A feladat keretében alapvetően biztosítja, hogy informatikai szolgáltatás kiesésével járó rendkívüli esemény esetén

- az informatikai szolgáltatás elfogadható időn belül és elfogadható adatveszteség mellett újraindítható legyen;
- az informatikai szolgáltatás kiesésének idejére azon kritikus fontosságú folyamatoknál, ahol ez indokolt a kieső informatikai szolgáltatás használata nélkül működtethető alternatív folyamat biztosítsa a szükséges minimális szinten a működést;
- a Hivatal működését érintő rendkívüli esemény esetén a Hivatal a szükséges tájékoztatási feladatokat szervezett módon végrehajtsa;
- az informatikai szolgáltatás újraindítását követően az ügyviteli folyamatok a normál működési szintnek megfelelően, a normál ügyviteli rend szerint folytathatók legyenek.

A fentieket figyelembe véve a vonatkozó kockázatokat szem előtt tartva a Hivatal informatikai rendszerei úgy kerültek kialakításra, illetve a külső szolgáltató által nyújtott informatikai szolgáltatásokra olyan rendelkezésre állási követelmények kerültek kikötésre, hogy azok költséghatékonyan támogassák a Hivatal feladatait, illetve az azok alapján az érintett ügyviteli folyamatokra levezethető rendelkezésre állási követelményeket.

A fenti követelmények érdekében számba vételre kerültek a Hivatal működését támogató informatikai szolgáltatások, a lehetséges rendkívüli események, amelyek alapján meghatározásra kerültek azok az intézkedések, amelyekkel csökkenthetők az informatikai szolgáltatások kieséséből származó kockázatok.

A meghatározott - informatikai szolgáltatás kiesésével járó - rendkívüli esemény bekövetkezése esetén végrehajtandó folyamat szükségességének meghatározásakor - az érintett ügyviteli folyamatok rendelkezésre állási követelményei mellett - figyelembevételre kerültek a Hivatal által használt informatikai rendszerek rendelkezésre állási képességei, illetve a külső féltől igénybe vett informatikai szolgáltatások esetén az azokra vállalt rendelkezésre állási paraméterek.

5.3.1. Mentések, helyreállítás, újraindítás

Az informatikában a legnagyobb értéket a számítógépen tárolt adatok jelentik. Ezek védelmében meghatározó jelentőségű a rendszeres biztonsági másolatok készítése, és azok megfelelő tárolása.

Rendszeres mentéseket kell készíteni a legalább 2-es biztonsági osztályba sorolt elektronikus információs rendszerről, ha annak tárolása a helyi hivatali szerveren van. Internetes elérésű

elektronikus információs rendszerek esetén – külső szolgáltató igénybevétele esetén – szerződésben kell meghatározni a mentések gyakoriságát.

A munkák során az automatikusan mentett dokumentumokon kívül létrehozott dokumentumok mentése az azt létrehozó munkatársak feladata.

A fontosabb file-okat tartalmazó adathordozókról hetente másolatot kell készíteni a szerveren erre a célra létrehozott helyre.

Szerver esetében az adatokat legalább 2 példányban kell menteni, és azokat egymástól fizikailag elkülönült helyiségben elzárt, a szerverterem tűzterétől elkülönülő térben, tűzbiztos helyen kell tárolni. A szerver mentését legalább hetente, illetve a hálózati aktív eszközökét a beállítás változtatásakor kell elvégezni.

A mentésből a rendszerek, a szoftverkörnyezet beállításainak, valamit a tárolt adatoknak teljes körűen visszaállíthatónak kell lennie a mentés pillanatának állapotára.

A mentett adatokhoz csak az arra jogosultak férhetnek hozzá, a Jegyző engedélyével.

5.4. Emberi tényezőket figyelembe vevő – személy-biztonság

5.4.1. Személybiztonsági eljárásrend

Az eljárásrend kiterjed a Hivatal teljes személyi állományára, valamint minden olyan természetes személyre, aki az érintett szervezet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. A munkaköri leírásokban meg kell határozni az általános és az adott munkakörhöz tartozó információbiztonsági feladatokat és felelősségeket, valamint tájékoztatást kell nyújtani arról, hogy milyen jogi felelősségük és kötelezettségük van az információbiztonsági előírások betartására vonatkozóan. A dolgozók információbiztonsági felelőssége vonatkozik az esetleges otthon végzett munkára, illetve a munkaidőn túli munkavégzésre is.

Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem a Hivatal munkatársa, az elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás, megkötése során kell, mint kötelezettséget érvényesíteni.

5.4.2. A munkaköri felelősség és az alkalmazás feltételei

Szabályzatokban, a munkakörökre vonatkozó feladat-leírásokban, a munkaköri leírásokban, kell rögzíteni az egyes munkakörökhöz tartozó feladatokat és felelősségi kört, a szükséges informatikai

jogosultságokat. Minden munkakörhöz csak a munkához feltétlen szükséges jogosultságokat kell megadni.

A Hivatalnak tájékoztatnia kell a dolgozókat arról, hogy milyen jogi felelősségük és kötelezettségük van az információbiztonsági előírások betartására vonatkozóan. A dolgozók információbiztonsági felelőssége arra az esetre is vonatkozik, ha nem a Hivatalban (pl. otthon), illetve a normál munkaidőn kívül dolgozik.

A munkahelyi vezető közvetlenül felelős azért, hogy az ellenőrzése alá tartozó felhasználók betartsák az Informatikai Biztonsági Szabályzat előírásait.

A Hivatal elektronikus információs rendszereit csak a jelen Informatikai Biztonsági Szabályzat 2. és 4. mellékletében található nyilatkozat és az ASP titoktartási nyilatkozat aláírása után lehet használatba venni.

5.4.3. A személyek ellenőrzése

A Hivatal az elektronikus információs rendszerhez való hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy megfelel-e a munkakör betöltéséhez szükséges feltételeknek és folyamatosan ellenőrzi annak fennállását. A vizsgálat magában foglalja az alábbiakat:

a) referenciák ellenőrzése,
b) a felvételre jelentkező életrajzának ellenőrzése a teljességre és pontosságra vonatkozóan,
c) a legmagasabb iskolai végzettség (szakképzettség) ellenőrzése,
d) nyelvtudást igazoló okiratok ellenőrzése,
e) hatóság által kibocsátott azonosító irat ellenőrzése,
f) erkölcsi bizonyítvány ellenőrzése.

Külső szerződő felek esetében az információ biztonsági felelős feladata az előzetes ellenőrzés elvégzése.

5.4.4. Munkavállaló belépésének információbiztonsági eljárásrendje

Új munkavállaló belépésekor a munkavégzéséhez szükséges eszközöket átadás/átvételi jegyzőkönyv aláírása ellenében biztosítja az Informatikus. A munkavállaló aláírásával igazolja, hogy az eszközöket működőképes állapotban vette át, és azt rendeltetésszerűen fogja használni. Biztosítani kell továbbá a hálózatba való belépéshez szükséges felhasználónevet és jelszót, valamint új felhasználói fiókot, e-mail fiókot.

Feladat	Felelős
Telefonszám biztosítása	Informatikus
Számítógép biztosítása	Informatikus
Hozzáférési jogok beállítása alkalmazásokhoz	Informatikus (alkalmazások esetében a jogosultságok beállítását az érintett szervezeti egységek vezetői igénylik)
e-mail cím kiosztása	Informatikus
Informatikai oktatások (felhasználói)	Informatikus
Informatikai biztonsági oktatás	Információ biztonsági felelős
Titoktartási nyilatkozat	Információ biztonsági felelős

5.4.5. Munkaviszony megszűnésének információbiztonsági eljárásrendje

A munkavállaló Hivatallal fennálló jogviszonyának megszűnése előtt köteles a használatában lévő eszközöket az informatikusnak átadni, aki megvizsgálja azokat, és visszavételi jegyzőkönyvben rögzítve igazolja, hogy az eszközök megfelelő állapotban kerültek leadásra. Az informatikusnak munkaállomás leadásakor ellenőriznie kell, hogy a felhasználó az átvételi elismervényben rögzített hardver-, szoftver specifikációval adja-e vissza azt. A munkavállaló által használt eszközökön lévő adatokról a rendszergazdának mentést kell készítenie, amit az irodavezető rendelkezésére kell bocsátania. Az irodavezető által megjelölt napon és órában az összes hozzáférési jogosultságot meg kell szüntetni, egyéni hitelesítő eszközeit vissza kell venni. A jogosultsági nyilvántartást aktualizálni kell. A felhasználó elektronikusan tárolt információit, e-mailjeit és egyéb általa létrehozott adatot menteni, archiválni kell az általa használt informatikai eszközről, szerver tárhelyről, illetve bármely egyéb adathordozóról. Az így archivált adatokat a törvényi előírásoknak megfelelően tárolni kell, illetve, ha szükséges a megadott idő után törölni a rendszerből.

A munkatársak kilépéséről az adott Irodavezető köteles értesíteni az elektronikus információ rendszer biztonságáért felelős személyt és az informatikust.

5.4.6. Fegyelmi intézkedések

A szabályok megszegéséről az észlelő haladéktalanul köteles tájékoztatni az elektronikus információ rendszer biztonságáért felelős személyt és a Jegyzőt, aki mérlegeli a tudomására jutott események súlyosságát.

A biztonsági előírások megsértőivel szemben fegyelmi felelősségre vonásra kerülhet sor, amelyet az elektronikus információ rendszer biztonságáért felelős személy által felterjesztett jelentés alapján a Jegyző kezdeményez. Az eljárás a jogszabályok és a Hivatal belső szabályai szerint történik.

5.4.7. Áthelyezések, átirányítások és kirendelések kezelése

A Hivatal vezetője értesíti a megfelelő munkavállalókat a jogviszonyváltozásról. Külső szerződő felek esetén az elektronikus információ rendszer biztonságáért felelős személy elvégzi a személy(ek) ellenőrzésére vonatkozó eljárást. Az Informatikus az engedélyek alapján logikai/fizikai hozzáférést biztosít az elektronikus információs rendszerhez. (3. melléklet) Áthelyezéskor – szükség esetén – elvégzi a megváltozott hozzáférési engedélyek módosítását vagy megszüntetését.

5.4.8. Viselkedési szabályok az interneten

Az internethez való kapcsolódás csak és kizárólag a munkavégzést szolgálja! A nem munkavégzést szolgáló hálózati sávszélesség foglalása és a nem a munkavégzéssel kapcsolatos adatok kiszolgálón való tárolása esetén a felhasználó figyelmeztetésben részesül. Ismételt előfordulása esetén az Informatikus jelentést tesz az információ biztonsági felelősnek, aki eljár az ügyben a Jegyző felé.

Tilos az internet használata a munkahelyi gépeken a Hivatali értékrenddel összhangba nem álló célokra, szerencsejátékokra, bármilyen kereskedelmi, illetve jogellenes célokra!

Az internet eléréseket biztosító számítógépekre a helyi hálózatra nem kapcsolódó munkaállomásokra vonatkozó szabályok érvényesek. Az internetes gépen minden esetben működtetni kell a vírusvédelmet.

A vírusok és az illetéktelen hozzáférések miatt tűzfalat kell konfigurálni. A tűzfal működése közben keletkező állományokat az informatikusnak rendszeresen ellenőrizni kell.

Az internetről csak Hivatali célból lehet fájlokat letölteni. Tilos fájlletöltő szolgáltatást használni! Különösen tilos jogvédett, illetve illegális tartalmak, fájlok letöltése, tárolása!

Közösségi oldalak használata a Hivatal munkaállomásain szigorúan tilos!

Az internetes oldalak elérése naplózásra kerülhet, a munkával összefüggésbe nem hozható oldalak elérhetőségét az Informatikus jogosult korlátozni.

5.5. Tudatosság és képzés

A munkavállalóknak, az elektronikus információs rendszerek felhasználóinak az informatikai eszközök és rendszerek biztonságos használatáról rendszeres oktatást kell tartani. Ezek során ismertetni kell az alapvető információbiztonsági fogalmakat, a felmerülő információbiztonsági fenyegetettségeket. Gondoskodni kell arról is, hogy a napi feladatok végzése során a felhasználók kellőképpen felkészültek legyenek a jelen Informatikai Biztonsági Szabályzatban foglaltak betartására.

5.5.1. Képzési eljárásrend

A Jegyző megfogalmazza, és kihirdeti a képzési eljárásrendet. A képzési eljárásrendben ki kell térni arra, hogy az elektronikus információs rendszereket csak olyan személyek használhatják, akik megfelelő számítástechnikai, informatikai, valamint szakmai ismeretekkel rendelkeznek az adott szoftver alkalmazásához. Magasabb informatikai szaktudást igénylő munkakörök betöltése esetén a szükséges szakirányú képzésben kell részt venni.

A képzési eljárásrendben a Hivatal megfogalmazza, hogy legalább a jogszabály által meghatározott gyakorisággal történő oktatással gondoskodni kell arról, hogy a felhasználókban tudatosodjanak az alapvető információbiztonsági fogalmak, illetve ismerjék meg a munkájuk során felmerülő információbiztonsági fenyegetettségeket. A hivatal dolgozóinak a választható kötelező továbbképzések során javasolt informatikával, információbiztonsággal vagy adatvédelemmel kapcsolatos képzésekben részt venni. Az SZMSZ-ben ki kell térni az új dolgozó munkába lépésekor az oktatással kapcsolatos teendőkre.

Az oktatáson, illetve továbbképzésen való részvétel az elektronikus információs rendszerrel kapcsolatba kerülő személyek számára kötelező és a megjelenést a résztvevők aláírásukkal kötelesek tanúsítani.

5.5.2. Biztonság tudatosság képzés

Az információ biztonsági felelős annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára.

Az Informatikus gondoskodik arról, hogy új elektronikus információs rendszerek bevezetését szoftver bemutató, illetve részletes rendszer használat, tesztelés, dokumentáció megismerés előzze meg az érintett dolgozók tekintetében.

A jelenleg használatban lévő elektronikus információs rendszerek cseréje esetében az Informatikus fokozott figyelemmel jár el az adatok megőrzése, védelme tekintetében és ezt tudatosítani kell.
Gondoskodni kell arról is, hogy a napi feladatok végzése során a felhasználók kellőképpen felkészültek legyenek a jelen Informatikai Biztonsági Szabályzat-ben foglaltak betartására.

5.5.3. Belső fenyegetés

A biztonságtudatossági képzés az érintett személyeket fel kell készíteni a belső fenyegetések felismerésére, és tudatosítani kell jelentési kötelezettségüket.
Ha a számítástechnikai rendszer üzemeltetése során kiderül a biztonság megsértése, illetve megsérülése, haladéktalanul meg kell kezdeni a vonatkozó intézkedések érvényesítését.
Az informatikai rendszert ért káresemények utólagos elemzését szükség esetén el kell végezni. (pl.: hardver hibák, szoftver hibák, bejelentkezések, hozzáférési kísérletek, gondatlan kezelések, vírusok stb.). Az információ biztonsági felelősnek kivizsgálást kell kezdeményeznie a beérkezett jelentés alapján és javaslatot kell tennie a Jegyző részére az esemény előfordulási esélyének csökkentése, illetve az okozott kár mérséklése érdekében.
Az oktatással elő kell segíteni, hogy a felhasználók felismerjék azokat az információbiztonságot fenyegető veszélyeket, amelyek a mindennapi munkájuk során érheti őket, és biztonsági kockázatot jelentenek a Hivatal védendő értékeire. Az oktatások sűrűségének mértékét a belső ellenőrzések során tapasztalt eredmények függvényében az információ biztonsági felelős határozza meg.

5.5.4. Szerepkör, vagy feladat alapú biztonsági képzés

A Jegyző feladata, hogy a Hivatal informatikai rendszereihez hozzáférő felhasználók esetén az adott feladat-, illetve munkakör betöltéshez szükséges képzettségre, tapasztalatra, gyakorlatra vonatkozó, illetve egyéb, a mindenkor hatályos jogszabályok és belső szabályozók által előírt követelmények ellenőrzése a jogviszony létesítése előtt megtörténjen, a jelölt a szükséges átvilágításon átessen.

