Ludányhalászi Közös Önkormányzati Hivatal Jegyzője

2./2018. számú

JEGYZŐI UTASÍTÁS

Ludányhalászi Közös Önkormányzati Hivatal

INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Érvényes: 2018.07.01.
Jóváhagyta: jegyző

Verziótörténet		
Verziószám	Dátum	Leírás
v1.0	2018.07.01.	első kiadás

Bevezetés

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 11.§ (1) bekezdés szerint a szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről, ennek keretében a törvény 11.§ (1) bekezdés f. pontja alapján kiadom az Informatikai Biztonsági Szabályzatot (továbbiakban: IBSZ).

Fogalomtár

Adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.
Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adatokon végzik.
Adatfeldolgozó: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi.
Adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás.
Informatikáért felelős szervezeti egység: a mindenkor hatályos Szervezeti és Működési Szabályzatában meghatározott, az informatikai feltételek biztosítására kijelölt szervezeti egység.
Informatikai biztonsági felelős (IBF): az elektronikus információs rendszerek biztonságáért felelős, a szervezet vezetője által kijelölt, vagy megbízott személy.
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 esemény, vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amely 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 események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.
Biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége.
Biztonsági szint: a szervezet felkészültsége az elvárt biztonsági feladatok kezelésére.
Elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese.
Felhasználó: egy adott információs rendszert igénybe vevők köre.

Fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikus jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és tűzvédelem.
Folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem.
Információ: 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.
Kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának 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.
Logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.
Mobil kód: olyan szoftver, amely egyik számítógépről a másikra irányít, ahol önműködően hajt végre meghatározott funkciókat, minimális felhasználói beavatkozással, vagy a nélkül.
Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személyek 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 elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanság) 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 rendszer gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági események feltárása.
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 működéséért felelős.
Védelmi feladatok: megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés.
Zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.

A dokumentum célja

Az IBSZ célja a Polgármesteri Hivatal informatikai biztonsági követelményrendszerének és környezetének meghatározása, mely leírja a biztonsági intézkedéseket, azok dokumentálásának és ellenőrzésének feladatait, az ehhez szükséges egyes szerepköröket és a végrehajtás gyakoriságát vagy idejét.

A dokumentum szervezeti hatálya

A szabályzat a Hivatal valamennyi olyan szervezeti egységére kiterjed, amely a Hivatal elektronikus információs rendszereit használja, üzemelteti, fejleszti, továbbá ilyen tevékenységeket irányít és ellenőriz.

A dokumentum tárgyi hatálya

Jelen dokumentum tárgyi hatálya kiterjed az informatikai eszközök elhelyezésére szolgáló létesítményekre (épületekre, telephelyekre), a Hivatalban található összes üzemelő, használatban lévő vagy a jövőben bevezetett, alkalmazott informatikai eszközre, rendszerre, azok környezetét alkotó rendszerelemre teljes életciklusában a tervezéstől, elkészítéstől, a rendszerből történő teljes kivonásáig, vagy megsemmisítésig.

A dokumentum személyi hatálya

Az elfogadott IBSZ vonatkozik:

- a Hivatal valamennyi köztisztviselőjére és munkavállalójára,
- a Hivatallal szerződéses kapcsolatba kerülő természetes vagy jogi személyekre, velük kötött megállapodás, vagy titoktartási nyilatkozatok alapján.

Kiadás dátuma, érvényessége

Jelen szabályzat a kihirdetés napján lép hatályba, és mindaddig érvényesnek tekintendő, amíg annak egy új változata jóváhagyásra nem kerül.

Az IBSZ-ben előálló bármilyen változás verziószám változással jár, melyet a Dokumentum történetben fel kell vezetni, feltüntetve a verziószámot a kibocsátás napját és a változások rövid összefoglalását.
Az IBSZ írásos formában minden résztvevő számára elérhető a Hivatal vezetőjénél.

A Szabályzat, illetve mellékleteinek felülvizsgálatára az alábbiak szerint kerül sor:

- évente egy alkalommal, a belső felülvizsgálatok során,
- rendkívüli, megváltozott körülmények hatására a felülvizsgálatot el kell végezni az alábbi események bármelyikének bekövetkezésekor:

- a Hivatal Szervezeti és Működési Szabályzata (a továbbiakban: SZMSZ) módosítása;
- a belső irányítás bármely egyéb írott eszközének az információbiztonságot érintő módosítása;
- az információbiztonságot is érintő jogszabály-változás, amennyiben annak hatálya a Hivatalra is kiterjed;
- az információkezelést és –feldolgozást végző vagy támogató folyamatokban, illetve a kezelt adatok körében beállt lényeges változás;
- a Hivatal tulajdonában vagy használatában lévő elektronikus információs rendszerekben, illetve azok fizikai környezetében beálló lényeges változás.
- minden olyan esetben, amikor a Szabályzatban leírtakhoz képest egyéb jelentős változás történik.

A mindenkori felülvizsgálat végrehajtása az IBSZ-ben meghatározott informatikai biztonsági felelős feladatát jelenti.

Figyelembe vett dokumentumok

Az IBSZ készítésekor az alábbi előírásokat, módszertani dokumentumokat vettük alapul:

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 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
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről
- 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
- Közigazgatás Informatikai Bizottság 25. sz. ajánlása, Magyar Informatikai Biztonsági Ajánlások, MIBIK, MIBÉTS.

Kapcsolódó dokumentumok

Az IBSZ elkészítéséhez felhasznált dokumentumok

- Polgármesteri hivatal SZMSZ

Biztonsági szintek és osztályok

A Hivatal 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 és a Kockázatkezelési eljárásrend alapján elvégezte az elektronikus információs rendszerek biztonsági osztályba sorolását, megállapította a Hivatal elvárt és aktuális biztonsági szintjét. A vizsgálatok alapján az informatikai rendszerek biztonsági osztályát és a Hivatal vagy szervezeti egységei biztonsági szintjét, illetve az indoklásokat a Hivatal vezetője által jóváhagyott *Osztályba és szintbe sorolás melléklet* tartalmazza. A biztonsági osztályba sorolás eredményét a kizárólag az érintettek és a Hatóság számára hozzáférhető *Rendszerbiztonsági terv*, a [NEIH-OVI] *Osztályba sorolás és védelmi intézkedés*, a szintbe sorolás eredményét a [NEIH-SZVI] *Szintbe sorolás és védelmi intézkedés* űrlapok (illetve XML állományok) tartalmazzák.

Az elektronikus információs rendszerek biztonságáért felelős személy vagy a Hivatal vezetője által megbízott személy feladata, hogy a rendszerek biztonsági osztályba sorolását elvégezze, a Hivatal biztonsági szintjét megállapítsa, *Osztályba és szintbe sorolás melléklet*-ben, *Rendszerbiztonsági tervben* vagy egyéb dokumentumban rögzítse, szükség esetén jelen Informatikai biztonsági szabályzatot aktualizálja, a hatósági adatszolgáltatást előkészítse és a jegyző számára előterjessze. A biztonsági osztályba sorolást, a Hivatal vagy szervezeti egység biztonsági szintbe sorolását, az Informatikai biztonsági szabályzatot a Hivatal vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért, gondoskodik a módosított szabályzat életbe léptetéséről, az elektronikus információs rendszerek biztonságáért felelős személy közreműködésével az adatszolgáltatás teljesítéséről a Hatóság (Nemzeti Kibervédelmi Intézet Nemzeti Elektronikus Információbiztonsági Hatóság) által előírt módon.

A besorolás alapján a 41/2015. (VII. 15.) BM rendeletben a Hivatalra és az elektronikus információs rendszereire érvényes biztonsági osztályhoz és szinthez rendelt követelményeket és azok megvalósításának módját a következő fejezet tartalmazza (adminisztratív, fizikai és logikai védelmi intézkedések). Az intézkedések és sorszámaik megegyeznek a rendelet követelményeivel.

Ha a Hivatal az elektronikus információs rendszernek csak egyes elemeit vagy funkcióit üzemelteti vagy használja – részben vagy teljesen –, a rendeletben meghatározott követelményeket ezen elemek és funkciók tekintetében kell teljesíteni. Ha az elektronikus információs rendszert több szervezet használja, az elektronikus információs rendszer üzemeltetője az üzemeltetés elektronikus információbiztonságához szükséges követelményeket az elektronikus információs rendszeren tevékenységet végző minden, elektronikus információs rendszerrel rendelkező szervezet tekintetében érvényesíti.
Az elektronikus információs rendszer üzemeltetője (szolgáltató) az üzemeltetés elektronikus információbiztonságához szükséges követelményeket úgy érvényesíti az elektronikus

információs rendszeren tevékenységet végző elektronikus információs rendszerrel rendelkező szervezetek tekintetében, hogy a követelményeknek való megfelelés az elektronikus információs rendszerrel rendelkező szervezet elektronikus információ-biztonsággal kapcsolatos eljárási rendjébe beépüljön. Az elektronikus információs rendszer üzemeltetője és az elektronikus információs rendszerrel rendelkező szervezetek az üzemeltetés elektronikus információ-biztonságához szükséges követelményeket az elektronikus információs rendszer üzemeltetésére kötött szerződésben rögzítik.

Adatosztályozás

A hivatal rendszereinek osztályozását a Nemzeti Elektronikus Információbiztonsági Hatóság által kiadott kockázatelemzési módszertan szerint kell elvégezni.
A Hivatal információrendszerében feldolgozott, továbbított, tárolt adatok kockázatarányos védelmének biztosítása érdekében az adatokat is be kell sorolni biztonsági osztályokba.
Az információrendszerekben elektronikusan tárolt adatok esetén az adatok azon halmazát, amelyekre a tárolás számítástechnikai körülményeiből adódóan jellemzően azonos védettség valósítható meg (közös adatbázis, azonos könyvtár), ugyanabba a biztonsági osztályba kell sorolni, mégpedig oly módon, hogy a halmaz egészére ki kell terjeszteni a halmaz legérzékenyebb elemének besorolását.
Az adatosztályozás során az adatokat szintén a kockázatelemzés eredményei alapján kell besorolni.
Alapelv és kiinduló állapot, hogy a rendszerekben kezelt adatok biztonsági osztálya megfelel az őket kezelő elektronikus információs rendszer biztonsági osztályának.
Az adatgazdák – az informatikai biztonsági vezető közreműködésével – az adatok osztályozását felülvizsgálják, és a besorolást megváltoztathatják vagy jóváhagyhatják

a) ha az információkezelést és –feldolgozást végző vagy támogató folyamatokban, illetve a kezelt adatok körében lényeges változás áll be;
b) a Hivatal tulajdonában vagy használatában lévő elektronikus információs rendszerekben lényeges változás áll be.

Biztonságtervezési eljárásrend

A Hivatal informatikai biztonságának tervezésekor elsősorban a következő dokumentumok a meghatározóak:

1. A Hivatal mindenkori Szervezeti és működési szabályzata
2. A Hivatal érvényben lévő információbiztonsági szabályzatai
3. Vonatkozó hatályos jogszabályok
4. Vonatkozó szabványok és ajánlások

A Hivatal informatikai stratégiájának megfelelően törekedni kell a lehetőségekhez képest legpontosabb előrelátásra, az elkövetkező beszerzési- vagy fejlesztési ciklusra. Kerülni kell az ad-hoc jellegű beszerzéseket, fejlesztéseket, módosításokat. Ilyeneket csak rendkívüli esetekben a rendkívüli helyzetre adott válaszul lehet alkalmazni.
A tervezés kiinduló pontja az Informatika, ahol a tervezéshez a következő főbb információkat kell mérlegelni:

- az Informatika fejlesztési terve szerint végrehajtandó fejlesztések,
- az elmúlt időszak felhasználói bejelentései, azok fontossága illetve gyakorisága szerint rangsorolva,
- egyéb szakmai információk (pl. GOVCert, NEIH, stb.), fejlemények (pl. hivatali átszervezések).

Az Informatika a fenti elvek alapján az éves költségvetés tervezéséhez igazítva előterjeszti a javaslatait a Hivatal vezetése számára az informatikai biztonsági célok megvalósításához és azok szervezeti integrációjához.

Felelősség

Az informatikai biztonság tervezését és az erőforrások megszerzését a Hivatal vezetője, a jegyző koordinálja.

Az információbiztonság szervezete

Cél: A biztonsági feladatok ellátására és ellenőrzésére azonosítható szerepkörök álljanak rendelkezésre.

Általános szabályok

A Hivatal vezetése e szabályzatban megfogalmazott világos iránymutatással, elkötelezettsége kinyilvánításával, az informatikai biztonsággal összefüggő felelősségi körök egyértelmű kijelölésével és elismerésével aktív módon támogatja az informatikai biztonságot a szervezeten belül.
A Hivatal elektronikus információs rendszerében az alábbiak szerint szét kell választani a biztonsági szempontból összeegyeztethetetlen funkciókat, és biztosítani kell a szervezet biztonsági szerepeinek elkülönülését.
A szerepkörökkel kapcsolatos általános – a szervezeti egység szintjén értelmezett –felelősségi szabályokat a Hivatal Szervezeti és Működési Szabályzata (SZMSZ), az egyes információbiztonsági szempontból releváns folyamatokban, eljárásokban értelmezett részletes feladatokat és felelősségi szabályokat az adott felhasználó munkaköri leírása tartalmazza.
Az SZMSZ további feladatokat, felelősségeket állapíthat meg a Hivatal munkatársai, szervezeti egységei számára.
Az információbiztonság elismerése a vonatkozó szabályzatok hatályba léptetésével, és az érintettek körében végzett tudatosítás és képzés keretében valósul meg.

Informatikai biztonsági felelős

A Hivatal vezetője informatikai biztonsági felelőst jelöl ki, és jelen Szabályzatban meghatározza, időszakosan felülvizsgálja az információbiztonsággal összefüggő felelősségi köröket.
Az információbiztonsággal kapcsolatos felelősség megoszlik az informatikai biztonsági felelős, az informatikai biztonsági vezető és az egyes felhasználók között.

Az információbiztonsági tevékenység koordinálását az informatikai biztonsági felelős végzi.

