Bodajk Város
Polgármestere

8053 Bodajk, Petőfi S. u. 60.
Tel.-fax: 22/410-001
E-mail: bodajkpm@t-online.hu

Ügyiratszám: Bod/4/2018.

Sorszám:180/2018.

Nyilvános ülés	☒
Zárt ülés	☐
Mötv. 46. § (2) a)	☐
Mötv. 46. § (2) b)	☐
Mötv. 46. § (2) c)	☐

Javaslat
szabályzatok jóváhagyására

Előadó:
Wurczinger Lóránt polgármester

Előkészítésben részt vett:
Nagy Csilla jegyző
Décsei Júlia ügyintéző
Hossó Anita hatósági csoportvezető
Dreska Tímea pénzügyi csoportvezető

Előzetesen tárgyalja:
Gazdasági Bizottság

egyszerű többség	☒
minősített többség	☐
Mötv. 50. §	☐
Mötv. 42. § …	☐
SzMSz 31. § (2) …	☐

Készült:
Bodajk, 2018. július 30.

Tisztelt Képviselő-testület!

Az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet határozza meg az ASP rendszerrel (a továbbiakban: ASP) kapcsolatos önkormányzati feladatokat, határidőket.
A kötelező csatlakozás kapcsán lehetőségünk volt arra, hogy a KÖFOP-1.2.1-VEKOP-16 számú Csatlakoztatási konstrukció az önkormányzati ASP rendszer országos kiterjesztéséhez című pályázat keretében a Működésfejlesztés és szabályozási keretek kialakítása alcímű forrásból az Informatikai Biztonsági Szabályzat, valamint az Iratkezelési Szabályzat felülvizsgálatát és elkészítését finanszírozzuk.
Tájékoztatom azon Tisztelt Képviselő-testületi és Bizottsági tagokat, akik részére papír alapon küldjük meg az előterjesztéseket, hogy a jelen előterjesztés mellékletét képező szabályzatok e-mailben kerülnek megküldésre, azok nagy terjedelme miatt.

Kérem a Tisztelt Képviselő-testületet, hogy a mellékelt Iratkezelési Szabályzatot, valamint a 2017. december 14-én a jegyző által kihirdetett Informatikai Biztonsági Szabályzatot megtárgyalni és elfogadni szíveskedjen.

Wurczinger Lóránt s. k.
polgármester

Határozati javaslat

szabályzatok jóváhagyásáról

A képviselő-testület a KÖFOP-1.2.1-VEKOP-16 számú Csatlakoztatási konstrukció az önkormányzati ASP rendszer országos kiterjesztéséhez című pályázat keretében elkészült:
- Informatikai Biztonsági Szabályzatot a melléklet szerinti tartalommal jóváhagyja,
- Iratkezelési Szabályzatot a melléklet szerinti tartalommal elfogadja.

A képviselő-testület felkéri a polgármestert, hogy a szabályzatokban foglaltak betartása érdekében szükséges intézkedéseket tegye meg.

Felelős: Wurczinger Lóránt polgármester
Határidő: folyamatos

Bodajki Polgármesteri Hivatal

B07 Informatikai Biztonsági Szabályzat (IBSZ)

Bodajk Város Önkormányzat jegyzője

1/2017. (XII. 14.) utasítása a Bodajki Polgármesteri Hivatal

informatikai biztonsági szabályzatáról

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Hatályos: 2017. december 14-étől

BODAJK VÁROS JEGYZŐJE

Nagy Csilla
jegyző

Tartalom

1. ÁLTALÁNOS RENDELKEZÉSEK 7
1.1. A Szabályozás célja 7
1.2. A Szabályozás hatálya 7
1.2.1. Az IBSZ személyi hatálya 7
1.2.2. Az IBSZ tárgyi hatálya 7
1.2.3. Az IBSZ időbeli hatálya 8
1.3. Az IBSZ alapelvei 8
1.4. Szerepkörök, tevékenységek, felelősségek 10
1.4.1. A hivatal vezetője 10
1.4.2. Az elektronikus információs rendszerek biztonságáért felelős személy 11
1.4.3. Üzemeltető, informatikus/rendszergazda 12
1.4.4. Honlaptartalom kezelő 12
1.4.5. Felhasználó 12
1.5. A vezetőség elkötelezettsége, a pénzügyi erőforrások biztosítása 13
1.6. Az IBSZ jogi háttere 13
2. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK 14
2.1. Információbiztonsági politika 14
2.2. Információbiztonsági stratégia 14
2.3. Az elektronikus információs rendszerek nyilvántartása 14
2.3.1. Elektronikus információs rendszerelem leltár 15
2.4. Biztonsági osztályba sorolás 15
2.5. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás 15
2.6. Biztonságtervezési eljárásrend 16
2.7. Rendszerbiztonsági terv 16
2.8. Személyi biztonság 17
2.9. Rendszer és szolgáltatás beszerzés 17
2.9.1. Beszerzési eljárásrend 17
2.9.2. A rendszer fejlesztési életciklusa 17
2.10. Biztonságelemzési eljárásrend 18
2.11. Tesztelés, felügyelet 18
2.12. Biztonsági eseménykezelési eljárásrend 19

3. ADATOK ÉS IT RENDSZEREK VÉDELME, BIZTONSÁGA 20
3.1. Fizikai védelmi intézkedések 20
3.1.1. Fizikai védelmi eljárásrend 20
3.1.2. Fizikai belépés ellenőrzése, belépési engedélyek 21
3.2. Hivatali és személyzeti szabályok 23
3.2.1. Felvételi eljárás során követendő szabályok, személyes követelmények 23
3.2.2. Képzési eljárásrend 23
3.2.3. Biztonság tudatosság képzés 24
3.2.4. Fegyelmi intézkedések 24
3.2.5. Eljárás a jogviszony megszűnésekor 26
3.3. Azonosítás és hitelesítés 26
3.3.1. Azonosítási és hitelesítési eljárásrend 26
3.3.2. Azonosításra, hitelesítésre szolgáló eszközök kezelése 27
3.3.3. hivatalon kívüli felhasználók azonosítása és hitelesítése 29
3.4. Hozzáférés védelem, jogosultság kezelés 29
3.4.1. Hozzáférés ellenőrzési eljárásrend 29
3.4.2. Felhasználói fiókok kezelése 30
3.4.3. Külső rendszerekből történő hozzáférés szabályozása 31
3.4.4. Azonosítás és hitelesítés nélkül engedélyezett tevékenységek 32
3.4.5. Nyilvánosan elérhető tartalom 32
3.4.6. Rendszerhasználat jelzése 32
3.5. Viselkedési szabályok az interneten 33
3.5.1. Elektronikus levelezés (e-mail) 34
4. AZ INFORMATIKAI RENDSZEREK ÜZEMELTETÉSE 36
4.1. Általános rendelkezések 36
4.2. Konfigurációkezelés 37
4.2.1. Konfigurációkezelési eljárásrend 37
4.2.2. Alapkonfiguráció 38
4.2.3. konfigurációváltozások felügyelete (változáskezelés) 38
4.3. Szoftverhasználat korlátozásai 38
4.3.1. Felhasználó által telepíthető szoftverek 39
4.4. Adathordozók védelme 39

4.4.1. Adathordozók védelmére vonatkozó eljárásrend 39
4.4.2. Adathordozók használata, hozzáférés az adathordozókhoz 40
4.4.3. Adathordozók újrafelhasználása, leselejtezése, megsemmisítése 40
4.5. Felkészülés a rendkívüli helyzetekre, katasztrófákra 41
4.6. Az elektronikus információs rendszer mentései 41
4.6.1. A felhasználók adatainak mentése 42
4.6.2. A szervereken tárolt adatok mentése 43
4.7. Az elektronikus információs rendszer helyreállítása és újraindítása 43
4.8. Karbantartás 43
4.8.1. Rendszer karbantartási eljárásrend 43
4.8.2. Rendszeres karbantartás 43
5. RENDSZER- ÉS INFORMÁCIÓ SÉRTETLENSÉG 44
5.1. Rendszer- és információsértetlenségre vonatkozó eljárásrend 44
5.2. Felügyelet 44
5.2.1. Felügyeleti eszközök 45
5.2.2. Biztonsági riasztások és tájékoztatások 45
5.3. Incidensek kezelése 45
5.3.1. Tanulás az incidensekből 46
5.4. Naplózás 46
5.4.1. Naplózható események 47
5.4.2. Naplóinformációk védelme 47
5.4.3. Napló tárkapacitás 47
5.4.4. Naplózási hiba kezelése 47
5.4.5. Naplóvizsgálat és jelentéskészítés 47
5.5. Kártékony kódok elleni védelem 48
5.6. Hibajavítás, biztonsági frissítések 49
6. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM 49
6.1. Rendszer- és kommunikációvédelmi eljárásrend 49
6.2. Határok védelme 49
6.3. Kriptográfiai kulcsok előállítása és kezelése 50
6.4. Hitelesítés szolgáltatók tanúsítványának elfogadása 50
6.5. Biztonságos név/cím feloldó szolgáltatások 50

6.6. Túlterheléses (szolgáltatás megtagadás alapú) támadás elleni védelem 51
6.7. Záró rendelkezések 51
7. MELLÉKLETEK 52
IBSZ 1. számú melléklet - Biztonsági osztályba sorolás 52

1. ÁLTALÁNOS RENDELKEZÉSEK

1.1. A Szabályozás célja

Bodajki Polgármesteri Hivatal (a továbbiakban: hivatal) Informatikai Biztonsági Szabályzatának (a továbbiakban: IBSZ) célja, hogy a vonatkozó jogszabályokkal (2013. évi L. törvény, 41/2015. (VII. 15.) BM rendelet, 257/2016. (VIII. 31.) Korm. rendelet, 679/2016. EU rendelet) és a hivatal belső rendelkezéseivel összhangban meghatározza a hivatal informatikai rendszerei által kezelt információvagyon bizalmassága, hitelessége, sértetlensége, valamint rendelkezésre állásának biztosítása, funkcionalitása és üzembiztonsága megőrzése érdekében betartandó elveket. Az IBSZ meghatározza az informatikai vezető és az információbiztonságért felelős személy feladatait, valamint az információs rendszer működtetői és felhasználói számára kötelező szabályokat. Az IBSZ kiemelt célja, hogy a hivatal informatikai rendszereinek zavartalan működése biztosítva legyen.

Jelen szabályzat a fentiek keretében védelmi eljárásokat határoz meg, intézkedési jogosultságot állapít meg, valamint ellenőrzési mechanizmusokat állít fel a szabálytalanságok felderítésére és a felelősség megállapítására.

1.2. A Szabályozás hatálya

1.2.1. Az IBSZ személyi hatálya

Az IBSZ személyi hatálya a hivatal valamennyi teljes- vagy részmunkaidős, valamint szerződéses dolgozójára kiterjed. Az IBSZ hatálya kiterjed a hivatal informatikai rendszerének üzemeltetésében és karbantartásában résztvevő cégekre, vállalkozókra, illetve magánszemélyekre (a továbbiakban: Szerződéses partnerek) *(B01 Szerződéses partnerek listája)* Az érintettekkel az IBSZ megfelelő pontjait ismertetni kell *(B03 IT felhasználói szabályzat)*, továbbá nyilatkozniuk kell az IBSZ rájuk vonatkozó előírásainak elfogadásáról és betartásáról az előírások szerinti munkavégzésükhöz *(B02 Nyilatkozat az IT biztonsági szabályok elfogadásáról)*.

Az IBSZ hatálya kiterjed minden olyan magánszemélyre, illetve gazdasági szervezetre, aki/ami munkavégzése kapcsán bármilyen informatikai eszközzel a hivatal informatikai infrastruktúrájához csatlakozik, illetve azt igénybe veszi. A csatlakozás kizárólag hivatali érdekből történhet.

1.2.2. Az IBSZ tárgyi hatálya

Az IBSZ tárgyi hatálya kiterjed:

- a védelmet élvező adatok teljes körére, felmerülési és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül;
- a hivatal tulajdonában lévő, illetve az általa bérelt, vagy használt valamennyi informatikai berendezésre (számítógépekre, azok tartozékaira és perifériáira);
- a különböző adathordozókra;
- a hivatal számítógépes hálózatára és annak elemeire;
- a számítógépes hálózathoz való kapcsolódást biztosító eszközökhöz tartozó modemekre (szolgáltatói modem, mobil stickek), hálózati útválasztókra (routerek), aktív elemekre és egyéb

olyan speciális eszközökre, melyek az informatikai eszközökhöz, illetve a hálózathoz illeszthetők (pl. switch, hub, pendrive, mobil adattároló, mobiltelefon, digitális fényképezőgép stb.);
- az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, üzemeltetési stb.);
- a rendszer- és felhasználói programokra;
- az adatok felhasználására vonatkozó utasításokra;
- az adathordozók tárolására és felhasználására;
- tulajdonviszonytól függetlenül (tulajdonolt, bérelt stb.) a hivatal területén (állandóan vagy ideiglenes jelleggel) telepített informatikai eszközökre, az azokkal kapcsolatos tevékenységre.

Az IBSZ a tárgyi hatálya alá tartozó elemek teljes életciklusára kiterjed, amely az alábbi szakaszokból áll:
- tervezési szakasz: a rendszer iránti igény, a rendszer célja és a vele szemben támasztott követelményeknek a leírása;
- fejlesztési/beszerzési szakasz: a rendszer fejlesztése, programozása, létrehozása, beszerzése;
- megvalósítási szakasz: a rendszer tesztelése, telepítése, testre szabása;
- üzemeltetés/karbantartás: a rendszer üzemelése, üzemeltetése, hardver- és szoftver-módosítások, karbantartás, események kezelése;
- visszavonás/selejtezés/megsemmisítés szakasz: információk, hardver és szoftver visszavonása az üzemelésből, törlése, megsemmisítése és hosszabb távú megőrzésre való felkészítése.

1.2.3. Az IBSZ időbeli hatálya

Az IBSz-t évente vagy jelentősebb infrastrukturális változás, illetve jogszabályváltozás esetén felül kell vizsgálni és szükség esetén módosítani szükséges, mind hivatali, mind informatikai szakmai szempontok szerint.

1.3. Az IBSZ alapelvei

A hivatal informatikai rendszereiben biztosítani kell informatikai és nem informatikai eszközök és módszerek kombinációjával az érzékeny adatok adatbiztonságát és az ilyen adatokat tároló, feldolgozó, továbbító rendszerek üzembiztonságát. Az egyes rendszerek tervezése és megvalósítása során – *a rendszerben kezelt adatok biztonsági osztályba sorolásának megfelelően* – kell a konkrét IT biztonsági ellenintézkedéseket meghatározni.