Főbb szerepkörök és képzések:

Szerepkör megnevezése	**Képzés megnevezése**
Jegyző	elektronikus információs rendszerek védelméért felelős vezető
Informatikus	elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy

Elektronikus információs rendszer biztonságáért felelős személy	elektronikus információ rendszer biztonságáért felelős személy

A Hivatal informatikai rendszereihez hozzáférő minden felhasználóját munkába állását követően tájékoztatást kap az informatikai rendszerek használatára vonatkozó szabályokról, az új belépő számára biztosításra kerül az informatikai biztonsági szabályok megismeréséhez és megértéséhez szükséges minden szükséges támogatás.

II. Fizikai védelmi intézkedések

6. Alapelvek

Az elektronikus információs rendszer fizikai környezetének kialakítása, működtetése és használata során az általános biztonsági előírások szerint kell eljárni, az alábbiak szerint:

a) az elektronikus információs rendszereket fizikailag védett, biztonságos helyre kell telepíteni, és a környezetet a berendezések gyártói által megadott fizikai feltételek szerint kell kialakítani, fenntartani;

b) a környezeti fizikai feltételeket (hőmérséklet, páratartalom, áramszolgáltatás stb.) folyamatosan ellenőrizni kell;

c) a megbízható működés biztosítása céljából a körülményeknek megfelelő legfontosabb klímatechnikai, épületgépészeti, áramellátó tartalékberendezésekről gondoskodni kell.

7. Fizikai és környezeti védelmi eljárásrend

7.1. Területek védelme, biztosítása

A Hivatal helyiségeinek és információinak védelme, a jogosulatlan, illetéktelen fizikai behatolás, károkozás és zavarkeltés megakadályozása céljából a hivatali helyiségeket informatikai biztonsági szempontból kategóriákba kell sorolni, melyek a következők lehetnek:

- **Zárt terület**: információ biztonsági szempontból kritikus területek (pl. szerverszoba), melyek különleges fizikai védelmet, szabályozott beléptetést igényelnek.
- **Kiemelt terület**: információ biztonsági szempontból fontos területek (pl. raktárak, áramellátó helyiségek, hálózati elosztó helyiségek), melyek fizikai védelmet (pl. biztonsági ajtó), szabályozott beléptetést igényelnek.
- **Ellenőrzött terület**: különleges fizikai védelmet nem igénylő olyan hivatali helyiségek (pl. irodák, folyosók), melyekben idegenek csak ellenőrzött módon tartózkodhatnak.
- **Nyilvános terület**: az előzőkbe nem sorolt (pl. ügyfélszolgálati tér) hivatali helyiségek.

Az egyes biztonsági zónák kapcsán a következő adminisztratív és műszaki védelmi intézkedéseket kell kialakítani:

Kategória	Adminisztratív és védelmi intézkedéseket
Zárt terület	Kártyás beléptető rendszer (ajánlott)
	Biztonsági ajtó
	Ablak esetén rács, illetve biztonsági fólia
	Több szerver esetén rackszekrény használata
Kiemelt terület	Biztonsági ajtó
	Ablak esetén rács, illetve biztonsági fólia
Ellenőrzött terület	Zárható ajtó
Nyilvános terület	Különleges fizikai védelmet nem igényel

Helyiségek biztonsági besorolása

A Hivatal az egyes helységeit a következő biztonsági kategóriákban sorolja be:

Kategória	Helyiség	Funkció
Zárt terület	Földszint 14. szoba	szerverszoba
Kiemelt terület	-	-
Ellenőrzött terület	Irodák	adminisztratív ügyek intézése
Nyilvános terület	az előzőkbe nem sorolt hivatali helyiségek (pl.: porta, folyosók)	

A területek védelmével, biztosításával kapcsolatos feladatok végrehajtásáért a Titkárság a felelős.

A különböző biztonsági zónák közötti mozgást ellenőrizni kell. A biztonsági zónákhoz meghatározott követelményeknek megfelelő adminisztratív és műszaki eljárásokat kell alkalmazni.

Azokat a területeket, ahol külső személyek is tartózkodhatnak, nyilvános területként kell kezelni, és a hozzáférési pontokon és zónahatárokon az ennek megfelelő védelmet kell kialakítani.

A Hivatalon belül zárt, kiemelt és ellenőrzött területen idegenek (pl. vendégek, ügyfelek) engedély nélkül nem közlekedhetnek. Ügyfélszolgálati időn kívül a Hivatal teljes területére kiterjed, hogy a belépő idegenek engedély nélkül nem közlekedhetnek.

7.2. A szerverszoba védelme

Elemi csapás (vagy más ok) esetén a szerverszobában bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- menteni a még használható eszközöket, anyagokat,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- új adatfeldolgozás, helyiségek kialakítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

A szerverszoba minimális igénye:

- a szerverszobát a legbiztonságosabb, legvédettebb területre kell telepíteni,
- a lehető legkevesebb nyílászáróval kell rendelkeznie,
- a helyiség nyílászáróit biztonsági ráccsal vagy biztonsági fóliával kell ellátni,
- váratlan áramkimaradás esetén a szervereket szünetmentes tápegységgel kell védeni, mellyel az áramellátás folyamatosságát biztosítani lehet.

7.3. A munkaállomásokra vonatkozó előírás

A munkaállomásokat úgy kell elhelyezni, illetve védeni, hogy csökkenjen a környezeti fenyegetésekből és veszélyekből eredő kockázat, valamint a jogosulatlan hozzáférés lehetősége. A megfelelő védelem eléréséhez a berendezéseket az alábbi biztonsági kategóriákba kell besorolni:

Kategória	Berendezések típusai
Kiemelt biztonság	Szerverek
	Menedzselhető hálózati eszköz elemek (router, switch)
Fokozott biztonság	Lokális személyi számítógépek
	Kábelelosztó szekrények
Normál biztonság	Az előző kategóriákba nem sorolható informatikai berendezések

A berendezéseket a biztonsági kategóriájuk alapján a következő biztonsági zónákba sorolt helyiségekbe kell elhelyezni:

Kategória	Fizikai biztonsági zónák
Kiemelt biztonság	Zárt terület
Fokozott biztonság	Kiemelt terület
Normál biztonság	Ellenőrzött terület vagy Nyilvános terület

A biztonsági zónákon belül a berendezéseket úgy kell elhelyezni, hogy azokhoz karbantartás, hibajavítás miatt a hozzáférhetőség biztosított legyen.

A munkaállomásokat csak zárható helyiségben szabad tárolni. Ha a helyiségben nem tartózkodik senki, az ajtót kulcsra zárva kell tartani.

7.3.1. Számítógép használatának előírásai

A munkaállomást és az informatikai eszközöket a napi munkavégzés befejezésekor ki kell kapcsolni. Ez alól kivételek azok az eszközök, amelyek automatikusan kikapcsolnak (hálózati nyomtatók vagy a modern monitorok többsége stb.). Az infokommunikációs eszközöket üzem közben letakarni, a szellőző nyílásokat eltakarni tilos!

7.3.2. „Üres asztal - tiszta képernyő" politika

Az „üres asztal - tiszta képernyő" politika megvalósítása az alábbiakat jelenti:

a) A monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő használata ajánlott);

b) A felhasználó a munkaállomását zárolni köteles, ha hosszabb időre elhagyja helyét;

c) A munkavégzés befejeztével a munkaállomásból ki kell jelentkezni, illetve ki kell azt kapcsolni, ettől eltérő utasítást az Informatikus adhat;

d) Elfelejtés esetére jelszóvédett, automatikus zárolás kerül beállításra, úgy, hogy az maximum 10 perc várakozást követően zárolja a számítógépet;

e) A felhasználóknak az infokommunikációs eszközök elhelyezésére szolgáló helyiséget be kell zárniuk, ha a helyiségben senki nem tartózkodik;

f) A kinyomtatott, faxolt vagy másolt iratokat nem szabad őrizetlenül a nyomtatókban, multifunkcionális eszközökben, faxokban hagyni.

g) Ügyfelet nem szabad felügyelet nélkül az irodában hagyni.

7.4. Az elektronikus információs rendszer elemeinek fizikai biztonsága

Az infokommunikációs eszközöket úgy kell elhelyezni, és védelmüket úgy kell kialakítani, hogy minimálisra csökkenjenek a környezeti hatások következtében megjelenő kockázatok, és minimálisra csökkenjen az illetéktelen hozzáférések lehetősége, de a munkavégzés hatékonysága ne romoljon.
A védelmi intézkedések biztosítják, hogy a különböző környezeti hatás miatt keletkező meghibásodások csökkenjenek. Ezért:

a) be kell tartani a tűzvédelmi előírásokat;

b) a Hivatal területére a normál háztartási vegyi anyagokon, tisztítószereken túl vegyi anyagot, robbanóanyagot behozni tilos;

c) a monitorokat úgy kell elhelyezni, hogy ki lehessen zárni azok illetéktelen leolvasását;

d) különös figyelmet kell fordítani az önkormányzati ASP rendszert elérő munkaállomások elhelyezésére, gondoskodni kell az illetéktelen hozzáférések megakadályozásáról.

e) a gépterem (szerverszoba) külső és belső helyiségeit biztonsági ráccsal és zárakkal kell felszerelni,

f) a szerverszobába való be- és kilépés rendjét szabályozni kell, csak az illetékes dolgozók tartózkodhatnak a gépteremben,

g) a szerverszoba kulcsának felvétele, illetve leadása csak aláírás ellenében történhet,

h) munkaidőn túl a szerverszobában csak engedéllyel lehet dolgozni,

i) a szerverszobába történő illetéktelen behatolás tényét az információ biztonsági felelősnek azonnal jelenteni kell,

j) az informatikai eszközöket csak a kijelölt dolgozók használhatják,

k) a munkaállomások rendeltetésszerű működéséért a felhasználó felelős.

7.4.1. Programok fizikai védelme

A védelem érdekében a felhasználás helyétől elkülönítetten, behatolástól védetten egy-egy másolati példányt kell tárolni a programkönyvtárba elhelyezett programokról.

7.4.2. Zárt és kiemelt területek kulcskezelési rendje

Zárt és kiemelt területeken található helyiségek, elválasztó ajtók esetében biztosítani kell, hogy a kulcsok központilag legyenek tárolva, és azokat csak az arra illetékesek vehessék fel.

A kulcsok – beleértve a tartalék kulcsokat is – központi tárolásának helye a Porta.

A helyiségeket napközben nyitva és őrizetlenül hagyni nem szabad.

7.4.3. Hálózati védelem

A kommunikációs rendszereket, hálózatokat úgy kell kialakítani, hogy biztosítsák a rajtuk keresztül folyó adatátvitel bizalmasságát, sértetlenségét és rendelkezésre állását. A hálózati kockázatok csökkentése érdekében a hálózati forgalmat és a kiosztott hálózati címeket folyamatosan figyelni, ellenőrizni kell, ennek felelőse az informatikus. Biztonsági esemény észlelésekor azonnal jelentést tesz az információ biztonsági felelősnek és követi az eljárásrendet.

7.4.4. Tűzvédelem

A tűzvédelem feladatait, sajátos előírásokat a szerverszobára és minden helyiségére vonatkozóan a Hivatal Tűzvédelmi Szabályzata tartalmazza.
A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.
Az informatikai eszköz elhelyezésére szolgáló helyiségben elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, illetve engedélyével szabad végezni.
A szerverszobában csak a napi munkavégzéshez szükséges mennyiségű gyúlékony anyagot szabad tárolni.

7.4.5. Védelem áramkimaradás, illetve –ingadozás esetén

Informatikai biztonsági szempontból a közműszolgáltatások közül az áramkimaradás, illetve ingadozás az egyetlen jelentős kockázatot jelentő fenyegetettség. Ennek megelőzése és kezelése érdekében a következő védelmi intézkedéseket kell alkalmazni az egyes fizikai biztonsági zónák esetében.

Kategória	Fizikai védelmi intézkedéseket
Zárt terület	Áramkimaradás és túlfeszültség elleni védelem, mely lehetővé teszi az eszközök legalább 10 percig történő működését

Kiemelt terület	Túlfeszültség ellen védő elosztók a munkatársak számítógépéhez.
Ellenőrzött terület	Túlfeszültség ellen védőelosztókat kell elhelyezni a kritikus alkalmazásokat használó munkatársak számítógépéhez.
Nyilvános terület	Túlfeszültség ellen védő elosztókat kell elhelyezni a kritikus alkalmazásokat használó munkatársak számítógépéhez.

A berendezések védelmének megteremtése a közműszolgáltatások kiesése kapcsán az informatikus feladata. A szükséges erőforrások biztosítása a Jegyző feladata.

7.4.6. Kábelezés biztonsága

Az épületeken belül a hálózati vezetékek kábelcsatornában kell vezetni. A kábelek elhelyezésekor, a használt anyagok kiválasztásakor figyelembe kell venni a kiszolgált informatikai erőforrások biztonsági besorolását. A kábeleket a várható fizikai igénybevételnek és a továbbított adatok kritikusságának megfelelően kell védeni, figyelembe véve az elektromágneses sugárzások be-, illetve kijutása (zavar, illetve információ) elleni védelmet is.

A belső hálózat kívülről történő elérése kizárólag engedélyezett módon, titkosított csatornán keresztül lehetséges.

A kábelezéssel kapcsolatos megelőzési, javítási és karbantartási feladatokat csak az információ biztonsági felelős előzetes engedélyével lehet végrehajtani.

7.4.7. Víz-, és más, csővezetékeken szállított anyag okozta kár elleni védelem

Biztosítani kell, hogy a víz-, és más, csővezetékeken szállított anyag esetében a Jegyző által kijelölt személyek részére hozzáférhetők legyenek a főelzáró szelepek.

III. Logikai védelmi intézkedések

8. Általános védelmi intézkedések

8.1. Engedélyezés

A Hivatalnak úgy kell kialakítania az általános védelmi intézkedéseit, hogy biztosított legyen

- az elektronikus információs rendszer és annak környezete biztonsági állapotának felügyelete,
- meghatározásra kerüljenek az információbiztonsággal összefüggő szerepkörök és felelősségi körök,
- kijelölésre kerüljenek az ezeket betöltő személyek,
- az elektronikus információbiztonsági engedélyezési folyamatok kerüljenek integrálásra a társasági szintű kockázatkezelési eljárásba, összhangban az informatikai biztonsági szabályzattal.
- az elektronikus információbiztonsággal kapcsolatos engedélyezés terjedjen ki minden, a társaság hatókörébe tartozó:
    - emberi, fizikai és logikai erőforrásra;
    - eljárási és védelmi szintre és folyamatra.

8.2. A szoftverhasználat korlátozásai, legszűkebb funkcionalitás

A Hivatal kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ. amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi, vagy más jogszabályoknak, valamint jelen Informatikai Biztonsági Szabályzatnak. Az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa, továbbá rendszeresen ellenőrzi, hogy tiltott, vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek ne legyenek a gépeken használatban.

A használatban lévő elektronikus információs rendszerekről naprakész nyilvántartást vezet, és rendszeresen ellenőrzi, hogy azok csak egy leltárba kerültek-e rögzítésre, nincsenek-e duplikálások a leltárban.

8.3. Elektronikus információs rendszer kapcsolódásai

A Hivatal csak a felügyelete alatt álló informatikai rendszer felett gyakorol kontrollt, a rendszer felügyelet nélküli összekapcsolása más szervezetek informatikai rendszerével nem engedélyezett.

Az összekapcsolást mind a Jegyzőnek, mind az informatikusnak, mind pedig az információ biztonsági felelősnek is jóvá kell hagynia.

Dokumentálni kell az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.

A kapcsolódó szerv csak a Hivatal által nyújtott interfészen keresztül csatlakozhat a rendszerhez.

Szerződésben vállalnia kell a kapcsolódó szervnek, hogy biztosítja a saját elektronikus információs rendszerében a technológiai végrehajtási rendelet által előírt legalább 2-es biztonsági osztályra előírt követelmények teljesülését.

Információbiztonsági incidens esetén a Hivatal jogosult a kapcsolatot felfüggeszteni.