Az informatikai biztonsági felelős feladatai

A Hivatalnál üzemeltetett elektronikus információs rendszerek információvédelemmel összefüggő tevékenységeinek jogszabályokkal és belső szabályzatokkal való összhangjának megteremtése, fenntartása, tervezése, szervezése, irányítása, koordinálása és ellenőrzése, a Hivatal informatikai biztonsági vezetőjének közvetlen irányítása alá tartozik.
Az Informatikai biztonsági felelős feladatai:

- Felméri és elemezi a szervezet működéséből eredő, az adat- és információvédelemmel kapcsolatos veszélyforrásokat, kidolgozza és döntésre előterjeszti az informatikai biztonság kialakítására, elérésére, fenntartására vonatkozó szabályokat, utasításokat, terveket.
- Részt vesz az informatikai biztonságot érintő egyéb szabályzatok elkészítésében, véleményezésében.
- Gondoskodik az informatikai biztonsági szabályzatok naprakészen tartásáról, az abban foglaltak betartásának ellenőrzéséről.
- Részt vesz az informatikai biztonság szempontjából fontos munkakörök betöltési szabályainak, feltételeinek kidolgozásában, az ilyen típusú munkakörbe jelentkező munkavállalók biztonsági szempontból történő ellenőrzésében.
- A projektek során – a beszerzési eljárás elindításától a projekt lezárásáig – feladata az informatikai- és információbiztonsági szabályok, elvárások érvényre juttatása.
- Figyelemmel kíséri az informatikai biztonsági eszközök állapotát, javaslatot tesz azok cseréjére, bővítésére.
- Lebonyolítja az informatikai biztonságra vonatkozó oktatást a Humánpolitikai csoport szervezésében.

Adatgazdák

Az adatgazdai intézmény célja a Hivatal adatvagyona számára a megfelelő biztonsági környezet kialakítása azáltal, hogy az adatok kezelésének szabályaival kapcsolatos felelősségek az adatokat ténylegesen felhasználó hivatali folyamatokra, szervezeti egységekre hárulnak.
A Hivatal egyes folyamatai, szervezeti egységei nevében, az általuk használt adatok vonatkozásában az adatgazdák állapítják meg az adatkezelés biztonsági követelményeit az információbiztonsági vezető segítségével és együttműködésével. Az egyes adatokhoz, adatbázisokhoz való hozzáférésre feljogosított személyek körét, jogosítványuk tartalmát az érintett adatok adatgazdái határozzák meg.
Az adatgazdák feladata, hogy a felelősségi körükbe tartozó adatok vonatkozásában megjelenési formájuktól függetlenül az adatok be- vagy átsorolását elvégezzék a különböző biztonsági osztályokba.
Az adatgazda a besorolásról írásban tájékoztatja az Informatikát. Az Informatika a besorolást átvezeti az általa vezetett adatosztályozási séma nyilvántartásában, továbbá – amennyiben

szükséges – kezdeményezi a besorolásnak megfelelő jelzés feltüntetését az adat nyomtatott megjelenési formáin.
Az adatgazdai teendők ellátása a Hivatal vezetőjének a feladata. A Hivatalvezető az adatgazdai tevékenységek ellátásával más munkatársát is megbízhatja.
Az adatgazda döntési joggal részt vesz az irodáján dolgozó felhasználóknak az adathozzáférési jogosultság-kezelési folyamatában.

Felhasználók

Felhasználó: a Hivatal összes, elektronikus információs rendszert használó munkatársa
Speciális felhasználó: adminisztrátori, root, stb. speciális jogosultsággal rendelkező felhasználók. Minden adminisztrátor egy felhasználó is egyben, csak egy speciális fiók abban a tekintetben, hogy ő teljes joggal rendelkezik az adott rendszer felett.
Külső felhasználó: a Hivatallal kapcsolatban álló külső felek a Hivatal biztonsági szabályainak és elvárásainak betartása mellett férhetnek hozzá a Hivatal elektronikus információs rendszeréhez.
A külső felhasználók hozzáférését a hozzáférés indokának megszűnte után azonnal, ill. az együttműködés lejártakor automatikusan meg kell szüntetni.

Feladatkörök szétválasztása

A feladatköröket és felelősségi területeket szét kell választani – és azt a jogosultsági rendszerben kezelni kell – a Hivatal vagyontárgyai jogosulatlan, illetve nem szándékos módosítása, illetve az azokkal való visszaélés lehetőségeinek csökkentése érdekében.
Meg kell határozni a biztonsági szempontból összeférhetetlen feladatokat, amelyek véletlen vagy szándékos károkozást tesznek lehetővé, és ezek szétválasztását érvényesíteni kell a szervezeti felépítésben, a munkakörök kialakításakor, valamint azokat a jogosultsági rendszerben is kezelni kell.

Külső szolgáltatók

A külső szolgáltatók és együttműködő partnerek igénybevétele esetén a szolgáltatási megállapodásokban (szerződésekben) kell kikötni a szolgáltatásra érvényes biztonsági követelményeket és szabályozást. Biztosítani kell a Hivatal számára az ellenőrzés feltételeit.
Minden érintett szereplővel titoktartási nyilatkozatot kell kitöltetni, melynek aláírásával felvállalja, hogy a birtokában levő információval nem él vissza.
A nyilatkozatnak tartalmaznia kell a titoktartás tárgyi hatályát, mely szerint milyen információk tartoznak védett információk közé, illetve melyek a minősített esetek (különösen védett információ kategóriák). A hatályos jogszabályoknak megfelelően a titoktartási kötelezettség megszegéséért kártérítési kötelezettséget kell megállapítani.
Amennyiben a Hivatal jogszabály alapján kijelölt szolgáltatót vesz igénybe a jogszabályban foglalt biztonsági előírások az irányadóak.
Az üzemi rendszerből származó adatokat csak tesztelési célból és csak anonimizálva lehet átadni a szállítónak.
A külső felekkel kötött megállapodásoknak vagy szerződéseknek pontosan tartalmazniuk kell:

- a megállapodásban részt vevő felek kölcsönös kötelezettségét,
- a joganyagokra vonatkozó felelősséget, pl. adatvédelmi jogszabályok kérdésében,
- szellemi tulajdonjogokat és a szerzői jog átruházását, valamint az együttes csoportmunka védelmét,
- a tevékenységük pontos meghatározását,
- a hozzáférési jogosultságaikat,
- a hozzáférés módját, idejét és korlátait, különös tekintettel a helyszíni munkavégzésre,
- a Hivatal biztonsági előírásainak- és kontrolljainak elfogadását,
- a titoktartási nyilatkozataikat,
- az ellenőrzés feltételeit, valamint az ezekről szóló jelentések meghatározását,
- a szerződésben lefektetett felelősségek auditálásának jogát, vagy az auditok további külső féllel történő elvégeztetésének jogát,
- a karbantartás és rendszerkövetés kérdéseit,
- a problémamegoldás folyamatát – ha lehetséges – az előre nem látható események figyelembevételével,
- a biztonsági eseményekről és a biztonság megsértéséről szóló jelentések, értesítések és kivizsgálások esetére vonatkozó intézkedéseket,
- a szerződés teljesítésébe további alvállalkozók bevonásának feltételeit, titoktartásra vonatkozó megállapodásokat.

Külső felek szolgáltatásaival kapcsolatos változásoknál biztosítani kell, hogy a változásokat csak a megfelelő jogosultságokkal lehessen kezdeményezni, és a végrehajtás ellenőrzött és dokumentált körülmények között történjen az igény felvetésétől az átadás-átvételig.
A külső szolgáltatókkal kötött szerződésekben szabályozni kell a változáskezelési eljárásokat a külső fél által nyújtott szolgáltatásokra, melyek a következőket biztosítják:

- a változások végrehajtása csak a megfelelő jóváhagyás után történjen,
- a végrehajtás során is érvényesüljenek a biztonsági előírások- és kontrollok,
- az átvétel során ellenőrzésre kerüljön a specifikációban/változási kérelemben leírtak teljesülése.

A külső szolgáltatóktól elvárt védelmi intézkedéseket az Informatika –lehetőleg automatizált eszközökkel - időszakosan ellenőrzi.
Minden harmadik féllel kötött megállapodás esetében rögzíteni kell a jelen Szabályzat által meghatározott biztonsági követelményeket. Ennek teljesítése érdekében informatikai biztonsági vonatkozású szerződést a Hivatal kizárólag a Hivatal vezetője és az Informatikai biztonsági vezető jóváhagyásával köthet.

Felelősség

Az információbiztonság szervezetével kapcsolatos felelősség megoszlik a Hivatal vezetője, a jegyző, az Informatikai biztonsági vezető és az Informatikai biztonsági felelős között.

Információs rendszerek kockázatkezelése
Cél: Annak biztosítása, hogy azonosíthatóak legyenek a tényleges informatikai fenyegetések, illetve, hogy a Hivatal vezetésének információt szolgáltasson az információbiztonsággal kapcsolatos döntések meghozatalához, az információbiztonsági célok megvalósulásához.

Kockázatelemzési alapelvek

A Hivatal számára az informális, alapszintű kockázatkezelés képezi az alapját az információbiztonsági védelmi intézkedések kiválasztásának.
Az informatikai kockázatelemzésnek illeszkednie kell a Hivatal teljeskörű kockázatelemzéséhez.
Az információbiztonsági kockázatok körébe tartozik az információs rendszerek tervezési, szervezési, fejlesztési, megvalósítási, üzemeltetési és monitorozási folyamataiban fellelhető minden olyan körülmény, amely az információbiztonsági követelmények (bizalmasság, sértetlenség, hitelesség, funkcionalitás, rendelkezésre állás) bármelyikének nem-teljesülésével fenyeget.
A kockázatelemzés során

- azonosítani kell a fenyegetéseket,
- értékelni kell a sérülékenységet, a sebezhető pontokat,
- értékelni kell a sebezhetőségek előfordulásának valószínűségét,
- meg kell becsülni a várható hatásokat.
- meg kell határozni az adott kockázatokhoz használt analizálás módszerét, amely lehet
    - mennyiségi
    - minőségi
    - vagy mennyiségi és minőségi.

Kockázatelemzési eljárásrend

A Hivatalban háromévente egyszer, vagy szükség esetén soron kívül, dokumentált módon, az informatikai biztonsági vezető vezetésével felül kell vizsgálni az információbiztonsági kockázatelemzést.
A kockázatelemzési folyamatban az Informatika delegált munkatársai, valamint az elemzett területek, folyamatok képviselői vesznek részt.
A Hivatal informatikai kockázatbecslése az alábbi lépésekből áll:

- A rendszer leírása
- A veszélyek meghatározása (emberi, természeti, környezeti)

- A sebezhetőségek elemzése
- Az óvintézkedések elemzése (technikai, üzemeltetési, menedzsment)
- A valószínűségek meghatározása (magas, közepes, alacsony)
- Hatáselemzés (kritikus, súlyos, mérsékelt, kismértékű)
- A kockázati szint meghatározása (alacsony, mérsékelt, magas, kritikus)
- Javaslat óvintézkedésekre
- Az eredmények dokumentálása

A kockázatelemzések eredményét kockázatelemzési jelentésben kell rögzíteni és a Hivatalban bevált gyakorlat szerint kell gondoskodni arról, hogy a kockázatelemzési eredmények a jogosulatlanok számára ne legyenek megismerhetők.
A kockázatok ismeretében meg kell határozni az elhárításhoz szükséges feladatokat és a kapcsolódó felelősségi köröket, erőforrásokat.
A kockázatértékelésnek tartalmaznia kell egy kockázati cselekvési tervet, amelynek célja, hogy költséghatékony ellenőrzési és biztonsági intézkedésekkel folyamatosan alacsony szinten tartsa a Hivatal kitettségét az informatikai fenyegetettségeknek.
A kockázatok értékelése során meg kell határozni a Hivatal kockázatviselési képességét, vagyis azt a kockázati szintet, amelynél magasabb információbiztonsági kockázatot a Hivatal nem vállalhat.
A kockázatértékelés keretében a kockázatok feltárása és mérése, a szervezeti célkitűzések, a kockázatbecslési eljárásban rejlő bizonytalanságok, valamint a biztonsági és ellenőrzési intézkedések költségeinek függvényében meg kell határozni az elfogadható kockázat szintjét.

Felelősség

A kockázatkezelés irányítása az informatikai biztonsági vezető felelőssége.

RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG

Cél: Megvédeni a Hivatal informatikai eszközeinek és elektronikus információinak bizalmasságát, sértetlenségét és rendelkezésre állását.

Rendszer- és információsértetlenségi eljárásrend

A Hivatal rendszer- és információsértetlenségének tervezésekor meg kell fontolni az elektronikus aláírás és/vagy az üzenet sértetlenségét garantáló biztosítékok használatát a hálózaton áthaladó információk védelmében.
Mivel a helyesen rögzített adatok is elromolhatnak akár a feldolgozás hibáitól, akár szándékos tevékenységektől, ezért a PH rendszereibe az ilyen meghibásodások felismerése érdekében ajánlatos érvényesítő ellenőrzéseket (validation check) beépíteni. Az alkalmazások tervezésével ajánlatos gondoskodni arról, hogy a korlátozások megvalósítása valóban minimalizálja a sértetlenség elvesztésére vezető feldolgozási hibák kockázatát.
Szoftvercsomagok módosítása előtt megfontolandó annak kockázata, hogy a módosítás a beépített szabályozásokat és a sértetlenséget biztosító folyamatokat veszélyezteti.

A rendszer- és információsértetlenség biztosításában fontos szerepet játszik az alkalmazói rendszerek használatára történő rendszeres oktatás, illetve az informatikai biztonság olyan szintű oktatása, amely kiterjed az elektronikus információs rendszerekben kezelt adatok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának megőrzése érdekében betartandó szabályokra és az érvényesítendő védelmi intézkedésekre.
Az Informatika a fenti elvek alapján időszakosan és szükség szerint előterjeszti a javaslatait a Hivatal vezetése számára a rendszer- és információsértetlenségi célok megvalósításához és azok szervezeti integrációjához.
A Hivatal elektronikus információs rendszerében alkalmas és hatásos titkosítást, az elektronikus információs rendszerekben szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveletekkel kell biztosítani, hogy védeni lehessen az információk bizalmasságát hitelességét és sértetlenségét.