A bizalmasság biztosítása lehetővé teszi, hogy az információ a jogosulatlan informatikai egyedek (személyek, csoportok, programok, folyamatok stb.) számára ne legyen elérhető, ne kerüljön nyilvánosságra. Érvényesülnie kell a hivatal és szervezetei által kezelt, felhasznált adatokhoz való hozzáférés tekintetében, elsősorban a szervereken és a felhasználói munkaállomásokon történő adathozzáférések és az adatkezeléseknél felhasznált adathordozók tekintetében, valamint a kommunikáció során.

Az egyedi elszámoltathatóságot a hivatali rendszerekben a felhasználókat egyértelműen azonosító és hitelesítő mechanizmusok megvalósításával és az egyes rendszerekben naplózandó események, a naplórekordok tartalmának meghatározásával és rögzítésével kell biztosítani, amennyiben az adott alrendszer technikailag ezt lehetővé teszi. A naplókat védeni kell a jogosulatlan hozzáférés, módosítás és törlés ellen.

Az információ és a rendszerek rendelkezésre állása érdekében a hivatali rendszerekben biztosítani kell a tárhelyek sértetlenségét, azonosítani kell a rendszerkomponenseket és rendszerkapcsolatokat. Eljárások és mechanizmusok akadályozzák meg a kártékony kódok rendszerbe jutását és az ottani károkozást. Mentési eljárásokat kell kidolgozni az adatokra, dokumentumtárakra, szoftverekre. Az eljárásokat tesztelni, dokumentálni kell. A mentéseknél a rendelkezésre állás biztosításán kívül a bizalmasság és sértetlenség követelményeit is biztosítani kell. Olyan alapszoftvereket és alkalmazásokat kell használni a hivatali rendszerekben, amelyek biztosítják, hogy a rendszer működésének megszakadása után minimális veszteséggel álljon vissza biztonságos állapotba.

A dokumentáltság elve érvényre juttatása érdekében a rendszerek adminisztrátorai számára a biztonságos konfiguráláshoz, használathoz szükséges ismereteket (telepítési, üzemeltetési leírások) tartalmazó telepítési- és használati leírást kell rendelkezésre bocsátani. Felhasználói leírást kell biztosítani az átlagos/általános felhasználó számára. A leírásokat hivatali fejlesztési erőforrások alkalmazása esetén az adott rendszer fejlesztését, kialakítását végző hivatali egységnek kell elkészíteni. Külső fejlesztő közreműködése esetén a fejlesztést végző külső munkatárs készíti el, együttműködve a fejlesztésért felelős hivatali egységgel.

A hitelesség biztosítása érdekében – ahol a hitelesség egy entitás (IT rendszeren belül elkülöníthető tulajdonsággal bíró személy, program, folyamat, adat stb.) olyan tulajdonsága, amely egy vagy több hozzá kapcsolódó tulajdonságot más egyed számára bizonyíthatóvá tesz - a hivatal belső kapcsolataiban a kommunikáló felek, hivatali egységek kölcsönösen és kétségtelenül ismerjék fel egymást és ez az állapot a kapcsolat egész idejére változatlanul fenntartható legyen.

A szükséges és elégséges ismeret elve alapján a rendszer minden felhasználónak biztosítja azokat – de csak azokat – az információkat és funkciókat, amelyek az adott felhasználó feladatainak ellátáshoz szükségesek. A hivatali rendszerekben a felhasználó csak azonosítás és hitelesítés után férhet hozzá a rendszerszolgáltatásokhoz.

Az információtartalom sértetlenségét biztosítani kell a hivatal rendszereiben az adattárolás, kezelés és továbbítás folyamán, azaz adatokat, dokumentumokat, programokat, hardvert és szoftvereszközöket, és ezek konfigurációit csak az arra jogosultak kezelhetik. Ezen elemek észrevétlenül nem módosulhatnak, törlődhetnek. Biztosítani kell, hogy a jogosultak a pontos és helyes információkat dolgozzák fel tevékenységük során.

Folyamatos ellenőrzés biztosítása

Az érintett hivatal folyamatba épített ellenőrzést vagy ellenőrzési tervet hajt végre, amely tartalmazza:

- az ellenőrizendő területeket;
- az ellenőrzések, valamint az ellenőrzéseket támogató értékelések gyakoriságát;
- az érintett hivatal ellenőrzési stratégiájához illeszkedő folyamatos biztonsági értékeléseket;
- a mérőszámok megfelelőségét;
- az értékelések és az ellenőrzések által generált biztonsággal kapcsolatos adatok összehasonlító elemzését;
- az érintett hivatal reagálását a biztonsággal kapcsolatos adatok elemzésének eredményére;
- az érintett hivatal döntését arról, hogy milyen gyakorisággal kell az elemzési adatokat az általa meghatározott személyi- és szerepkörökkel megismertetni (ideértve azok változásait is).

A rendszer életciklus szakaszaiba épített biztonság elvének teljesítése céljából a rendszer teljes életciklusában érvényesülnie kell az információbiztonsági szempontoknak.

A feladatok elkülönítése elvének teljesítése érdekében a szerepkörök kialakítása során a feladatokat úgy kell szétosztani az érintettek között, hogy ne egyetlen személy kezében összpontosuljon a hivatal informatikai rendszereinek adminisztrálása és biztonsági ellenőrzése.

A hivatal elektronikus információs rendszerének kapcsolódása szempontjából szabályozza és belső engedélyhez köti az elektronikus információs rendszerének kapcsolódását más elektronikus információs rendszerekhez, dokumentálja az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.

A hivatal elektronikus információs rendszerének kapcsolódása szempontjából belső engedélyhez köti az elektronikus információs rendszereinek összekapcsolását.

A hivatal külső elektronikus információs rendszerekhez való kapcsolódásokhoz az IBSZ-ben szabályrendszert állít fel és alkalmaz, amelynek eredménye lehet az összes kapcsolat engedélyezése vagy tiltása, meghatározott kapcsolatok engedélyezése, meghatározott kapcsolatok tiltása.

A hivatal cselekvési tervet készít, ebben mérföldköveket és felelősöket határoz meg. A kockázatkezelési stratégia és a kockázatokra adott választevékenységek prioritása alapján meghatározott időnként felülvizsgálja és karbantartja a cselekvési tervet. Ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni a hiányosság megszüntetése érdekében. Ha a meghatározott biztonsági szint alacsonyabb, mint az érintett hivatalra érvényes szint, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni az előírt biztonsági szint elérése érdekében.

Előzetes tesztelés és megerősítés

A hivatal kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét. A konfiguráció megváltoztatása előtt az új verziót tesztelni kell, ezután dönteni kell annak megfelelőségéről, továbbá dokumentálni kell az elektronikus információs rendszer változtatásait az éles rendszerben történő megvalósítása előtt.

A hivatal megvizsgálja az elektronikus információs rendszerben tervezett változtatásoknak az információbiztonságra való hatását még a változtatások megvalósítása előtt.

1.4. Szerepkörök, tevékenységek, felelősségek

Az informatikai biztonsággal kapcsolatos feladatok szerepkörökhöz rendeltek. A szerepkörök szerinti felelősök kijelölése elsősorban a munkaköri leírásokban történik. Az informatikai infrastruktúra biztonságos működtetésében, illetve az informatikai rendszerekben kezelt adatok védelmének tárgykörében a következő szerepkörök kerülnek meghatározásra:

1.4.1. A hivatal vezetője

A hivatal vezetője a Jegyző (továbbiakban: a hivatal vezetője). Felelős az informatikai rendszerben tárolt adatok védelméért és az adatok biztonságáért. Hatáskörében jogosult a számítógépes adatvédelem és az adatbiztonság megszervezésére és ellenőrzésére.

Feladatai:

- Az irányadó biztonsági osztály tekintetében biztosítja a jogszabályban meghatározott követelmények teljesülését a hivatalra és információs rendszerre vonatkozóan is.
- Biztonságért felelős személyt nevez ki *(B04 IT Biztonsági Felelős megbízása)*, erről a hatóságok felé tájékoztatást nyújt (*NEIH_REG_1465381745324.frm.enyk*)
- Meghatározza a hivatal elektronikus információs rendszereinek felhasználóira vonatkozó szabályokat *(B07 IBSZ)*.
- Meghatározza a hivatal elektronikus információs rendszerei védelmének felelőseire, feladataira, és az ehhez szükséges hatáskörre vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot *(B07 IBSZ)*.
- Gondoskodik az oktatásról, az információbiztonsági ismeretek szinten tartásáról *(B08 IT biztonsági oktatási terv és napló)*.
- Kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik a megfelelésről *(B09 IT kockázatértékelés)*.
- Gondoskodik az események nyomon követhetőségéről *(B10 IT biztonsági események naplója)*.
- Biztonsági esemény bekövetkezésekor gondoskodik a gyors és hatékony reagálásról, ezt követően a biztonsági esemény kezeléséről, az érintettek haladéktalan tájékoztatásáról *(B10 IT biztonsági események naplója)*.
- Ha külsős erőforrást vesz igénybe, akkor szerződéses kötelemként gondoskodik a törvényben foglaltak teljesüléséről. A hivatal vezetője ebben az esetben is felelős a meghatározott feladatokért, kivéve, ha jogszabály által kijelölt központosított szolgáltatót kell igénybe venni. Ebben az esetben a szolgáltató felett felügyeletet gyakorló miniszter a felelős.
- Megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.
- A hatóságok felé az ellenőrzés lefolytatásához szükséges feltételeket biztosítja.

1.4.2. Az elektronikus információs rendszerek biztonságáért felelős személy

Az elektronikus információs rendszerek biztonságáért felelős személyt (továbbiakban: IBF) a hivatal vezetője nevezi ki *(B04 IT Biztonsági Felelős megbízása)*. Az IBF felel a hivatalnál előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:

- A hivatal vezetőjének közvetlen adhat tájékoztatást, jelentést.
- Gondoskodik a hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról.
- Elvégzi vagy irányítja a fenti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését.
- Előkészíti a hivatal elektronikus információs rendszereire vonatkozó IBSZ-t.
- Meghatározza a rendszerek biztonsági beállításaival kapcsolatos elvárásokat, jogokat, feladatokat.
- Véleményezi az elektronikus információs rendszerek biztonsága szempontjából a hivatal ezen tárgykört érintő szabályzatait és szerződéseit.
- Biztosítja a 2013. évi L. törvény és a 41/2015. (VII. 15.) BM rendelet szerinti követelmények teljesülését.

Az elektronikus információs rendszer biztonságáért felelős személy a 2013. évi L. törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről köteles tájékoztatni a hivatal vezetőjét és a jogszabályban meghatározott szervet.

Az elektronikus információs rendszer biztonságáért felelős személy a hivatal vezetőjének támogatásával biztosítja az e szabályzatban meghatározott követelmények teljesülését. A hivatal valamennyi elektronikus információs rendszerének a tervezésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében közreműködik.

Ha a hivatal az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, akkor az elektronikus információs rendszer biztonságáért felelős személy jogosult a közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatokat, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.

Az elektronikus információs rendszer biztonságáért felelős személy e szabályzat szerinti feladatai és felelőssége más személyre át nem ruházható.

1.4.3. Üzemeltető, informatikus/rendszergazda

Feladata az informatikai infrastruktúra üzemeltetése, fejlesztése és biztonságos működésének elősegítése.

Felelős

- a szerverek és a rajtuk futó alapszoftverek, operációs rendszerek, szolgáltatások, adatbáziskezelők, fájl- és nyomtatószerverek működtetéséért;
- a hivatal mentési rendjében foglaltak szerint az adatmentések elvégzéséért, a mentett adatok biztonságos tárolásáért, a szükséges visszaállításokért;
- a standard felhasználói alkalmazáskörnyezet és az általa nyújtott szolgáltatások és segédalkalmazások, továbbá a ráépülő általános irodai alkalmazások komponensei, továbbá a hivatal felhasználói környezetében már megszokott általános alkalmazások és felhasználói segédprogramok, valamint a hálózati nyomtatók működtetéséért;
- az aktív és passzív hálózati eszközök működtetéséért, rendelkezésre állásáért;
- az adatbázisban tárolt adatok és szoftverek rendelkezésre állásáért, a hozzáférők adminisztrálásért.

1.4.4. Honlaptartalom kezelő

A hivatal honlapjának tartalomkezelését a hivatal ügyintézői végzik.

A jogszabály által előírt kötelezően nyilvános közadatokat az ügyintéző közvetlenül módosítja a honlapon a változásnak megfelelően.

1.4.5. Felhasználó

A hivatali rendszerek nem üzemeltető felhasználója.

- Ismernie kell az IBSZ-ben szereplő előírásokat, illetve azokat maradéktalanul be kell tartania.

- Rendelkeznie kell az általa használt berendezésekre és szoftverekre vonatkozó előírásokkal, valamit ismernie kell azok tartalmát.
- Tevékenysége megkezdésekor ellenőriznie kell, hogy az általa használt eszközök üzemképesek-e és azok beállítása az előírásoknak megfelelő-e.
- Köteles figyelemmel kísérni az általa használt berendezések és szoftverek állapotát és az esetleges meghibásodást vagy helytelen működést azonnal jeleznie kell a közvetlen vezetőnek.
- Munkája során figyelnie kell arra, hogy illetéktelen személyek lehetőleg ne tartózkodjanak az adat/információ feldolgozása során a helyiségben.
- Tevékenysége befejezésekor a használt programokból szabályszerűen ki kell lépjen.
- Hálózati információ igénybevételét követően a hálózatból szabályosan ki kell lépjen.
- A berendezéseket szükség esetén az előírásoknak megfelelően le kell állítania, illetve az áramellátásukat meg kell szüntetnie.
- A helyiségből utolsóként való távozáskor meg kell győződnie a helyiség biztonságos lezárásáról.

1.5. A vezetőség elkötelezettsége, a pénzügyi erőforrások biztosítása

A hivatal vezetősége elkötelezett az információbiztonság menedzselése iránt. Ennek megfelelően:

- Az információbiztonság ügyének szükséges mértékű publicitást biztosít a hivatal keretein belül, valamint gondoskodik a munkatársak megfelelő felvilágosításáról, tájékoztatásáról, oktatásáról;
- A szükséges anyagi-, humán- és technikai erőforrásokat biztosítja;
- A beruházások, beszerzések során tervezi az információbiztonsági stratégia megvalósításához szükséges forrásokat, dokumentálja e követelmény alá eső kivételeket.
- Az információbiztonság irányítására felelőst delegál és ruház fel a szükséges jogokkal;
- Gondoskodik a biztonsági dokumentációkban található előírások betartásáról, auditot folytathat le (*B11 IT Biztonsági auditjelentés*) és be nem tartás esetére szankciókat határoz meg, illetve foganatosít a köztisztviselőkre vonatkozó törvények (2011. évi CXCIX. törvény, 31/2012 (III. 7.) Korm. rendelet) szerint;
- Támogatja a rendszer használóinak az információbiztonságot fejlesztő törekvéseit.