Szabványos, sérülékenységektől mentes kriptográfiai eszközökkel gondoskodni kell az átvitt adatok bizalmasságának és sértetlenségének biztosításáról.

IP szinten korlátozni kell a kapcsolódást.

Az összekapcsolás feltételeinek fennállását legalább évente ellenőrizni kell.

Az engedélynek tartalmaznia kell az összeköttetés pontos paramétereit, interfész-leírását (cél, technikai megvalósítás, átvitt információk, biztonsági követelmények).

8.4. Belső rendszerkapcsolatok

A Hivatal elektronikus információs rendszer több elemből épül fel, melyek bizonyos interfészeken kapcsolódhatnak egymáshoz. Valamennyi interfészt dokumentálni kell, és előzetesen jóvá kell hagyatni az információ biztonsági felelőssel.

8.5. Külső kapcsolódásokra vonatkozó korlátozások

A Hivatal határvédelmének működtetése során minden kapcsolatot tiltani kell, csak a működéshez szükséges portokat, protokollokat és szolgáltatásokat szabad engedélyezni. Amennyiben az értelmezhető, úgy az érintett kapcsolatnál IP alapú korlátozást kell bevezetni és gondoskodni kell a megfelelő azonosításról és hitelesítésről, valamint az átvitt adatok sértetlenségéről és bizalmasságáról.

Minden kapcsolatot előzetesen jóvá kell hagyatni az információ biztonsági felelőssel.

9. Konfigurációkezelési eljárásrend

Az elektronikus információs rendszerekről nyilvántartást kell vezetni, s ennek az alábbiakat kell tartalmaznia:

- rendszer megnevezése,
- leírása,
- a rendszer biztonsági osztálya,
- a fejlesztő/kapcsolattartó elérhetősége,
- példányszám és tárolás helye,
- az átadás ideje,
- módosítások megnevezése és ideje.

A munkaállomásokról, informatikai eszközökről nyilvántartást kell vezetni, és ennek az alábbiakat kell tartalmaznia:

- az eszköz hálózati neve
- megnevezése
- használatának helye,
- használójának neve, beosztása,
- üzembe helyezésének ideje

Az elektronikus információs rendszerek alapkonfigurációja tartalmaz minimum 1 db asztali számítógép konfigurációt (az adott kor technikai fejlettségének alap hardver elemeinek, alkatrészeinek felhasználásával), internet csatlakozással, tartományba léptetve, vírusirtóval ellátva, telepítve a megfelelő információs rendszerrel, szükség esetén nyomtatóval.

A már meglévő konfigurációkat felül kell vizsgálni és a kockázatelemzéssel összhangban frissíteni kell a hardveres és szoftveres veszélyeztető tényezők kiküszöbölése érdekében.

Az elektronikus információs rendszerben bekövetkező változásokat a Hivatal haladéktalanul dokumentálja, és a szükséges alapkonfigurációbeli módosításokat elvégzi.

A munkaállomások tekintetében az alábbi rendelkezéseket kell betartani:

- Ha a munkaállomások nincsenek jól védhető helyen, védelmükről szoftveres úton gondoskodni kell.
- Ha a felhasználó napközben magára hagyja a gépet, zárolást kell alkalmaznia.
- Vírusirtó programot futtatni csak az informatikus felügyelete mellett szabad.
- Olyan floppy lemezeket, pendrive-okat, külső winchestereket, SD kártyákat, melyeken a formázás után az operációs rendszer rossz szektorokat mutat ki, tilos felhasználni.
- A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos. Fali csatlakozó meghibásodása, megrongálódása esetén azonnal szólni kell az informatikusnak.

- Az informatikai eszközt és tartozékait helyéről elvinni az informatikus tudta és engedélye nélkül nem szabad.

A szerverszobában, valamint a munkaállomásoknál ételt, italt fogyasztani tilos!

9.1. A szoftver használat korlátozásai

A Hivatalban kizárólag a Jegyző által engedélyezett, jogtiszta, a megfelelő licence-el rendelkező szoftvereket lehet használni.

Az alkalmazott szoftverekről leltárt kell vezetni.

Szabad vagy nyílt forráskódú szoftverek használatba vételét a Jegyző engedélyezi. Ezen szoftvereket használatba vétel előtt biztonságos körülmények között tesztelni kell.

A másolatok és szétosztások ellenőrzése érdekében a telepítőkészleteket és a licenceket tartalmazó dokumentumokat páncélszekrényben kell tárolni és a hozzáféréseket ellenőrizni kell.

A szerzői jogokkal védett szellemi termékek felhasználását nyomon kell követni.

9.2. Programok telepítése

Lokális gépekre programot csak az Informatikus tudtával lehet telepíteni. A telepítést dokumentálni kell. A dokumentálásnak tartalmaznia kell azt, hogy milyen programot, mikor és ki telepített fel a számítógépre. A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt. A programokról nyilvántartást kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:

- a program azonosítója,
- alapfeladatai,
- szolgáltatásai,
- biztonsági osztálya
- a rendszert felügyelő személy neve, elérhetősége
- a program fejlesztőjének neve,
- kapcsolattartó neve, elérhetősége

A program dokumentáció a rendszer-dokumentációnak része. A programok nyilvántartásáért és működőképes állapotban való tartásáért az Informatikus a felelős.

A hálózatra idegen programot, adatot másolni csak az Informatikussal történt egyeztetés után lehet. Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal. Vírusfertőzés gyanúja esetén az informatikust azonnal értesíteni kell.

Az intézmény informatikai eszközeiről programot, illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.

9.3. Külső elektronikus információs rendszerek szolgáltatásai

A Hivatal a szolgáltatási szerződésben követelményként fogalmazza meg az általa igénybe vett elektronikus információs rendszerekkel szembeni elvárásokat, hogy ezek megfeleljenek az érintett szervezet elektronikus információ biztonsági követelményeinek. Dokumentálja a külső szervezet feladatait és a kezelt adatok és folyamatokkal kapcsolatos kockázatok szerint az információ biztonsági követelményeknek való megfelelést .

9.4. A rendszer fejlesztési életciklusa

A Hivatal saját fejlesztésű szoftvert nem alkalmaz. A beszerzések alkalmával kötött szerződések szabályozzák az adott szoftver rendszerkövetési elvárásait, az elektronikus információs rendszer teljes életútjára vonatkozóan.

A rendszer életciklus szakaszai: követelmény meghatározás, beszerzés, értékelés, üzemeltetés és fenntartás, kivonás (archiválás, megsemmisítés).

9.5. A felhasználó által telepített szoftverek

A felhasználók semmilyen alkalmazást nem telepíthetnek a munkaállomásaikra. A rendszerprogramok, illetve a felhasználói alkalmazások telepítését a kiszolgálókra és munkaállomásokra csak az Informatikus végezheti el.

A felhasználók munkaállomásain telepített alkalmazások megfelelőségét az információ biztonsági felelős szúrópróbaszerűen ellenőrzi.

10. Karbantartási, javítási eljárásrend

Az informatikai eszközök hibátlan és üzemszerű működését biztosítani kell. A Hivatal a karbantartásokat ütemezetten, a javításokat igény szerint hajtja végre. A tervszerűen végzett

karbantartás ellenére is megtörténhet, hogy az eszközök meghibásodnak. A javítást elsődlegesen az Informatikusnak kell végrehajtania.

Amennyiben ez nem lehetséges (pl. idő, alkatrész vagy szakértelem hiányában) úgy

- a javításra – előzetes árajánlat kérést követően – külső karbantartó cég kerül bevonásra, vagy
- az eszköz selejtezésre kerül (pl. az eszközt már nem lehet, vagy nem éri meg javítani, mert drága vagy elavult, ezért cseréje indokolt).

A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése, a szervízellátás biztosítása. A karbantartási munkákat tervezetten, körültekintően és gondosan kell elvégezni.

- A munkák szervezésénél figyelembe kell venni:
  - a gyártó előírásait, ajánlatait,
  - a tapasztalatokat,
  - a hardver tesztek által feltárt hibákat.
- Alapgép szétbontását (kivéve a garanciális gépeket) csak az Informatikus végezheti el.

Abban az esetben, ha saját erőből a karbantartás nem végezhető el, akkor az informatikus kezdeményezi a jegyzőnél külső fél (karbantartó) megbízását.

Karbantartási tevékenységet csak olyan külső fél végezhet, aki érvényes szerződéssel rendelkezik, a titoktartási nyilatkozatot aláírta és dokumentált formában megismerte a Hivatal vonatkozó információbiztonsági előírásait.

A karbantartást végző külső felekről nyilvántartást kell vezetni, melynek minimálisan a következőket tartalmaznia:

a) szervezet megnevezése,

b) szerződésszám,

c) szerződés időtartama,

d) szerződéses kapcsolattartó neve, elérhetősége,

e) karbantartás végzők neve, elérhetősége,

f) szerződés tárgya, hatálya (mely rendszerelemre terjed ki).

Külsős szerződő fél munkavégzése esetén az informatikus biztosítja a folyamatos felügyeletet a karbantartás során.

A külső féllel kötött szerződébe kell foglalni, hogy a karbantartást felügyelők jogosultak kérni a karbantartást végző személy személyazonosságának igazolását illetve hogy a karbantartást végző személynek kötelessége a felszólításra a szükséges iratokat bemutatni.

A Hivatal berendezéseit csak szállító levél kiállításával, valamint az Informatikus engedélyével lehet elszállítani. Az elszállított gépekről eltávolítani csak azokat az adatokat kell, amelyek az adatvédelmi szabályzatban kijelölésre kerültek.

A visszavételezéskor, a bizonylat aláírását megelőzően, az Informatikusnak a javítás eredményességéről meg kell győződnie. A karbantartás során igénybe vett adathordozókat használatba vétel előtt kártékony kód elleni ellenőrzésnek kell alávetni.

A szerviz, valamint a külső elektronikus információs rendszerek szolgáltatóival kötött szerződésekben rögzíteni kell a karbantartási feladatokat és a karbantartások gyakoriságát. Az üzemeltetési tevékenység során az Informatikus rendszeresen teszteli a beépített információbiztonsági intézkedések megfelelőségét és hatékonyságát.

10.1. Távoli karbantartás

Távoli karbantartást csak a rendszergazdai feladatokat ellátó munkatársak végezhetnek. Az önkormányzati ASP rendszert használó munkaállomásokon távoli képernyő átvétel nem engedélyezett.

A távoli hozzáférések során VPN kapcsolatot kell alkalmazni, mely megfelelő erősségű titkosítással, ismert sérülékenységet nem tartalmazó kriptográfiai algoritmussal épül fel. A VPN kapcsolódáskor a kapcsolódó felet egyedileg kell azonosítani és hitelesíteni. A távoli karbantartás elvégeztével a távoli félnek bontania kell a VPN kapcsolatot. A távoli karbantartásokról a rendszergazdának nyilvántartást kell vezetni. Távoli hozzáféréseket csak olyan eszközről lehet kezdeményezni, melyen

a) naprakész, memóriában rezidens kártékony kód elleni védelem fut,

b) naprakész, gyártó által támogatott operációs rendszer és alkalmazások futnak,

c) a helyi tűzfala bekapcsolásra került.

11. Selejtezési és megsemmisítési eljárások

A Selejtezési és megsemmisítési eljárások célja annak biztosítása, hogy a selejtezett eszközökön tárolt információk visszaállítása ne legyen lehetséges.

Ennek megfelelően valamennyi olyan berendezés esetében, amely tárolóeszközt foglal magába, az Informatikus az érzékeny adatok és engedélyezett szoftverek eltávolítása érdekében a selejtezést megelőzően a tárolóeszközt

- biztonságos módon felülírja (amennyiben lehetséges), illetve

- amennyiben az eszköz megsemmisítésre is kerül, úgy fizikailag használhatatlanná teszi (pl. a merevlemez megfúrásával).

11.1. Selejtezés dokumentálása

A selejtezésről a selejtezési bizottság jegyzőkönyvet vesz fel, melynek dokumentálása a Leltározási és selejtezési szabályzatban leírtaknak megfelelően történik. A berendezések biztonságos selejtezésével és újrafelhasználásával kapcsolatos feladatok végrehajtásának felelőse a Selejtezési bizottság.

A selejtezés megtörténtét az informatikai elektronikus nyilvántartásban is át kell vezetni.

12. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

Új eszközök használatba vételét a Jegyző engedélyezi. Az SZMSZ-ben, a munkaköri leírásokban, az Informatikai Biztonsági Szabályzatban rögzíteni kell, az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési eljárási folyamatokat. Meg kell határozni az információbiztonsággal összefüggő szerepköröket és az ezeket betöltő személyeket. Integrálni kell az elektronikus információbiztonsági engedélyezési folyamatokat a szervezeti szintű kockázatkezelési eljárásba.

12.1. Adathordozók védelmére vonatkozó eljárásrend

Az adathordozók védelmére vonatkozó eljárásrend magába foglalja a számítógépek, adathordozók biztonságos, megbízható működtetésének feltételeit, miszerint:

- A Hivatal csak engedélyezett adathordozót szabad használni. A szervezet vezetője, az Informatikus, illetve az információ biztonsági felelős a hozzáférési jogosultságok szabályozásával engedélyezheti, korlátozza, vagy tilthatja egyes, vagy bármely adathordozó típusok, és az elektronikus információs rendszerek használatát;
- az adathordozókat könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak;
- a használni kívánt adathordozót (CD, DVD, pendrive, külső winchester, SD kártya) a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni;

- a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek;
- adathordozót más szervezetnek átadni csak engedéllyel szabad;
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni;
- az adathordozók logikai védelmét az operációs rendszer és az ehhez tartozó ellenőrző, file-kezelő rutinok alkalmazásával lehet biztosítani;
- tilos a magáncélú adathordozókat szolgálati célra igénybe venni, illetve tilos szolgálati adathordozókat magáncélra igénybe venni;
- tilos olyan adathordozó használata, melynek tulajdonosa nem azonosítható, ilyen esetben az elektronikus információ rendszer biztonságáért felelős személynek kell az adathordozót átadni.

Az számítógépek belső adathordozóihoz az Informatikus férhet hozzá. Szükség esetén a munkavállalók külső adathordozókhoz az elektronikus információ rendszer biztonságáért felelős személy és a jegyző engedélyével férhetnek hozzá vagy használhatják, figyelembe véve a rendszerbiztonsági és adatvédelmi szabályokat.

12.2. Az adathordozók megőrzése

Adathordozót az irodából ki-, illetve oda bevinni csak az elektronikus információ rendszer biztonságáért felelős személy vagy az Informatikus engedélye alapján lehet.

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

12.3. Az adathordozók karbantartása

Az adathordozók állapotát évenként ellenőrizni kell.

12.4. Adathordozók tárolása

A Hivatal elektronikus információs rendszereinek kiszolgáló oldali adathordozóit a szerverhelyiségben kell tárolni. A felhasználók részére kiosztott mobil adathordozókat használaton kívül zárható irodabútorban kell tárolni.

12.5. Adathordozók szállítása

A felhasználók részére biztosított mobil adathordozók a felhasználók részéről korlátozás nélkül szállíthatók. A kiszolgáló oldali adathordozók szállítására az Informatikus jogosult. Ebben az esetben a szállítást dokumentálni kell.

12.6. Adathordozók törlése

Az Informatikus a helyreállíthatatlanságot biztosító törlési technikákkal vagy az adathordozó teljes fizikai megsemmisítésével törli az elektronikus információs rendszer meghatározott adathordozóit a leselejtezés, a szervezeti ellenőrzés megszűnte, vagy (törlés esetén) újrafelhasználásra való kibocsátás előtt. Az adatok vagy adathordozó megsemmisítéséről a megsemmisítést végző feljegyzést készít.

12.7. Ismeretlen tulajdonos

A Hivatal elektronikus információs rendszereiben tilos nem a hivatal tulajdonát képező adathordozót csatlakoztatni.

12.8. Adathordozók selejtezési eljárásrendje

Olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért, selejtezni kell.