Felügyelet

A Hivatal különböző eszközökkel felügyeli az elektronikus információs rendszereit, hogy észlelhesse a kibertámadásokat, vagy a kibertámadások jeleit, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat és azonosítsa az elektronikus információs rendszerei jogosulatlan használatát.
Felügyeleti eszközöket alkalmaz a hozzáféréssel és használattal kapcsolatos alapvető információk gyűjtésére; és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére. Védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben és erősíti az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel.
A Hivatal informatikai biztonsági adminisztrátorai havi jelentést készít az elektronikus információs rendszerek felügyeleti információival az informatikai biztonsági vezető számára.

Felelősség

A Hivatal rendszer- és információsértetlenségének biztosítása az informatikai biztonsági vezető feladata.

Személyi biztonság
Cél: Az informatikai eszközökkel kapcsolatba kerülő munkaköröket csak megfelelően képzett és ellenőrzött munkatársak töltsék be.

Ellenőrzött munkatársak alkalmazása

Az informatikai munkatársak munkába állását meg kell, hogy előzzék a kezelt adatok érzékenységével arányos mélységű, a fontos és bizalmas munkakörökre vonatkozó szabályok szerinti ellenőrzések.
A nemzetbiztonsági követelmények szerinti ellenőrzéseken túl a kockázattal arányos mértékben mérlegelni kell a munkatárs egyéni tulajdonságait is (pl. felelősségtudat, elkötelezettség, terhelhetőség, koncentrálóképesség, pániktűrő képesség stb.).

Az információbiztonsági szempontból kritikus informatikai munkaköröket betöltő munkatársak esetében az alkalmasságot rendszeresen felül kell vizsgálni.

Alkalmazási feltételek

Szerződéses kötelezettségük részeként, az alkalmazottaknak, és a külső szerződőknek el kell fogadniuk, és alá kell írniuk alkalmazási szerződésük (pl. munkaszerződés, munkaköri leírás, vállalkozói szerződés) feltételeit és kikötéseit, amelyeknek rögzíteniük kell az alkalmazottak és a szervezet információbiztonsággal kapcsolatos személyes kötelezettségeit és felelősségét.
Az érintett munkatársakkal olyan titokvédelmi nyilatkozatot kell aláíratni, amely a munkaviszony megszűnte után is meghatározott időtartamig kötelezi őket a titoktartásra.

Személyekhez fűződő jogok

A Hivatal elektronikus információs rendszerei kizárólag a Hivatal jogszabályokban előírt feladatainak elvégzésére szolgálnak, a felhasználók azokat kizárólag hivatali feladataikkal összefüggésben jogosultak használni.
A Hivatal az egyes felhasználók által privát célból kezelt adatok, azaz fájl- vagy adatbázisszervereken tárolt állományok, adatok vagy az elektronikus levelezőrendszerben küldött, vagy kapott levelek és csatolt állományaik tekintetében – nem szankcionálja a személyes használatot, amennyiben az

a) nem veti fel jogszabálysértés gyanúját,
b) nem sérti a Hivatal belső szabályait,
c) nem akadályozza az elektronikus információs rendszerek rendeltetésszerű használatát.

A magáncélú adatkezelés alkalmazása során a felhasználónak kell bizonyítania, hogy a privát célból kezelt adatállományt jogszerűen birtokolja.
A Hivatal dolgozói és az elektronikus információs rendszer egyéb felhasználói tudomásul veszik, hogy az általuk a privát célból kezelt adatokba, Hivatal tulajdonát képező hardvereszközbe (pl.: asztali gép, laptop, tablet, okostelefon, pen-drive, flash-drive stb.) a Hivatal biztonsági incidens gyanúja vagy kivizsgálása esetén korlátozás és előzetes értesítés nélkül betekinthet, azokat bizonyítékként fegyelmi és/vagy jogi eljárásban felhasználhatja.
A magáncélú adatkezelés szabályaira a Hivatal köteles minden dolgozójának vagy felhasználójának a figyelmét írásban – a munkavégzésre irányuló jogviszony kezdetén – felhívni; a tájékoztatás megtörténtét a dolgozó aláírásával igazolja a Humánpolitika csoportnál.

További szabályozás

A munka-, tűz- és balesetvédelmi oktatás anyagát a vonatkozó szabályzatok tartalmazzák.

Felelősség

Ellenőrzött munkatársak alkalmazásával kapcsolatos felelősség megoszlik a Hivatal vezetője, az Informatikai biztonsági vezető és az Információbiztonsági felelős között.

Fizikai és környezeti biztonság
Cél: A védett erőforrások fizikai védelmének kockázatarányos megvalósítása.

Biztonsági zónák

Az informatikai helyiségekben csak az arra felhatalmazott személyek tartózkodhatnak.
A szervezet 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. Ide tartoznak a 2. fejezetben felsorolt információs rendszerek.
- **Nyilvános terület:** az előzőekbe nem sorolt (pl. ügyfélszolgálati tér) hivatali helyiségek.

Adminisztratív és műszaki védelmi intézkedések

Gondoskodni kell arról is, hogy a helyiségek megfelelően el legyenek választva, az ajtók be legyenek csukva, a legutoljára távozó személy nyitott irodát nem hagyhat maga után.
Az egyes biztonsági zónák kapcsán a következő adminisztratív és műszaki védelmi intézkedéseket kell kialakítani:

Kategória	Adminisztratív és védelmi intézkedéseket
Zárt terület	• Kártyás beléptető rendszer • Biztonsági ajtó • Ablak esetén rács, illetve biztonsági fólia • Riasztó berendezés • Több szerver számítógép esetén rack-szekrény használata
Nyilvános terület	• Különleges fizikai védelmet nem igényel

Belépés- és mozgásellenőrzés

A különböző biztonsági zónák közötti mozgást ellenőrizni kell. A biztonsági zónákhoz meghatározott követelményeknek megfelelő adminisztratív és műszaki eljárásokat kell alkalmazni.
A telephelyek kiválasztása és kialakítása során törekedni kell a közforgalmú (külső személyek által is használt) területek lehető legnagyobb mértékű elválasztására az üzemi területektől.
Azokat a területeket, ahol külsős személyek, látogatók is tartózkodhatnak, nyilvános területként kell kezelni, és a hozzáférési pontokon és zónahatárokon az ennek megfelelő védelmet kell kialakítani.
A Hivatalon belül zárt területen idegenek (pl. vendégek, ügyfelek) engedély nélkül nem közlekedhetnek. Ügyfélszolgálati időn kívül a Hivatal teljes területére kiterjed az a szabály, hogy a belépő idegenek engedély nélkül nem közlekedhetnek.

Az engedélyt a Információs szolgálaton keresztül az a munkatárs adhatja meg, akihez az idegen érkezett. Az idegen személyek, valamint a saját munkatársak zárt területre történő belépéséről az Információs szolgálatnak nyilvántartást kell vezetni a következő adatok feljegyzésével:

- a belépő személy neve, munkahelye,
- a belépés ideje,
- a belépés célja,
- a kísérő személy neve, szervezeti egysége,
- a kilépés ideje.

A zárt területeket belépés- és mozgásellenőrző rendszerrel kell védeni, és itt ellenőrzési pontokat kialakítani minimálisan a következő intézkedések megvalósításával:

- személy azonosságának ellenőrzése,
- be- és/vagy kilépés idejének rögzítése.

A belépés- és mozgásellenőrző rendszer működtetése a Gondnokság feladata.
A munkaállomások elhelyezésénél (fizikai telepítés) minden esetben kiemelten kell gondoskodni a berendezések biztonságáról, az illetéktelen hozzáférés megelőzéséről, megakadályozásáról.
Azon irodahelyiségeket, ahol munkaállomás működik tilos felügyelet nélkül hagyni, ha a helyiségben senki sem tartózkodik, azt be kell zárni.
Zárt területre idegenek belépése (pl. karbantartás, takarítás céljából) csak az informatikai biztonsági vezető engedélyével és felügyeletével történhet. A zárt területre történő belépés a kísérő személy beléptető kártyájával lehetséges.
Ha a belépést biztosító kártyát valaki elveszíti, vagy a kártyája kompromittálódik, a felelősök megszüntetik az érintett kártyák belépési jogosultságát és értesítik erről az informatikai biztonsági vezetőt. Ha fennáll a veszélye, hogy a teljes rendszer kompromittálódott, úgy a legrövidebb időn belül javaslatot tesznek a megfelelő megoldásra (pl. a teljes rendszer cseréje) a Hivatal vezetőjének.
Az informatikai helyiségekbe való belépés az alábbi személyek számára engedélyezhető:

a) Informatika dolgozói
b) a Belső Ellenőrzés informatikai ellenőrzést végző dolgozója
c) a telephelyek informatikai helyiségei esetén az adott szerv informatikai támogatásért felelős dolgozói.

Az Informatika vezeti és folyamatosan aktualizálja az informatikai helyiségekbe való belépésre felhatalmazott személyek nyilvántartását.
A Hivatal minden naptári év elején felülvizsgálja a belépésre jogosult személyek listáját.

Informatikai helyiségek kiválasztása, kialakítása

Az informatikai infrastruktúra (szerverek, hálózati csomópontok) elhelyezésének és az egyes központi, tartalék és telephelyi informatikai helyiségek kiválasztásának és kialakításának során legalább az alábbi információbiztonsági szempontokat kell figyelembe venni:

a) az egyes informatikai helyiségekben elhelyezésre kerülő informatikai eszközök üzemeltetési előírásaiban megfogalmazott környezeti paramétereknek megfelelő környezet;

b) környezeti behatások
   (i) automatikus tűzjelző (füstérzékelő) és riasztó berendezés,
   (ii) automata tűzoltó készülék,
   (iii) automata légtechnikai berendezés a szerverek üzemeltetéséhez előírt tiszta levegő, hőmérséklet és páratartalom folyamatos biztosításához,
   (iv) pormentes környezet, szigetelt nyílászárók,
   (v) fémből készült bútorok, antisztatikus burkolat,
   (vi) elhelyezés vizesblokktól távol (pincében, víz által elárasztható helyen semmiképp)
   (vii) elhelyezés gázvezetéktől, kazántól, illetve bármilyen tűz- és/vagy robbanásveszélyes helytől a lehető legtávolabb,
   (viii) elhelyezés bármilyen mágneses, elektromágneses sugárforrástól védetten; behatolás védelem,
   (ix) a MABISZ biztonságtechnikai ajánlása B/I. pontja szerinti teljes mechanikai fizikai védelem,
   (x) a MABISZ biztonságtechnikai ajánlása C/I/2. pontja szerinti részleges elektronikai jelzőrendszer,
   (xi) a MABISZ biztonságtechnikai ajánlása C/II. pontja szerinti beléptető rendszer,
   (xii) elhelyezés bejárattól, ügyféltértől távolabb, mindenképpen olyan helyen, ahová csak a portaszolgálaton át lehet eljutni, lehetőség szerint további fizikai védősávokkal (zárt folyosó, recepció) védve,
   (xiii) elhelyezés oly módon, hogy maga az informatikai helyiség ne legyen feltűnő, frekventált helyen (pl. büfé, dohányzásra kijelölt folyosószakasz mellett), de az ahhoz vezető úton egy idegen jó eséllyel találkozzon hivatali dolgozóval,
   (xiv) elhelyezés oly módon, hogy a helyiségek helye és jelentősége ne legyen bárki számára nyilvánvaló ("low profile").
c) áramellátás és áramvédelem,
   (i) szűrt és teljes túlfeszültség-védelemmel ellátott elektromos hálózat,
   (ii) szünetmentes ideiglenes tartalék áramforrás (UPS), amely 30 percig, de legalább a tartós tartalék áramforrás beindításáig képes az önálló áramellátás biztosítására,
   (iii) szünetmentes tartós tartalék áramforrás, amely képes az önálló áramellátás biztosítására, amíg az áramellátás beindul (a jelenlegi 2,5 órát képes teljesíteni),
   (iv) villámvédett számítógépes hálózati csatlakozások,
   (v) azokat az aktív hálózati eszközöket, amelyek nem a szerverszobában vannak elhelyezve egyedi villám és túláram-védelmet is biztosító szünetmentes, legalább 30 percnyi áthidalási idővel rendelkező tápegységgel kell ellátni.

A telephelyeken az informatikai infrastruktúra eszközeit (szerverek, hálózati csomópontok) külön helyiségben, illetve ennek hiányában az általános környezeti és behatolás védelmet biztosító helyiségen belül zárható szekrényben kell tárolni.

Közműszolgáltatások biztosítása

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 intézkedések
Zárt terület	Áramkimaradás és túlfeszültség elleni védelem, mely lehetővé teszi az eszközök legalább 30 percig történő működését.

Kábelezés biztonsága

Az épületeken belül a hálózati vezetékeket kábelcsatornában vagy a falakban erre a célra kialakításra került csövekben 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. Például, amennyiben egy kábel nyilvános helyen van felszerelve – kábel csatorna használata mellett – és érzékeny adatok továbbítódnak rajta, akkor a kábelen átmenő forgalmat mindenképp titkosítani kell, hogy a lehallgatásból származó kockázatokat csökkenteni lehessen.
A belső hálózat kívülről történő elérése kizárólag engedélyezett módon, VPN csatornán keresztül lehetséges.
A kábelezéssel kapcsolatos megelőzési, javítási és karbantartási feladatokat csak az Informatikai biztonsági vezető előzetes engedélyével lehet végrehajtani.

További szabályozás

Az informatikai erőforrások fizikai védelmének részletes szabályait illetően a Hivatal vagyonvédelmi és biztonsági intézkedései az irányadóak.

Felelősség

A területek védelmével, biztosításával kapcsolatos feladatok végrehajtásának felelőssége megoszlik a Hivatal vezetője a jegyző, Informatikai biztonsági vezető, Informatikai biztonsági felelős között.

Információs rendszerek beszerzése
Cél: Annak biztosítása, hogy a biztonság az elektronikus információs rendszereknek szerves részét képezze.