Mivel a hivatali információvagyon biztonsága nem kizárólag az annak kezelésével megbízott személyek feladata és felelőssége, ezért a vezetőség elvárja, hogy a hivatal minden dolgozója és szerződéses partnere sajátjának tekintse az információ biztonságának ügyét, és azt külön utasítás nélkül támogassa feladatán és hatáskörén belül.

1.6. Az IBSZ jogi háttere

- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 41/2015. számú BM rendelet
- az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet
- általános adatvédelemről szóló 679/2016. EU rendelet (GDPR)

- az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról szóló 466/2017. (XII. 28.) Korm. rendelet

2. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

2.1. Információbiztonsági politika

A hivatal megfogalmazza és kihirdeti az információbiztonsági politikát (a továbbiakban: IBP) *(B06 Információbiztonsági Politika)*, melyben meghatározza a kiberbiztonsági célokat, kifejti az alkalmazott biztonsági alapelveket és megfelelőségi követelményeket, valamint bemutatja a vezető beosztású tagjainak elkötelezettségét a biztonsági feladatok irányítása és támogatása iránt.

Az IBP felülvizsgálata és esetleges frissítése évente vagy az elektronikus információs rendszert érintő változások, illetve jogszabályváltozás esetén esedékes.
Felelős: a hivatal vezetője

2.2. Információbiztonsági stratégia

A hivatal megfogalmazza és kihirdeti az információbiztonsági stratégiát (a továbbiakban: IBS), *(B05 Információbiztonsági Stratégia)* amely meghatározza a biztonságpolitikai célok megvalósításának módszerét, eszközrendszerét, ütemezését. Az IBS illeszkedik a hivatal más stratégiáihoz, így különösen a költségvetési és humánerőforrás tervezéshez, fejlesztéshez, jövőképhez, illetve a működtetett minőségirányítási, vagy információbiztonság-irányítási rendszerekhez.

Az IBS felülvizsgálata és esetleges frissítése évente, vagy az elektronikus információs rendszert érintő változások esetén, illetve jogszabály változás esetén esedékes.
Felelős: a hivatal vezetője

2.3. Az elektronikus információs rendszerek nyilvántartása

A hivatal az elektronikus információs rendszereiről nyilvántartást vezet *(B12 IT leltár)*. A nyilvántartást elektronikus formában vezeti és gondoskodik annak naprakészségéről.

A nyilvántartásnak minden rendszerre nézve tartalmaznia kell:

- annak alapfeladatait;
- a rendszerek által biztosítandó szolgáltatásokat;
- az érintett rendszerekhez tartozó licenc számot (amennyiben azok a hivatal kezelésében vannak);
- a rendszer felett felügyeletet gyakorló személy azonosító- és elérhetőségi adatait;
- a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító- és elérhetőségi adatait, valamint ezen hivatalok rendszer tekintetében illetékes kapcsolattartó személyeinek azonosító- és elérhetőségi adatait.

A különböző adatokat nem szükségszerűen egy nyilvántartásban kell tárolni, hanem logikus módon szétválaszthatók. Az adatok feltöltéséről mindig az adott rendszerrel kapcsolatos feladatot elvégző informatikus gondoskodik.

Minden rendszereszközt a beszerzéssel egyidejűleg fel kell venni a nyilvántartásba. A nyilvántartásból rendszereszközt kivenni csak annak selejtezésekor lehet.

2.3.1. Elektronikus információs rendszerelem leltár

A hivatal az elektronikus információs rendszerének elemeiről elektronikus formában vezetett nyilvántartást vezet, mely az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmazza. Rendszeres felülvizsgálatokkal gondoskodni kell arról, hogy a nyilvántartás mindig naprakész legyen, pontosan tükrözze az elektronikus információs rendszer aktuális állapotát. *(B12 IT leltár)*
Felelős: rendszergazda

2.4. Biztonsági osztályba sorolás

Adatbiztonság szempontjából a hivatal kezelésében lévő elektronikus formában tárolt információkat, eszközöket, erőforrásokat és szolgáltatásokat a kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából 1-től 5-ig terjedő skálán – a kockázat növekedésével arányosan növekvő - biztonsági osztályokba kell sorolni. A besorolás eredményét melléklet formában rögzíteni kell a szabályzatban is. *(B12 IT leltár)*

A besorolást minimum kétévente, de minden, az elektronikus információs rendszereket érintő változás után, illetve jogszabályváltozás esetén felül kell vizsgálni és szükség esetén ismételten el kell végezni.

2.5. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

Az új belépő munkatársak a belépéskori oktatás *(B08 IT biztonsági oktatási terv és napló)* és a titoktartási nyilatkozat *(B14 Titoktartási nyilatkozat)* aláírása után kaphatnak hozzáférést a rendszerekhez. A belépő munkatárs új hozzáférési jogkörét, illetve nem új belépő munkatárs hozzáférési jogkör változtatását a felettes vezetője határozza meg.

A meghatározás során a csoportvezető a *B15 Hozzáférések igénylése és letiltása* formanyomtatványon összegzi az általa szükségesnek tartott hozzáféréseket és azokat jóváhagyatja a hivatal vezetőjével. Amennyiben a hivatal vezetője nem járul hozzá a kért jogosultságok kiadásához, úgy az ahhoz való hozzáférést megtilthatja, de ezen döntését indokolnia kell az igénylő felé, aki az IBF döntését kérheti a jogosultság kiadásának kérdésében.

A jóváhagyott formanyomtatványt az igénylő vezető továbbítja az érintett rendszer adminisztrátora felé, akinek felelőssége, hogy csak a jóváhagyott jogosultságokat állítsa be. A rendszergazdának tilos az engedélyben nem szereplő jogosultságot beállítani. A beállítások megfelelőségét az IBF szúrópróbaszerűen ellenőrizheti.

Amennyiben az információbiztonsági szabályozásban, feladat- vagy felelősségi köröket érintő változások következnek be, úgy a változtatásokat vezetői jóváhagyás után át kell vezetni a munkaköri leírásokba és azokat aláírással érvényesíttetni az érintettekkel. Amennyiben a módosított munkaköri leírásokkal kapcsolatban az érintett munkavállalóknak észrevétele van, azt az IBF felé tehetik meg.

Amennyiben a változások vállalkozói szerződéseket érintenek, úgy a hivatal vezetése kezdeményezi az érintett vállalkozói szerződések módosítását, illetve kiegészítését a biztonsági követelményeknek megfelelően és menedzseli a szerződések módosítását és azok aláírással történő érvényesítését.

Új munkakörök kialakítása során a hivatal vezetője tájékoztatja az IBF-et a munkakör feladatairól és tervezett jogosultságairól. Az IBF javaslattal élhet a munkakör feladatainak biztonsági vonatkozásait illetően.

2.6. Biztonságtervezési eljárásrend

A hivatal szükség esetén...

- megfogalmazza, a hivatalra érvényes követelmények szerint dokumentálja, és a munka- és feladatkörük miatt érintettek számára kihirdeti a biztonságtervezési eljárásrendet mely a biztonságtervezési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
- a biztonságtervezési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a biztonságtervezési eljárásrendet.

Biztonságtervezési szempontból a hivatal az alábbi időszakokat definiálja az információs rendszerek életciklusának tekintetében:

- követelmény meghatározás;
- fejlesztés vagy beszerzés;
- megvalósítás vagy értékelés;
- üzemeltetés és fenntartás;
- kivonás (archiválás, megsemmisítés).

A rendszerbiztonság tervezésekor a hivatal az információs rendszerek valamennyi életciklusára vonatkozóan szem előtt tartja a *B06 Információbiztonsági Politiká*ban megfogalmazott célokat és követelményeket, valamint a gyártói és iparági előírásokat, ajánlásokat.

2.7. Rendszerbiztonsági terv

A hivatal az elektronikus információs rendszeréhez rendszerbiztonsági tervet készít *(B17 Rendszerbiztonsági terv)*, amely...

- összhangban áll hivatali felépítésével vagy hivatali szintű architektúrájával;
- meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait (biztosítandó szolgáltatásait), biztonságkritikus elemeit és alapfunkcióit;
- meghatározza az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát;
- meghatározza az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;
- a vonatkozó rendszerdokumentáció keretébe foglalja az elektronikus információs rendszer biztonsági követelményeit;
- meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedés bővítéseket, végrehajtja a jogszabály szerinti biztonsági feladatokat;
- gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is);

- belső szabályozásában, vagy a rendszerbiztonsági tervben meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszer rendszerbiztonsági tervét;
- frissíti a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások, és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;
- elvégzi a szükséges belső egyeztetéseket;
- gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

Ha egy adott információs rendszer jelentősége nem indokolja, illetve a jogi-, szabályozási- és üzemeltetési körülmények nem teszik lehetővé, a hivatal vezetője az IBF egyetértésével eltekinthet az adott rendszerre vonatkozó rendszerbiztonsági terv készítésétől.

2.8. Személyi biztonság

A hozzáférési jogosultságot igénylő felhasználóval szembeni elvárásokat, a rá vonatkozó szabályokat, felelősségeket, az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységeket jelen dokumentum, valamint az adott rendszerdokumentáció tartalmazza. A hozzáférés engedélyezése előtt a hozzáférési jogosultságot igénylő személynek írásbeli nyilatkozatot (*B02 Nyilatkozat az IT biztonsági szabályok elfogadásáról*) kell tennie arról, hogy az érintett rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja.

2.9. Rendszer és szolgáltatás beszerzés

2.9.1. Beszerzési eljárásrend

A hivatal...

- megfogalmazza és a hivatalra érvényes követelmények szerint dokumentálja, valamint a hivatalon belül kihirdeti a beszerzési eljárásrendet (*B18 Beszerzési eljárásrend*), mely a hivatal elektronikus információs rendszerére, az ezekhez kapcsolódó szolgáltatások és információs rendszer biztonsági eszközök beszerzésére vonatkozó szabályait fogalmazza meg (akár az általános beszerzési szabályzat részeként), és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
- a beszerzési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a beszerzési eljárásrendet.

2.9.2. A rendszer fejlesztési életciklusa

Az informatikai eszközök különböző beszerzési eljárásmódjainak alkalmazásánál fokozottan szem előtt kell tartani, hogy a szóban forgó eszköz megfeleljen a jelen szabályzatban rögzített információbiztonsági követelményeknek.

A hivatal az elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri információbiztonsági helyzetüket. Fejlesztés esetén már a rendszer tervezésénél fokozottan figyelembe kell venni az információbiztonsági előírásokat, ajánlásokat. A hivatal a fejlesztési életciklus egészére meghatározza és dokumentálja az információbiztonsági szerepköröket és felelősségeket, valamint a hivatalra érvényes szabályok szerint kijelöli az ezen szerepköröket betöltő, ezekért felelős személyeket.

Az informatikai üzemeltetés az általa kiadott/telepített informatikai eszközökről (hardver, szoftver, fejlesztett rendszerek kiadása, telepítése, verziókövetés) naprakész nyilvántartást vezet *(B12 IT leltár)*.

2.10. Biztonságelemzési eljárásrend

A hivatal szükség szerint megfogalmazza, és az érintett hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett hivatalon belül kihirdeti a biztonságértékelési eljárásrendet, amely a biztonságértékelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő, valamint a biztonságértékelési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a biztonságértékelési eljárásrendet.

A hivatal biztonságértékelési tervet készít, melyben meghatározott gyakorisággal értékeli az elektronikus információs rendszer és működési környezete védelmi intézkedéseit, kontrollálja a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését, elkészíti a biztonságértékelés eredményét összefoglaló jelentést, valamint gondoskodik a biztonságértékelés eredményét összefoglaló jelentésnek az érintett hivatal által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismeréséről.

A biztonsági értékelés tartalmazza:

- az értékelendő (adminisztratív, fizikai és logikai) védelmi intézkedéseket;
- a biztonsági ellenőrzések eredményességét meghatározó eljárásrendeket;
- az értékelési környezetet, az értékelő csoportot, az értékelés célját, az értékelést végzők feladatát.

Az érintett hivatal kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.

2.11. Tesztelés, felügyelet

A hivatal megfogalmazza és dokumentálja, valamint kihirdeti az elektronikus információs rendszer tesztelésével, képzésével és felügyeletével kapcsolatos eljárásokat, amelyek támogatják a tesztelési, képzési és felügyeleti tevékenységek fejlesztését és fenntartását, valamint folyamatos időbeni végrehajtását. A hivatal felülvizsgálja a tesztelési, képzési és ellenőrzési terveket a kockázatkezelési stratégia és a lehetséges, vagy bekövetkezett biztonsági események súlya alapján.

Az érintett hivatal kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.

A hivatal az elektronikus információs rendszerei és alkalmazásai tekintetében legalább kétévente sérülékenység tesztet végeztet, ha azt az elektronikus információs rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik, valamint olyan esetben, amikor új, lehetséges sérülékenység merül fel az elektronikus információs rendszerrel vagy alkalmazásaival kapcsolatban.

A sérülékenység tesztet külső hivatal bevonásával azon elektronikus információs rendszerek tekintetében végezteti el, amelyek az érintett hivatal felügyelete, irányítása alatt állnak. Az elektronikus információs rendszer különleges jogosultsághoz kötött - úgynevezett privilegizált - hozzáférést biztosít az érintett hivatal által kijelölt rendszerelemekhez a sérülékenység teszt végrehajtásához.

A tesztet végző...

- kimutatást készít a feltárt hibákról, valamint a nem megfelelő konfigurációs beállításokról;
- végrehajtja az ellenőrzési listákat és tesztelési eljárásokat;
- felméri a sérülékenység lehetséges hatásait;
- elemzi a sérülékenység teszt eredményét;
- megosztja a sérülékenység teszt eredményét a jegyzővel és a rendszergazdával;
- olyan sérülékenységi teszteszközt alkalmaz, melynek sérülékenység feltáró képessége könnyen bővíthető az ismertté váló sérülékenységekkel;
- meghatározza, hogy egy támadó milyen információkat képes elérni az elektronikus információs rendszerben, és ennek elhárítására javítási javaslatokat tesz.

Hivatalos sérülékenység vizsgálatot kizárólag a Kormányzati Eseménykezelő Központ (GovCERT-Hungary) végezhet. A teszt eredményének függvényében az informatikai vezető utasításokat ad a rendszergazdának a feltárt hiányosságok megszüntetésére vonatkozóan.