Selejtezni kell:

- a fizikailag sérült, javíthatatlan, a gyári, raktározási hibából követően felhasználásra alkalmatlan CD-t, DVD-t, pendrive-ot;
- az alkalmatlan CD-ket, DVD-ket, pendrive-okat fizikai roncsolással használhatatlanná kell tenni;
- bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adathordozókról, törlő programokkal kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót;
- a selejtezésről (3 példányban) Jegyzőkönyvet kell készíteni (15. melléklet), melynek az alábbi adatokat kell tartalmaznia:
    - a selejtezendő adathordozók tulajdonosának megnevezését, a selejtezés időpontját,
    - milyen adathordozók, és azok mely adatai kerülnek selejtezésre, a selejtezést végzők aláírását.

A selejtezési Jegyzőkönyvek nem selejtezhetőek.

Minősített, titkos adatokat tartalmazó adathordozókat selejtezni nem lehet, ezen adatokat tartalmazó adathordozókat Az államtitkokról és szolgálati titkokról az 1995. évi LXV. törvény utasítása szerint kell kezelni.

12.9. Kriptográfiával kapcsolatos szabályozás

Amennyiben a Hivatal kriptográfiai eljárást használ, ez csak szabványos eljárás lehet. A használat módja lehetőség szerint az aktuálisan elfogadott modern algoritmusokat használja, kerülve a régi vagy ismert sebezhetőségekkel rendelkező eljárásokat. A kommunikációs csatornák kriptográfiai védelmére törekedni kell, a lehetőségek szerint a technikailag és a rendelkezésre álló szoftver lehetőségei szerint a használatkor ismert biztonságos konfigurációt használhat, ezt rendszeresen felül kell vizsgálni.

Amennyiben a Hivatal maga állít elő vagy használ más által generált kriptográfiai kulcsot, így annak szabályozására, tárolására, megsemmisítésére szabályozást készít a kriptográfiával védett adat milyenségével összhangban.

Kriptográfiai eszköz vagy szoftver alapértelmezett beállításokkal, telepítés során létrejött vagy a telepítőcsomagban található értékekkel nem vehető használatba.

13. Rendszer és információsértetlenségre vonatkozó eljárásrend

13.1. Hibajavítás

A rendszerprogramokkal kapcsolatos bármely konfigurálási, hangolási műveletet csak az Informatikus végezhet. Az alkalmazáson végzendő, annak bármely funkcióját megváltoztató művelethez – beleértve a verzióváltást és egyéb, jelentős beavatkozást igénylő hangolást is - a Jegyző engedélye szükséges.

Az Informatikusnak biztosítania kell, hogy a rendszerszoftver naprakész állapotban legyen, és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek az üzemeltetők számára. Az alapszoftver módosítással egy időben a változásokat a dokumentációban is át kell vezetni.

A felhasználói adatok és alkalmazások védelme érdekében a szoftverek módosítása (frissítés, verzióváltás) folyamán az alkalmazáshoz és az adatokhoz történő illetéktelen hozzáférést és az illetéktelen próbálkozást meg kell akadályozni. Gondoskodni kell arról, hogy a telepített alkalmazások, fájlok ne károsodjanak, és a követelményeknek megfelelően működjenek.

Új hardverek üzembe állításakor a fentieket kell értelemszerűen alkalmazni. Gondoskodni kell arról, hogy a munkaállomásokon telepített operációs rendszerek és egyéb segédprogramok naprakészek legyenek.

13.2. Microsoft termékek biztonsági frissítéseinek telepítése

A Microsoft termékek biztonsági frissítéseinek a telepítéséről a megjelenésüktől számított 1 héten belül gondoskodni kell. A biztonsági frissítéseket az Informatikusnak előzetesen tesztelni kell.

13.3. Nem Microsoft termékek biztonsági frissítéseinek telepítése

A nem Microsoft termékek frissítését a gyártói ajánlások figyelembevételével kell elvégezni. A biztonsági frissítések telepítése az Informatikus feladata.

13.4. Kártékony kódok elleni védelem

A szerverek és munkaállomások vírusvédelmére az alábbi szabályokat kell betartani:

- Minden munkaállomásra és szerverre vírusellenőrző szoftvert kötelező telepíteni.
- A vírusellenőrző programnak minden újonnan érkezett állománnyal kapcsolatos fájlművelet esetén meg kell vizsgálni az adathordozó tartalmát. Ha az adathordozón a vírusellenőrző program vírust talált, nem engedhet másolást, futtatást, amíg a vírusoktól nem mentesítik az adathordozót.
- A vírusellenőrző programot úgy kell konfigurálni, hogy rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren, a hálózati belépési és kilépési pontokon, amikor fájlokat letöltik, megnyitják, vagy elindítják.
- Biztosítani kell a vírusvédelmet ellátó programok, valamint a vírusok adatait tartalmazó állományok rendszeres, gyártó által kibocsátott verziók telepítésével történő mielőbbi frissítését.
- A felhasználók részéről tilos a vírusellenőrző szoftver beállításainak módosítása.

13.5. Az elektronikus információs rendszer felügyelete

Az Informatikus feladata az elektronikus információs rendszer felügyelete a következők szerint:

- azonosítja az elektronikus információs rendszer jogosulatlan használatát,

- védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;
- meghatározott gyakorisággal biztosítja az elektronikus információs rendszer felügyeleti információkat a Jegyzőnek és az elektronikus információ rendszer biztonságáért felelős személynek.

13.6. Biztonsági riasztások és tájékoztatások

A Hivatalnak az információ biztonsági felelős útján folyamatosan figyelemmel kell kísérnie a Kormányzati Eseménykezelő Központ által kiadott riasztásokat, valamint a Nemzeti Elektronikus Információbiztonsági Hatóság által közzétett értesítéseket.
Az információ biztonsági felelősnek meg kell vizsgálnia, hogy az adott riasztás vagy értesítés érinti-e a Hivatalt, illetve annak elektronikus információs rendszereit és szükség esetén belső riasztást kell kiadnia az érintett szerepkörök részére.

13.7. Bemeneti információ ellenőrzés

Az önkormányzati ASP rendszer esetében meg kell határoznia a Jegyzőnek, hogy mely Hivatali munkaállomásról jogosult a felhasználó elérni az önkormányzati ASP rendszert. A működtető által kiadott kliens oldali tanúsítvány telepítésével biztosítható a munkaállomás belépési pontjának érvényessége.

13.8. A kimeneti információ kezelése és megőrzése

A kimeneti információk (pl.: nyomtatás) kezelésével és szétosztásával kapcsolatban a Hivatal Iratkezelési Szabályzatával összhangban a következők az előírások:

a) gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről,
b) gondoskodni kell arról, hogy a kimeneti információhoz történő fizikai és logikai hozzáférés csak az arra jogosított személyekre korlátozódik,
c) gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat,
d) biztosítani kell, hogy a megsemmisítési eljárások során az kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.

14. Adatkezelési eljárásrend

A Hivatal alapelve az ügyféladatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása, tehát meg kell valósítani, hogy mindenki csak ahhoz az adathoz juthasson hozzá, amire a munkájához szüksége van, és olyan mértékben, amennyire az adott munkafolyamathoz szükséges.
Minden dolgozóval, aki az adatok gyűjtése, felvétele, tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése során információkhoz jut adatkezelési nyilatkozatot kell aláíratni. Az adatkezelési nyilatkozat naprakészen tartásáért az elektronikus információ rendszer biztonságáért felelős személy a felelős.
Az informatikai feldolgozás során keletkező adatok minősítője a Jegyző.
Különös védelmi utasítások és szabályozások nem mondhatnak ellent a törvények és a jogszabályok mindenkori előírásainak.
A titkot képező adatok védelmét, a feldolgozás – az adattovábbítás, a tárolás – során az operációs rendszerben és a felhasználói programban alkalmazott kriptográfiai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver védelem).
A hivatali titoknak minősülő adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot.
A kijelölt dolgozók előtt a titokvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.
Minősített adatok esetén, az információhoz való hozzáférést a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység – adatbázisokhoz való hozzáférés, a fájlba vagy mágneslemezre történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető.
A további adatkezelési szabályokat a Hivatal Adatvédelmi Szabályzata tartalmazza.

15. Naplózási eljárásrend

Az elektronikus információs rendszerek és a szerver által generált naplófájlokat naponta át kell tekinteni. A naplófájlok áttekintéséért, értékeléséért az Informatikus felelős. Köteles havonta jelentést készíteni az elektronikus információ rendszer biztonságáért felelős személynek a naplófájlok kiértékeléséről. Köteles a naplófájlokat 1 hónapig megőrizni, azokat biztonságos helyen tárolni a visszakereshetőség érdekében. Jogosulatlan hozzáférés vagy annak a kísérlete esetén azonnal jelenteni kell azt az információ biztonsági felelősnek.

16. Az informatikai feldolgozás folyamatának védelme

16.1. Azonosítási és hitelesítési eljárásrend

- Az adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- csak tesztelt adathordozóra lehet adatállományt rögzíteni,
- hozzáférési lehetőség:
  - a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá).
  - az adatok bevitele során alapelv, hogy azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

A szerverek rendszergazda jelszavát és az operációs rendszerek rendszergazda jelszavát lezárt borítékban, zárható szekrényben kell tárolni.

16.2. Azonosító kezelés

Az Informatikus hozzárendeli az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz vagy eszközhöz, meghatározott időtartamig megakadályozza az azonosítók ismételt felhasználását, meghatározott időtartamú inaktivitás esetén letiltja az azonosítót. Az ASP rendszerben ez az adatgazda, azaz a Tenant feladata.

16.3. Jelszó (tudás) alapú hitelesítés

A Hivatalban csak olyan azonosítási rendszert lehet alkalmazni, mely nem tárolja a jelszót nyílt formában.

16.4. Birtoklás alapú hitelesítés

Az önkormányzati ASP rendszer csak e-személyi használatával és jelszó alapú azonosítás és hitelesítés után érhető el. Az e-személyi tartalmazza a birtokláshoz szükséges adatokat (magán kulcs és egyéb azonosító adatok).

Kiemelt figyelmet kell fordítani az e-személyi megőrzésére.

16.5. A hitelesítésre szolgáló eszközök kezelése

Az Informatikus, amennyiben hitelesítésre szolgáló eszköz használatban van, ellenőrzi annak kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát, meghatározza annak kezdeti tartalmát. Meghatározza a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, meghatározza a minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit. Lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor. A hitelesítésre szolgáló eszköz használója köteles megőrizni rendelkezésére bocsátott eszköz bizalmasságát és sértetlenségét.

A hitelesítésre szolgáló eszközt másnak átadni szigorúan tilos! Amennyiben ez a szabály sérült, ennek tényét jelzi a szervezet vezetője felé, aki intézkedik a kapcsolódó jogosultságok visszavonásáról, szükség szerint az eszköz cseréjéről. Hitelesítésre szolgáló eszköz használatbavételekor, amennyiben van alapértelmezett értéke, ezt meg kell változtatni, e-nélkül nem vehető használatba!

A Hivatal a munkavállalóknak kiadott jelszavakat nem tárolja és nem továbbítja.

Azoknál az elektronikus információs rendszereknél, ahol hardver token alapú hitelesítést kell alkalmazni, csak a Hivatal által meghatározott minőségi követelményeknek megfelelő hardver tokent szabad alkalmazni.

16.6. A hitelesítésre szolgáló eszköz visszacsatolása

Az elektronikus információs rendszer fedett visszacsatolást (nem szolgáltat hibás bejelentkezés esetén használható információt) biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

16.7. Azonosítás és hitelesítés (szervezeten kívüli felhasználók, személyes vagy megbízható harmadik fél)

Az elektronikus információs rendszerhez a hozzáférési jogosultságot az Informatikus biztosítja az engedélyezett feladatok és tevékenységek alapján a Jegyző vagy az elektronikus információ rendszer biztonságáért felelős személy engedélyével, az általa engedélyezett és szükséges időtartamra. A felhasználót az ilyen módon kiadott jogosultság egyedileg kell, hogy azonosítsa.

16.8. Hitelesítés szolgáltatók tanúsítványának elfogadása

Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat fogadhatja el az érintett szervezeten kívüli felhasználók hitelesítéséhez.

17. Hozzáférés ellenőrzési eljárásrend

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

- közlésre szánt és/vagy bárki által megismerhető adatok,
- bizalmas és belső szabályozóval védett adatok
- személyes adatok
- minősített, titkos adatok.

Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik.

Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot. Az érintettekkel ezt ismertetni kell. Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

Az adatok védelmét, a feldolgozás – az adattovábbítás, a tárolás - során az operációs rendszerben és a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver adatvédelem).

17.1. A felelősségek szétválasztása

A Hivatal elektronikus információs rendszereinek működése során a következő felelősségeket és szerepköröket kell szétválasztani, valamint biztosítani kell az ezeknek megfelelő jogosultságokat:

a) információbiztonsági felelős nem tölthet be informatikus, fejlesztő és EIR adminisztrátor szerepet;

b) Az informatikus nem tölthet be fejlesztő szerepet;

c) A jóváhagyó személye nem lehet azonos a végrehajtóval.

17.2. Legkisebb jogosultság elve

A Hivatal elektronikus információs rendszereiben a jogosultságok kezelésekor a szükséges, minimum elvet kell követni, azaz mindenki csak annyi jogosultságot kapjon, ami a munkája elvégzéséhez nélkülözhetetlen.
A felhasználó a munkaállomásán nem kaphat helyi rendszergazda jogot.

17.3. Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni. Minden felhasználónak jelszóval kell védenie a munkaállomását és az általa használt elektronikus információs rendszereit. Ezeket a jelszavakat illetéktelen személyektől gondosan védeni kell.
A jelszavaknak az alábbi minimális követelménnyel kell rendelkeznie:

- A hálózati jelszó legalább 8 karakterből álljon, kis és nagybetűk, valamint számok.
- Az alkalmazáshoz szükséges jelszavaknak a fejlesztő által megadott feltételeknek kell eleget tenniük.
- A jelszó nem lehet azonos a felhasználó névvel, annak becézett formájával, egymás után következő számokkal, vagy könnyen visszafejthető kifejezéssel.
- A hálózatba kötött számítógépek esetében a felhasználóknak a hálózati, illetve ennek hiánya esetén helyi bejelentkezési jelszavakat havonta meg kell változtatniuk.
- Ahol ezt az operációs rendszer támogatja, 5 sikertelen bejelentkezés után az operációs rendszernek le kell tiltani a felhasználó fiókját.
- A jelszó megváltoztatásakor az új jelszó nem lehet azonos a korábban használt 5 jelszóval.
- A jelszót nem szabad több személy között megosztani.
- A felhasználók jelszavát a felhasználón kívül senki sem ismerheti.
- A jelszót soron kívül meg kell változtatni, ha az illetéktelen személy tudomására jutott, vagy juthatott.

Külső felek által kért távoli hozzáférés biztosítása esetén a külső fél köteles írásban megkérni a hozzáférést az elektronikus információ rendszer biztonságáért felelős személytől, amelyben leírja a hozzáférés paramétereit, célját, idejét, az információs rendszerben végzett munka leírását.
Külső felek által kért helyszíni hozzáférés is biztonsági kockázatot rejt, ezért ebben az esetben is előre írásban egyeztetett paraméterek mellet adható ki a hozzáférés.

17.4. Felhasználói fiókok kezelése

Az Informatikus:

- meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait, és ezek típusait,
- megnevezi az elektronikus információs rendszer jogosult felhasználóit, és a hozzáférési jogosultságokat,
- kijelöli a felhasználói fiókok fiókkezelőit,
- ellenőrzi a felhasználói fiókok használatát, és szükség esetén törli ezeket.

Külső közreműködők által üzemeltetett rendszerek esetén (pl. weboldal, ASP szolgáltatás) a fentieket azzal az eltéréssel kell alkalmazni, hogy ha az Informatikus közvetlenül nem tudja a fiókokat kezelni, értesíti az üzemeltetőt (ASP esetén a Tenantot) vagy egyéb fiókkezelőt a fiókok létrehozásának vagy megszüntetésének, vagy módosításának szükségességéről.