Rendszerbiztonsági tervezés

A Hivatal jövőben fejlesztendő elektronikus információs rendszereihez rendszerbiztonsági tervet is kell készíteni.
A Hivatal jelenlegi és jövőben fejlesztendő elektronikus információs rendszereinek hatóköre megegyezik jelen szabályzat „A dokumentum hatálya" pontjában leírt hatókörrel. A rendszerek architektúráját az Informatika folyamatosan összehangolja a Hivatal mindenkori szervezeti felépítésével, amely a hatályos Szervezeti és Működési Szabályzatban található.
A PH információs rendszereinek alapfeladata a Hivatal üzemszerű működésének támogatása, alapfunkciói pedig az adott rendszertől annak műszaki és üzleti specifikációjában elvárt speciális szolgáltatások.
A Hivatal elektronikus információs rendszereinek biztonságkritikus elemei a

- „Fizikai és környezeti biztonság"
- „Védelem a rosszindulatú és mobil kódok ellen"

fejezetekben vannak részletezve.
A Hivatal elektronikus információs rendszereinek működési körülményeit és a többi rendszerhez való kapcsolatait a rendszerek jövőbeni fejlesztésekor a tervezés során kiemelten kell kezelni és a Hivatal mindenkori biztonsági előírásaival összehangolni. Az elemzés során kialakult és elvárt biztonsági követelményeket a vonatkozó rendszerek fejlesztési dokumentációjában kell rögzíteni. A követelményeknek megfelelő védelmi intézkedéseket és a jogszabály szerinti biztonsági feladatokat a szükséges egyeztetések után- az informatikai biztonsági vezető határozza meg, és az Informatikai hajtja végre.

Biztonsági követelmények meghatározása

Elektronikus információs rendszerek beszerzésekor, tervezésekor és átvételekor alapvető szempont, hogy a Hivatal minimalizálja a meghibásodások és biztonsági rések keletkezésének kockázatát.
Tervezni kell a beszerzéskor a jövőben várható kapacitásköveteImént annak érdekében, hogy csökkenthető legyen a Hivatali elektronikus információs rendszere túlterhelésének kockázata. Átvétel és használatba vétel előtt meg kell állapítani, dokumentálni és bevizsgálni az új rendszerek üzemeltetési követelményeit, különös tekintettel a Hivatal biztonsági előírásaira.
A fejlesztés vagy beszerzés kezdete előtt, az információs rendszerekre vonatkozó biztonsági kockázatokat elemezni kell, ez alapján meg kell határozni a vonatkozó biztonsági intézkedéseket és a fejlesztés ennek megfelelő pontos követelményeit. A biztonsági elvárásokat rögzíteni kell az ajánlatkérési dokumentációban, teljesítésük módját, megfelelőségét pedig értékelési szempontként kell meghatározni. A fejlesztési ciklusok során „Az információbiztonság szervezete" fejezetben leírt feladat- és felelősségi körök érvényesek.
A Hivatal minden fejlesztés, megvalósítás vagy értékelés, üzemeltetés és fenntartás, illetve kivonás (archiválás, megsemmisítés) esetén kiemelt figyelmet kell, hogy fordítson a szervezet információbiztonsági követelményeire, szabályaira.

Berendezések beszerzése

Az informatikai szolgáltatások vagy berendezések megtervezésekor, kiválasztásakor és a beszerzések lebonyolításakor 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 szükségletek),
- installálás, üzembe-helyezés,
- bekerülési költség, elvárt haszon, üzemeltetési költség,
- garanciális, karbantartási és támogatási elvárások.

A fenti 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 (brand name) származó berendezések megvásárlására, mivel ez megkönnyíti az eszközök üzembe-helyezését, karbantartását és javítását.

Amennyiben megfelelő anyagi források rendelkezésre állnak a Hivatalnak törekednie kell – a létfontosságú feladatokat ellátó eszközökből – hardver hidegtartalék létrehozására.

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. Ilyen esetekben - a Kiemelt biztonsági kategóriába tartozó eszközöknél - a szállítótól meg kell követelni a bejelentést követő 12 órán belüli megjelenést és a hiba javításának megkezdését.

Az új rendszerek átvétele csak a dokumentált rendszerkövetelmények meglétének ellenőrzése után történhet meg. Ellenőrizni kell többek között a következőket:

a) a teljesítőképességi és a számítógépkapacitás-követelményeket,
b) a hibajavító és az újraindítási eljárások terveit,
c) a rutin üzemeltetési eljárások előkészítését és bevizsgálását,
d) a megállapodások szerinti biztonsági óvintézkedések megtételét,
e) a hatékony kézi (manuális) eljárásokat,
f) annak bizonyítékait, hogy az új rendszer üzembe helyezése nem lesz ellenkező, káros hatással a meglévő rendszerekre, különösen nem a feldolgozási csúcsidőkben.
g) annak bizonyítékait, hogy figyelmet fordítottak arra a hatásra, amit az új rendszer üzembe helyezése okoz a szervezet általános biztonságára,
h) az új rendszerek üzemeltetésének, valamint használatának a betanítását.

Telepítés, konfigurációkezelés

A Hivatal minden informatikai eszközének telepítését, bármilyen módosítását, cseréjét az Informatikai biztonsági vezető kezdeményezi, azt a Hivatal vezetője hagyja jóvá, majd az engedélyezést követően a feladatot az Informatika hajtja végre.
A Hivatal az elektronikus információs rendszereihez egy-egy alapkonfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges elemeit.
Az új belépő munkatársak részére a hivatal vezetőjének igénye szerint az informatikus biztosítja a munkaállomást és a munkakörhöz szükséges jogosultságokat.
A munkaállomásokat csak a feladat ellátásához szükséges beállításokkal és programokkal szabad telepíteni.
A munkaállomáson egyedi hozzáférést kell biztosítani, ezáltal lehetővé téve, hogy a munkaállomást csak az arra jogosult Felhasználók használhassák.

Fejlesztési, teszt és üzemeltetési környezet különválasztása

A fejlesztési-, teszt környezeteket és üzemi környezetet logikailag és lehetőség szerint fizikailag is szét kell választani egymástól.

Belső fejlesztések

A Hivatalban csak kisebb, nem kulcsfontosságú alkalmazások fejlesztése történhet házon belül. Ezekben az esetekben a fejlesztési és a fejlesztői teszt környezetet a fejlesztő saját számítógépén kell kialakítani.
A felhasználói tesztelésre és az éles üzemi használatra külön környezetet kell kialakítani valamely, a belső alkalmazásokat futtató szerveren.

Külső fejlesztések

A Hivatal alkalmazásainak egy részét külső szállítók fejlesztik. Ezekben az esetekben a fejlesztői és vállalkozói tesztelési környezet kialakítása és használata a szállító kötelezettsége. A vállalkozói teszteléshez a Hivatal nem adhat át az éles rendszeréből származó adatokat.
Üzemi környezetbe csak úgy kerülhet valamely alkalmazás, ha az már túlesett a vállalkozói és a hivatali teszteléseken.
A hivatali felhasználói teszteléshez szükséges környezetet a Hivatal szerverén kell kialakítani, ügyelve arra, hogy az megfeleljen az éles üzemi környezet beállításainak. A teszt környezetben éles adatok nem tárolhatóak, kivéve, ha próbaüzemi tesztelés történik. A teszt környezethez, az abban futó alkalmazáshoz a szállítónak hozzáférést biztosítani csak az Informatikai biztonsági vezető engedélyével szabad.
A teszt környezetben futó rendszer nem rendelkezhet közvetlen kapcsolattal egyetlen más éles rendszerrel sem. Ettől eltérni csak az Információbiztonsági felelős engedélyével szabad.
A teszt környezet alkalmazható oktatói környezetként is.
Az éles üzemi környezetet logikailag és lehetőség szerint fizikailag is szét kell választani a teszt környezettől. Az üzemi környezethez, az abban futó alkalmazáshoz a szállítónak hozzáférést biztosítani csak az Informatikai biztonsági vezető engedélyével szabad.

Üzemelő szoftverek

A Hivatal számítógépein, valamint alkalmazások futtatására alkalmas egyéb eszközein (pl. mobiltelefon, tablet, PDA) kizárólag az Informatika által telepített alkalmazások használhatók. Emellett a megbízható szoftverek használata, az információ kiszivárgási veszélyének csökkentése érdekében:

- szabályozni kell a szoftverek telepítésének és üzemeltetésének elvárt folyamatát,
- biztosítani kell, hogy a fejlesztők és karbantartók csak azokhoz a rendszerekhez férjenek hozzá, amelyekre munkájukhoz feltétlenül szükségük van.

A telepített szoftvereket minden naptári év elején ellenőrizni kell, a következők szerint:

- Össze kell írni a Hivatal jogos tulajdonában lévő szoftverek licenceit legalább a következő adatokkal:
  - Licenctulajdonos
  - Szoftver
    - neve,
    - verziószáma,
    - nyelve,
    - hozzáférés/használati jog száma,
    - licenc esetleges lejárati dátuma,
    - speciális használati feltételek,
    - birtokba kerülési irat (számla) száma és dátuma.
- Össze kell gyűjteni a Hivatal eszközeire telepített szoftvereket legalább a következő adatokkal:
  - Licenctulajdonos,
  - Szoftver
    - neve,
    - verziószáma,
    - nyelve,
    - telepítés darabszáma,
    - felhasználója,
    - számítógép azonosító,
- Meg kell állapítani az eltéréseket és ezek rendezésére cselekvési tervet kell készíteni.

Vagyonleltár

Valamennyi informatikai vagyontárgyat egyértelműen azonosítani kell és valamennyi fontos vagyontárgyról a vonatkozó szabályozással (Leltározási szabályzat) összhangban éves gyakorisággal leltárt kell felvenni és azt meg kell őrizni.

A telepített eszközöket minden naptári év elején ellenőrizni kell és a meglévő nyilvántartással össze kell hangolni.

Felelősség

Az elektronikus információs rendszerek beszerzésének előkészítése az Informatikai biztonsági vezető hatáskörébe tartozik.

Információs rendszerek karbantartása

Cél: Az információs rendszerek megbízható működésének biztosítása, a váratlan hibák elhárítására fordítandó erőforrások minimalizálása.

Berendezések karbantartása

A berendezések karbantartási terve biztosítja a berendezések előírt (idő vagy igénybevételi) intervallumonként történő szakszerű karbantartását.
A külső szolgáltató által karbantartott berendezésekre vonatkozóan a Hivatalnak külön karbantartási szerződést kell kötnie a szolgáltatóval, mely tartalmazza a karbantartások ütemezését (idő vagy igénybevétel alapján), a végrehajtandó feladatokat és az elvégzett munka dokumentálását.
Az Informatika által karbantartott eszközök tervszerű karbantartása éves gyakorisággal történik, mely az elemek, részegységek tisztítását, illetve az elöregedett vagy hibás alkatrészek cseréjét foglalja magában.
A karbantartások végrehajtását lehetőség szerint munkaidőn kívül, vagy amennyiben az nem lehetséges, az érintett munkatársakkal egyeztetve munkaidőben kell végrehajtani.
Mivel a munkálatok kisebb-nagyobb üzemkieséssel is járhatnak, ezért az érintett dolgozókat szükség szerint e-mailben is értesíteni kell a karbantartás megkezdésének időpontjáról, illetve tervezett befejezéséről.
A berendezések javítása, karbantartása csak ellenőrzött körülmények között, szakember által hajtható végre.

Berendezések meghibásodása

A tervszerűen végzett karbantartás ellenére is megtörténhet, hogy a berendezések meghibásodnak. A javítást elsődlegesen az Informatika munkatársainak kell végrehajtania.
Amennyiben ez nem lehetséges (pl. idő, alkatrész vagy szakértelem hiányában) úgy

- a javításra – előzetes árajánlatkérést követően – külső 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).

Amennyiben számítógépről, vagy egyéb adatot tároló vagy hordozó eszközről van szó, úgy a kiszállítás vagy selejtezés előtt gondoskodni kell arról, hogy azon adat ne maradjon.

Berendezések és adathordozók szállítása

Informatikai berendezéseket (beleértve az adathordozókat is) a Hivatalból kivinni csak a jegyző Informatikai biztonsági vezető engedélyével lehet.
A berendezések beszerzése, javítása, karbantartása alkalmából történő szállítása megfelelő óvatossággal, lehetőleg gyári védőcsomagolásban, ütés-, rázás-, és beázásmentesen végzendő el.
Amennyiben a berendezés javítását külső cég végzi, úgy a berendezés átadását és visszavételezését is szállítólevéllel dokumentálni kell.
A szállítólevélben – vagy a külső cég által átadott bizonylaton – rögzíteni kell a következőket:

- az átadás célja (pl. szervizelésre elszállítás),
- az átadott berendezés részletes leírása (leltári szám),
- a hiba leírása (átadáskor),
- a javítás eredménye (visszavételezéskor),
- átadás-átvétel dátuma,
- átadó-átvevő neve, szervezeti egysége, aláírása

A visszavételezéskor, a bizonylat aláírását megelőzően, az Informatika munkatársának a javítás eredményességéről meg kell győződnie és alapos biztonsági ellenőrzést kell végeznie.
A Hivatal fizikai határain túlra történő szállításuk közben az információt tartalmazó adathordozókat védeni kell a jogosulatlan hozzáféréstől, a visszaélésektől, illetve a megrongálástól.
Amennyiben másik fél és a Hivatal elektronikus információs rendszere is lehetővé teszi, úgy az adathordozón található információkat titkosítani kell,
Különlegesen érzékeny adatokat tartalmazó adathordozókat kizárólag a Hivatallal munkaviszonyban álló munkatárs (pl. kézbesítő) szállíthat. Az adatok átadás-átvétele csak a megfelelő, az adathordozó tartalmát is leíró bizonylat mindkét fél általi aláírásával történhet meg. Bejövő adathordozó csak az Informatika által végrehajtott végpontvédelmi (vírus, trójai, stb.) ellenőrzést követően adható át az érintett szervezeti egységnek.
A kimenő adathordozók szállítását – egyszeri vagy folyamatos engedély formájában – az Informatikai biztonsági felelőssel engedélyeztetni kell.

Berendezések tervezett cseréje

A berendezések tervszerű cseréjét azok fizikai és technikai elavulása teszi szükségessé. Ennek megfelelően a berendezések tervszerű cseréjének meghatározott időtartama 3-5 év. Számítógépek esetében ennél gyakoribb tervezett cserére abban az esetben kerülhet sor, ha a számítógépen olyan alkalmazások használata válik szükségessé, melyek igénylik a nagyobb kapacitást, biztonságot vagy rendelkezésre állást.

Selejtezés

A berendezések, azok elemei (pl. merevlemez) csak akkor selejtezhetők, ha a meghibásodott alkatrész gazdaságosan nem javítható vagy elöregedés, elavulás miatt az alkatrész cseréje szükséges, és azt máshol nem lehet felhasználni. A hibás és az elöregedett alkatrészeket egymástól egyértelműen elkülönítetten kell tárolni.