2.12. Biztonsági eseménykezelési eljárásrend

A hivatal eseménykezelési eljárást dolgoz ki a biztonsági eseményekre, amelyek magukban foglalják az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és a helyreállítást;

- egyezteti az eseménykezelési eljárásokat az üzletmenet-folytonossági tervéhez tartozó tevékenységekkel;
- az eseménykezelési tevékenységekből levont tanulságokat beépíti az eseménykezelési eljárásokba, a fejlesztési és üzemeltetési eljárásokba, elvárásokba, továbbképzésekbe és tesztelésbe;
- nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági eseményeit;
- mindenkitől, aki az elektronikus információs rendszerrel, vagy azok elhelyezésére szolgáló objektummal kapcsolatban áll megköveteli, hogy jelentsék a biztonsági esemény bekövetkeztét, vagy ha erre utaló jelet, vagy veszélyhelyzetet észlelnek;
- jogszabályban meghatározottak szerint jelenti a biztonsági eseményekre vonatkozó információkat az elektronikus információs rendszerek biztonságának felügyeletét ellátó szerveknek;
- tanácsadást és támogatást nyújt az elektronikus információs rendszer felhasználóinak a biztonsági események kezeléséhez és jelentéséhez;
- biztonsági eseménykezelési tervet dolgoz ki, amely...
    - az érintett hivatal számára iránymutatást ad a biztonsági esemény kezelési módjaira;
    - ismerteti a biztonsági eseménykezelési lehetőségek struktúráját és hivatalát;
    - átfogó megközelítést nyújt arról, hogy a biztonsági eseménykezelési lehetőségek hogyan illeszkednek az általános hivatalba;
    - kielégíti az érintett hivatal feladatkörével, méretével, hivatali felépítésével és funkcióival kapcsolatos egyedi igényeit;
    - meghatározza a bejelentésköteles biztonsági eseményeket;
    - meghatározza és folyamatosan pontosítja a biztonsági események kiértékelésének, kategorizálásának (súlyosság stb.) kritériumrendszerét;
    - támogatást ad a biztonsági eseménykezelési lehetőségek belső mérésére;

- meghatározza azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására;
- kihirdeti és tudomásul veteti a biztonsági eseménykezelési tervet a biztonsági eseményeket kezelő (névvel és/vagy szerepkörrel azonosított) személyeknek és hivatali egységeknek;
- meghatározott gyakorisággal felülvizsgálja a biztonsági eseménykezelési tervet;
- frissíti a biztonsági eseménykezelési tervet, figyelembe véve az elektronikus információs rendszer és a hivatal változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat;

- gondoskodik arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, módosítható;
- biztonsági eseménykezelési képzést biztosít az elektronikus információs rendszer felhasználóinak a számukra kijelölt szerepkörökkel és felelősségekkel összhangban;
- a képzést a biztonsági eseménykezelési szerepkör vagy felelősség kijelölését követő, meghatározott időtartamon belül, vagy amikor ezt az elektronikus információs rendszer változásai megkívánják, vagy meghatározott gyakorisággal tartja.

3. ADATOK ÉS IT RENDSZEREK VÉDELME, BIZTONSÁGA

Jelen fejezet alkalmazása során figyelemmel kell lenni a más jogszabályban meghatározott tűz-, vagyon- és személyvédelmi, valamint a személyes adatok kezelésére vonatkozó rendelkezésekre, valamint arra, hogy e fejezet rendelkezései az adott létesítmény bárki által szabadon látogatható vagy igénybe vehető területeire nem vonatkoznak.

3.1. Fizikai védelmi intézkedések

Azon helyiségek kijelölése, illetve kialakítása során, amelyekben a hivatal kiemelt fontosságú kiszolgáló számítógépei (szerverei) kerülnek elhelyezésre, különös figyelmet kell fordítani a fokozott biztonságra. A helyiség (szerverszoba) közelében nem üzemelhet tűz- és robbanásveszélyes raktár. A helyiségben független áramellátással működő tűzjelző rendszert kell kiépíteni, a bejárat közelében az informatikai eszközökhöz megfelelő oltóberendezést kell elhelyezni. A berendezések üzembiztonságát az előírásoknak megfelelően időszakosan ellenőrizni kell. A szerverszobában az erőforrások biztonságos működéséhez szükséges szinten kell tartani a hőmérsékletet és páratartalmat (klímaberendezés), valamint figyelni kell ezek szintjét.

3.1.1. Fizikai védelmi eljárásrend

A fizikai és környezeti biztonságra vonatkozó óvintézkedések a hivatali rendszereknek helyet adó létesítmények, a rendszer-erőforrások és a működést biztosító alapszolgáltatások védelmével kapcsolatban fogalmaznak meg szabályokat annak érdekében, hogy a számítástechnikai szolgáltatások megszakadását, eszközök ellopását, a fizikai károkozást, az információk jogosulatlan felfedését, a rendszer sértetlenségének elvesztését megakadályozzák.

A hivatal szükség esetén legalább éves gyakorisággal felülvizsgálja és frissíti a fizikai védelmi eljárásrendet.

A hivatali számítógépek és adathordozók fizikai védelmét biztosítani kell a hivatalban lopás, rongálás, megsemmisülés ellen értékarányos módszerekkel és eljárásokkal (pl. élőerős védelem és fizikai védelem – rácsok, ajtók, riasztóberendezés).

A hardverek és adatok részleges vagy teljes megsemmisülésével fenyegető tüzek megelőzése és elhárítása a *Tűzvédelmi Szabályzat* rendelkezései szerint történik.

Az infrastrukturális gyengeségek és hiányosságok kivédése érdekében az egyes rendszerek biztonsági osztályba sorolása után gondoskodni kell a megfelelő infrastruktúra biztosításáról. Ilyenek lehetnek a következők: szünetmentes áramellátás, hőmérséklet és páratartalom szabályozó rendszer, beléptető rendszer stb.

A hivatal informatikai rendszeréhez nem a hivatali infrastruktúrájához tartozó (pl. magántulajdonú) számítástechnikai, kommunikációs, multimédiás berendezést vagy adathordozót kapcsolni tilos! Amennyiben hivatali érdekből szükséges ilyen eszköz használata, úgy az csak a hivatal vezetőjének vagy az IBF-nek az engedélye alapján, az informatikus bevonásával, dokumentálási kötelezettség mellett végezhető el *(B21 Idegen eszköz használatának engedélyezése)*.

A hivatal tulajdonában lévő vagy bérelt számítástechnikai berendezések behozatala, kivitele (javítás céljából, máshol történő használatra stb.) csak hivatali céllal lehetséges, amelyet az IBF vagy a hivatal vezetője engedélyezhet *(B22 IT eszköz kiviteli-behozatali engedélye)*. Ezeket az eseteket dokumentálni kell. Nem kell alkalmanként dokumentálni a személyes használatra, név szerint, tartósan átadott eszközök mozgatását (pl. hivatali laptopok, telefonok stb.) *(B28 IT eszközök használatba adása és visszavétele)*.

A javítás céljából a hivatalból kikerülő eszközök esetében biztosítani kell, hogy a hivatal által kezelt adatok ne kerüljenek ki. Olyan meghibásodott eszközök (PC, mobil eszköz, szerver stb.), amelyekben az adathordozók védendő adatokat tartalmazhatnak, nem kivihetők az adathordozó alkatrésszel. Ebben az esetben az adathordozót (merevlemez, statikus memória egység stb.) a javítás idejére cserealkatrésszel kell a gépben helyettesíteni, vagy ha nem szükséges ez az alkatrész a működéshez, akkor az eredeti adathordozó és cserealkatrész nélkül kell javítási célból kivinni a hivatalból. Az eredetileg használt adathordozót a javítás után vissza kell helyezni az eszközbe, vagy arról az adatokat az új eszközre át kell tenni. Amennyiben az eredeti adathordozó alkatrész nem kerül vissza az adott eszközbe, úgy az adathordozót a szabályzat „4.4 Adathordozók védelme" fejezetében meghatározottak szerint kell kezelni.

3.1.2. Fizikai belépés ellenőrzése, belépési engedélyek

A hivatal székhelyén 3 biztonsági zóna van elkülönítve:

1. zóna A bejutás ellenőrzötten lehetséges, látogató felügyelet nélkül bent tartózkodhat. Informatikai eszköz nem lehet a zónában. A zónába tartozó helyiségek: *folyosó, előtér*

2. zóna A bejutás kulccsal vagy beléptető rendszerrel lehetséges, látogató csak felügyelettel tartózkodhat a területen. A zónába tartozó helyiségek: *iroda*

3. zóna A bejutás kulccsal vagy beléptető eszközzel, csak ideiglenesen, belépési naplót vezetve lehetséges. A kiemelt fontosságú informatikai eszközöket itt kell elhelyezni. Kizárólag az

informatikus (rendszergazda, IBF) tartózkodhat bent kíséret nélkül, másokat az informatikusnak kell kísérni. A zónába tartozó helyiségek: *szerverszoba*

A 2. és 3. zónába tartozó helyiségeket – amennyiben nem folyik bennük munkavégzés – kulcsra zárva kell tartani kell védeni. A helyiségek kulcsait elzárva kell tartani és csak az arra jogosultaknak szabad kiadni.

Az új belépő munkatársak kulcsokat csak a belépést követő oktatás *(B08 IT biztonsági oktatási terv és napló)* megtörténte és a titoktartási nyilatkozat *(B14 Titoktartási nyilatkozat)* aláírása után kaphatnak. A belépő munkatárs új belépési jogosultságait, illetve nem új belépő munkatárs belépési jogosultságainak változtatását az érintett terület vezetője határozza meg. A meghatározás során a terület vezetője a *B15 Hozzáférések igénylése és letiltása* formanyomtatványon összegzi az általa szükségesnek tartott belépési jogosultságokat és azokat jóváhagyatja a hivatal vezetőjével.

A jóváhagyott *B15 Hozzáférések igénylése és letiltása* formanyomtatvány továbbításra kerül a kulcsok/azonosító kártyák/kódok kiosztásának felelőse felé, akinek felelőssége, hogy csak a vezetőség által jóváhagyott jogosultságokat állítsa be, csak a megfelelő kulcsokat/kódokat adja ki. Amennyiben felmerül a jóváhagyás hiteltelenségének gyanúja, úgy azt köteles a kulcskiadás előtt igazoltatni a vezetőség megkérdezésével. A kulcsokat vagy kódokat évente cserélni kell, a jogosultságok felülvizsgálatával együtt.

A helyiség (szerverszoba) közelében nem üzemelhet tűz- és robbanásveszélyes raktár. A helyiségben tűzjelző rendszert kell kiépíteni, amelynek üzembiztonságát az előírásoknak megfelelően időszakosan ellenőrizni kell.

A helyiséget mindig zárva kell tartani. A helyiség kulcsait munkaidőben csak az informatikai vezető, illetve az általa felhatalmazott informatikus veheti fel, mivel a szerver sértetlensége, rendelkezésre állása az ő felelősségük. A felvétel tényét minden esetben nyilván kell tartani a *B25 Szerverszoba belépési nyilvántartás* nyomtatványon. A nyomtatványt legalább egy évre visszamenőleg meg kell őrizni. Munkaidőn kívül a kulcsokat elzártan kell tartani. A helyiségben idegen személy felügyelet nélkül nem tartózkodhat. A belépések rögzítése történhet elektronikus beléptető rendszer használatával is. Ebben az esetben csak az informatikai vezető és az általa felhatalmazott informatikus kártyája nyithatja az ajtót, illetve ők ismerhetik az ajtónyitó kódokat.

A belépésre jogosultak listáját mindig naprakészen kell tartani (*B23 Belépésre jogosultak*), akinek a belépése már nem indokolt, el kell távolítani a listáról, a belépési jogosultságot igazoló dokumentumait/eszközeit vissza kell vonni.

A belépési jogosultságokat a belépési pontokon ügyintézők ellenőrzik, szükség esetén a látogatók (vendégek, ügyfelek) belépéseiről nyilvántartást vezet a látogatóktól elkért fényképes igazolvány alapján. A belépési nyilvántartás tartalmazza a látogató nevét és személyi igazolványának számát. A nyilvántartás adatvédelmi okokból egy hónap után megsemmisítendő. A látogatók csak kísérettel mozoghatnak a hivatal 2. és 3. zónába tartozó területein. A zónahatárokon biztosági kamerát kell üzemeltetni.

Az elektronikus információs rendszereknek helyt adó létesítményekbe belépésre jogosultakról a hivatal nyilvántartást vezet a *B23 Belépésre jogosultak* listáján, és belépési jogosultságot igazoló eszközöket (pl. kitűzők, azonosító kártyák) bocsáthat ki a részükre *(B24 Azonosító kártya)*.

A hivatal által meghatározott ideig (de legalább egy évig) megőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt látogatói belépésekről szóló információkat. A hivatal azonnal átvizsgálja a látogatói belépésekről készített információkat és/vagy felvételeket, ha a rendelkezésre álló információk jogosulatlan belépésre utalnak.

A hivatal helyiségeiben a szükség szerint vészvilágítást és menekülési útvonal jelzéseket kell elhelyezni, illetve üzemeltetni.

3.2. Hivatali és személyzeti szabályok

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed a hivatal teljes személyi állományára, valamint minden olyan természetes személyre, aki a hivatal elektronikus információs rendszereivel kapcsolatba kerül vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszerrel tényleges vagy feltételezhető kapcsolatba kerülő személy nem a hivatal alkalmazottja, a jelen fejezet szerinti elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás, megkötés során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

3.2.1. Felvételi eljárás során követendő szabályok, személyes követelmények

A hivatal meghatározza a felvételi eljárás során követendő szabályokat *(B26 Felvételi eljárásrend)*, személyes követelményeket. A követelményeket a Munkaköri leírásokban rögzíti.

3.2.2. Képzési eljárásrend

A felhasználói állományt az informatikai biztonság megvalósítása érdekében munkakörüknek megfelelően képezni kell, a fejlesztői, üzemeltetői állománynak pedig folyamatosan szinten kell tartania és fejlesztenie kell az informatikával és informatikai biztonsággal kapcsolatos ismereteit. A felhasználói személyi állományt új rendszerek bevezetésekor képezni kell. A hivatalban alkalmazott új dolgozót - vezetője kérése alapján- soron kívül kell oktatni a rendszer használatáról.

A követelmények és a ténylegesen rendelkezésre álló erőforrások összevetése alapján évente oktatási terv *(B08 IT biztonsági oktatási terv és napló)* készül. Ez tartalmazza a szükséges oktatásban résztvevők körét, az oktatás/képzés témakörét és követelményeit. A tervezett képzéseknél figyelembe kell venni a minőségi, környezeti, a munkahelyi egészségvédelmi és biztonsági, illetve az információbiztonsági célok kapcsán megfogalmazott, jövőben elvárt kompetenciákat.