17.5. Szoftver védelem

Rendszerszoftver védelem

A rendszergazdának biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

Teendők a következők:

- a rendszerszoftver módosításához a Jegyző engedélye szükséges,
- név szerint kell kijelölni azokat a személyeket, akik a rendszerszoftverben módosításokat végezhetnek,
- a módosítással egy időben, a dokumentációban is a változásokat át kell vezetni, a változtatásokról nyilvántartást kell vezetni.

17.6. Elektronikus levelezés védelme

A hatékony belső és külső kommunikáció érdekében a Hivatal elektronikus levelező szolgáltatást biztosít a felhasználóknak. Minden felhasználó rendelkezik hivatali e-mail címmel. Ezeket tilos magánlevelezésre, társasági minőségben használni (pl. regisztráció weboldalakra, online játék oldalakra, közösségi oldalakra stb.)! A Hivatal által nem támogatott levelezőrendszerek (pl. Gmail, Freemail, Yahoo, Citromail, stb.) használata munkavégzésre nem engedélyezett. Az elektronikus levelek és csatolmányok védelmi előírásai megegyeznek az egyéb dokumentumok védelmének előírásaival. Az elektronikus levelek tartalmát vírusellenőrzésnek vetjük alá. A Jegyző különleges és

indokolt esetben, vagy hatósági megkeresésre utasíthatja az elektronikus információ rendszer biztonságáért felelős személyt, hogy ellenőrizze a felhasználói postafiókot és a kérésnek megfelelően feljegyzést készítsen a Jegyzőnek.

17.7. Hozzáférés ellenőrzés érvényesítése

Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez. A hivatal vezetője határozza meg, hogy a felhasználó hogyan és milyen adatkörben jogosult külső információs rendszerben a hivatal által ellenőrzött adatokat feldolgozni.

17.8. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

A Hivatalnál nincs azonosítás vagy hitelesítés nélkül engedélyezett tevékenység.

17.9. Jogosult hozzáférés a biztonsági funkciókhoz

A Hivatal elektronikus információs rendszereiben a jelen Informatikai Biztonsági Szabályzatban megfogalmazott logikai védelmi intézkedések végrehajtása érdekében a következő biztonsági funkciók kerülnek megállapításra:

a) tűzfalak, behatolás-detektáló rendszerek üzemeltetése, konfigurálása

b) kártékony kód elleni védelem üzemeltetése, konfigurálása

c) operációs rendszerek üzemeltetése, konfigurálása

d) elektronikus információ rendszerek adminisztrálása

e) mentési rendszer üzemeltetése, konfigurálása

17.10. Nem privilegizált hozzáférés a biztonsági funkciókhoz

A biztonsági funkciók eléréséhez kifejezetten erre a célra létrehozott, egyedi azonosítóval lehet hozzáférni, melyet a napi munkavégzéshez tilos felhasználni.

17.11. Privilegizált fiókok

A biztonsági funkciók elérésére az Informatikus jogosult.

17.12. A munkaszakasz zárolása

A Hivatal munkaállomásain 10 perc inaktivitás után automatikusan életbe lépő képernyőzárolást kell alkalmazni, melyet csak a hálózati vagy a munkaállomáshoz tartozó jelszó megadását követően lehet inaktiválni.

17.13. Képernyőtakarás

A munkaszakasz zárolását oly módon kell megvalósítani, hogy a zárolási képernyőn vagy a felhasználó által beállított háttérkép, vagy egy üres képernyő látszódjon.

17.14. A munkaszakasz lezárása

A felhasználó a munkaidő végeztével köteles a munkaállomását kikapcsolni.

17.15. Vezeték nélküli hozzáférés

A Hivatalban csak az információ biztonsági felelős által jóváhagyott vezeték nélküli (továbbiakban: WiFi) hozzáférési pont létesíthető. A Hivatalban ad-hoc WiFi hálózat nem létesíthető.
Valamennyi hozzáférési pontot a Hivatal által biztosított eszközön kell létrehozni. Biztosítani kell a hozzáférési pontok felügyeletét. Minden hozzáférési pont részére külön VLAN-t kell létrehozni, úgy, hogy a hálózatok között nem lehet átjárás és az egy hálózatban lévő eszközök sem érhetik el egymást. Az internet és a belső hálózat elérése a központi tűzfalon keresztül történhet.
Valamennyi hozzáférési pont esetében szabványos, ismert sérülékenységektől mentes kriptográfiai megoldással támogatott azonosítást és hitelesítést kell alkalmazni.

17.16. Mobil eszközök hozzáférése

Mobil eszközzel csak a Hivatal által biztosított elektronikus levelezéshez lehet hozzáférni. Ebben az esetben csak a Hivatal által biztosított mobil eszköz használható.

17.17. Titkosítás

A Hivatal által biztosított mobil eszközökön be kell kapcsolni a teljes eszköz vagy tároló titkosítást.

17.18. Elektronikus információs rendszerek külső használata

A Hivatal tevékenységéből adódóan nem indokolt külső rendszerből hozzáférni a hivatalban működő elektronikus informatikai rendszerhez. Amennyiben erre mégis szükség van, az információ biztonsági felelőssel és az Informatikussal egyetértésben, meghatározott célból, meghatározott ideig engedélyezhető a külső hozzáférés úgy, hogy a hozzáférést végző személye azonosítható legyen.

17.19. Korlátozott használat

Külső elektronikus információs rendszert abban az esetben lehet a Hivatal elektronikus információs rendszereihez történő hozzáférés céljából felhasználni, hogy ha:

a) egyedi felhasználás során a külső elektronikus információs rendszerben az információ biztonsági felelős előzetesen ellenőrizte, vagy

b) cégszerű felhasználás során szerződésben rögzítették.

17.20. Hordozható adattároló eszközök

A távoli hozzáférésekhez alkalmazott VPN kapcsolatot úgy kell beállítani, hogy a kapcsolat idejére a mobil adathordozó eszközök ne legyenek csatlakoztathatók a VPN kapcsolatot létesítő eszközhöz.

17.21. Információ megosztás

A Hivatal elektronikus információs rendszereiben kezelt adatok külső fél részére történő továbbítása előtt az érintett felhasználónak meg kell vizsgálnia, hogy a vonatkozó szerződés vagy jogszabály alapján az adat átadható-e. Különös figyelmet kell fordítani a jogszabály által védett adatok továbbítására. Adattovábbítás esetén figyelembe kell venni a Hivatal Adatvédelmi Szabályzatában foglaltakat is. Az információ megosztással kapcsolatos követelményeket az adott terület vezetőjének ismertetnie kell a felhasználókkal.

17.22. Nyilvánosan elérhető tartalom

A Hivatal honlapja nyilvánosan hozzáférhető információkat tartalmaz. A honlap kezelésére kijelölt személy felelős azért, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat, valamint az adattartalom valós, hiteles legyen.

A szervezet vezetője vagy az általa felhatalmazott személy a felelős személyt kioktatja annak biztosítása és felismerése érdekében, hogy a nyilvánosan elérhető információk ne tartalmazzanak nem

nyilvános információkat. A szervezeten belül egy az adatokkal kapcsolatosan kompetens személynek át kell vizsgálnia a javasolt tartalmat közzététel előtt. A közzétett tartalmakat rendszeresen át kell vizsgálni annak érdekében, hogy ne tartalmazzanak nem nyilvános információt és/vagy elavult, téves információkat.

17.23. Külső elektronikus információs rendszerek szolgáltatásai

A Hivatal a szolgáltatási szerződésben követelményként fogalmazza meg az általa igénybe vett elektronikus információs rendszerekkel szembeni elvárásokat, hogy ezek megfeleljenek az érintett szervezet elektronikus információbiztonsági követelményeinek. Dokumentálja a külső szervezet feladatait és a kezelt adatok és folyamatokkal kapcsolatos kockázatok szerint a információbiztonsági követelményeknek való megfelelést ellenőrzi.

18. Biztonsági események bejelentésének eljárásrendje

A biztonsági események gyors és hatékony elhárítása érdekében az alábbi bejelentési eljárást vezetjük be. A Hivatal munkatársai az őket érintő, illetve az általuk észlelt információbiztonsági eseményekről kötelesek haladéktalanul értesíteni a közvetlen munkahelyi vezetőjüket, az Informatikust és az elektronikus információ rendszer biztonságáért felelős személyt. A biztonságot érintő eseményről jelentést kell készíteni jelen szabályzat 16. mellékletében található űrlapon.

Ha az elektronikus információ rendszer biztonságáért felelős személy úgy ítéli meg, hogy az esemény magas kockázattal veszélyezteti a védendő értékeket, a jogszabályoknak megfelelően köteles a Hatóságnak jelenteni azt. Továbbá kivizsgálást kell kezdeményeznie a jelentés alapján és javaslatot kell tennie a Jegyzőnek az esemény előfordulási esélyének csökkentése, illetve az okozott kár mérséklése érdekében.

Amennyiben a biztonsági esemény egyértelműen az információbiztonsági szabályok megszegéséből adódott, fegyelmi eljárást kell kezdeményezni.

19. Fegyelmi eljárásrend

Az a munkavállaló, aki az Informatikai Biztonsági Szabályzatban foglaltakat megsérti, vagy nem tartja be és ezzel a Hivatalnak anyagi vagy erkölcsi kárt okoz, ellene a Jegyző fegyelmi eljárást kezdeményez, és rá a közszolgálati tisztviselőkről szóló 2011. évi CXCIX törvény 155. §-ban

meghatározott fegyelmi felelősségi, fegyelmi büntetési tételek a mérvadók. Bűncselekmény elkövetése estén a büntetőjogi felelősség is fennáll.

20. Belső ellenőrzés

A Hivatal éves belső ellenőrzési ütemtervében rögzíti az ellenőrzés módját.

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszerben meglévő veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése, illetve annak megakadályozása, hogy az megismétlődjön.

21. Önkormányzati ASP rendszerrel kapcsolatos biztonsági követelmények meghatározása

A 257/2016. (VIII. 31.) Korm. rendelet 2. melléklete tartalmazza a minimumkövetelményekhez tartozó megfelelés elvárását. Ez alapján ki kell alakítani azt az informatikai infrastruktúra környezetet, amellyel biztosított az önkormányzati ASP rendszer használata. Adminisztratív, fizikai és logikai védelmi intézkedések terén a jelen Informatikai Biztonsági Szabályzat megfelelő pontjai a mérvadók és betartandók az önkormányzati ASP rendszer használata során.

22. Záró rendelkezések

Az Informatikai Biztonsági Szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat. A munkaköri leírások elkészítéséért, aktualizálásáért a szervezeti egység vezetője (irodavezető) a felelős.

A szabályzatot jogszabályi, technológiai vagy szervezeti változás esetén módosítani kell.

Az Informatikai Biztonsági Szabályzat 2019. év január hó 1. napjával lép hatályba.

Celldömölk, 2019. január 1.

CELLDÖMÖLKI KÖZÖS ÖNKORMÁNYZATI HIVATAL 1.

Farkas Gábor
jegyző

Jóváhagyta:

Fehér László
polgármester

CELLDÖMÖLK VÁROS POLGÁRMESTERE

MELLÉKLETEK

1. melléklet

Elektronikus információ rendszer biztonságáért felelős személy kijelölése

Jelen szabályzat 3.2.2. pontja alapján az elektronikus információ rendszer biztonságáért felelős személy feladatai ellátásával megbízott munkavállaló:

- neve: Némethné Berki Veronika
- beosztása: elektronikus információ biztonságért felelős személy

Kelt: Celldömölk, 2019. január 1.

CELLDÖMÖLKI KÖZÖS ÖNKORMÁNYZATI HIVATAL 1.

Farkas Gábor
jegyző

Záradék: az elektronikus információ rendszer biztonságáért felelős személy feladatai ellátására való kijelölést tudomásul veszem, a Szabályzatot és az abban foglaltakat megismertem és magamra nézve kötelezőnek ismerem el.

Kelt: Celldömölk, 2019. január 1.

aláírás

2. melléklet

Megismerési nyilatkozat

Az Informatikai Biztonsági Szabályzatban foglaltakat az oktatás során megismertem.

Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

Név	Beosztás	Kelt	Aláírás

3. melléklet

Felhasználói jogosultság és változás nyilvántartás

Felhasználó:	**Beosztás:**	**Szervezeti egység:**
Dátum:	**új** **változás** **törlés**	

Alkalmazás megnevezése:	**Igény részletezése:**	**Jogosultság:**

A felhasználó tudomásul veszi, hogy:

- a rábízott adatokért és jogosultságokért személyes felelősséget vállal,
- felhasználói-azonosítóját és jelszavát nem szolgáltathatja ki más személynek,
- a saját számítógépén és a hozzákapcsolódó rendszerekben létrehozott és kezelt állományok beleértve az elektronikus levelezést is –, a Celldömölki Közös Önkormányzati Hivatal tulajdonát képezik, ezért a Hivatal szabályzatokban és utasításokban feljogosított ellenőrző szerveinek, ezekhez az állományokhoz, a vizsgálathoz szükséges mértékig betekintési joga van.

Kelt: Celldömölk,

_____ felhasználó

_____ engedélyező / jegyző

A jogosultságot a kérelemnek megfelelően beállítottam:

_____ informatikus

4. melléklet

Nyilatkozat

Alulírott (név: ,.....

beosztás:.....szervezeti

egység: .....), kijelentem, hogy a Celldömölki Közös Önkormányzati Hivatal Informatikai Biztonsági Szabályzatának tartalmát megismertem és elfogadom, hogy azt munkám során betartom, illetve betartatom (vezetők esetén).

....., 201 . .....

.....

Aláírás

5. melléklet

Információbiztonsági tájékoztatás

1. A Celldömölki Közös Önkormányzati Hivatalban (továbbiakban: a Hivatal) működő elektronikus információs rendszereket a Hivatal kizárólag hivatali munkavégzés céljából biztosítja a munkavállalók részére, az elektronikus információs rendszerekben keletkező és ott tárolt, kezelt adatok, információk vonatkozásában a Hivatal fenntartja magának a tulajdonjogot.
2. A Hivatalnak továbbra is hozzáférési lehetősége van a korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz.
3. A Celldömölki Közös Önkormányzati Hivatallal fennálló köztisztviselői jogviszony megszűnésének napjától, a munkavállalónak a Hivatal elektronikus információs rendszereihez való hozzáférési jogosultsága megszűnik. Legkésőbb ezen a napon köteles a használatában lévő, a Hivatal elektronikus információs rendszerével kapcsolatos valamennyi eszközt hiánytalanul, sértetlenül munkáltatója részére visszaszolgáltatni.
4. Közszolgálati jogviszonyának megszűnését követően nem jogosult a Hivatal elektronikus információs rendszereiben tárolt, közszolgálati jogviszonya folytán készített, illetve megismert adatokat felhasználni, azokat további személyek tudomására hozni, valamint a megismert és használt elektronikus információs rendszerek összetételéről, felépítéséről, működéséről további személyek számára bárminemű információt közölni.
5. A 4-es pontban megfogalmazott jogellenes magatartásnak polgári- és büntetőjogi következményei lehetnek.
6. Jelen tájékoztatás célja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 41/2015. (VII.15.) BM rendelet 3. § (1) bekezdésében foglaltak szerint, az e rendelet 3. számú mellékletében meghatározott követelményeknek a 4. számú melléklet 3.1.6.4.1.3. pontjában meghatározott módon való megvalósítása.

Celldömölk, 2019. január 1.