A Hivatal a leselejtezésre kerülő eszközöket átadja egy megfelelő jogosítvánnyal rendelkező társaságnak, hogy annak környezetbarát megsemmisítése megtörténhessen.
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 Informatika munkatársa 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).

A selejtezésről a selejtezési bizottság jegyzőkönyvet vesz fel.
A selejtezés megtörténtét az informatikai vagyontárgyak nyilvántartásában is át kell vezetni.

Szoftverváltoztatások elvei

Amennyiben külső vagy belső tényezők szükségessé teszik az operációs rendszer(ek) változtatását, az operációs rendszer alapértelmezett átvizsgálása után az alkalmazási rendszert ellenőrizni és tesztelni kell annak biztosítása érdekében, hogy a változtatás a működőképességgel és a biztonsággal ne ütközzön.
Éles rendszerbe történő beillesztés előtt a változásokat, szoftverfrissítéseket, hibajavításokat az alkalmazásokkal is tesztelni kell.
Ha az egyéb (nem operációs rendszer) szoftvercsomagoknál változtatás, frissítés, karbantartás szükséges, úgy az eredeti szoftvert meg kell tartani és a változtatásokat egy egyértelműen azonosított másolaton kell végrehajtani. Szabványos szoftverfrissítési folyamatot kell alkalmazni, hogy a legkorszerűbb elfogadott alkalmazási frissítések legyenek telepítve az összes jogosított szoftverhez.
Minden egyes változtatást teljes egészében meg kell vizsgálni és dokumentálni úgy, hogy szükség esetén ismét alkalmazni lehessen a szoftver jövőbeli javított kiadásaihoz.
Az informatikusok a legfontosabb szoftverek (operációs rendszerek, leggyakoribb kiegészítők, stb.) frissítéseit illetve azok elérhető hibajavításait folyamatosan, heti szinten figyelik és szükség szerint tesztelik valamint a lehető leggyorsabban akár beavatkozás nélkül telepítik.
A hibajavítások eljárásait a konfigurációkezelési eljárásokba is be kell építeni.

Karbantartás dokumentálása

Az információs rendszereken végrehajtott karbantartási, változtatási, javítási munkálatokat az adott rendszer nyilvántartásába lefűzött Munkalapokon kell rögzíteni a következő adatok vezetésével:

- leltári szám,
- berendezés típusa, neve,
- karbantartás típusa (tervszerű, hibajavítás),
- érintett szervezeti egység,
- karbantartás módja, eredménye,
- bejelentés időpontja (hiba esetén)

- karbantartó személye, cége (külső cég esetén)
- karbantartást ellenőrizte (pl. ha külső fél végezte a karbantartást).

Rendszerdokumentáció

Az elektronikus információs rendszerek felhasználói leírásai a belső intranet hálózaton hozzáférhetők az összes munkatárs számára.
Az elektronikus információs rendszerekkel kapcsolatos további rendszerdokumentációkat (pl. rendszertervek, üzemeltetési dokumentumok) egyetlen könyvtárban, rendszerenként különböző elnevezésű alkönyvtárakban kell tárolni.
Az egyes alkönyvtárakhoz – és így az adott rendszer dokumentációjához – kizárólag az Informatikán belül az adott rendszer üzemeltetője, és az informatikai biztonsági felelős férhet hozzá olvasási joggal. Írási joggal az adott könyvtárra kizárólag az Informatikai biztonsági vezető rendelkezhet.
A dokumentációk naprakészen tartásának, a változások átvezetésének felelőse az adott rendszer üzemeltetője, melybe bevonhatja a rendszer szállítóját, amennyiben a vele kötött szerződés ezt lehetővé teszi.
A rendszerdokumentáció aktualizálását évente egyszer, vagy a rendszert vagy környezetét érintő jelentősebb változás esetén kell végrehajtani.

Felelősség

Az információs rendszerek karbantartásával kapcsolatos feladatok végrehajtása az Informatikai biztonsági vezető feladata, ideértve különösen az ütemezési, jóváhagyási és ellenőrzési feladatokat is

Hozzáférés-ellenőrzés

Cél: Az erőforrásokhoz és információkhoz való hozzáférési jogok megadásának és megvonásának szabályozása.

Az információ-hozzáférés szabályozása

Alapelv, hogy minden felhasználó csak azokhoz az erőforrásokhoz és információkhoz férhessen hozzá, amelyek a munkájához mindenképp szükségesek.
A Hivatal tulajdonában vagy használatában lévő valamennyi számítógépen tárolt adathoz hozzáférés csak a személyazonosság és a megfelelő jogosultság ellenőrzését követően lehetséges; megvédve az elektronikus információs rendszereket a jogosulatlan hozzáféréstől. Hitelesítés és azonosítás nélkül csak a Hivatal honlapjának publikus oldalai használhatók egyéb felhasználói tevékenység nem.
A különböző alkalmazásokban funkciónként, illetve egyes adatkörökre vonatkozóan szükséges a hozzáférés szabályozása, a jogosulatlanok kizárása. A funkció, illetve adatkörre vonatkozó korlátozások lehetőségét az alkalmazás fejlesztésének időszakában kell megtervezni és az alkalmazást ennek megfelelően implementálni.
A Hivatal elektronikus információs rendszerei meggátolják az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha a Hivatal vezetője engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél. Az elektronikus információs rendszerek elkülönített végrehajtási tartományt használnak minden végrehajtó folyamat számára.

A hozzáférési jogok kezelése

A Hivatal nem használ külön fizikai hitelesítési eszközöket az információs rendszereihez való hozzáféréshez, csak a felhasználói név+jelszó párost.
Valamennyi információs rendszerhez és szolgáltatáshoz való hozzáférés megadására és visszavonására hivatalos felhasználó regisztrálási, módosítási és regisztráció megszüntetési eljárást kell alkalmazni.

Igénylés

A Hivatal rendszerét használók számára – a Humánpolitikai csoport előzetes írásbeli tájékoztatása alapján – az rendszergazda hozza létre és vonja vissza a felhasználói azonosítót.
Az rendszergazda nyilvántartást vezet a Hivatal elektronikus információs rendszerének felhasználói azonosítóiról, a felhasználók aktuális jogosultságairól. Ezt a nyilvántartást csak az rendszergazda módosíthatja.
A Hivatalba belépő, illetve felhasználói munkakörbe átlépő dolgozóknak a Humánpolitikai csoport jogosultságigénylő lapot állít ki, amelyben igazolja, hogy a dolgozó jogosult felhasználói azonosító igénylésre.
A jogosultságigénylő lapon a felhasználó közvetlen vezetője illetve a hozzáférésre kijelölt rendszerek adatgazdája meghatározza a dolgozó munkakörét és megjelöli

a) a felhasználó számára munkakörének ellátásához szükséges elektronikus információs rendszereket és jogosultsági csoportokat, továbbá
b) az adott felhasználó esetében a munkakörhöz általánosan meghatározott jogosultsági csoportoktól eltérő további jogosultsági igényeket és az eltérés indoklását. Ez utóbbi esetben is csak a dokumentált jogosultsági csoportot vagy csoportokat lehet megjelölni.

Az egyedi jogosultsági igény nem lehet ellentétes a Hivatal feladatkör-elhatárolási szabályaival.

Kiadás és érvényesítés

Az rendszergazda a jogosultságigénylő lap alapján a felhasználóhoz

a) hozzárendel egy felhasználói azonosítót,
b) megadja a felhasználó kezdeti jelszavát, aminek
   i. meg kell felelnie a jelszavakkal kapcsolatos szabályoknak és
   ii. egyedinek kell lennie, nem használható rendszeresen ugyanaz a karaktersorozat,
c) megadja a felhasználó számára igényelt jogosultságokat,
d) a felhasználói azonosítót aktív állapotba helyezi.

Az rendszergazda a jogosultságigénylő lapon

a) rögzíti a felhasználói azonosítót,
b) dokumentálja az azonosító létrehozásának és jogosultságok beállításának időpontját.

Az rendszergazda nem adhatja meg a jogosultságot, amennyiben megítélése szerint az igényelt jogosultságok nyilvánvalóan megsértik a Hivatal feladatkör-elhatárolási szabályait. Ez esetben az rendszergazda– a jogosultságigénylő lap másolatának továbbításával és az eljárás felfüggesztésének közlésével – tájékoztatja a vezetőjét és az Informatika vezetőjét. Az Informatika vezetője – szükség esetén az adatgazdával és a felhasználó vezetőjével konzultálva – felülvizsgálja az egyedi igényt és írásban engedélyezheti az informatikai biztonsági adminisztrátornak az eljárás folytatását.

Módosítás

A felhasználói azonosító módosítását a felhasználó kezdeményezheti névváltoztatáskor (pl. házasságkötés miatt), valamint a biztonsági adminisztrátor az egyes rendszerek felhasználó azonosító konvencióinak szabványosítása miatt és/vagy új azonosító-képző szabályok bevezetésekor. Szintén kezdeményezheti a felhasználói jogosultságok módosítását a felhasználó követlen felettese a munkatárs munkakörének, feladatának megváltozásakor.

A felhasználói azonosító módosításakor a kiadás és érvényesítés szabályait kell értelemszerűen alkalmazni.

A jogosultságok módosításakor a kiadás és érvényesítés szabályait kell értelem szerűen alkalmazni.

Elfelejtett jelszó esetén a felhasználó írásbeli kérésére új jelszót kell kiadni. Ez esetben is a kiadás és érvényesítés szabályait kell értelem szerűen alkalmazni.

Visszavonás

A felhasználói azonosítókat inaktív állapotba kell helyezni, ha tulajdonosuk munkavégzésre irányuló jogviszonya megszűnt, vagy öt egymást követő sikertelen bejelentkezési kísérlet történt (ilyen esetekben az adott azonosító véglegesen is letiltható).
A Hivatalból kilépő vagy más munkakörbe áthelyezésre kerülő dolgozók esetén a felhasználó közvetlen vezetője jogosultságigénylési lapon tájékoztatja az informatikai biztonsági adminisztrátort a jogosultság, illetve a felhasználói azonosító visszavonásáról. (áthelyezés esetén a kiadás és érvényesítés szabályait kell alkalmazni)
Amennyiben a közszolgálati jogviszony megszüntetés/áthelyezés körülményei alapján feltételezhető, hogy a felhasználó esetleg visszaélésre tesz kísérletet, úgy a közvetlen vezetőnek gondoskodnia kell arról, hogy a jogosultságok (illetve szükség esetén a felhasználói azonosító) visszavonása megtörténjen, mielőtt a dolgozó annak okáról tudomást szerezne.
Az rendszergazda a jogosultságigénylési lap alapján törli a felhasználó azonosítóit, visszavonja az összes jogosultságát.
A visszavonási eljárás dokumentálására a kiadás és érvényesítés dokumentációs szabályait kell értelemszerűen alkalmazni.
A Hivatalból kilépő dolgozó elektronikus postafiókját, személyes könyvtárának, továbbá az általa használt számítógép(ek) merevlemezének tartalmát (szükség esetén kilépés előtt) archiválni, majd ha az archiválás ellenőrzötten sikeres volt, törölni kell.

Ellenőrzés

A felhasználók hozzáférési jogait rendszeresen át kell tekinteni, hogy minden felhasználó csakis azokhoz az információkhoz férhessen hozzá, amelyek munkájához aktuálisan szükségesek.
A különböző rendszerek biztonsági üzemeltetési kézikönyvének tartalmaznia kell a felhasználói azonosítók, jelszavak és jogosultság

a) kiadásának, módosításának, felfüggesztésének, törlésének,
b) megsértés detektálásának (észlelésének), és
c) ellenőrzésének

rendszer specifikus eljárásait.
A Hivatal információs rendszerei fedett visszacsatolást kell, hogy biztosítsanak a hitelesítési folyamat során, hogy megvédjék a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.
Meg kell oldani, hogy mindegyik információs rendszer egyedileg azonosítsa és hitelesítse az érintett szervezeten kívüli felhasználókat, és tevékenységüket. A Hivatal információs rendszerei csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat fogadhatnak el a szervezeten kívüli felhasználók hitelesítéséhez.
Alkalmazás funkciónként, illetve egyes adatkörökre (adatminősítés, biztonsági szint stb. szerint) vonatkozóan szükséges a hozzáférés szabályozása, a jogosulatlanok kizárása. A funkció, illetve adatkörre vonatkozó korlátozások lehetőségét az alkalmazás fejlesztésének időszakában kell megtervezni és az alkalmazást ennek megfelelően implementálni, mivel ez utólag már nehezen megvalósítható.

Speciális jogosultságok kezelése

Az általános összeférhetetlenségi szabályoktól való speciális eltérés kockázati tényező, ezért az ilyen jogosultságok kiadását mindenképp kerülni kell. Amennyiben valamilyen elkerülhetetlen ok miatt mégis létre kell hozni ilyet, akkor azt csak dokumentáltan, s csak a feltétlenül szükséges időtartamra szabad adni.
A rendszer-segédprogramok használata különös lehetőségeket teremt nehezen ellenőrizhető manipulációkra, ezért ezek használatát különös figyelemmel kell szabályozni és a szabályzatban foglaltakat ellenőrizni. A fejlesztő eszközökhöz, az adatbázisokhoz közvetlen hozzáféréseket lehetővé tevő segédprogramokhoz való hozzáférés csak indokolt esetben engedélyezhető és a tevékenység végén az engedélyt vissza kell vonni, és lehetőleg ki kell zárni az ellenőrizhetetlen származású programok használatát.
Az eljárásrend alkalmazásának hatására csökken annak a kockázata, hogy a speciális jogosultságok nem megfelelő menedzselése miatt a rendszer működésében hibák keletkeznek, vagy illetéktelen helyre kerülnek védendő adatok.

A felhasználói jelszókezelés

A jelszavak a felhasználó számítógépes szolgáltatásokhoz való hozzáférési jogosultságának hitelesítésére szolgálnak. A jelszókezelő rendszernek hatékonyan és interaktívan kell biztosítania a megfelelő színvonalú jelszavak használatát.