Ezeken túlmenően a hivatal nyitott munkatársainak egyéni teljesítményét javító igények tekintetében is, és ezért – eseti elbírálás alapján – figyelembe veszi a vezetők és a beosztottak saját továbbképzési igényét is, ha azok összhangban vannak a hivatal hosszú távú stratégiájával.

Az oktatás mellett a teljes felhasználói állománnyal ismertetni kell az IBSZ rájuk vonatkozó előírásait (*B03 IFSZ*). A felhasználók nyilatkozatot adnak arról, hogy az ismertetés megtörtént, a szabályzatban foglaltakat megértették és azokat maradéktalanul betartják *(B02 Nyilatkozat az IT biztonsági szabályok elfogadásáról)*.

3.2.3. Biztonság tudatosság képzés

A hivatal annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára:

- az új felhasználók kezdeti képzésének részeként (*B08 IT biztonsági oktatási terv és napló*);
- új szerepkörbe vagy felelősségbe kerülésükkor
- amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
- legalább évente informatikai és IT-biztonsági képzés, ismeret-felfrissítés (*B08 IT biztonsági oktatási terv és napló*).

3.2.4. Fegyelmi intézkedések

A biztonsági előírásokat megsértőkkel szemben fegyelmi eljárás indul. Fegyelmi eljárást az érintett munkavállaló közvetlen vezetője, az IBF, illetve a hivatal vezetője kezdeményezhet írásban *(B27 IT biztonsági fegyelmi eljárás kezdeményezése és jegyzőkönyve)*. A kezdeményezésnek tartalmaznia kell:

- a fegyelmi eljárást kezdeményező nevét, beosztását;
- a valószínűsíthető fegyelmi vétséget elkövető (érintett) nevét, beosztását;
- az észlelés idejét, módját;
- a fegyelmi vétség elkövetésének idejét, módját, körülményeit;
- a keletkező károk és egyéb következmények kifejtését;
- a kezdeményezés idejét.

A hivatal vezetője a kezdeményezést elbírálja, melyről értesítést küld a kezdeményezőnek és az IBF-nek. Kitűzi továbbá a fegyelmi eljárás feltáró megbeszélésének időpontját és meghatározza az azon résztvevő személyek körét.

A fegyelmi eljárás az alábbi szakaszokra tagolódik:

- feltáró megbeszélés;
- adatgyűjtés, adatértékelés;
- záró megbeszélés.

A feltáró megbeszélésen jelen van:

- a hivatal vezetője;
- az eljárást kezdeményező;
- az eljárásban érintett személy;
- az IBF, amennyiben biztonságot érintő fegyelmi vétségről van szó;
- az eseményben érintett egyéb személyek;
- azok, akiket erre a megbeszélésre a hivatal vezetője meghív.

A feltáró megbeszélést a hivatal vezetője vezeti. A megbeszélés során az eljárást kezdeményező személy felvázolja az általa tapasztalt vélhető fegyelmi vétséget. Az ismertetés során a kezdeményező személynek prezentálnia kell az eseményről begyűjtött bizonyítékait, illetve meg kell neveznie azokat a személyeket, akik érintettek, illetve egyéb bizonyítékokat tudnak szolgáltatni.

Ezt követően a fegyelmi eljárásban érintett személy reagál a kezdeményező személy által felvázoltakra. Ennek során meg kell neveznie azon pontokat, amelyekkel egyetért, amelyekkel nem ért egyet, illetve amelyekkel részben ért egyet. Ezen kifejtés során a kezdeményezőnek nincs lehetősége azonnali

interakciókra. A hivatal vezetőjének feladata és felelőssége, hogy biztosítsa az érintettnek a teljes kifejtés lehetőségét. Ezt követően a jelenlévők véleményezik, megvitatják a helyzetet. A feltáró megbeszélésről jegyzőkönyvet *(B27 IT biztonsági fegyelmi eljárás kezdeményezése és jegyzőkönyve)* kell készíteni, mely tartalmazza:

- a fegyelmi eljárás kezdeményezésének hivatkozási számát;
- a fegyelmi eljáráson jelenlévőket;
- a fegyelmi eljárás lefolytatásának idejét, helyét;
- a fegyelmi eljáráson elhangzottakat, meghivatkozva a személyt.

Amennyiben szükséges, a feltáró megbeszélést követően újabb adatok begyűjtése kezdeményezhető az esetleges tisztázatlan körülmények tisztázására. A rendelkezésre álló adatok alapján az eljárást vezető döntést hoz a fegyelmi eljárás tárgyát képező témában, mely során állásfoglalást alakít ki azt illetően, hogy

- a fegyelmi vétség megvalósult-e, ha igen, akkor milyen formában nyilvánult meg;
- kik érintettek a fegyelmi vétségben, kik felelősök annak megvalósulásában és milyen mértékben;
- a meghatározott felelősségek milyen szankcionálási eljárást vonnak maguk után;
- szükséges-e a büntetőjogi felelősségeket vizsgálni, s ha igen, azt mi módon kezdeményezi a hivatal.

A záró megbeszélésen részt vesznek:

- a hivatal vezetője;
- az eljárást kezdeményező;
- az eljárásban érintett személy;
- az IBF, amennyiben biztonságot érintő fegyelmi vétségről van szó;
- azok, akiket erre a megbeszélésre a hivatal vezetője meghív.

A záró megbeszélésről jegyzőkönyv készül, mely tartalmazza:

- a fegyelmi eljárás kezdeményezésének hivatkozási számát;
- a fegyelmi eljáráson jelenlévőket;
- a fegyelmi eljárás lefolytatásának idejét, helyét;
- a hivatal vezetője állásfoglalását a fentiekben részletezett kérdésekben.

A jegyzőkönyvről másolatot kap az érintett személy, az eredetit pedig a hivatal őrzi meg.

Fegyelmi eljárás érvényesítése

Az érvényesítés során a hivatal vezetőjének állásfoglalására alapozva a szükséges teendők meghatározásra kerülnek, kijelölik azok elvégzésének felelőseit és az elvégzés határidejét. Ezen feladatokat a fegyelmi eljárás jegyzőkönyvére kell felvezetni *(B27 IT biztonsági fegyelmi eljárás kezdeményezése és jegyzőkönyve)*, de a kiadott másolaton ezeket nem kell szerepeltetni.

Amennyiben az elektronikus információbiztonsági szabályokat nem a hivatal személyi állományába tartozó személy sérti meg, úgy a hivatal érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti új eljárásokat.

3.2.5. Eljárás a jogviszony megszűnésekor

A munkavállaló jogviszonyának megszűnése esetén a munkavállaló felettes vezetője gondoskodik a kilépő információs rendszerrel vagy annak biztonságával kapcsolatos feladatainak ellátásáról a jogviszony megszűnését megelőzően. A jogviszony megszűnésekor a jogviszonyt megszüntető személy gondoskodik arról, hogy a kilépő esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzze (hozzáférések megszüntetése, jogosultságok visszavonása).

A hivatal ellenőrzi, hogy a kilépő felhasználó személyes használatában található-e informatikai eszköz, illetve gondoskodik ezek visszavételéről *(B28 IT eszközök használatba adása és visszavétele)*. A hivatal a kilépő számára igazolja, hogy a hozzáférési jogokat törölte, illetve a felhasználó a hivatal felé elszámolt. A kilépőt tájékoztatni kell az esetleg rá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről.

A hivatal meghatározott ideig megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és hivatali információkhoz. Adatvédelmi okokból a hivatali felhasználóneveket/azonosítókat úgy szükséges létrehozni, hogy azok személyes adatot ne tartalmazzanak (pl. ugyintezo1@hivatal.hu).

3.3. Azonosítás és hitelesítés

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a hivatal felhasználóit, a felhasználók által végzett tevékenységet.

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a különleges jogosultsághoz kötött - úgynevezett privilegizált - felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

3.3.1. Azonosítási és hitelesítési eljárásrend

A hivatalban alkalmazott informatikai rendszerekben felhasználói azonosítást és hitelesítést kell alkalmazni a jogosulatlan személyek tevékenységének megakadályozása és az elszámoltathatóság megvalósítása érdekében.

Az alábbi követelmények szerint az azonosítási folyamatban a felhasználó megadja azonosságát a rendszer felé, melyre a felhasználói azonosító szolgál.

A hitelesítés a felhasználó állítólagos azonosságának a bizonyítására szolgál. A hivatal informatikai rendszereiben legalább tudás alapú (jelszavas) hitelesítést kell alkalmazni. A hitelesítési adatokhoz való hozzáférés korlátozása érdekében az ilyen adatokat védeni kell a jogosulatlan megismerés, módosítás, törlés ellen.

Az azonosítási és hitelesítési adatok és eszközök kezelésére, az azonosítás és hitelesítési folyamatra az alábbi általános szabályokat minden rendszerben/alrendszerben be kell tartani:

- A hivatal kijelölt informatikusai gondoskodnak arról, hogy a rendszerben szereplő minden felhasználói azonosító valós, engedélyezett felhasználóhoz tartozzon.
- A rendszergazdai feladatokat ellátó személyek részére az adminisztratív és a felhasználói feladatok ellátására külön azonosítót kell létrehozni, az adminisztrátori azonosítót csak rendszergazdai feladatok ellátására szabad használni!

- A hivatal kijelölt informatikusainak az azonosítási adatokat naprakészen kell tartani: az új felhasználókat be kell vezetni a rendszerbe, a hivatalból, hivatali egységből, munkakörből stb. eltávozott munkatársak jogait vissza kell vonni.
- A hitelesítő eszközök személyre szólóan kerülnek kiadásra és nyilvántartásra, így kezelésükért, használatukért és tárolásukért a felhasználók felelnek.
- A hivatal informatikai rendszereihez hozzáférő felhasználóknak egyedi módon azonosítaniuk kell magukat. Más felhasználók azonosítóinak használata TILOS!
- Az azonosító/hitelesítő eszközöket TILOS másnak odaadni, a jelszavakat másnak átadni, elmondani és/vagy leírni. A tiltás teljes mértékben vonatkozik arra is, hogy az egyedi eszközt/jelszót vezetőnek, rendszergazdának, külső informatikai szakembernek sem szabad átadni, még abban az esetben sem, ha azt kifejezetten kérik!
- Jelszó használata esetén a felhasználó által választott jelszónak megfelelő biztonságúnak kell lennie. A megfelelő jelszavakra (legalább) az alábbi kritériumok igazak (ezt technológiai eszközökkel bizonyos rendszerek kényszeríthetik is):
  - legalább 8 karakter hosszú;
  - nem szótári szó, illetve annak egyszerű kiegészítése, pl. anna78;
  - nem egyszerű sorozat (pl. 123456, abcdef, asdfgh);
  - tartalmaz számokat, kis- és nagybetűket.
- Amennyiben egy hivatali munkaállomáson több felhasználó is jogosult dolgozni, úgy a feladat elvégzése után (mielőtt másik felhasználó a géphez hozzáférne) a rendrendszerből ki kell jelentkezni!
- Megosztott, vagy csoport felhasználói fiókokhoz tartozó hitelesítő eszközöket vagy adatokat a csoport tagjainak változása esetén vissza kell vonni, majd újra kell generálni az aktuális állapotnak megfelelően.
- A saját egyéni munkaállomás időleges elhagyásakor nem lehet a számítógépet bárki által hozzáférhetően hagyni, védelméről gondoskodni kell (kikapcsolás, kijelentkezés, jelszavas képernyővédelem stb.)!
- A felhasználói jelszavakat legalább háromhavonta meg kell változtatni.

A felhasználó távollétében történő elkerülhetetlen hozzáférést az illetékes vezető kezdeményezhet az IBF-nél. Amennyiben a hozzáférést az IBF engedélyezi, úgy azt a hivatal kijelölt munkatársa lehetővé teszi a következő módon:

- rendszergazdai hozzáféréssel megváltoztatja a felhasználó jelszavát;
- a felhasználó hozzáférésével végrehajtja az engedélyezett feladatot;
- a megváltoztatott jelszót az illetékes közvetlen vezetője kapja meg;
- ezt a felhasználó visszatérésekor az első rendszerbe lépéskor a felhasználónak meg kell változtatnia.

3.3.2. Azonosításra, hitelesítésre szolgáló eszközök kezelése

Az azonosításra, hitelesítésre szolgáló eszközök kiadása előtt az azt végző munkatárs vagy hivatal:

- meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát (pl. kezdeti jelszó), melyet az adott rendszer telepítése során a végfelhasználónak meg kell változtatni;
- kiosztáskor ellenőrzi az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát, illetve biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;

- meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;
- a hitelesítésre szolgáló eszköztípusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket;
- dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, kompromittálódott vagy a sérült eszközöket;
- megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;
- megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;
- lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

Az elektronikus információs rendszer fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

Sikertelen belépés esetén a hivatal által meghatározott esetszámkorlátot alkalmaz a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire. Amennyiben a sikertelen bejelentkezési kísérletekre felállított esetszámkorlátot a felhasználó túllépi, automatikusan zárolja a felhasználói fiókot vagy csomópontot meghatározott időtartamig, vagy meghatározott módon késlelteti a következő bejelentkezési kísérletet.

A felhasználói azonosítók/jelszavak elvesztését/elfelejtését, illetve vélelmezett kompromittálódását azonnal jelezni kell a hivatal vezetője vagy az IBF felé. Elfelejtett jelszó esetében a rendszergazda új kezdeti jelszót állít be, amelyet az első bejelentkezéskor meg kell változtatni. Azonosító kompromittálódása esetén a kompromittált azonosítóhoz tartozó jogokat azonnal le kell tiltani és ki kell vizsgálni, hogy történt-e jogosulatlan hozzáférés az informatikai rendszerhez. Az IBF engedélyével a rendszergazda a kompromittálódott azonosító helyett az érintett felhasználónak a munkájához szükséges másik azonosítót biztosít.

A szerepköröknek megfelelő, leginkább az üzemeltetéshez köthető rendszergazdai és bizonyos rendszereknél a rendszer-visszaállítási jelszavakat szükség esetén tárolni kell a következő módon:

- Minden ilyen jogosultsági adatot (rendszer neve, hozzáférés módja, felhasználónév, jelszó) redundánsan, két darab külön adathordozóra mentve, megfelelő titkosítású jelszótároló programban rögzítetten, szerepkörönként külön adatbázisban, melynek mesterkulcsát (jelszavát) az adathordozó mellett, szerepkörönként lezárt, lepecsételt és legalább két jogosult személy által aláírt borítékban kell tárolni.
- A borítékba az adatokat úgy kell elhelyezni, hogy azok ne legyenek „átvilágíthatók", felbontás nélkül ne legyenek olvashatók. A borítékokra kívül rá kell írni az utolsó módosítás dátumát és a megbontás okát (pl. audit vagy jogosult távolléte miatti vezetői bontás), ilyen eseteket követően a szerepköri jogosultaknak célszerű a jelszavakat lecserélni.
- A jelszótárolóban a korábbi jelszavak a History alatt, időmegjelöléssel megtalálhatók. A változtatást végző jogosult köteles a hasonló szerepkörűeknek jelezni a változtatás tényét, adattartalmát. Ha a szerepkörhöz rendelt jogosult végez szabályzatban előírt kötelező jelszóváltást a tárolt adatokban, akkor nincs szükség borítékbontásra.
- A borítékot zárt biztonsági szekrényben kell tárolni az illetéktelen hozzáférés elkerülése érdekében.