.....
jegyző

A fenti tájékoztatást tudomásul vettem:

Celldömölk, 201

.....
köztisztviselő neve

.....
aláírása

6. melléklet

Hardver eszköz nyilvántartás

Kötelező adattartalom:

- Számítógép hálózati neve
- Felhasználó neve
- Beosztása
- Processzor típusa, frekvenciája
- Memória mérete, típusa
- Háttértár mérete, típusa
- Operációs rendszer, teljesítmény
- Office verziója
- Adobe Reader verziója
- Böngésző típusa
- Egyéb program

7. melléklet

Szoftver nyilvántartás

ELEKTRONIKUS INFORMÁCIÓS RENDSZER NYILVÁNTARTÁS

Elektronikus információs rendszer megnevezése:	
Alapfeladatai:	
Biztosított szolgáltatások:	
Licenc szám:	
Rendszerfelügyeletet gyakorló személy:	
Azonosító adatai, elérhetőségei:	
Szállító/fejlesztő/karbantartó szervezetek elérhetőségi adatai:	
Kapcsolattartó személy:	
Elérhetőségei:	

8. melléklet

Biztonsági osztályba sorolási útmutató

Minden egyes elektronikus információs rendszerben kezelt adatfajtát kategorizálni kell a bizalmasság, a sértetlenség és a rendelkezésre állás szerint annak alapján, hogy mekkora kár éri a szervezetet, hogy ha az adatnak valamelyik jellemzője sérül.

A biztonsági osztályba sorolást az információ biztonsági felelős készíti elő az adatgazdák bevonásával, akik előzetesen kijelölésre kerültek az általuk kezelt adatok vonatkozásában.

A károk meghatározásához a következő kárérték-táblázatokat kell használni.

A bizalmasság kárérték-táblázata

Kárérték szint/Kárfajta	Anyagi kár	Társadalmi politikai hatás	Jogszabályi következmény
1. nem értelmezhető	-	Nyilvános adat	-
2. csekély kár	100.000 Ft	Kínos helyzet a szervezeten belül	Belső szabályozóval védett adat bizalmassága sérül, néhány személyes adat sérül
3. közepes kár	1.000.000 Ft	Bizalomvesztés a szervezet középvezetésében, bocsánatkérést és/vagy fegyelmi intézkedést igényel.	Tömeges személyes adat bizalmassága sérül
4. nagy kár	10.000.000 Ft	Bizalomvesztés a szervezet felső vezetésében, a középvezetésen belül személyi konzekvenciák	különleges adat bizalmassága sérül
5. nagyon nagy kár	100.000.000 Ft	Súlyos bizalomvesztés a szervezet felső vezetésében, a szervezet felső vezetésén belül személyi konzekvenciák	Kiemelten tömeges különleges adat bizalmassága sérül

A sértetlenség kárérték-táblázata

Az elektronikus információs rendszer vagy az abban tárolt adat pontatlansága esetén a kár mértéke:

Kárérték szint/Kárfajta	Anyagi kár	Közvetett anyagi kár	Társadalmi politikai hatás
1. jelentéktelen kár	10.000 Ft	1 emberórával állítható helyre	Nincs bizalomvesztés, a probléma a szervezeten belül marad
2. csekély kár	100.000 Ft	1 embernappal állítható helyre	Kínos helyzet a szervezeten belül
3. közepes kár	1.000.000 Ft	1 emberévvel állítható helyre	Bizalomvesztés a szervezet középvezetésében, bocsánatkérést és/vagy fegyelmi intézkedést igényel.
4. nagy kár	10.000.000 Ft	1-10 emberévvel állítható helyre	Bizalomvesztés a szervezet felső vezetésében, a középvezetésen belül személyi konzekvenciák
5. nagyon nagy kár	100.000.000 Ft	10-100 emberévvel állítható helyre	Súlyos bizalomvesztés a szervezet felső vezetésében, a szervezet felső vezetésén belül személyi konzekvenciák

A rendelkezésre állás kárérték-táblázata

Az elektronikus információs rendszer vagy az abban tárolt adatok rendelkezésre állásának elvesztése esetén (nem elérhető a rendszer vagy az adat) a kár mértéke:

Kárérték szint/Kárfajta	Anyagi kár	Közvetett anyagi kár	Társadalmi politikai hatás
1. jelentéktelen kár	10.000 Ft	1 emberórával állítható helyre	Nincs bizalomvesztés, a probléma a szervezeten belül marad
2. csekély kár	100.000 Ft	1 embernappal állítható helyre	Kínos helyzet a szervezeten belül
3. közepes kár	1.000.000 Ft	1 emberévvel állítható helyre	Bizalomvesztés a szervezet középvezetésében, bocsánatkérést és/vagy fegyelmi intézkedést igényel.
4. nagy kár	10.000.000 Ft	1-10 emberévvel állítható helyre	Bizalomvesztés a szervezet felső vezetésében, a középvezetésen belül személyi konzekvenciák
5. nagyon nagy kár	100.000.000 Ft	10-100 emberévvel állítható helyre	Súlyos bizalomvesztés a szervezet felső vezetésében, a szervezet felső vezetésén belül személyi konzekvenciák

9. melléklet

Szoftverek biztonsági osztályba sorolása

Az informatikai rendszer megnevezése	Rendszer leírása	Adatgazda	Üzemeltető	A rendszerben kezelt adatok	Besorolás			Információs rendszer biztonsági osztálya	A szervezet biztonsági szintje
					Bizalmasság	Sértetlenség	Rendelkezésre állás		
EBR42	Pályázati elszámolási rendszer	Műszaki Iroda	Magyar Államkincstár – (felhő alapú)	Pályázati elszámolási adatok	1	1	1	1	
EADAT	bérjegyzékek, könyvelési tételek	Pénzügyi Iroda	MÁK (-felhő alapú)	Főkönyvi adatok, könyvelési adatok, folyószámla, tárgyi eszköz, stb	2	2	1	2	
KIRA	Államkincstári bérszámfejtő, időnyilvántartó prg.	Pénzügyi Iroda	MÁK (-felhő alapú)	Bérszámfejtési adatok	2	2	1	2	
ÖNEGM	Lakossági természetbeni juttatások rendszere	Pénzügyi Iroda	MÁK (-felhő alapú)	Lakossági természetbeni juttatás adatok	2	2	1	2	
CSTINFO	Szociális családi támogatás rendszer	Titkárság	MÁK (-felhő alapú)	Csak adat lekérdezés történik, MÁK rögzítés	1	1	1	1	

PTR	Települési támogatások, rendszeres gyermekvédelmi kedvezmény	Titkárság	MÁK (-felhő alapú)	Települési támogatások, személyes adatok	2	2	1	2
KONTROLLER	iktató program	Titkárság	Hivatal -szerver	minden bejövő, kimenő dokumentáció	1	1	1	1
TÉR	Dolgozók teljesítményértékelése	Irodavezetők	MÁK (-felhő alapú)	Hivatali dolgozók teljesítmény adatai	2	2	1	2
PROBONO-UNI	Hivatali képzési rendszer	minden munkavállaló	MÁK (-felhő alapú)	Hivatali dolgozók képzettségi, kompetencia adatai	2	2	1	2
ETDR	Építéshatósági nyilvántartás	Műszaki Iroda	NISZ- felhő	Építményekkel kapcsolatos dokumentáció	2	2	1	2
OENY	Országos építésügyi nyilvántartás	Műszaki Iroda	NISZ -felhő	Épület, építési nyilvántartási adatok	1	1	1	1
NVR	választási rendszer	Helyi Választási Iroda	NISZ -felhő	névváltozás, átjelentkezés,	2	2	2	2
VÁKÍR	Választási rendszer	Helyi Választási Iroda	NISZ -felhő	Önkormányzati választási adatok	2	2	2	2
NJT	kormányhivatallal történő törvényességi s kapcsoltatás	Titkárság	Közig és Igazságügyi Min.	önkormányzati rendeletek.	2	2	1	2

				bizottsági Címzetes Főjegyzőkönyvek				
ASZA	anyakönyvezési rendszer	Titkárság	felhő alapú	Anyakönyvi adatok, személyes adatok	2	2	1	2
Backup szerver		Titkárság	Hivatal	teljes aktív dir, dokumentáció , users, közös mappa	2	2	2	2

10. melléklet

Információs rendszerelemek be/kiszállításának nyilvántartása

Információs rendszerelem megnevezése:	
Gyári száma:	
Az eszközt átadó személy neve:	
Munkahelye:	
Beosztása:	
Az eszközt átvevő személy neve:	
Munkahelye:	
Beosztása:	
Az átadás időpontja:	
Az átvétel időpontja:	

Kelt: Celldömölk,

_____ átadó

_____ átvevő

11. melléklet

Karbantartók nyilvántartása

Karbantartó megnevezése:	
Kapcsolattartó neve:	
Elérhetőségei:	
Karbantartott eszközök/szoftverek megnevezése:	

12. melléklet

Titoktartási nyilatkozat

Alulírott

Név: _____

Anyja neve: _____

Lakcím: _____

Sz. ig. szám: _____

a ..... munkatársa kijelentem, hogy

a **Celldömölki Közös Önkormányzati Hivatal,** mint **Megrendelő,**

valamint .....

mint **Vállalkozó**

között

.....tárgyú,

..... **-én megkötött vállalkozási/megbízási/szállítási szerződés**

keretében elvégzett feladatok során tudomásomra jutott információkat és adatokat bizalmasan kezelem és megtartom. A tudomásomra jutott információkat, adatokat az érdekkörön kívüli személlyel nem közlöm. Ezen felelősségem fennáll azt követően is, ha a

.....-vel való szerződéses jogviszonyom bármely okból megszűnik.

Celldömölk, 201 .....

.....

Nyilatkozó

	Tanú 1	**Tanú 2**
Aláírás:	_____	_____
Neve:	_____	_____
Anyja neve:	_____	_____
Lakcím:	_____	_____
Sz. ig. szám:	_____	_____

13. melléklet

Kockázatelemzési és kezelési módszertan

Az egyes vagyonelemek gyenge pontjait és fenyegetettségeit KIB 25. számú ajánlása: 25/1-3. kötet: Az Információbiztonság Irányításának Vizsgálata (IBIV) 1.0 verzió segédletei alapján a következőképpen állapítja meg:

A kockázat meghatározása során a veszély megvalósulásának valószínűsége és az okozható kár alapján, az adott veszélyt képviselő sérülékenység kihasználhatósága és ennek hatása alapján történik. A veszélyeztetett információk vagy azok csoportjaira külön-külön meg kell állapítani a kockázatot, a teljesség kialakítása céljából.

A gyakorlatban célszerű kategóriákkal dolgozni, amelyek az adott környezet működéséhez igazodnak.

A hatások kategorizálása a közigazgatás szemszögéből:

- **Alacsony**, várhatóan korlátozott hátrányos hatást gyakorol a közigazgatási szervezet műveleteire vagy a szervezet eszközeire.
    - A korlátozott hátrányos hatás azt jelenti, hogy a szolgáltatási képességet oly mértékben és olyan időtartamra csökkentheti, hogy a szervezet képes végrehajtani ugyan elsődleges funkcióit, de a funkciók hatásossága észrevehetően csökken. Az ügyek lefolytatásában fennakadást okoz, de a sikeres lefolytatást és határidők betartását nem veszélyezteti.
    - A szervezeti eszközök kisebb mértékű károsulását eredményezi.
    - Kisebb mértékű pénzügyi veszteséget okoz.
    - A jogbiztonságot kisebb mértékben veszélyezteti, a személyes és/vagy közhiteles adatok védelmével kapcsolatban felmerül a lehetőség, hogy a helyzet javítása nélkül az adatok védelme sérülhet.
- **Fokozott**, várhatóan komoly hátrányos hatást gyakorol a közigazgatási szervezet műveleteire vagy a szervezet eszközeire.
- **Kiemelt**, várhatóan súlyos vagy katasztrofális hatást gyakorol a közigazgatási szervezet műveleteire vagy a szervezet eszközeire.

A bekövetkezési valószínűsége lehet:

- **Magas** – bármikor előfordulhat. mert pl. gyakori esemény, vagy a támadást bárki végrehajthatja. Ilyen lehet például egy vírustámadás.
- **Közepes** – gyakran előfordulhat, pl. célzott számítógépes betörés a rendszerbe.
- **Alacsony** – az előfordulása a vizsgált rendszer vagy szervezet működési idejéhez képest nem gyakori. Ilyen lehet például tűzeset vagy természeti csapás.

A várható kár és a bekövetkezés valószínűsége alapján a kockázat is kategorizálható:

Hatás/valószínűség	*alacsony*	*közepes*	*magas*
alacsony	mérsékelt	alacsony	alacsony
fokozott	jelentős	mérsékelt	alacsony
kiemelt	kritikus	jelentős	mérsékelt

VÉDELMI INTÉZKEDÉSEK

A védelmi intézkedések, alábbi csoportosítása, amely segíti a veszélyekhez rendelt intézkedések kidolgozását, azon az alapon, hogy a veszélyt megelőzni, észlelni, vagy javítani kívánjuk:

- **Megakadályozó** (preventív): a megelőzés során olyan tevékenységeket kell végrehajtani, amely lehetetlenné teszi a veszélyes esemény bekövetkeztét (pl. email tartalomszűrés, amellyel megelőzzük vírusok levelezésen keresztüli bejutását).
- **Észlelő** (detektáló): az észlelés során a már folyamatban lévő támadást, károkozást próbáljuk – lehetőleg minél hamarabb – észlelni, majd ez alapján megszüntetni, mielőtt lényegi károkozásra kerülne sor. Ilyen például a behatolás jelző (IDS) rendszer használata, amely gyanús hálózati forgalom esetén riasztást ad. Az észlelés alapján azután más tevékenységeket is végezhetünk.
- **Helyreállító** (korrektív): a javító intézkedés a már megtörtént esemény által okozott kárt csökkenti vagy szünteti meg. Javító intézkedés például a rendszer visszaállítása mentésből, de ilyen intézkedés akár az is, ha biztosítással rendelkezünk, amely kár esetén biztosít fedezetet.

Ezt a hármast szokás az angol megnevezések alapján **PreDeCo**-nak (Preventive – megakadályozó, Detective – észleli, Corrective – helyreállító) nevezni.

Az egyes veszélyforrásokra vonatkozóan megállapíthatók a védelmi intézkedések, ezek kidolgozása során használhatjuk a CIA (bizalmasság, sértetlenség vagy rendelkezésre állás) elvet, minden veszélyforráshoz hozzárendelve az általa képviselt kockázatot, az azt megvalósító bizalmasság, sértetlenség vagy rendelkezésre állás sérülését és az ezeket megelőző, detektáló vagy javító intézkedéseket.

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
elektronikus információsrendszerek, végponti állomások	Érzékeny adatok ellopása, adat fájlok törlése, ellopása, módosítása.	Hozzáférés védelem beállítása.
	Rosszindulatú program (vírus, trójai faló, stb.) bejuttatása a rendszerbe.	Vírusvédelmi rendszer alkalmazása.
	Vírus, trójai faló, féreg aktiválódása, pl. email csatolmány megnyitásakor.	Vírusvédelmi rendszer alkalmazása.
	Végrehajtható programok, script-ek (Java Applet, JavaScript, VB Script, CGI, stb.) letöltése, pl. az állomás DoS támadásra való felhasználására a felhasználó tudtán kívül.	Böngésző biztonsági beállítása.
	Web és alkalmazásba csomagolt ActiveX objektumok, amelyek a programozó szándékától függően a legkülönbözőbb károkat (gépleállítás, konfiguráció feltérképezés, monitor/billentyűzet elvétel, stb.) okozhatják.	Böngésző biztonsági beállítása.
	Ismeretlen forrásból érkező emailek és azok csatolmányainak megnyitása.	Vírusvédelmi rendszer alkalmazása, felhasználó oktatása.
	Az Internet böngészőkben meglévő biztonsági „lyukak" megszüntetésére szolgáló javító programok letöltésének elmulasztása. A biztonsági „lyukak" kihasználásával elérhetők a végponti felhasználó érzékeny adatai (jelszó, az állomás konfigurációja, fájlnevek, fájl struktúra, a meglátogatott (weblapok címei, stb.).	Legújabb verziók, frissítések telepítése.
	A munkaállomásra letöltött adatlapok (kérdőív, adatszolgáltató formanyomtatvány, stb.) programhibái. A szolgáltatott adatok rejtjelezés nélküli elküldése.	Csak megbízható forrásból származó program használata.
	Vírusvédelmi program frissítésének elmulasztása.	Rendszeres, automatikus frissítés.
	Az igénybevett szolgáltatás letagadása.	Naplózás.
	A munkaállomás ellopása.	Követelményrendszer szerinti fizikai biztonság kialakítása.