A Hivatal az alábbi elvárásokat érvényesíti a jelszavak kezelésével kapcsolatosan:

a. tegye lehetővé a felhasználók számára jelszavuk kiválasztását és megváltoztatását;
b. kényszerítse ki az ideiglenes jelszavak megváltoztatását az első bejelentkezéskor;
c. kényszerítse ki a megfelelő minőségű jelszavak használatát;
d. kényszerítse ki a jelszóváltoztatást, frissítést időszakonként;
e. tiltsa meg a korábban használt jelszavak ismételt felhasználását;
f. beíráskor ne jelenítse meg a jelszavakat a képernyőn;
g. a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hasító érték tárolást) és nem továbbítja;
h. változtassa meg a szállító alapértelmezett jelszavát a szoftver installálása után.

Jelszógondozási folyamattal kell a jelszavak kiosztását ellenőrizni, úgy, hogy:

a. szükség esetén a felhasználók kötelezhetők arra, hogy nyilatkozatban vállalják a számukra kiadott, vagy általuk képzett jelszavaik titokban tartását;
b. biztosítani, hogy a kezdeti jelszavak is biztonságos körülmények között kerüljenek a felhasználóknak átadásra.

A felhasználói jelszavak képzéséhez az alábbi szabályokat kell betartani:

a. a jelszó legalább nyolc karakter hosszú legyen, és - ahol műszakilag az megvalósítható - törekedni kell arra, hogy tartalmazzon a kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;

b. a jelszavakat a rendszergazda vagy az elektronikus információs rendszer biztonságáért felelős által – a Rendszerbiztonsági tervben vagy egyéb módon – meghatározott időközönként meg kell változtatni;
c. a jelszavakat két napon belül nem szabad megváltoztatni;
d. az előző jelszavak újra használatát kerülni kell;
e. zárolás esetén előre beállított időtartam eltelte után engedélyezze vissza a felhasználói fiókot.

Az elektronikus információs rendszerekben a jelszavak használatának és képzésének részletes szabályai a következők:

a. a felhasználó a jelszavát köteles titokban tartani;
b. a jelszószabályok betartása minden felhasználónak jól felfogott érdeke. A felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el az elektronikus információs rendszerben;
c. a felhasználói jelszavakat – informatikai rendszerenként – nyilván kell tartani, azokat zárt, a felhasználó által a lezárás mentén aláírt, dátummal és névvel ellátott, a jegyző által meghatározott, tűzbiztos, megfelelő mechanikai védelemmel ellátott páncélszekrényben kell tárolni. Egyéb helyen tilos leírni;
d. ha bármilyen jel mutat arra, hogy a jelszó illetéktelen kézbe jutott, azonnal meg kell változtatni, értesíteni kell a rendszergazdát és az elektronikus információs rendszer biztonságáért felelős személyt;
e. nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé, pl. makróra, vagy funkció billentyűre;

A jelszó minél komplexebb, annál kisebb a valószínűsége, hogy visszaélésre kerül sor. A jelszavak képzésénél az alábbi szempontokat kell betartani:

a. könnyen megjegyezhető, és nehezen kitalálható legyen;
b. semmi olyasmin ne alapuljon, aminek alapján valaki kitalálhatja, ilyenek a nevek, telefonszámok, születési dátumok, stb.;
c. ne legyen a gépnévre vagy a felhasználói névre utaló;
d. ne legyen sorozat.

A fenti szabályok az elektronikus információs rendszerek által technikailag kikényszeríthető részét a rendszergazdának kell beállítani.

A felhasználó felelőssége, ha jelszavának neki felróható mulasztása miatti megismerése révén valaki a nevében visszaélést követ el az elektronikus információs rendszerben.

A Hivatal a magas biztonsági követelményű, saját felelősségi körébe tartozó elektronikus információs rendszerekre vonatkozóan hardver token alapú hitelesítése esetén olyan mechanizmusokat alkalmaz, amely megfelel az eljárásrendben meghatározott minőségi követelményeknek, vagy:

a. az elektronikus információs rendszer nyilvános kulcsú infrastruktúra alapú hitelesítés esetén ellenőrzi a tanúsítványokat egy elfogadott megbízható pontig tartó tanúsítványlánc felépítésével és ellenőrzésével, beleértve a tanúsítvány állapot információ ellenőrzését is;
b. kikényszeríti a megfelelő magánkulcshoz való jogosult hozzáférést;
c. összekapcsolja a hitelesített azonosságot az egyéni vagy csoport fiókkal;
d. megvalósítja a visszavonási adatok helyi tárolását a tanúsítványlánc felépítésének és ellenőrzésének támogatására arra az esetre, amikor a visszavonási információk a hálózaton keresztül nem elérhetők.

A Hivatal a magas biztonsági követelményű, saját felelősségi körébe tartozó elektronikus információs rendszerekre vonatkozóan tulajdonság alapú hitelesítést alkalmaz, azaz a felhasználó egyedi azonosítást lehetővé tevő tulajdonságai alapján végzi el az azonosítást.
Személyes vagy megbízható harmadik fél általi regisztráció

A Hivatal szükség esetén eljárásrendben meghatározott hitelesítő eszköz átvételéhez olyan regisztrációs eljárást követel meg, melyet meghatározott regisztrációs szervezet folytat le az érintett szervezet által meghatározott személyek vagy szerepkörök jóváhagyása mellett.

Az ASP Központtól kapott szoftveres tanúsítvány és annak jelszava nem adható át az ASP Központ által nem feljogosított személynek. Az önkormányzati ASP rendszerben csak a „257/2016. (VIII. 31.) Korm. rendelet az önkormányzati ASP rendszerről" jogszabályban említett szereplők végeznek, illetve végeztetnek központilag fejlesztői, üzemeltetői, működtetői tevékenységet. Bárminemű fejlesztői tevékenységet az ASP Központ vezetője engedélyez írásban.

Felhasználói felelősségek

A felhasználók a Hivatal elektronikus információs rendszereihez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezettek, ahol nyilatkozatukkal igazolják, hogy az elektronikus információs rendszer használatához kapcsolódó, rájuk vonatkozó biztonsági szabályokat és kötelezettségeket megismerték, saját felelősségükre betartják.
A jelszavakkal kapcsolatos szabályok megszegéséből, így különösen a más jelszavának megismerésével elkövetett esetleges visszaélés következményeiért a szabályokat megszegő felhasználók a felelősek.
A Hivatal évente legalább egy alkalommal felülvizsgálja és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet a viselkedési szabályok betartását. Változás esetén a hozzáférési nyilatkozatot az érintett felhasználókkal ismételten aláíratja.

Felhasználói informatikai biztonsági követelmények

A hálózati bejelentkezéshez a felhasználóknak felhasználónévvel és jelszóval kell azonosítaniuk magukat.
A munkaállomásokon telepített operációs rendszert úgy kell beállítani, hogy ha a munkatárs 15 percen túl nem használja a rendszert, az automatikusan lezárja a munkaállomást, és a munka újbóli megkezdésekor felhasználónév, jelszóval kell a munkatársnak azonosítania magát.
A külső felhasználókat a kapcsolati alrendszerek megfelelő kialakításával, a belső felhasználókat (alkalmazottakat) szabályzatokkal kell kötelezni arra, ha őrizetlenül hagyják a berendezéseiket, akkor (akár logikailag, akár fizikailag) zárják le azokat.
A belső felhasználókat (alkalmazottakat) kötelezni kell arra, hogy csak az aktuális munkához szükséges dokumentumokat tartsák az asztalon/képernyőn, és ne hagyják ezeket a dokumentumokat, adatokat felügyelet nélküli hozzáférhető helyen.

Nyilvánosan hozzáférhető információk kezelése

A Hivatal a nyilvánosan hozzáférhető információkat a honlapján teszi közzé.
A nyilvánosan hozzáférhető információk (beleértve a közérdekű adatokat) sértetlensége érdekében adminisztratív és technikai intézkedéseket kell kidolgozni, melyben ki kell térni az információ változtatásának eljárásrendjére, új információ közzététele előtt követendő eljárásra és egyes információk törlésének eljárásaira is.
A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban kell elhelyezni, elkülönítve a belső szervezeti hálózattól.
Ezen túlmenően az Önkormányzat honlapja, mint informatikai célrendszer védelme érdekében technikai intézkedéseket kell meghatározni és rögzíteni az informatikai célrendszer biztonsági tervében.

Távmunka és távoli elérés szabályai

Azokon az eszközökön, amelyeken önkormányzati ASP rendszer van használatban, vagy adat továbbítódik rá, tilos olyan alkalmazást használni, amely az eszközt az ASP Központon kívüli harmadik féllel köti össze, és amellyel lehetőség van távoli támogatásra, vezérlésre, távoli hozzáférésre, képernyő átvételére stb.

A fentieken túlmenően a Hivatal a magas biztonsági követelményű elektronikus információs rendszerekre vonatkozóan megköveteli, saját felelősségi körébe tartozó elektronikus információs rendszerei esetén biztosítja:

a. kidolgozza és dokumentálja minden engedélyezett távoli hozzáférés típusra a felhasználásra vonatkozó korlátozásokat, a konfigurálási vagy a kapcsolódási követelményeket és a megvalósítási útmutatókat;
b. engedélyezési eljárást folytat le az elektronikus információs rendszerhez történő távoli hozzáférés feltételeként;
c. az elektronikus információs rendszer figyeli és ellenőrzi a távoli hozzáféréseket;

d. kriptográfiai mechanizmusokat kell alkalmazni a távoli hozzáférés munkaszakaszok bizalmasságának és sértetlenségének a védelmére;
e. minden távoli hozzáférést felügyelt hozzáférés ellenőrzési ponton keresztül kell irányítani az elektronikus információs rendszerben.
f. a privilegizált parancsok végrehajtásához és biztonságkritikus információk eléréséhez távoli hozzáférést csak meghatározott és elfogadott igény esetén engedélyez;
g. dokumentálja és indokolja az engedélyezett hozzáféréseket a rendszerbiztonsági tervben.

Felelősség

A hozzáférés-ellenőrzés szabályainak elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikai biztonsági vezető hatáskörébe tartozik.

Védelem a rosszindulatú és mobil kódok ellen
Cél: Meg kell akadályozni, hogy a szervezet működésében zavart, adatvesztést vagy adatkiszivárgást okozzon bármilyen rosszindulatú kód (vírus, trójai stb.).

Rosszindulatú kód elleni védelem

Olyan adminisztratív és technikai intézkedéseket kell alkalmazni, amelyek megakadályozzák a rosszindulatú kódokat tartalmazó programok bejutását, alkalmazását.
A Hivatal számítógéphálózatában csak olyan alkalmazások, kódok futtathatók, amelyek előzetesen átestek az informatikai csoport biztonsági ellenőrzésén. A Hivatal rendszereiben (különös tekintettel a különböző internetes böngészőkre) le kell tiltani minden olyan kód futtatását, amelyek nem szükségesek a felhasználók munkájához.
A Hivatal számítógéphálózatába és -hálózatából, csak központi vírus- és rosszindulatú kód-ellenőrzésen átesett adatok továbbíthatók.
A Hivatal számítógéphálózatában – a biztonsági architektúra részeként – többkomponensű behatolás-érzékelő rendszert kell folyamatosan működtetni. Ennek a rendszernek az ellenőrzése, illetve jelzéseinek a figyelemmel követése megegyezik a „Naplózás és incidenskezelés" részletesen leírt feladatokkal.
Minden külső adatcserére lehetőséget adó alkalmazás csak biztonsági ellenőrzés mellett üzemeltethető. Ilyen szempontból kritikus üzemeltetési területek:

- e-mail;
- Internet;
- külső adathordozó felhasználásával történő adatcserét használó alkalmazások;
- USB, CD-rom, illetve egyéb külső adathordozó fogadására képes eszközzel ellátott munkaállomások, tabletek, stb.

A végpontvédelmi (vírus, spam, trójai, stb.) definíciós adatok érvényességi dátumát a vírusvédelmi felelősnek naponta ellenőrizni kell. Az ellenőrzésnek ki kell terjednie arra is, hogy az automatikus szétosztás is megtörtént-e, illetve, hogy a kliens komponensek számára a legfrissebb definíciós állomány áll-e rendelkezésre. Amennyiben a definíciós állomány az utóbbi hat órában nem frissült, úgy az rendszergazda köteles haladéktalanul megtenni a megfelelő lépéseket.

További szabályozás

Rosszindulatú kód elleni védelem részletes szabályozása a Hivatal hatályos Vírusvédelmi Szabályzatában, található.

Felelősség

A rosszindulatú kód elleni védelem felelőse az Informatikai biztonsági vezető.

Adatkezelés

Cél: Biztosítani, hogy a Hivatal elektronikus információs rendszere konzisztens legyen az adatkezelés területén abban, hogy az elvárt eredményt hozza az elvárt teljesítmény mellett.

Alapkövetelmények

A Hivatal elektronikus információs rendszereiben tárolt és feldolgozott adatok vonatkozásában az egyes ügyviteli és üzemeltetési folyamatok eljárási szabályaiban gondoskodni kell arról, hogy az adatok sértetlensége az adatkezelés során biztosított legyen.
A 2. fejezet szerinti kettes, vagy az ettől magasabb biztonsági osztályba sorolt adatokat:

a) a bevitel után titkosítottan kell tárolni, kezelni vagy továbbítani,
b) külső adatátviteli csatornák használata során meg kell győződni arról, hogy az átvitel során nem történt adatmódosulás, illetve
c) hogy az átvitel megtörtént.

Információbiztonsági szempontból az adat-előkészítési folyamatok ügyviteli szabályainak:

a) biztosítaniuk kell az adatok teljes körűségét, pontosságát és érvényességét;
b) tartalmazniuk kell az összes forrásdokumentumra vonatkozó engedélyezési eljárásokat;
c) gondoskodniuk kell az átvételi, a jóváhagyó és az esetleges konverziós szerepkörök megfelelő szétválasztásáról;
d) biztosítaniuk kell, hogy a jóváhagyott adatok teljes körűsége, pontossága és érvényessége az előkészítés további szakaszaiban is fennáll;
e) tartalmazniuk kell a hibásnak minősülő forrásdokumentumok kezelésének eljárásait;
f) tartalmazniuk kell az egyes forrásdokumentumok biztonsági osztályainak megfelelő követelmények teljesítésének módját.