3.3.3. hivatalon kívüli felhasználók azonosítása és hitelesítése

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a hivatalon kívüli felhasználókat és tevékenységüket.

Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság (NMHH) elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatja el a hivatalon kívüli felhasználók hitelesítéséhez.

3.4. Hozzáférés védelem, jogosultság kezelés

3.4.1. Hozzáférés ellenőrzési eljárásrend

A hivatal minden informatikai rendszerében, erőforrásaival, szolgáltatásaival kapcsolatban, az adott eszköz, erőforrás, adat, dokumentumtár stb., biztonsági osztályától függően, a szükséges és elégséges ismeret elvének betartásával kell alkalmazni a hozzáférés-védelmi és a jogosultságkezelési intézkedéseket. Minden, az IBSZ hatálya alá eső adatot a központi informatikai rendszerben, a központi logikai, fizikai rendszerek védelme alatt, központi hozzáférés-védelmi és jogosultságkezelési rendszer ellenőrzése mellett kell menedzselni az egyedi elszámoltathatóság elvének érvényre juttatásával. A hozzáférés-védelmi követelmények a hivatal informatikai rendszereiben alkalmazandó rendszertől függenek.

Az információkhoz való hozzáférési lehetőséget (jogosultságot) a felhasználó által betöltött munkakör (szerepkör) alapján kell meghatározni (szerepkör alapú hozzáférés). A szerepkörök definiálása a hivatal munkafolyamatain, hivatali struktúráján, a hierarchikus és funkcionális kapcsolatokon alapul.

A hivatalba újonnan belépő felhasználók informatikai rendszerhez történő hozzáférését az erre szolgáló igénylőlapon *(B15 Hozzáférések igénylése és letiltása)* az érintett hivatali egység vezetője kezdeményezi. A felhasználói hozzáférést és az indokoltan kért jogosultságokat a hivatal vezetőjének engedélye után a rendszergazda adja meg.

A hivatal informatikai rendszereiben működő szolgáltatások (pl. megosztott könyvtárak) esetén a szolgáltatás indítását engedélyező dokumentumban meg kell jelölni a szolgáltatásért (logikailag) felelős vezetőt, és a szolgáltatás tulajdonosát. Amennyiben a feldolgozott adatok, illetve a szolgáltatás jellege alapján a szolgáltatás jellemzően valamelyik szakterületekhez kapcsolható (pl. gazdálkodási adatokról szóló kimutatások, pénzügy, személyügy stb.), úgy annak a területnek a vezetőjét kell szolgáltatás tulajdonosnak kijelölni.

A szolgáltatás tulajdonos által definiált hozzáférés-védelem elve szerint a szolgáltatás tulajdonosa által meghatározott szabályok (engedélyezés) alapján kell az adott szolgáltatáshoz történő hozzáférési jogosultsági kört kialakítani. A szolgáltatás tulajdonosa által megfogalmazott szabályok alapján kell beállítani a megfelelő (pl. könyvtárak esetén: olvasás, írás, törlés) hozzáférési módot. A jogosultságok beállítását az informatikai rendszerben az informatikus végzi el.

A munkaállomásokon és a szervergépeken technikailag is korlátozni kell az úgynevezett alternatív bootolási lehetőségeket (pl. DVD, USB, Ethernet stb.). Ezekre az eszközöket csak karbantartási és javítási célból lehet olyan rendszerrel működtetni, amely nem az üzemszerűen rátelepített operációs rendszer.

A munkaállomásokon és szervereken telepített szoftverek, alkalmazások és szakalkalmazások esetében kiemelt figyelmet kell fordítani az automatikusan létrejövő felhasználókra, hozzáférésekre, jogosultságokra (administrator, guest, root stb.), ezek kezdeti jelszavát meg kell változtatni és/vagy zárolni kell a használatát. Szintén kiemelt figyelmet kell fordítani a teszt jelleggel létrehozott felhasználókra, hozzáférésekre. Ezeket a felhasználókat, hozzáféréseket, amikor használatuk már nem szükséges és indokolt, meg kell szüntetni. Amennyiben a hozzáférések szükségesek (pl. valamilyen rendszerszolgáltatás miatt), úgy legalább a magasabb szintű biztonságukról gondoskodni kell, így vagy át kell őket nevezni, vagy a nem szükséges jogosultságokat el kell venni ezektől a felhasználóktól. Az ilyen felhasználók alapértelmezett jelszavait meg kell változtatni megfelelő erősségű jelszavakra. Szakalkalmazások esetében a fejlesztőknek kerülniük kell az automatikus felhasználói, alapértelmezett jelszóval működő hozzáférések használatát.

A felhasználó szerepkörének megváltozása esetén (pl. más osztályra kerül, munkaköre megváltozik) az informatikus a hivatal vezetőjétől kapott írásos információk alapján a régi szerepkörhöz tartozó jogosultságot a felhasználótól elveszi, majd a szükséges új szerepkörnek megfelelő jogosultságokat megadja. *(B15 Hozzáférések igénylése és letiltása)*

A felhasználó jogviszonyának megszűnése esetén az informatikus vezetője a személyzeti munkatárstól kapott nyomtatványon *(B28 IT eszközök használatba adása és visszavétele)* igazolja, hogy a hozzáférési jogokat törölte, illetve a felhasználó az informatikai vezető felé elszámolt.

Az informatikai rendszerhez, alrendszerekhez történő hozzáférési engedélyeket évente felül kell vizsgálni (pl. távoli hozzáférések, internet elérés, külső levelezés stb.). Az esetlegesen már nem indokolt jogosultságokat, hozzáféréseket meg kell szüntetni.

3.4.2. Felhasználói fiókok kezelése

A felhasználók kizárólag felhasználói jogosultsággal dolgozhatnak a munkaállomásokon, rendszergazdai jogosultságokat nem kaphatnak. Kivételt képeznek e szabály alól azon szakalkalmazások munkaállomásai, ahol a szoftver működéséhez szükségesek az emelt szintű jogok, itt a zavartalan munkavégzés miatt ez engedélyezett. Az így rendelkezésre álló jogokat a felhasználó nem használhatja semmilyen üzemeltetői feladatra (pl. programok telepítése, leállítása stb.), csak és kizárólag a szakalkalmazás használata miatt birtokolhatja ezeket!

A munkaállomásokon a felhasználóknak tilos hálózati szolgáltatásként mappákat/fájlokat megosztani. Amennyiben a megosztás szakmailag indokolt, úgy a közvetlen vezető kezdeményezésére, az IBF jóváhagyásával a megosztást a munkaállomás adminisztrátora hozza létre. Valamennyi megosztás esetén szigorúan kell meghatározni a hozzáféréseket, törekedni kell arra, hogy ne legyenek általános megosztások. Csak azok a felhasználók és munkaállomások kaphatnak jogot az erőforrások elérésére, amelyeknek ez a munkájukhoz valóban szükséges.

A hivatal minden irodájában biztosítani kell a hálózati csatlakozás lehetőségét. A hálózati erőforrásokhoz való hozzáférést különböző szintű hálózati jogosultságok biztosítják. Ezek a jogok az alábbi tevékenységek elvégzését tehetik lehetővé:

- hálózat kezeléséhez szükséges programok közös használata;
- közös nyomtató használata;
- internet böngészés;
- elektronikus levelezés;

- adatbázisok elérésének biztosítása;
- alkalmazások és adatok elérésének biztosítása.

A hálózaton található fájlokra, könyvtárakra (mappákra) kiosztható jogosultságok:
- olvasási jog;
- írási (módosítási, létrehozási) jog;
- törlési jog.

A hivatali informatikai rendszerben az egyes számítástechnikai rendszerek, szoftverek készítői által gyárilag a felhasználók részére biztosított védelmi eljárásokat (pl. a Microsoft Word jelszavas védelme) a felhasználók – a hivatali adatok rendelkezésre állásának biztosítása érdekében – nem használhatják!

A felhasználók számára tilos nem engedélyezett erőforrások, szolgáltatások, jogosultságok megszerzése vagy ennek kísérlete. Tilos más felhasználó munkájának zavarása, állományaikhoz történő bármilyen illetéktelen hozzáférés vagy annak kísérlete.

A hozzáférésvédelmi és jogosultságkezelési elemek, alrendszerek megbízható adminisztrálása érdekében a felhasználói hozzáféréseket megvalósító rendszerek működtetését (ahol a technológia lehetővé teszi) megbízható módon naplózni, és a naplótartalmat az engedélyezett jogosultság-igénylések alapján ellenőrizni kell.

A munkaállomás adminisztrátorát értesíteni kell, ha...
- a felhasználói fiókokra már nincsen szükség;
- a felhasználók kiléptek vagy áthelyezésre kerültek;
- az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak.

A felhasználói fiókok a fiókkezelési szabályokkal összhangban rendszeres időközönként, legalább évente felülvizsgálandók *(B30 Felhasználói fiókok kiosztása és felülvizsgálata)*.

A hivatal további feladatai:
- meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait és ezek típusait;
- kijelöli a felhasználói fiókok fiókkezelőit;
- kialakítja a csoport- és szerepkör tagsági feltételeket;
- meghatározza az elektronikus információs rendszer jogosult felhasználóit, a csoport- és szerepkör tagságot és a hozzáférési jogosultságokat, valamint (szükség esetén) az egyes felhasználói fiókok további jellemzőit (*B30 Felhasználói fiókok kiosztása és felülvizsgálata*).

3.4.3. Külső rendszerekből történő hozzáférés szabályozása

A hivatal
- meghatározza és dokumentálja felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban;
- külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

Külső cégek folyamatos üzemeltetési feladatainak ellátása érdekében (pl. szerverek és szakalkalmazások karbantartása) a cégek megbízott munkatársai állandó távoli hozzáférést kaphatnak az általuk felügyelt rendszerhez. Ezeket a hozzáféréseket a cégeknek az IBSZ betartásával, bizalmasan és a szakmai normáknak megfelelően kell kezelniük.

Távoli hozzáférést kaphatnak a hivatal azon munkatársai, akik a hivatal által biztosított, távoli munkavégzésre alkalmas eszközzel rendelkeznek.

A távoli hozzáféréshez használt azonosítókat, jogosultságokat a hivatal informatikusa dokumentáltan *(B15 Hozzáférések igénylése és letiltása)* adja ki, az azonosítóért felelős személy pontos meghatározásával. Az azonosítóért felelős személy ezt aláírásával igazolja.

A távoli hozzáférésű munkaállomások biztonságáért minden esetben a távoli gép felhasználója és/vagy üzemeltetője a felelős, így felelős a távoli gépről a hivatal infrastruktúrájában végrehajthatott cselekményekért is.

A hivatal informatikai infrastruktúráját távoli elérése csak titkosított kapcsolaton keresztül történhet. A rendszerhez történő csatlakozás csak a szükséges időre korlátozódhat, a munka végeztével a kapcsolatot bontani kell.

3.4.4. Azonosítás és hitelesítés nélkül engedélyezett tevékenységek

A számítógépes munkahely kialakítását követően a számítógépen dolgozók azonosítására, valamint a jogosultságok meghatározására van szükség. A számítógép használatakor egyedi azonosítókat kell alkalmazni, melyek hiányában a munkaállomásra a belépés nem lehetséges, így az elektronikus információs rendszeren belül semmilyen tevékenységre nincs lehetőség.

3.4.5. Nyilvánosan elérhető tartalom

Nyilvánosan hozzáférhető rendszerként definiálja a hivatal a publikus weboldalát. Az oldal üzemeltetéséért felelős hivatali egység vezetőjének gondoskodni kell az azon publikált információk törvényi megfelelőségéről és valódiságáról, sértetlenségéről. Tilos törvénybe, jogszabályba ütköző, vagy a jó ízlést és közerkölcsöt sértő tartalmat közzétenni. A felkerülő tartalmakat minden esetben ellenőrizni kell a hivatali egység vezetőjének és csak a jóváhagyása után publikálhatók az információk. A publikus weboldalnak gondosan szegmentáltnak kell lennie a hivatal belső hálózatától arra alkalmas eszközzel. Gondoskodni kell a weboldal jogosult használata közben kieszközölhető jogosulatlan elérések megakadályozásáról.

3.4.6. Rendszerhasználat jelzése

A rendszerhez való hozzáférés előtt a felhasználó figyelmeztető üzenetet vagy jelzést kap arról, hogy...

- a felhasználó az érintett hivatal elektronikus információs rendszerét használja;
- a rendszer használatot figyelhetik, rögzíthetik, naplózhatják;
- a rendszer jogosulatlan használata tilos és büntetőjogi vagy polgárjogi felelősségre vonással jár;
- a rendszer használata egyben a felhasználó előbbiekbe történő beleegyezését is jelenti;
- Az elektronikus információs rendszer a figyelmeztető üzenetet vagy jelzést mindaddig a képernyőn tartja, amíg a felhasználó közvetlen műveletet nem végez az elektronikus információs rendszerbe való bejelentkezéshez vagy további rendszer hozzáféréshez.

Nyilvánosan elérhető rendszerek esetén...

- kijelzi a rendszer használat feltételeit, mielőtt további hozzáférést biztosít;
- amennyiben felügyelet, adatrögzítés vagy naplózás történik, kijelzi, hogy ezek megfelelnek az adatvédelmi szabályoknak;

- leírást biztosít a rendszer engedélyezett felhasználásáról.

Vezeték nélküli hozzáférés esetén...

- belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán;
- engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.

Az elektronikus információs rendszer a figyelmeztető üzenetet vagy jelzést mindaddig a képernyőn tartja, amíg a felhasználó közvetlen műveletet nem végez az elektronikus információs rendszerbe való bejelentkezéshez vagy további rendszerhozzáféréshez.

Mobil eszközök hozzáférés ellenőrzése

A hivatal belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre és engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

3.5. Viselkedési szabályok az interneten

A hivatal e-mail és Internet használati jogokkal rendelkező dolgozói a munkájukkal kapcsolatban használhatják a hivatal által biztosított Internet szolgáltatást.

A belső hálózaton Internet-kapcsolatot létesíteni kizárólag tűzfalon keresztül lehet. Nem megengedett a hivatal informatikai hálózatába kapcsolt hordozható és asztali munkaállomásokról modemes, mobiltelefonos vagy egyéb, nem hivatali kapcsolat létrehozása Internet-szolgáltatókkal.