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
Mobil eszközök	Mobil eszköz ellopása	Az előírt fizikai védelmi eszközök alkalmazása. Követelményrendszer szerinti hozzáférés-védelem és rejtjelezés alkalmazása.
Internet	A felhasználó login adatainak (felhasználói-azonosító, jelszó) lehallgatása, ezek segítségével a felhasználó megszemélyesítése.	Rejtjelezett adatátviteli csatorna használata.
	Érzékeny adatok lehallgatása.	Rejtjelezett adatátviteli csatorna használata.
	Adatok lehallgatás és továbbítása megváltoztatott tartalommal elleni védelme.	Hozzáférés-vezérlés kialakítása. Rejtjelezett adatátviteli csatorna. Egyszer használatos jelszó.
	E-mail-ek, elektronikus dokumentumok eltérítése.	Hozzáférés-vezérlés kialakítása.
Tűzfal	Tűzfal-biztonságpolitika hiánya vagy hiányos volta.	Tűzfal-biztonságpolitika elkészítése, vagy aktualizálása.
	Ad hoc vagy nem a biztonságpolitikának megfelelő biztonsági beállítás, vagy üzemeltetés.	Biztonsági beállítások rendszeres ellenőrzése, naplózás, riasztás.
	Portok letapogatása.	Tűzfal biztonsági beállítása.
	IP cím megszemélyesítés, a támadó a védett hálózaton működő számítógép (pl. szerver) IP címét megszerezve egy belső munkaállomást „szimulálva" a tűzfalon keresztül fér hozzá a szerveren levő adatállományokhoz.	Megfelelő hálózati biztonságpolitika, architektúra terv kialakítása.
	Visszaélés, forrás útvonalválasztással. A támadó a védett belső hálózat felépítésének ismeretében a saját gépében meghatározott útvonallal és belső IP címmel belső gépet „játszik el" és fér hozzá az útvonal végén levő belső géphez.	Megfelelő hálózati biztonságpolitika, architektúra terv kialakítása. Hálózati végpont IP címhez, MAC címhez kötése.
	Szerver típus specifikus biztonsági lyukak az operációs rendszerben. Az aktuális javító- és szerviz csomagok telepítésének elmulasztása.	Operációs rendszerek biztonsági frissítéseinek folyamatos figyelése, végrehajtása.
	A tűzfal távoli, pl. Interneten keresztül történő adminisztrálása.	Tűzfal adminisztrálása csak védett hálózatból, vagy konzolról.

	Vírusvédelmi programok frissítésének elmulasztása.	Vírusvédelmi rendszer folyamatos frissítése.
	Hiányos biztonsági naplózás. A biztonsági naplók értékelésének elmulasztása vagy rendszertelensége.	Minden jelentős biztonsági esemény naplózása, naplózott események folyamatos értékelése.
	Hiányos fizikai biztonság.	Követelményrendszer szerinti fizikai biztonság kialakítása.

14. melléklet

Önkormányzati ASP rendszer biztonsági osztályba sorolása

NEM NYILVÁNOS!

Alkalmazás neve	Alkalmazás leírása	A rendszer elvárt biztonsági osztálya		
		Bizalmasság	Sértetlenség	Rendelkezésre állás
ASP – KERET	Önkormányzati ASP – keretrendszer	4	4	4
ASP – ADÓ	Önkormányzati ASP – önkormányzati adórendszer	4	4	4
ASP - BUGNET	Önkormányzati ASP – támogató rendszer (hibajegykezelő)	2	2	2
ASP – GAZDÁLKODÁS	Önkormányzati ASP – gazdálkodási rendszer	3	3	3
ASP - HAGYATÉK	Önkormányzati ASP – hagyaték leltár rendszer	3	3	3
ASP – INGATLANVAGYON-KATASZTER	Önkormányzati ASP – ingatlanvagyon-kataszter rendszer	3	3	3
ASP – IPAR ÉS KERESKEDELEM	Önkormányzati ASP – ipar- és kereskedelmi rendszer	3	3	3
ASP – IRATKEZELŐ	Önkormányzati ASP – Iratkezelő rendszer	3	3	3
ASP – PORTÁL	Önkormányzati ASP – települési portál rendszer, valamint elektronikus ügyintézési portál rendszer, ideértve az elektronikus űrlap-szolgáltatást	3	3	2

Az ASP Központ a változtatás jogát fenntartja!

15. melléklet

Selejtezési jegyzőkönyv

Készült: .....év ..... hó .... napján.

Jelen vannak:

Selejtezési Bizottság részéről (név, beosztás):

A Selejtezési Bizottság (továbbiakban: Bizottság) megállapítja, hogy jelen eljárás keretében végrehajtandó selejtezés engedélyezése Celldömölki Közös Önkormányzati Hivatal Jegyzőjének hatáskörbe tartozik.

A Bizottság megtekintette az előkészített eszközöket, megvizsgálta selejtezésük/leértékelésük indokoltságát.

A Bizottság a jegyzőkönyv mellékletében felsorolt eszközök hulladékkénti kezelését javasolja.

A szükséges intézkedések megtételéért (raktárra vétel, értékesítés, megsemmisítés) .....informatikus felelős.

Aláírások:

.....

.....

.....

A selejtezési jegyzőkönyvben foglaltakkal egyetértek, az abban felsorolt eszközök selejtezését/leértékelését, illetve megsemmisítését jóváhagyom.

Elrendelem a változások nyilvántartásokon történő keresztülvezetését, valamint a selejtezésből hasznosítható készletek hasznosításának végrehajtását.

Kelt: Celldömölk, 20.....

.....

jegyző

Selejtezési jegyzőkönyv melléklete

Megnevezése	Azonosító szám	Mennyiség	M.e.	Nettó érték Ft	Bruttó érték Ft	Selejtté válás oka	Hasznosítás módja

16. melléklet

Biztonsági események jelentése

A biztonsági esemény megnevezése:

A tapasztalás helye és idő pontja:

Az érintett személyek megnevezése:

Az esemény pontos leírása:

Az észlelő neve:

Dátum:_____év___hó___nap ....

Észlelő aláírása IBF aláírása

Az esemény kivizsgálásának leírása:

Tett intézkedés leírása:

Az intézkedés életbelépésének időpontja:

Végleges-e az intézkedés:

	Igen
	Nem

Igényel-e kockázatelemzést az esemény:

	Igen
	Nem

Dátum:_____év___hó___nap ....

Információbiztonsági felelős jegyző

17. melléklet

CELLDÖMÖLKI KÖZÖS ÖNKORMÁNYZATI HIVATAL INFORMATIKAI BIZTONSÁGI KÉZIKÖNYVE

Felhasználói Házirend

Általános rész

1. A Házirend célja

A Házirend célja, hogy a Celldömölki Közös Önkormányzati Hivatalban (továbbiakban: a Hivatal) az informatikai eszközöket és az elektronikus információs rendszereket használó felhasználók megismerjék azokat a feltételeket, szabályokat, amelyek betartása szükséges az informatikai eszközök és elektronikus információs rendszerek folyamatos és biztonságos működése érdekében. Továbbá jelen Házirend alapul szolgál a felhasználók általános informatikai biztonsági oktatásának.

A Hivatal elektronikus információs rendszereinek védelme érdekében a Hivatal kidolgozta az Informatikai Biztonsági Szabályzatát. Az Informatikai Biztonsági Szabályzat (továbbiakban: az IBSZ) tartalmazza valamennyi információbiztonsággal kapcsolatos szabályt, melynek betartásával az érintettek által elvárt szinten tartható a Hivatal elektronikus információs rendszereinek és az azokban kezelt adatok biztonsága bizalmasság, sértetlenség és rendelkezésre állás szempontjából.

Az IBSZ számos olyan védelmi intézkedést tartalmaz, amely közvetlenül nem kapcsolódik a Hivatal felhasználóihoz, ezért a jelen Házirendnek az is célja, hogy egy kivonatot adjon az IBSZ felhasználókra vonatkozó előírásairól, illetve néhány helyen kiegészítse és tovább részletezze az IBSZ-ben foglalt magasabb szinten meghatározott követelményeket.

1.1. A Házirend általános követelményei

A Házirend előírásainak alkalmazása, betartása, illetve betartatása, az IBSZ *1.1. Szervezeti-személyi hatály* pontban megjelöltek számára kötelező. A szabályok be nem tartása jogi, munkaügyi, illetve szerződésben meghatározott következményeket vonhat maga után. A Házirend el nem olvasása nem mentesít a felelősség alól.

Az információbiztonsági előírások betartása megvédi a Hivatalt és annak felhasználóit, ügyfeleit, partnereit, adataik és információik jogosulatlan vagy véletlenszerű nyilvánosságra jutásától, módosításától, megrongálódásától, megsemmisülésétől.

A munkahelyi vezető közvetlenül felelős azért, hogy az ellenőrzése alá tartozó felhasználók betartsák a Házirend előírásait.

A Hivatal elektronikus információs rendszereit csak az IBSZ *4. mellékletében* található nyilatkozat aláírása után lehet használatba venni.

2. Bevezetés

A Hivatal által kezelt információk érzékenysége miatt azok védelme, azaz bizalmas kezelése, sértetlensége, valamint megfelelő szintű rendelkezésre állása kritikus tényező.

A hivatali ügyviteli folyamatok zökkenőmentes működése nagymértékben az informatikai eszközeire és az elektronikus információs rendszereire épül, így ezek kiesése, vagy megsemmisülése esetén a Hivatal egyes funkciói működésképtelenné válhatnak, valamint a Hivatal által kezelt érzékeny információk illetéktelen kezekbe kerülhetnek.

A Hivatal elektronikus információs rendszereinek minden felhasználója személyes felelősséggel tartozik a munkájával kapcsolatban a birtokában lévő, illetve a tudomására jutott adatok, információk megfelelő kezeléséért, az informatikai biztonsági szabályok betartásáért.

3. A felhasználó jogai, kötelességei és felelőssége

A felhasználóknak az elektronikus információs rendszerek használata során a következők a kötelességeik, jogaik és felelősségeik.

3.1. A felhasználó kötelessége

Az információk védelmét azok keletkezésének, feldolgozásának, szétosztásának, tárolásának és selejtezésének teljes folyamata, életciklusa során biztosítani kell.

- A felhasználó köteles az általa használt informatikai eszközöket és az elektronikus információs rendszereket rendeltetésüknek megfelelően használni. Köteles a tőle elvárható gondossággal eljárni az eszközök használata során, védeni azokat a rongálás vagy szándékos károkozástól.
- A felhasználó a használatába adott eszközökön csak a munkavégzéséhez szükséges feladatokat végezheti, magán célokra nem használhatja azt. Tilos az eszközök személyes haszonszerzés, illetve nem a hivatal érdekében történő használata. Tilos a politikai (a hivatali feladatokon kívüli) vagy erkölcsi, vagy más törvénybe, vagy jó erkölcsbe ütköző anyagok készítése, tárolása, közlése,

megjelenítése a hivatal eszközein. Az eszközöket a hivatal helyiségeiből csak külön engedéllyel szabad kivinni.

- Minden felhasználónak bizalmasan kell kezelnie valamennyi felhasználói azonosító, jelszó, eToken, kulcs, vagy bárminemű egyéb, a Hivatal erőforrásaihoz hozzáférést biztosító eszközt. A személyi azonosító kódokat, jelszavakat szigorúan titokban kell tartani. Még a közeli munkakapcsolatban álló, egymást jól ismerő kollégák sem közölhetik ezeket egymással.
- A Hivatalban az alkalmazottak csak a Hivatal tulajdonát képező számítógépeket és engedélyezett szoftvereket használhatják. Ettől eltérni csak az elektronikus információbiztonsági felelős vagy az informatikus engedélyével lehet.
- Az informatikust kivéve, tilos a Hivatal számítógépeire szoftvereket telepíteni, és azokat futtatni.
- Kizárólag a munkavégzéshez szükséges adathordozók használata engedélyezett.
- Amennyiben a felhasználó olyan adatokhoz fér hozzá, amelyek kezelésében nem illetékes, a hibát jeleznie kell munkahelyi vezetőjének.
- Valamennyi alkalmazott köteles azonnal értesíteni a rendszergazdát minden olyan körülményről, ami az informatikához kapcsolódó tevékenység fennakadásához, megszakadásához vezethet. A rendszergazda szükség esetén értesíti az információbiztonsági felelőst, aki megteszi a további, szükséges intézkedéseket.
- Az önkormányzati ASP központtól kapott szoftveres tanúsítvány nem adható át az önkormányzati ASP központ által fel nem jogosított személynek. A tanúsítványhoz tartozó jelszót tilos nyilvánosságra hozni.
- Az információbiztonságot veszélyeztető események kivizsgálására irányuló felülvizsgálatokban a felhasználó köteles együttműködni a kivizsgálókkal.
- A Hivatal a vonatkozó adatvédelmi jogszabályok figyelembevételével jogosult a felhasználó hivatalos elektronikus levelezését és internetforgalmát monitorozni.
- A felhasználó számára büntetőjogi, illetve munkajogi felelősségre vonás terhe mellett tilos illetéktelenül más felhasználó jogosultságainak használata, a hálózat monitorozása, felderítése, jelszavak kipróbálása, illetve ezek kísérlete is.
- A rendszergazdát kivéve, tilos a Hivatal számítógépeire szoftvereket telepíteni, és azokat futtatni.

A nyomtatásra, szkennelésre, fénymásolásra, faxolásra alkalmas készülékek, multifunkcionális eszközök használatánál ügyelni kell arra, hogy:

- az érzékeny információt tartalmazó nyomtatványok ne maradjanak a készülékben és a készülék mellett;
- véletlen vagy szándékos e-mail cím elírás során, félretárcsázás vagy hibásan tárolt szám beütése esetén az üzenetek illetéktelenek személyekhez kerülhetnek;

3.2. A felhasználó jogai

A felhasználó jogosult:

- a beállított jogosultságának megfelelően, a munkájához szükséges adatállományok elérésére,
- információbiztonsági képzésre,
- a működtetéshez szükséges támogatás igénylésére, a munkavégzéshez szükséges általa nem ismert szoftverek használatához támogatást kérni,
- meghibásodás, üzemzavar esetén az elhárítás igénylésére.

3.3. A felhasználó felelőssége

A felhasználó felelősséggel tartozik:

- a felhasználó a rábízott eszközöket nem adhatja kölcsön harmadik személynek kockáztatva így az eszköz épségét, és az esetlegesen rajta lévő adatok bizalmasságát, sértetlenségét.
- a szabályok betartásáért;
- a birtokában lévő, vagy tudomására jutott adatok, információk bizalmasságának megfelelő kezeléséért;
- a személyére szóló és védett területre belépést biztosító kártyájának/kártyáinak védelméért és át nem ruházásáért;
- az elektronikus információs rendszerben végzett műveletekért;
- a Hivatal informatikai eszközeinek szakszerű kezeléséért;
- a személyi használatra átvett eszközök megfelelő fizikai védelméért.

4. Az információ kezelésének szabályai

4.1. Munkaállomások hozzáférés védelme

A felhasználó munkaállomást csak saját nevével és jelszavával belépve használhat. Harmadik fél csak a munkaállomás felhasználója munkahelyi vezetőjének előzetes írásbeli engedélyével használhatja az adott munkaállomást, ebben az esetben is a személyesen hozzárendelt egyedi azonosító használatával. Hibaelhárítás vagy támogatás esetén a rendszergazda saját azonosítójával a felhasználó engedélyével léphet be a meghibásodott munkaállomásra.

A felhasználónak rendszergazdai jog nem adható!

4.2. A hozzáférés kiosztás folyamata

A munkaállomásra és az elektronikus információs rendszerekbe a belépést lehetővé tevő azonosítót a munkahelyi vezető igényli a felhasználóknak, az IBSZ *5.4.4. fejezetében* leírt folyamat szerint.

A hálózati belépést lehetővé tevő azonosítót és a kezdeti jelszót az informatikus személyesen adja át az új felhasználónak. Az átadás során az informatikus az azonosító használatáról, a kezdeti jelszó megváltoztatásáról és az egyéb testre szabási lépésekről oktatásban részesíti a felhasználót.