Az adatbeviteli folyamatok ügyviteli és informatikai üzemeltetési szabályainak:

a) gondoskodniuk kell az adatrögzítést megelőző megfelelő jóváhagyási eljárásról;
b) gondoskodniuk kell az átvételi, az engedélyezési, a jóváhagyási és az adatrögzítési funkciók megfelelő szétválasztásáról;
c) biztosítaniuk kell a munkaállomás és a felhasználó egyértelmű azonosítását és gondoskodniuk kell azok folyamatos használatáról;
d) biztosítaniuk kell a rögzített adat és a forrásdokumentum közötti kapcsolat (iktatószám, vagy más alkalmas egyedi azonosító) rögzítését;
e) biztosítaniuk kell, hogy a hibák felismerését biztosító ellenőrzések a hiba keletkezésének helyéhez minél közelebb kerüljenek elvégzésre;
f) tartalmazniuk kell a hibásan rögzített adatokkal kapcsolatos javítási és eszkalációs (problémamegoldó, menedzselő) eljárásokat;
g) tartalmazniuk kell az adatbevitelhez kapcsolódó engedélyezési szabályok betartásáért viselt felelősség egyértelmű kijelölését.

Az adatfeldolgozást végző alkalmazásoknak tartalmazniuk kell a hibák megelőzését, felfedezését és korrigálását szolgáló funkciókat.
Az adatfeldolgozási folyamatok ügyviteli és informatikai üzemeltetési szabályainak:

a) tartalmazniuk kell a hibák kijavításának és a javítás jóváhagyásának eljárásait;

b) gondoskodniuk kell a feldolgozások során a feldolgozott vagy visszautasított tranzakciók naplózásáról;
c) biztosítaniuk kell, hogy csak az engedélyezett tranzakciók feldolgozására kerül sor;
d) gondoskodniuk kell az adatfeldolgozás operatív és engedélyezési funkcióinak megfelelő szétválasztásáról;
e) biztosítaniuk kell, hogy az adatok teljes körűsége, pontossága és érvényessége a feldolgozási tevékenységek folyamán megmaradjon;
f) gondoskodniuk kell az adatfeldolgozással és a hibajavítással kapcsolatos felelősségek egyértelmű kijelöléséről.

Az outputok kezelésével és szétosztásával kapcsolatos ügyviteli és informatikai üzemeltetési szabályoknak:

a) gondoskodniuk kell az outputok tartalmi ellenőrzéséről;
b) gondoskodniuk kell arról, hogy az outputokhoz való fizikai és logikai hozzáférés csak az arra jogosított személyekre korlátozódik;
c) gondoskodniuk kell arról, hogy a jogosult személyek időben megkapják az elkészült outputokat;
d) tartalmazniuk kell az egyes outputok biztonsági osztályainak megfelelő követelmények teljesítésének módját
e) tartalmazniuk kell az outputok tárolására és kezelésére vonatkozó szabályokat és eljárásokat;
f) biztosítaniuk kell, hogy a megsemmisítési eljárások során az outputok tartalma helyreállíthatatlanul megsemmisüljön!

Adatcsere, adattovábbítás

Az adatcsere, adattovábbítás biztonságáról a szervezetek között olyan megállapodást kell kötni, amely mindkét fél által támasztott követelményeknek megfelel.
A külső szervezetekkel történő adatcserét csak a szervezettel kötött megállapodás alapján lehet végezni, melyben rögzíteni kell az adattovábbítás technikai és adminisztratív eljárásait. Az alkalmazott védelmet az informatikai célrendszer által kezelt és átadott információ biztonsági besorolásának megfelelően kell kialakítani, és a védelmi intézkedéseket a célrendszer biztonsági tervében kell rögzíteni. A megállapodásban részletezett eljárásnak ki kell térnie az adatkéréstől az adat megérkezésének visszaigazolásáig minden lépésre, és egyértelműen definiálnia kell a folyamatban résztvevők felelősségét.
Biztosítani kell az elektronikus üzenetekben továbbított információk biztonságát és rendelkezésre állását. Ehhez meg kell határozni azokat az eljárásokat, amelyeket az elektronikus üzenetek továbbítása során alkalmaznak. Az érintett informatikai célrendszerekkel kapcsolatos eljárásokat, védelmi intézkedéseket (pl. az elektronikus aláírás, időbélyegzés használata, titkosítás) az informatikai célrendszer biztonsági tervében kell rögzíteni.

Hálózati határvédelem

A Hivatal felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt.
Az elektronikus információs rendszerek csak a Hivatal biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódhatnak külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.
A Hivatal számára bizalmas hálózati kapcsolatnak számít a Hivatal központjainak belső hálózata, valamint a telephelyek belső hálózata, minden egyéb hálózat nem bizalmas hálózatnak számít, olyannak, amelyről azt kell feltételezni, hogy veszélyt jelent a Hivatal biztonsága számára.
A Hivatal székhelye és telephelyei között VPN kapcsolatot kell kialakítani.
A bizalmas és a nem bizalmas hálózatokat csak a Hivatal tűzfalán keresztül lehet összekapcsolni.
A tűzfalak konfigurációja során gondoskodni kell arról, hogy csak az engedélyezett kapcsolati lehetőségek legyenek elérhetők.
Belső hálózatban lévő számítógép egyedi külső hálózati kapcsolattal csak indokolt esetben, közvetlen vezetői kezdeményezés alapján az Informatikai biztonsági vezető egyedi engedélyével rendelkezhet. Az ilyen számítógépeken a Hivatal számítógép-hálózatához való kapcsolódáskor nem engedélyezett a külső kapcsolat és a belső hálózat egyidejű használata.
A Hivatal számítógép-hálózata és külső hálózatok közötti kapcsolat során csak az engedélyezett protokollok továbbíthatók, minden egyéb protokoll továbbítása tilos.
Hivatal számítógép-hálózatában alkalmazható külső kommunikációs protokollok köréről– az rendszergazda javaslatára, az üzemeltetés véleményének figyelembe vételével – az Informatikai biztonsági vezető dönt.
A Hivatal számítógép-hálózata egytartományos rendszer. Tilos olyan munkaállomást vagy mobil eszközt csatlakoztatni a Hivatal hálózatra, amely nem bizalmas hálózati kapcsolattal is rendelkezik, vagy nem tagja a hivatali tartománynak.
A Hivatal számítógép-hálózatának vezeték nélküli hálózati szegmensein, valamint a nem bizalmas csatornán keresztüli bizalmas kapcsolat során titkosított adatkapcsolatot kell kialakítani.
A titkosított adatkapcsolat technikai specifikációját az Informatikai biztonsági vezető hagyja jóvá.

Hálózati adatátvitel biztonsága

A belső hálózatokon az adatforgalomban kizárólag engedélyezett protokollok használhatók.
A belső hálózaton engedélyezett protokollok körét – az üzemeltetők javaslata, továbbá a biztonsági adminisztrátorok véleménye alapján – az Informatikai biztonsági vezető határozza meg.
Az engedélyezett protokollok körének kialakításakor külön kell kezelni a felhasználók és az üzemeltetők, biztonsági üzemeltetők számára, illetve az átviteli közeg szinten és az állomás szinten engedélyezett protokollokat.
Hordozható számítógépeket, tableteket, okostelefonokat csak a rendszer-üzemeltető által elvégzett ellenőrzés után lehet a Hivatal számítógép-hálózatára kapcsolni.

A Hivatal számítógép-hálózatában a felhasználói hitelesítés adatait (felhasználó azonosító,jelszó) titkosítva kell továbbítani.

Felelősség

Az adatcsere, adattovábbítás biztonsági eljárásaival kapcsolatos feladatok megoszlanak az Informatikai biztonsági vezető, és az Informatikai biztonsági felelős között.

Adatmentés

Cél: Az elviselhetetlen mértékű adatvesztés megakadályozása, és az elvárt időn belüli adat visszaállítás biztosítása.

Információk biztonsági mentése

Minden, a Hivatal kezelésében vagy használatában lévő, elektronikus formában tárolt információról biztonsági mentéseket kell készíteni.
Olyan mentési rendet kell kialakítani, ami biztosítja az adatok visszaállíthatóságát a Hivatal által meghatározott követelmények szerint (elvárt visszaállítás idő, maximálisan elviselhető adatvesztés stb.).
A mentések gyakoriságát, a mentés módját, a használt adathordozót és a tárolási helyet a fentiek figyelembevételével kell kiválasztani, és ki kell dolgozni azokat az eljárásokat, amelyek teljesítik a követelményeket.
Az eljárások kidolgozása után az érintettek számára oktatás szükséges, és elengedhetetlen a teljes visszaállítási eljárás tesztelése is.
Ki kell dolgozni a mentések ellenőrzésének (ellenőrző visszatöltés) rendjét is (többpéldányos mentés, külső helyszínen tárolás).
A mentési, visszaállítási eljárást évente és releváns változások esetén felül kell vizsgálni, és naprakésszé kell tenni.

Mentési eljárás

Biztonsági mentéseknek kell készülnie

a) az online elérhető (éles, tartalék, teszt) adatbázisokról és fájlrendszer könyvtárakról,
b) az offline elérhető (archivált) adatbázisokról és fájlrendszer könyvtárakról,
c) szoftverek telepítőkészletéről.

Normál (Teljes-FULL): azaz minden mentési folyamattal mentésre kerül az összes állomány, függetlenül az előző mentés időpontjától és annak státuszától.
Inkrementális: azaz csak az előző mentés óta változott állományok kerülnek mentésre.
A mentéseket ütemezett feladatként, automatikusan kell elvégezni, minden hétköznap.
Az automatikus mentés elindítását munkaidőn túl kell ütemezni, hogy az alkalmazások ne legyenek használatban és ne legyenek nyitott állományok. Emiatt az automatikus mentést 22:00-ra kell ütemezni. A mentés eredményességét és futási idejét a mentés másnapján az informatikai biztonsági adminisztrátornak kell ellenőriznie. Minden rendellenességet jeleznie kell az informatikai biztonsági vezetőnek.
A mentés a Backup számítógépre való másolással történik.
A napi mentéseket úgy kell végrehajtani, hogy a fájlszerverek felhasználói könyvtárait szervezeti egységenként külön tömörített állományként kell a Backup számítógépre másolni.
Az alkalmazások mentése külön tömörített állományként történik, melyeket a Backup számítógépre kell másolni.
Az adatbázis szerverek saját mentést készítenek, melyeket szintén a Backup számítógépre kell másolni.

Archiválási eljárás

Az előző heti napi mentések közül a pénteki mentést kell archiválni hétfő reggel. Az archiválás során a pénteki mentést kifejezetten erre a célra beszerzett szalagos egységre.
Az archivált állományokat tartalmazó szalagos egységeket egyedi azonosítóval kell ellátni, és tűzálló páncélszekrényben kell tárolni. A szalagos egységekről nyilvántartást kell vezetni.
Az archiválást az Informatikai biztonsági vezető, vagy az általa kijelölt informatikai munkatárs jogosult elvégezni.
Az archivált állományokat tartalmazó szalagos egységeket évente selejtezni kell. A selejtezés során az egy éven túli archív állományokat tartalmazó szalagos egységeket meg kell semmisíteni. Az archív állományok selejtezéséről jegyzőkönyvet kell rögzíteni.

Visszatöltés mentési állományból

A visszatöltés igénylését az adott szervezeti egység vezetője írásban kezdeményezheti az Informatikai biztonsági vezetőnek címzett e-mail-ben. Az e-mail-nek tartalmaznia kell, hogy

a) melyik állomány visszatöltését igényli;
b) milyen dátumú állomány visszaállítását igényli;
c) milyen célból igényli az állomány visszaállítását

Az Informatikai biztonsági vezető megvizsgálja, hogy milyen okai vannak a visszatöltési igénynek. Ezek lehetnek:

a) adatvesztés/programhiba;
b) felhasználói hiba;
c) természeti katasztrófa.

Amennyiben adatvesztés vagy programhiba történt, az Informatikai biztonsági vezető gondoskodik a hiba elhárításáról. Katasztrófa esetén a Katasztrófatervnek megfelelően jár el.
Az Informatikai biztonsági vezetőnek meg kell vizsgálnia, hogy a visszatöltéssel nem sérülnek, illetve változnak meg az adott rendszer adatai. A visszatöltés jogosságát az Informatikai biztonsági vezető dönti el az adott rendszer adatgazdájával történt egyeztetés után. Amennyiben az ellenőrzés nem talált kizáró okot, és a visszatöltési kérelemben megadott dátumú mentés elérhető, az adott napi állományt vissza kell tölteni a kért helyre.
A sikeres visszatöltés tényét jegyzőkönyvben kell rögzíteni

Mentések általános szabályai

A mentéseket tartalmazó adathordozókra rá kell vezetni az alábbi adatokat:

a) a rendszer (alkalmazás) elnevezését,
b) a mentés jellegét,
c) a mentés példánysorszámát és azt, hogy összesen hány példány készült,
d) az adatállomány nevét,
e) az információ mentést kérő iroda megnevezését,
f) a mentés időpontját (év/hó/nap; óra:perc).

A mentések egyes példányait az alábbi helyszíneken kell tárolni:

a) az első példányt a Hivatal mindenkori elsődleges informatikai központjában, illetve abban a létesítményben, ahol a mentés visszatöltése elvégezhető;
b) a második példányt az adott rendszer tartalék központjában; annak hiányában a Hivatal egy erre kijelölt, az első példány tárolási helyétől kellő földrajzi távolságban lévő létesítményében.

A mentések adathordozóit kizárólag a Hivatal informatikai helyiségeinek valamelyikében, legalább 60 perces tűzállóságot garantáló, zárható szekrényben kell tárolni, biztosítva az adathordozó gyártója által előírt környezeti paraméterek teljesülését.
A mentési eljárásokat úgy kell kialakítani, hogy a mentések második példánya minden késedelem nélkül jusson el tárolási helyére, és a szállítás során gondoskodjanak biztonságáról.

Felelősség

A mentési és visszaállítási eljárások felelőse az Informatikai biztonsági vezető, míg annak időszakos ellenőrzése az Informatikai biztonsági felelős hatáskörébe tartozik.

Adathordozók kezelése
Cél: Biztosítani kell, hogy az adathordozók, illetve a rajtuk tárolt adatok a Hivatalból kikerülve se sérülhessenek, módosulhassanak, vagy kerülhessenek illetéktelen kezekbe.