Az internetszolgáltatás magáncélú használata nem megengedett. Az internetforgalom automatikusan, szoftveres alapon szűrésre kerül, így bizonyos tartalmak nem látogathatók, technológiai eszközzel is tiltásra kerülnek. A technikai szűréstől függetlenül a felhasználóknak az internetszolgáltatás használatának folyamán a következő szabályokat kell betartaniuk:

- Az interneten csak a hivatali munkával kapcsolatos oldalakat lehet látogatni. Tilos a pornográf, online játék, fogadási, csevegő, letöltő és törvénybe ütköző tartalmakat szolgáltató oldalak látogatása, ezekről letölteni, ilyen tartalmakat és helyeken publikálni, adatokat cserélni, adatot tárolni!
- Az Internetről programok letöltése, telepítése és futtatása nem megengedett. Igény esetén az informatikus előzetes bevizsgálás után engedélyezheti programok letöltését és futtatását. A bevizsgálás során ellenőrizni kell...
  - a letölteni kívánt program vírusmentességét;
  - hogy a letölteni kívánt program képes-e működni abban a környezetben, amelybe a letöltést tervezik;
  - hogy a letöltés nem sért-e szerzői jogot.
- Információbiztonsági megfontolásokból tilos a hivatalban a csevegő programok használata (pl. Skype, MSN, Gtalk, IRC, ICQ stb.). Ezen programok futtatása is tilos! A programok hivatali érdekből történő használatára (pl. Skype a kommunikációs költségek csökkentésére) a hivatal vezetője adhat dokumentált módon engedélyt (*B31 Telepíthető nem szakalkalmazások listája*).
- Amennyiben az Interneten keresztüli kommunikáció (főként levelezés) nem titkosított és egyértelműen azonosítható formában (digitális aláírás, fokozott biztonságú elektronikus aláírás)

kerül lebonyolításra, nem megengedett a bizalmas vagy annál magasabb minősítésű, védett információt tartalmazó üzenet küldése kizárólag az Interneten keresztül azonosított feleknek mindaddig, amíg a másik fél megbízható, az Internettől független azonosítása meg nem történik. Az információk minősítését a 2009. évi CLV. törvény és a 243/2016. (VIII.17.) Korm. rendelet szabályozza.

- Tilos a hivatallal kapcsolatos belső információk nyilvános oldalakon való bárminemű közzététele.
- Tilos a munkavégzéssel kapcsolatos adatok továbbítására, tárolására nem magyarországi illetőségű email- és felhőszolgáltatás (pl. Gmail, Dropbox) igénybevétele.

Információbiztonsági vizsgálat, illetve hibakeresés céljából a hivatal informatikai rendszereinek teljes hálózati forgalma megfigyelhető és rögzíthető. A felhasználó az IBSZ ismeretéről és elfogadásáról szóló nyilatkozatával *(B02 Nyilatkozat az IT biztonsági szabályok elfogadásáról)* elfogadja, hogy a rendszer használata egyben a felhasználó beleegyezését is jelenti a figyelésbe és rögzítésbe. Elektronikus levelek esetén a megfigyelés nem terjed ki a levelek tartalmára. A levelek az alábbi technikai tulajdonságok alapján kerülnek vizsgálatra: kéretlen levelek, vírusokat tartalmazó levelek, informatikai támadásokat megvalósító üzenetek, adathalászatot megkísérlő üzenetek.

Ha a dolgozó internethasználata a munka elvégzésének rovására megy (pl. hivatali munkához nem kapcsolódó vagy nagy hálózati terhelést okozó tevékenységet folytat vagy biztonsági fenyegetést jelentő oldalakat látogat), az informatikus jelzi a dolgozó közvetlen vezetőjének, aki megteszi a szükséges intézkedéseket. Amennyiben az intézkedés eredménytelen marad, az érintett munkatárs vezetője utasítására a felhasználó internethozzáférését az informatikus részlegesen vagy teljesen letiltja.

Az internetkapcsolatok üzemeltetéséért felelős vezetőnek joga van az internethozzáférés tartalmi, időbeli, sávszélességbeli és szolgáltatásbeli korlátozásához, amennyiben ez az Internet önkormányzati célú használatának biztosításához szükségessé válik. A korlátozásról a felhasználókat előzetesen tájékoztatni kell.

3.5.1. Elektronikus levelezés (e-mail)

Az e-mail szolgáltatás a hivatal által a felhasználók részére a hivatali elektronikus levelezés céljaira biztosított eszköz. Az e-mail rendszer, valamint a rendszerben előállított, elküldött és megkapott levél is a hivatal felügyelete alá tartozik.

A hivatal elektronikus levelezési rendszere korlátozott mértékben, és a szabályzatban rögzített feltételek betartása mellett használható nem hivatali (személyes) levelezés céljára. Az elektronikus levelező rendszer felhasználója a rendszer használatával automatikusan aláveti magát ezeknek a korlátozásoknak.

A hivatal e-mail rendszerén mindennemű jogszabályellenes tartalom továbbítása és tárolása tilos.

A hivatal nevében folytatott elektronikus levelezésre kizárólag az erre a célra biztosított elektronikus levelezési cím, a rendszeresített levelező (kliens) program, illetve az informatikus által engedélyezett levelezési szolgáltatás használható. A beállítások (működési paraméterek) meghatározásáért és beállításáért az informatikus felelős.

Az elektronikus levelező rendszerben tárolt és továbbított dokumentumok elektronikus kezelésénél is be kell tartani az érvényben lévő ügyviteli, iratkezelési és adatkezelési szabályokat.

Minden elektronikus postaládával rendelkező felhasználó köteles elektronikus postaládájának tartalmát figyelemmel kísérni oly módon, hogy legalább a munkakezdéskor és a munkavégzés befejezését megelőzően meggyőződjön róla, hogy érkezett-e új üzenete, és amennyiben igen, akkor azokat érkeztesse, kezelje (tekintse meg, tegye meg a szükséges egyéb intézkedéseket).

Az elektronikus levelező rendszer használata során nem megengedett:

- nagy mennyiségű és méretű, személyes jellegű üzenetek küldése;
- kéretlen reklámok és hirdetések közzététele;
- lánclevelek terjesztése, továbbítása;
- a felhasználóknak a hivatali e-mail címüket nem hivatalos minőségben használni (pl. magánlevelezés, regisztráció letöltési oldalakon, online játék oldalakon stb.);
- a levelek fejlécének megváltoztatása, hamis levelek küldése;
- olyan üzenetek, illetve csatolt fájlok küldése, továbbítása, amelyek törvénytelenségeket vagy arra való felhívást tartalmaznak, fenyegetők, összességében sértik a hivatal jó hírét, általánosan elfogadott erkölcsi szabályba vagy jogszabályba ütköznek;
- a tévesen címzett, másnak szóló levelek felhasználása;
- a hivatal által biztosított e-mail címre érkező üzenetek átirányítása külső (nem a hivatal elektronikus levelező rendszerében létrehozott) e-mail címre.

A levelezési rendszer személyes célokra az elektronikus levelezésre vonatkozó szabályok betartásával és csak akkor használható, ha az nem sérti a hivatal érdekeit.

Az elektronikus levelek címzése során minden felhasználónak körültekintően kell eljárnia az alábbiak figyelembevételével:

- Csoportos levelező, elosztási lista (pl. „mindenki", „x osztály", „hivatali dolgozók") alkalmazása során meg kell győződni arról, hogy valóban szükséges-e minden, a csoportba tartozó címzett részére elküldeni az üzenetet.
- Titokvédelmi vagy egyéb biztonsági, bizalmassági okokból, amennyiben a levelek címzettjei nem szerezhetnek tudomást egymásról vagy egymás e-mail címéről, akkor a levél „Titkos másolat" (BCC) kategóriáját kell alkalmazni a címzés során.

Csoportos levelező, elosztási lista létrehozása iránti igényt a hivatali egység vezetőjének jóváhagyásával az üzemeltetői csoporthoz kell eljuttatni, amely a szükséges vizsgálatok, egyeztetések elvégzését követően az IBF közreműködésével dönt az igény kielégítéséről és intézkedik annak beállítása érdekében.

A központilag létrehozott csoportos levelező, elosztási listák karbantartása az informatikus feladata. Ennek elvégzéséhez a lista összeállítását kezdeményező hivatali egység, illetve a hivatal munkavállalóinak változása esetén a munkaügyi vezető köteles az informatikus számára adatokat biztosítani.

A hivatal a levelező rendszer működését akadályozó mennyiségű és méretű adat elektronikus levélként való továbbítását korlátozza. A küldhető csatolmányok típusáról és méretéről az informatikus ad kérésre felvilágosítást, valamint segítséget nyújt a nagyméretű fájlok küldésében.

A postaládára vonatkozó korlátozások

A felhasználó e-mail postaládájának mérete korlátozott, melynek méretét az informatikus határozza meg a technikai lehetőségek figyelembevételével. A meghatározottnál nagyobb postaládára vonatkozó igényt a hivatali egység vezetőjének jóváhagyásával az informatikushoz kell eljuttatni, aki a szükséges

vizsgálatok, egyeztetések elvégzését követően dönt az igény kielégítéséről és intézkedik annak beállítása érdekében.

Amennyiben a hivatali levelezésben – pontos címzés mellett – az elektronikus levelező rendszertől a kézbesítés során kézbesíthetetlenségre utaló hibajelzés érkezik, akkor a felhasználónak – szükség szerint az informatikus megkeresésével – fel kell tárnia ennek okát annak érdekében, hogy üzenete ne vesszen el.

Az elektronikus levelek méretét, valamint a levélhez csatolt fájlok típusát az informatikus korlátozhatja a rosszindulatú kódok terjedésének megakadályozása céljából és azért, hogy biztosítsa a hivatali levelezés megfelelő szolgáltatási szintjét. A korlátozás miatt nem továbbított levelekről, csatolt fájlokról a küldő értesítést kell kapjon.

Ismeretlen feladótól érkező, gyanús csatolt fájlt tartalmazó, vagy ismeretlen linket ajánló (pl. idegen nyelvű, láthatóan reklámcélú, olyan dokumentumra hivatkozó, amiről a címzett nem tud) elektronikus üzenetek csatolmányait, illetve a kapott linkeket nem szabad megnyitni, az ilyen leveleket törölni kell.

4. AZ INFORMATIKAI RENDSZEREK ÜZEMELTETÉSE

4.1. Általános rendelkezések

Az informatikus feladata a felhasználók informatikai támogatása, a szolgáltatások folyamatos, hivatali időben való rendelkezésre állásának biztosítása, a felmerülő biztonsági problémák azonosítása, azok megbízható kezelése és a biztonságért felelős személy tájékoztatása a felmerült problémákról, észlelt jelenségekről.

Az informatikus

- felelős az informatikai rendszer és a hálózat működőképességéért;
- felelős a hálózati szolgáltatások, csatlakozások üzembiztonságáért, koordinálásáért;
- gondoskodik az informatikai eszközök tervszerű megelőző karbantartásáról;
- felelős a folyamatos, hivatali időben való rendelkezésre állásért, a jelentkező hibák mielőbbi szakszerű ellátásáért.

A felhasználóknak tilos a gépek megbontása, a hardver konfigurációk megváltoztatása, a számítógépes hálózat megbontása, átstrukturálása, gépek, eszközök engedély nélküli csatlakoztatása.

A hivatal hálózatára számítógépet csak akkor lehet rácsatlakoztatni, ha a hálózati csatlakozás főbb paraméterei (fizikai és logikai címek, a hálózati struktúrában elfoglalt hely stb.) rögzítésre kerültek, és a csatlakozást az informatikus engedélyezte. Amennyiben valaki számítógépet vagy egyéb számítástechnikai berendezést önhatalmúlag csatlakoztat a hálózatra, úgy az informatikus köteles a berendezést azonnali hatállyal a hálózatról lekötni és az illetéktelen eszközcsatlakozást végrehajtó ellen vezetőjének bevonásával, felelősségének megállapítása érdekében fegyelmi, kártérítési, illetve egyéb eljárást kezdeményezni.

Tilos a felhasználóknak a hálózat kábeleinek szándékos kihúzása a fali csatlakozóból vagy a gépből. Számítástechnikai eszközt és tartozékait helyéről elvinni az informatikus és az eszköznyilvántartással foglalkozó hivatali egység tudta és engedélye nélkül tilos.

A számítógépes hálózathoz és az informatikai szolgáltatásokhoz a hozzáférés munkaidőben biztosított. Az ettől eltérő igényeket legkésőbb három munkanappal korábban kell jelezni az informatikus részére, aki amennyiben az üzemeltető személyzet biztosítható és technikailag is megoldható, akkor a hozzáférést lehetővé teszi.

A munka végeztével a felhasználónak az eszközök működésének megfelelően / üzemszerűen a használt alkalmazásokból ki kell jelentkeznie és ki kell kapcsolnia az informatikai eszközöket. A munkavégzés 15 percnél hosszabb átmeneti felfüggesztése esetén a használt alkalmazásokból, programokból ki kell lépni. Az informatikus által végzendő karbantartási, szoftver frissítési munkák időtartamában az informatikus kérésére az adott alkalmazásokkal történő munkavégzést 15 percen belül üzemszerű kilépéssel és/vagy leállítással be kell fejezni.

Az informatikai eszközöket rendeltetésszerűen kell használni: a számítógépen és perifériáin papírokat és egyéb tárgyakat tárolni nem lehet, a szellőző nyílásokat szabadon kell hagyni, a billentyűzetet védeni kell a szennyeződésektől, a számítógép közelében enni-inni, dohányozni nem szabad!

4.2. Konfigurációkezelés

4.2.1. Konfigurációkezelési eljárásrend

A hivatal...

- megfogalmazza, és a hivatalra érvényes követelmények szerint dokumentálja, valamint a hivatalon belül kihirdeti a konfigurációkezelési eljárásrendet, mely a konfigurációkezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- a fizikai védelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a konfigurációkezelési eljárásrendet;
- ha hatókörébe tartozik, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza...
  - a rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését;
  - a biztonsági funkciók hatékony alkalmazását és fenntartását;
  - a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket.
- megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely tartalmazza...
  - a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját;
  - a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit;
  - a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához;
  - gondoskodik arról, hogy az információs rendszerre vonatkozó – különösen az adminisztrátori és fejlesztői – dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható;
  - gondoskodik a dokumentációknak az érintett hivatal által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről.