Az önkormányzati ASP szakrendszereihez történő csatlakozás többtényezős hitelesítéssel történik. A felhasználónak rendelkeznie kell felhasználói azonosítóval és jelszóval, amit az ASP Tenant rendszergazda oszt ki. Valamint rendelkeznie kell E-személyivel, valamint kártyaolvasóval. Az E-személyihez csak a hozzá tartozó PIN kód megadásával lehet hozzáférni. A sikeres azonosítást és hitelesítést követően lehet használni az ASP rendszer jogosultság alapján beállított szakrendszereit.

4.3. Hálózati hozzáférés, hozzáférés az egyes elektronikus információs rendszerekhez

A Hivatal vezetése felügyeli az elektronikus információs rendszerek használatát a visszaélések megakadályozására és jogosult annak használatát ellenőrizni.

A Hivatal informatikai eszközein működtetett elektronikus információs rendszereket a felhasználó a számára beállított jogosultságnak megfelelően használhatja az alábbiak szerint:

- A felhasználó a számítógépbe/hálózati szolgáltatások eléréséhez személyre szóló azonosítót és jelszót kap, mely a belépéshez szükséges bizalmas információkat tartalmaz.
- Az azonosító és a megfelelő erősségű és titokban tartott jelszó használatával a belépő védelemmel rendelkezik a nevében történő visszaélések ellen, ezért a személyre szóló azonosítót és jelszavát szigorúan védeni kell, és a kezdeti jelszót első bejelentkezéskor meg kell változtatni.

A felhasználói jelszavak képzéséhez az alábbi szabályokat kell betartani:

- a jelszó legalább nyolc karakter hosszú legyen, és tartalmaznia kell kis és nagybetűt és számot;
- a jelszavaknak a fejlesztő által megadott feltételeknek kell eleget tenniük.
- a jelszó nem lehet azonos a felhasználó névvel, annak becézett formájával, egymás után következő számokkal, vagy könnyen visszafejthető kifejezéssel.
- a hálózatba kötött számítógépek esetében a felhasználóknak a hálózati, illetve ennek hiánya esetén helyi bejelentkezési jelszavakat havonta meg kell változtatniuk.

- ahol ezt az operációs rendszer támogatja, 5 sikertelen bejelentkezés után az operációs rendszernek le kell tiltani a felhasználó fiókját.
- a jelszó megváltoztatásakor az új jelszó nem lehet azonos a korábban használt 5 jelszóval.
- a jelszót nem szabad több személy között megosztani.
- a felhasználók jelszavát a felhasználón kívül senki sem ismerheti.
- az előző jelszavak újra használatát kerülni kell.
- a felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el az informatikai rendszerben,
- a felhasználói jelszót TILOS leírni,
- ha bármilyen jel mutat arra, hogy a jelszó nyilvánosságra került, azonnal értesíteni kell az információbiztonsági felelőst és meg kell változtatni,
- nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé,
- a jelszó minél komplexebb, annál kisebb a valószínűsége, hogy nevünkben visszaélést követnek el.

4.4. Hozzáférés védelem mobil infokommunikációs eszköz esetén

A hordozhatóság miatt sokkal nagyobb veszélynek vannak kitéve a mobil informatikai eszközök, ezért ezek esetében is jelszót kell használni a rendszerbe történő belépéshez. A jelszavas védelem megnehezíti a hozzáférést, de lopás, vagy elvesztés esetén a merevlemezt eltávolítva az ott tárolt adatok így hozzáférhetők. A fentiek miatt fokozottan kell törekedni ezen eszközök fizikai védelmére is az elvesztés, illetve ellopás ellen. Nyilvános helyeken történő használatnál ügyelni kell arra, hogy illetéktelenek ne olvashassák el a képernyő tartalmát, az eszközhöz illetéktelenek ne férhessenek hozzá.

Mobil infokommunikációs eszközök esetén rendszergazda jog felhasználónak nem adható.

4.5. Adatmentések, az adathordozók nyilvántartása és tárolása

Az adatokat nem a helyi munkaállomáson, hanem a központi fájlszerver megfelelő könyvtáraiban kell tárolni, ahol biztosított azok rendszeres mentése és biztonságos tárolása.

Az Informatikus nem vállal felelősséget a helyi munkaállomáson tárolt adatokért.

Az Informatikus a központi fájlszerveren tárolt adatokról meghatározott módon és gyakorisággal mentést készít. Ebből adódóan lehetőség van az állományok visszaállítására a mentés időpontjának

megfelelő tartalommal. Speciális mentési igényekről az informatikust írásban értesíteni kell, és egyeztetni kell a kivitelezés lehetőségéről.

Az adat visszaállítást az adatgazda írásbeli (e-mail) igénye alapján az informatikus végzi el.

A feljegyzésnek tartalmaznia kell a visszaállítani kívánt adat:

- utoljára ismert pontos helyét;
- megnevezését, és
- a visszaállítandó időpontot.

A felhasználónak a jogviszonyának megszűnésekor a munkaállomásán és a központi tárhelyen tárolt adatok törlése tilos!

4.6. Adathordozók kezelése

Az adathordozók védelme magában foglalja az adathordozók biztonságos, megbízható működtetésének feltételeit, miszerint:

- a Hivatal csak engedélyezett adathordozót szabad használni. A szervezet vezetője, az Informatikus, illetve az információ biztonsági felelős a hozzáférési jogosultságok szabályozásával engedélyezheti, korlátozza, vagy tilthatja egyes, vagy bármely adathordozó típusok, és az elektronikus információs rendszerek használatát;
- az adathordozókat könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak;
- a használni kívánt adathordozót (CD, DVD, pendrive, külső winchester, SD kártya) a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni;
- a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek;
- adathordozót más szervezetnek átadni csak engedéllyel szabad;
- tilos a magáncélú adathordozókat szolgálati célra igénybe venni, illetve tilos szolgálati adathordozókat magáncélra igénybe venni;
- tilos olyan adathordozó használata, melynek tulajdonosa nem azonosítható, ilyen esetben az elektronikus információ rendszer biztonságáért felelős személynek kell az adathordozót átadni.

Az számítógépek belső adathordozóihoz az Informatikus férhet hozzá. Szükség esetén a munkavállalók külső adathordozókhoz az elektronikus információ rendszer biztonságáért felelős

személy és a Jegyző engedélyével férhetnek hozzá vagy használhatják, figyelembe véve a rendszerbiztonsági és adatvédelmi szabályokat.

5. Felhasználók számítógépes környezete

5.1. Számítógépek és a hálózat kezelési előírásai

A felhasználó felelős az informatikai eszközön és az elektronikus információs rendszerekben általa végzett, nyilvánvalóan szakszerűtlen művelet következményeiért.
A felhasználó semmilyen informatikai eszközt nem helyezhet üzembe, a Hivatal belső hálózatához idegen infokommunikációs eszköz nem csatlakoztatható, a munkaállomások elhelyezését, telepítési módját nem változtathatja meg. Semmilyen szoftvert nem telepíthet, nem törölhet, és nem módosíthat. Erre csak az Informatikus jogosult.

5.2. Internethasználat, web böngészés

Az Internethez való kapcsolódás csak és kizárólag a munkavégzést szolgálja!
Az Internet és az elektronikus levelezés használatának főbb szabályai:

- A nem munkavégzést szolgáló hálózati sávszélesség foglalása (pl. nagyméretű állományok letöltése, on-line rádió hallgatása), és a magánadatok kiszolgálón történő tárolása esetén a felhasználó figyelmeztetésben részesül. Ismételt előfordulás esetén az informatikus jelentést tesz az információbiztonsági felelősnek, aki eljár az ügyben a jegyző felé.
- Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, kiiktatása.
- Tilos Internetes vagy más jellegű szolgáltatást nyújtó külső féllel engedély nélküli hálózati kapcsolat kialakítása.
- Tilos az elektronikus információs rendszerek használata a Hivatali értékekkel összhangban nem álló célokra, vagyis pl. szexuális jellegű fájlok fogadására, küldésére, fenyegetésre vagy megfélemlítésre, megkülönböztetésre, gyűlölködésre, fegyverekkel és illegális drogokkal való kereskedésre, erőszakra, internetes- illetve szerencsejátékokra, bármilyen kereskedelmi illetve jogellenes tevékenységre.
- Tilos külföldi felhő-alapú tárhely-szolgáltatások (pl.: Dropbox, Google Drive) igénybevétele hivatali adatok tárolására.

- Az internetről csak hivatali célból lehet fájlokat letölteni! Tilos fájlletöltő szolgáltatások használata. Különösen tilos jogvédett, illetve illegális tartalmak, fájlok letöltése, tárolása!
- Az internetes oldalak elérése monitorozásra és naplózásra kerülhet, a munkával összefüggésbe nem hozható oldalak elérhetőségét az informatikus jegyzői utasításra jogosult korlátozni.

5.3. E-mail használat

A Hivatal által biztosított elektronikus levelezési cím és az elektronikus levelezési szolgáltatás kizárólag hivatali munkavégzés céljára biztosított, ezért a felhasználóknak tilos a hivatali e-mail címüket nem hivatalos minőségben használni (pl.: regisztráció letöltési weboldalakra, on-line játék oldalakra, közösségi oldalakra stb.)!

A Hivatal által nem támogatott levelezőrendszer (pl.: gmail, freemail, citromail) használata hivatali munkavégzésre nem engedélyezett.

A felhasználók alapértelmezésben a levelezés során csak a saját postaládájukat tudják kezelni, mások postaládáit nem látják.

Zavaró, félreinformáló levelek, spam-ek küldése, jogtalan megrendelések elindítása tilos, és eljárást vonhat maga után.

Ismeretlen helyről származó e-mail-t megnyitni nem szabad, mert maga a levél vagy annak csatolmánya vírus lehet, ezért ilyen esetben értesíteni kell az Informatikust, aki megvizsgálja a levelet, és ha szükséges olvasatlanul törli.

6. Vírusvédelem

6.1. A vírusvédelem alkalmazásának előírásai

Az Informatikus a számítógépek vírusok elleni védelmére rendszeresen frissített vírusvédelmi rendszert üzemeltet. Ez a védelem kiterjed a kiszolgálók, munkaállomások valamint a teljes Internet és elektronikus levélforgalom folyamatos ellenőrzésére. Új vírus megjelenése esetén még így is előfordulhat fertőzés, valamint csatolmányok, CD és DVD lemezek, cserélhető adathordozók, illetve internetről letöltött fájlok használata esetében.

Vírusvédelem nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem használható!

Ha a vírus helye nem lokalizálható, az informatikus jogosult a hálózat egyes funkcióit, vagy a teljes hálózat felhasználói szolgáltatásait a vírusveszély elhárításáig felfüggeszteni.

6.2. Teendők vírusgyanú esetén

Vírusgyanú esetén a felhasználó köteles azonnal értesíteni az informatikust, aki azonnal intézkedik.

7. Az informatikai eszközök fizikai védelme

7.1. Számítógép használatának előírásai

A munkaállomást és az informatikai eszközöket a napi munkavégzés befejezésekor ki kell kapcsolni. Ez alól kivételek azok az eszközök, amelyek automatikusan kikapcsolnak (hálózati nyomtatók vagy a modern monitorok többsége stb.). Az infokommunikációs eszközöket üzem közben letakarni, a szellőző nyílásokat eltakarni tilos!

7.2. „Üres asztal - tiszta képernyő" politika

Az „üres asztal - tiszta képernyő" politika megvalósítása az alábbiakat jelenti:

h) A monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő használata ajánlott);

i) A felhasználó a munkaállomását zárolni köteles, ha hosszabb időre elhagyja helyét;

j) A munkavégzés befejeztével a munkaállomásból ki kell jelentkezni, illetve ki kell azt kapcsolni, ettől eltérő utasítást az Informatikus adhat;

k) Elfelejtés esetére jelszóvédett, automatikus zárolás kerül beállításra, úgy, hogy az maximum 10 perc várakozást követően zárolja a számítógépet;

l) A felhasználóknak az infokommunikációs eszközök elhelyezésére szolgáló helyiséget be kell zárniuk, ha a helyiségben senki nem tartózkodik;

m) A kinyomtatott, faxolt vagy másolt iratokat nem szabad őrizetlenül a nyomtatókban, multifunkcionális eszközökben, faxokban hagyni.

n) Ügyfelet nem szabad felügyelet nélkül az irodában hagyni.

7.3. Mobil infokommunikációs eszközök védelme

A munkaállomásokra vonatkozó előírásokon kívül az alábbi védelmi szabályokat kell betartani:

a) mechanikai és használati sérülések elkerülése érdekében követni kell a géphez kapott használati útmutatót;

b) cserélhető kártyák, tokenek behelyezésénél, és eltávolításánál szintén a használati utasítást kell követni;

A mobil informatikai eszközök ellopása esetén:

a) az ellopás tényét a lehető leggyorsabban jelenteni kell az információbiztonsági felelősnek és a munkahelyi vezetőnek;

b) értesíteni kell a rendőrséget;

c) ha nem a Hivatalban történt a lopás, értesíteni kell az adott hely vezetését;

d) valamennyi rendőrségi jelentést meg kell őrizni és a Hivatal részére át kell adni.

Infokommunikációs eszköz elvesztése:

Bármely infokommunikációs eszköz eltűnését a lehető leggyorsabban jelenteni kell a munkahelyi vezetőnek és az információbiztonsági felelősnek és tájékoztatni kell őket arról, hogy a berendezés tartalmaz-e bárminemű érzékeny információt

8. Információbiztonsági események kezelése

Információbiztonsági eseménynek minősül minden 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, így különösen

a) a szolgáltatás, a berendezés vagy az eszközök elvesztése;

b) a rendszer hibás működése vagy túlterheléses támadás;

c) emberi hibák;

d) a szabályzatoknak vagy irányelveknek való nem megfelelés;

e) a fizikai biztonsági rendelkezések megsértése;

f) nem ellenőrzött rendszerbeli változások;

g) a szoftver vagy hardver hibás működése;

h) hozzáférési előírások megsértése;

i) kártékony kód általi fertőzés;

j) a nem teljes vagy nem pontos működési adatokból eredő hibák;

k) a bizalmasság és sértetlenség megsértése;

l) az elektronikus információs rendszerrel való visszaélés.

8.1. Jelentés a biztonsági eseményekről

A biztonságot érintő eseményekről a felfedezésük után, haladéktalanul tájékoztatni kell a felfedező közvetlen munkahelyi vezetőjét és az informatikust. Az informatikus értesíti az információbiztonsági felelőst, aki jogosult az esemény kivizsgálására.

Amennyiben a biztonsági esemény érinti az elektronikus információs rendszerek vagy az önkormányzati ASP rendszer által nyújtott szolgáltatásokat vagy közvetlenül azokban következik be, az eseményt jelenteni kell az elektronikus információs rendszerek és az önkormányzati ASP rendszer működtetőjének is.

A biztonságot érintő eseményekről szóló jelentések elkészítésére az IBSZ *16. mellékletét* kell használni.

8.2. Jelentés a szoftverzavarokról

Az elektronikus információs rendszerekben tapasztalt szoftverzavarokat jelenteni kell az informatikusnak. Szoftverzavarra utaló jelek lehetnek, amikor az alkalmazás nem a várt eredményt adja vagy nem a megszokott képernyőképek jelennek meg.

A jelentéshez az IBSZ *16. mellékletét* kell használni. Szoftverzavarok esetén legalább a következő feladatokat végre kell hajtani:

a) fel kell jegyezni a zavaró jelenséget és a képernyőn megjelenő minden üzenetet és

b) be kell szüntetni az adott számítógép használatát.

A felhasználóknak tilos a hibásnak feltételezett szoftvert eltávolítaniuk az elektronikus információs rendszerből, illetve kísérletet tenni a hiba elhárítására.

A hibaelhárítást és helyreállítást az informatikus hajthatja végre.

Abban az esetben, ha feltételezhető az információbiztonság sérülése, akkor az eseményt az informatikusnak jelentenie kell az információbiztonsági felelősnek, aki kivizsgálja az eseményt.