Adathordozók kezelése

Ki kell dolgozni valamennyi adathordozó kezelésének eljárásait, kiemelt figyelmet fordítva a telephelyen kívüli védelemre. A szabályzatnak ki kell terjednie a teljes élettartamra, a nyilvántartásra, a selejtezésre, a frissítésekre, több példány készítésére. Kiemelt figyelmet kell fordítani az USB eszközökre, a memóriakártyákra, a mobiltelefonok és tabletek tárolóegységeire. Az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, jogosítványuk tartalmát az érintett adatok adatgazdái határozzák meg.
Az adathordozókat alkalmazásuk megszűnésekor a felhasználóktól be kell gyűjteni, és erről átadás-átvételi bizonylatot kell kitölteni. A még felhasználható, nem sérült adathordozókon olyan felszabadítást kell végezni, amely garantálja a tárolt adatok visszaállíthatatlanságát; ezt legalább – amennyiben lehetséges – véletlen tartalommal való felülírással, majd törléssel és formattálással lehet elérni. A törlési mechanizmusokat az információ biztonsági osztályával arányos erősségnek és sértetlenségnek megfelelően kell alkalmazni.
Az adatok törlését vagy az adathordozók selejtezését bármely felhasználó kezdeményezheti, de a művelet végrehajtását csak az adatgazda előzetes írásos jóváhagyásával lehet megkezdeni.
Az adattörlés és a selejtezés végrehajtása kettős hitelesítéshez kötött, azaz legalább két megfelelően képzett informatikus részvétele szükséges a végrehajtáshoz és ezek egyike az informatikai biztonsági vezető kell hogy legyen.

Adathordozók törlése

A rendszergazda a helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törli az elektronikus információs rendszer meghatározott adathordozóit a leselejtezés, a szervezeti ellenőrzés megszűnte, vagy újrafelhasználásra való kibocsátás előtt úgy, hogy a törlési mechanizmusokat az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően alkalmazza. A selejtezésről minden esetben jegyzőkönyvet kell felvenni. A törlésre alkalmazott eszközöket és módszerek hatékonyságát a rendszergazda szükséges gyakorisággal teszteli.

Az adathordozók selejtezésének szabálya Informatikai biztonsági eljárásrendben rögzített.

Adathordozók megsemmisítésének dokumentálása

Az adatok törlését és az adathordozók selejtezésének folyamatát egyaránt jegyzőkönyvezni kell, legalább a következő adatokkal:

- az adathordozó azonosítója,
- a törlés vagy selejtezés oka,
- a törlés vagy selejtezés módszere

- a törlést vagy selejtezést végző személy(ek) neve, és beosztása,
- a törlést vagy selejtezést jóváhagyó személy neve, és beosztása,
- selejtezett alkatrész tárolási módja (raktár, vagy megsemmisítés)
- a törlés vagy selejtezés időpontja.

A selejtezés megtörténtét az informatikai vagyontárgyak nyilvántartásában is át kell vezetni.

Felelősség

Az adathordozók kezelésével kapcsolatos feladatok végrehajtásának felelőse az Informatikai biztonsági vezető, míg annak időszakos ellenőrzése az Informatikai biztonsági felelős hatáskörébe tartozik.

Biztonsági helyzet- és eseményértékelés
Cél: Gondoskodni arról, hogy a biztonsági események és zavarok okozta kár minimális legyen, továbbá hogy a véletlen biztonsági eseményeket megfigyelés alatt tartsák, és azokból okuljanak.

Naplózás és incidenskezelés

Az ASP tenant adminisztrátornak (Ludányhalászi, Nógrádszakál, Piliny) törekednie kell a legkisebb jogosultság kiosztásához a felhasználók körében. A jogosultságok kiosztásánál javasolt figyelembe venni a szervezeti és működési szabályzatot, amely nem kerülhet ellentmondásba ezen szabályzattal.
Az ASP Központ egy esetleges biztonsági incidens során a tenant adminisztrátoroknak privilégiumokkal járó jogosultságkiosztását számon kérheti. Biztonsági audit során, ha az indokoltnál magasabb hozzáférés állapítható meg egyes felhasználók esetében, annak oka jegyzőkönyvben kell, hogy szerepeljen. Általánosságban megállapítható, hogy a jogosultságok kiosztója is felelőssé tehető a gondatlanságból bekövetkezett biztonsági események kapcsán.
Biztonsági incidensek esetén a Hivatal IBSZ-e szerint kell eljárni (dokumentálás, eljárások, ellenőrzés, utóvizsgálat stb.), azonban az önkormányzati ASP-t ért incidensek észlelését jelenteni kell az ASP Központ felé is a Kormányzati Eseménykezelő Központ mellett (utóbbi esetén az észlelés nem feltétlenül jelentkezik a Hivataloknál, de kizárni sem lehet). A jelentés nem tartalmazhat olyan szenzitív adatot (pl. személyes adatot), elemeket, amelyet harmadik fél nem ismerhet meg. Az incidens nem feltétlenül a kliens oldali eszközön jelentkezett, még ha azt az ASP rendszer felhasználója úgy véli, emiatt fontos az eszkalálás.
Ennek bejelentési felülete az ASP hibabejelentő rendszer. Az ASP Központ a bejelentéseket fogadja, továbbítja az illetékes terület felé és a jogszabály szerinti lépéseket megteszi.

A Hivatal elektronikus információs rendszereiben automatikus naplót kell vezetni az elektronikus információs rendszerek biztonsági szempontból lényeges tevékenységeiről.
A különböző naplóbejegyzésekben be kell gyűjteni elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.
Az rendszergazda egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő szervezeti egységgel, hogy növelje a kölcsönös támogatást.
Az informatikai biztonsági vezető megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.
Az automatikusan készülő naplókban (naplóbejegyzés generálás) rögzíteni kell legalább az alábbi eseményeket:

- be- és kijelentkezéseket;
- sikertelen bejelentkezési kísérleteket;
- jogosulatlan hozzáférési kísérleteket;
- jogosultság megadáskor a megadott jogosultságokat;

- az operátori konzol riasztásait és üzeneteit;
- a rendszerriasztásokat, meghibásodási jelentéseket;
- felhasználók felvételét, törlését;
- jogosultsági csoportokban beálló változásokat (új csoport létrehozása, jogosultsági csoporthoz tartozó elemi jogosultságok megváltozása, stb.);
- felhasználók jogosultságaiban beálló változásokat;
- naplózási funkciók indítását és leállítását
- naplóállomány létrehozását, törlését; (külön jegyzőkönyvben rögzítve);
- a naplózási konfigurációban beálló változást (külön jegyzőkönyvben rögzítve);
- a rendszerdátum, -idő megváltoztatását;
- hardverkonfiguráció megváltozását;
- nyilvános hálózaton keresztüli kapcsolat
  - létrehozása és bontása,
  - ellenoldali fél azonosítása,
  - forgalom jellege,
  - továbbított vagy fogadott állomány neve, elérési útvonala.

Az eseményekhez a naplózó funkciónak hozzá kell rendelnie (amennyiben értelmezhető):

- a felhasználó azonosítóját,
- a számítógép azonosítóját (IP cím),
- a dátumát és időpontját, (a rendszernek a belső rendszerórát kell használnia a naplóbejegyzések időbélyegeinek előállításához, és időbélyegeket kell rögzítenie a naplóbejegyzésekben a koordinált világidőhöz - úgynevezett UTC - vagy a Greenwichi középidőhöz - úgynevezett GMT - rendelhető módon)
- a hozzáféréskor elért állományokat,
- a használt programot.

A különböző rendszerek naplóállományainak egységes értelmezhetőségének érdekében olyan naplózási architektúrát kell kialakítani, ami biztosítja, hogy:

- ahol csak technikailag lehetséges, a naplózás szerveroldalon történjen,
- a naplózás a lehető legkevesebb számú naplóállomány használatával történjen,
- automatikus mechanizmus gondoskodjon az egyes eszközök rendszerórájának szinkronizálásáról,
- automatizált megoldások támogassák a különböző naplóállományok összefésülését, feldolgozását és elemzését.

A naplóállományokhoz írási jogosultsággal humán felhasználók nem férhetnek hozzá, a naplóállományokból a törlés nem engedélyezett.

Az egyes naplóállományokhoz, vagy azok részeihez olvasási jogosultsággal rendelkezhet (amennyiben munkaköre, feladata ellátásához arra szüksége van)

- a jegyző,

- rendszergazda,
- a belső ellenőr.

Biztosítani kell, hogy az elektronikus információs rendszer megvédje a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.
A naplóbejegyzéseket a Hivatalon belüli információ megőrzési követelményeknek megfelelő időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.
Az informatikai biztonsági vezető lehetővé teszi az adatgazdák és a Hivatal vezetői számára, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire.

Biztonsági szempontból releváns események eszkalációja

Az informatikusoknak naponta ellenőriznie kell a naplóállományok bejegyzéseit.
Incidens esemény bekövetkeztekor, vagy ennek alapos gyanúja esetén a Hivatal információrendszerének automatikusan jelentést kell generálnia és elküldenie az informatikusoknak és az üzemeltetés vezetőjének.
Az információbiztonsági szabályok megsértéséről az informatikusoknak jelentést kell tennie az üzemeltetés vezetőjének, aki:

- minősíti az incidenst a körülmények ismeretében, vagy
- eseti szakértői csoportot hoz létre az incidens körülményeinek kivizsgálására.

Az Informatikai biztonsági vezető, az incidens súlyának ismeretében dönt a következményekről, az incidens kezeléséről a hibák javításáról.
A biztonsági esemény kivizsgálásának eredményéről az üzemeltetés vezetője értesíti a Jegyzőt, aki dönt a további esetleges fegyelmi, jogi eljárásról.

Ügy és üzletmenet-folytonosság

A Hivatalnak azonosítania kell a kritikus működési folyamatokat és beépítenie a működésfolytonosságot az informatikai biztonság irányítási követelményeibe más folytonossági követelményekkel, amelyek olyan szempontokra vonatkoznak, mint műveletek, személyzettel való ellátás, anyagok, szállítás és eszközök.
Az üzemzavarok, biztonsági meghibásodások, szolgáltatás-elvesztés és szolgáltatás rendelkezésre-állási követelményeit működési hatáselemzésnek kell alávetni.
A BCP/DRP terv készítésekor alapelvként kell kezelni, hogy a Hivatal számára a megfelelő üzletmenet-folytonosság az elektronikus információs rendszer folyamatos üzemi működésének az a szintje, amely során a kiesés kockázatának szintje a szervezet számára még elviselhető. Az elviselhetőség határát az üzletmenet – támogatás szempontjából kritikus rendszereinek – egy meghatározott (maximált) kiesési ideje határozza meg.

Felelősség

A biztonsági helyzet- és eseményértékelés az Informatikai biztonsági vezető hatáskörébe tartozik.

Oktatás, képzés, tudatosítás

Cél: Folyamatosan gondoskodni arról, hogy a felhasználók tudatában legyenek az informatikai biztonság fenyegetéseinek, és motiválva legyenek a szervezet információvédelmi szabályzatainak és intézkedéseinek a betartására. A felhasználók legyenek oktatva a biztonsági eljárásokról és az adatfeldolgozó eszközök helyes használatáról a lehetséges biztonsági kockázatok minimalizálása érdekében.

Oktatás végrehajtása

A felhasználói oktatás a biztonsági elképzeléseket is figyelembe vevő Képzési Terven kell, hogy alapuljon.

A szervezet valamennyi munkatársát, és ahol szükséges, a harmadik fél felhasználóit is, megfelelő képzésben kell részesíteni a szervezet biztonsági szabályairól és eljárásairól. Ezeket az ismereteket rendszeresen, naprakész ismeretek közlésével fel kell újítani. A képzés foglalja magába a biztonsági követelményeket, a jogi felelősséget, az üzleti óvintézkedéseket, valamint az informatikai eszközök helyes használatát, például a bejelentkezési eljárást, a szoftverek használatát. Az informatikai biztonságtudatossági képzés elvégzését az elektronikus információs rendszer használója aláírásával igazolja. Aláírásként elfogadható a Hivatal belső elektronikus információs rendszerén belül érkezett egyértelmű és pontosan beazonosítható elektronikus visszajelzés is (e-mail, amennyiben kialakításra kerül, intranetes „elfogadom/tudomásul vettem" stb.)

E képzés nélkül a Hivatal elektronikus információs rendszereit használni tilos.

A képzést azelőtt kell lefolytatni, még mielőtt a felhasználók megkapnák a hozzáférési jogot (jogosultság) az elektronikus információs rendszerekhez, vagy az adatokhoz.

Az általános biztonságtudatosítási képzés mellett, melynek mindenkire vonatkoznia kell a szervezetben, különleges biztonsági képzés is szükséges az informatikai biztonsággal foglalkozó személyzet számára. A biztonsági képzés mélységének az informatikának a szervezeten belüli általános fontosságához kell igazodnia, és az adott szerep biztonsági követelményeinek megfelelően kell változnia.

A Hivatal dolgozói számára el kell készíteni egy Felhasználói Informatikai Biztonsági Kódexet, amely tartalmazza

a) a felhasználók számára lényeges informatikai biztonsági szabályok összefoglalását;
b) a Hivatal elektronikus információs rendszereinek használatával kapcsolatosan elvárt és tiltott magatartásokat, továbbá azok megsértésének szankcióit;
c) a Hivatal elektronikus információs rendszerei számára nagy kockázattal járó fenyegetések és veszélyforrások minél közérthetőbb magyarázatát, a biztonságtudatosság fokozása érdekében.

A Felhasználói Informatikai Biztonsági Kódex felülvizsgálata része az IBSZ felülvizsgálatának

Az informatikai biztonságtudatossági képzést a Humánpolitikai csoport szervezi, tematikáját és előadóját az Informatika biztosítja.

Felelősség

Az oktatás megszervezése a szervezet vezetőjének hatáskörébe tartozik az elektronikus információs rendszer biztonságáért felelős közreműködésével.

Tartalomjegyzék

Hatályba lépés

Jelen intézkedés 2018. július 1. napján lép hatályba és visszavonásig érvényes.

Ludányhalászi, 2018.

jegyző

LUDÁNYHALÁSZI KÖZÖS ÖNKORMÁNYZATI HIVATAL