4.2.2. Alapkonfiguráció

Az érintett adminisztrátorok és adatgazdák az IBF közreműködésével elektronikus információs rendszereikhez egy-egy alapkonfigurációt fejlesztenek ki, dokumentálják és karbantartják azt, leltárba foglalva annak lényeges elemeit *(B32 Konfigurációkezelési eljárásrend és alapkonfigurációk)*.

A hivatal az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa, valamint meghatározza a tiltott vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát. (legszűkebb funkcionalitás)

A hivatal...

- meghatározza a működési követelményeknek még megfelelő, de a biztonsági szempontból a lehető leginkább korlátozott módon – a „szükséges minimum" elv alapján – az elektronikus információs rendszerben használt információtechnológiai termékekre kötelező konfigurációs beállítást, és ezt ellenőrzési listaként dokumentálja (*B33 Kötelező konfigurációs beállítások ellenőrző listája*);
- elvégzi a konfigurációs beállításokat az elektronikus információs rendszer valamennyi elemében;
- a meghatározott elemek konfigurációs beállításaiban azonosít, dokumentál és jóváhagy minden eltérést;
- figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait, a hivatal belső szabályzataival és eljárásaival összhangban.

4.2.3. konfigurációváltozások felügyelete (változáskezelés)

A hivatal...

- meghatározza a változáskezelési felügyelet alá eső változástípusokat;
- meghatározza az egyes változástípusok esetén a változáskezelési vizsgálat kötelező és nem kötelező elemeit, előfeltételeit (csatolt dokumentációk, teszt jegyzőkönyvek stb.);
- megvizsgálja a változáskezelési felügyelet elé terjesztett, javasolt változtatásokat, majd kockázatelemzés alapján jóváhagyja, vagy elutasítja azokat;
- dokumentálja az elektronikus információs rendszerben történt változtatásokra vonatkozó döntéseket;
- megvalósítja a jóváhagyott változtatásokat az elektronikus információs rendszerben;
- visszakereshetően megőrzi az elektronikus információs rendszerben megvalósított változtatások dokumentumait, részletes leírását;
- auditálja és felülvizsgálja a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket.

Előzetes tesztelés és megerősítés

A konfiguráció megváltoztatása előtt az új verziót tesztelni kell, ezután dönteni kell annak megfelelőségéről, továbbá dokumentálni kell az elektronikus információs rendszer változtatásait az éles rendszerben történő megvalósítása előtt.

4.3. Szoftverhasználat korlátozásai

A hivatal bármely informatikai rendszerére csak az informatikus telepíthet szoftvert, *a felhasználónak szoftvertelepítésre és bizonyos beállítások módosítására nincs sem joga, sem lehetősége.* A hivatal

informatikai eszközeire TILOS illegális és/vagy nem jogtiszta szoftvert telepíteni! A hivatal informatikai infrastruktúrájában a feladatok végrehajtására kizárólag a hivatal által megvásárolt licencű kereskedelmi szoftver termékeket és/vagy szabad szoftvereket lehet alkalmazni. Minden illegális, vagy nem a munkavégzést szolgáló szoftvert, adatot törölni kell a rendszerből. Ezt a műveletet a felhasználó tudtával az informatikus végzi el.

Illegális szoftverek használata esetén a felhasználóval szemben felelősségének megállapítása érdekében fegyelmi, kártérítési, illetve egyéb eljárás indulhat.

A telepítést megelőzően a hivatalban vírusvédelmi célokra üzembe állított eszközzel meg kell vizsgálni a szoftver esetleges vírusfertőzöttségét. Amennyiben technikailag/technológiailag lehetséges, úgy az új szoftvercsomagról biztonsági másolatot kell készíteni. Az installálást csak a munkapéldányról szabad végezni. Az eredeti példányt biztonságos helyen kell tárolni.

A hivatal infrastruktúrájában található eszközökre idegen program, adat másolása tilos!

4.3.1. Felhasználó által telepíthető szoftverek

A felhasználók az informatikai eszközöket hivatali munkavégzés céljára kapják. A felhasználók jogosultsága a belső hálózaton csak a rendszergazda által telepített egységes irodai alkalmazások és szolgáltatások használatára, illetve a munkájukhoz szükséges alkalmazói programok futtatására terjed ki. A hivatal informatikai infrastruktúráját magán célú használatra igénybe venni TILOS!

Ettől eltérni csak a hivatal vezetője vagy az Információbiztonsági Felelős (IBF) írásbeli engedélyével, akkor is kizárólag mobil eszközök esetében szabad (notebook, tablet, mobiltelefon, mobil adathordozók). Az engedély feltétele felhasználói nyilatkozat tétele arról, hogy az adott felhasználó - a tűzfallal leválasztott nyilvános részek (pl. free/vendég wifi) kivételével (*6.2. pont*) - nem használja a hivatal belső informatikai struktúráját *(B34 IT eszköz kivonási kérelem)*. Ebben az esetben a felhasználót a kockázatokról tájékoztatni kell, aki a nyilatkozattétellel lemond a hivatal nem nyilvános hálózatának bármilyen használati lehetőségéről és a kivont eszköz hardver- és szoftverkarbantartását is átvállalja. Karbantartási kötelezettsége nem terjed ki garanciális javítás ügyintézésére, azt továbbra is az informatikai üzemeltetésért felelős hivatali egység feladata.

4.4. Adathordozók védelme

4.4.1. Adathordozók védelmére vonatkozó eljárásrend

A hivatal által használt hordozható külső adattárolókat (pl. flash diskek, pendrive-ok, memóriakártyák, hordozható HDD-k) egyedi azonosítóval kell ellátni, kivételt képeznek ez alól az optikai adathordozók (CD, DVD) és a hajlékonylemezek, amely tárolók csak számszerűen kerülnek nyilvántartásba. Az egyedi azonosítóval ellátott hordozható adathordozók pontos helyéről naprakész adatbázist kell vezetni *(B35 Mobil adattárolók nyilvántartása)*.

A használni kívánt adattárolót a tárolásra kijelölt helyről kell kivenni és használatot követően oda kell visszahelyezni. A munkaasztalokon és a számítógépekben csak azok az adathordozók lehetnek, amelyek a munkavégzéshez szükségesek.

Fontos adatokat tartalmazó adathordozókról másolatot kell készíteni, melyeket egymástól elkülönítetten, lehetőleg külön szobában, szekrényben kell elhelyezni.

4.4.2. Adathordozók használata, hozzáférés az adathordozókhoz

A hivatali informatikai rendszerekben kezelt adatok, dokumentumok (a 2013. évi L. törvény által definiált) bizalmasságát, hitelességét, sértetlenségét és rendelkezésre állását biztosítani kell, ezért a hivatal nyilvántartást vezet az egyes adathordozó-típusokhoz való hozzáférésre feljogosított személyek köréről, valamint jogosítványuk tartalmáról. A nyilvántartást a hivatal rendszeres időközönként felülvizsgálja, aktualizálja *(B35 Mobil adattárolók nyilvántartása)*.

Minden munkatársnak kötelessége az adattárolók rendeltetésszerű használata. A hivatal adathordozói csak a munkavégzéshez szükséges adatok és szoftverek tárolására hivatottak. A hivatal tulajdonában lévő hordozható külső adattárolók (flash diskek, pendrive-ok, memóriakártyák, hordozható HDD-k) hivatalon kívüli használata csak kivételes esetben, írásbeli vezetői engedéllyel lehetséges.

A felhasználók külső adathordozót az informatikai hálózatra csak a jegyző vagy az informatikus írásbeli engedélyével, vírusellenőrzés után csatlakoztathatják. A vírusellenőrző programot lehetőség szerint úgy kell beállítani, hogy automatikusan elvégezze az ellenőrzést külső eszköz csatlakoztatásakor.

Meghibásodás esetén a munkatársak kötelesek jelenteni azt az informatikus felé. A további felhasználásra alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni. A bizalmas adatokat tartalmazó adathordozókról törlő programokkal kell az adatokat eltávolítani, majd ezt követően kell fizikailag megsemmisíteni. Eszköz külső partner által történő szervizelése esetén a szállítás előtt gondoskodni kell az adathordozó tartalmának visszaállíthatatlan módon történő törléséről. Meghibásodott eszköz cseréje esetén – garanciális esetben is – adathordozó csak úgy vihető ki a hivatal területéről, ha arról minden adat visszaállíthatatlan módon törlésre került.

4.4.3. Adathordozók újrafelhasználása, leselejtezése, megsemmisítése

Az adathordozók biztonságához szorosan kapcsolódik az, hogy adathordozók újrafelhasználása, illetve selejtezése után is biztosítani kell a védendő adatok bizalmasságát.

Amennyiben az adathordozó eszközök (flash diskek, pendrive-ok, memóriakártyák, hordozható HDD-k) újrafelhasználásra kerülnek, úgy biztosítani kell, hogy az új felhasználó(k) jogosulatlanul ne férjenek hozzá a korábban az eszközön tárolt adatokhoz (pl. munkaállomás használható merevlemezének más munkaállomásba szerelése esetén). Ebben az esetben az eszközökön biztonságos törlést kell végrehajtani úgy, hogy a teljes adathordozón található valamennyi adat, partíció legalább háromszor kerüljön felülírásra véletlen adatfolyammal. Azt, hogy az adathordozó törlése sikeres volt-e, a törlést végző minden esetben ellenőrzi. Azokat az adathordozókat, amelyeket nem lehet engedélyezett módon törölni, újra felhasználni tilos, az ilyen eszközöket fizikailag meg kell semmisíteni.

Amennyiben az adathordozó oly mértékben sérült vagy elhasználódott, hogy a további használata lehetetlen vagy célszerűtlen, úgy azt selejtezni, majd fizikailag meg kell semmisíteni.

A selejtezési eljárás folyamán az adathordozókon olyan eljárást kell végrehajtani, amelyek megakadályozzák azt, hogy a későbbiekben ezekről az eszközökről adatokat lehessen visszanyerni. Ennek megfelelően a következő adatmegsemmisítési módszerek kerülnek meghatározásra: FDD, CD, DVD, pendrive, SSD esetén az erre alkalmas adatmegsemmisítő eszközzel be kell zúzni azokat. Merevlemezek esetén a mágneslemezeket el kell távolítani az eszközből, majd az erre alkalmas adatmegsemmisítő eszközzel be kell zúzni azokat.

4.5. Felkészülés a rendkívüli helyzetekre, katasztrófákra

A hivatal teljes informatikai rendszerére *B36 Informatikai Működésfolytonossági- és Katasztrófa-Elhárítási Terv* készül, amely megfogalmazza, hogyan lehet a hivatal kritikus funkcióit üzemben tartani vagy biztonságos üzemüket minél hamarabb visszaállítani a különböző mértékű problémák bekövetkezése esetén.

A hivatal...

- összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;
- meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági tervet;
- az elektronikus információs rendszer vagy a működtetési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálja az üzletmenet-folytonossági tervet;
- tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és hivatali egységeket;
- gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható;
- meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;
- rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről;
- jelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket;
- fenntartja a hivatal által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is;
- kidolgozza a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

A *B36 Informatikai Működésfolytonossági- és Katasztrófa-Elhárítási Terv* tartalmazza többek között a kritikus fontosságú rendszerek és erőforrások azonosítását, azok alapfeladatait, alapfunkcióit, a rendelkezésre állás biztosításának módját (redundáns rendszerek, tartalékképzés stb.), az ehhez kapcsolódó vészhelyzeti követelményeket, valamit a hivatali adatvagyon mentési- archiválási- és helyreállítási rendjét.

A kidolgozott stratégiák (előkészületek, eljárások dokumentálása, oktatás) megvalósításához a *B36 Informatikai Működésfolytonossági- és Katasztrófa-Elhárítási Terv*ben foglaltak szerint felelősöket kell kijelölni. A tervet az elektronikus információs rendszer vagy a működtetési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálni kell. A terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és hivatali egységeket minden esetben tájékoztatni kell.

4.6. Az elektronikus információs rendszer mentései

A hivatali informatikai rendszerekben kezelt adatok, dokumentumok bizalmasságát, hitelességét, sértetlenségét és rendelkezésre állását biztosítani kell.

A biztonsági mentések gyakoriságának összhangban kell állnia a mentett adatok, illetve programok biztonsági besorolásával, elvesztésük, sérülésük kockázatával és hatásával *(B09 IT kockázatértékelés)*, valamint a hivatal ügyintézési ciklusával.

Az informatikai infrastruktúrában a biztonsági mentési eljárást, annak pontos leírását, valamint az ehhez tartozó feladatokat, szabályokat a *B37 Mentési rend* című dokumentum szabályozza részletesen a következő alapelvek betartásával. A dokumentum elkészítésért az informatikus felelős.

Az informatikus feladata a felhasználói rendszerekben leírtakon felüli *rendszeres és időszakos biztonsági mentések elvégzése*. A mentéseket úgy kell végezni, hogy az adatbázisok konzisztenciája biztosítva legyen, illetve az egyéb munkaállomások hálózati munkáját ne akadályozza.

A mentési rendszert a technológiai és gazdasági lehetőségek figyelembevételével a lehető legnagyobb mértékben automatizálni kell, hogy minimalizálni lehessen az emberi tényezőből adódó hibák előfordulásának valószínűségét Ennek koordinációjáért és a szükséges források tervezéséért az informatikus felelős.

A szoftverekről változtatás előtt biztonsági mentést kell készíteni, melynek felelőse a rendszergazda. *A mentést követően az adathordozót a szerver szobától eltérő helyiségben* (lehetőség szerint a szerverszobával nem azonos épületben), erre a célra rendszeresített biztonsági szekrényben, elzárva kell tárolni. Törekedni kell arra, hogy a mentések tárolása fizikailag biztonságos legyen, védeni kell őket az illetéktelen hozzáférésektől, illetve a különböző fizikai behatásoktól (tűz, víz, mágnesesség stb.). A biztonsági mentéseket hibajelzésmentesen, visszatölthető módon kell elkészíteni. Ennek érdekében a mentések felhasználhatóságát, amennyiben technikailag lehetséges, szúrópróbaszerűen tesztelni kell, illetve a mentési eljárásba épített automatikus ellenőrzéseket kell végrehajtani. Ennek betartásáért a biztonsági mentés elvégzésével megbízott rendszergazda tartozik felelősséggel. Sikertelen mentés esetén a lehető legrövidebb időn belül meg kell ismételni a mentést.

A 466/2017. (XII. 28.) Korm. rendeletben foglalt archiválási kötelezettségnek a hivatal az önkormányzati ASP rendszer útján tesz eleget.

4.6.1. A felhasználók adatainak mentése

A felhasználók munkaállomásokon lévő adatait a mentési eljárások nem kezelik, ezért *a felhasználók a munkájukhoz tartozó fontos dokumentumokat a fájlszerverek megfelelő kijelölt területein kötelesek tárolni!*

A mentés elmaradásából eredő, a szerverre nem mentett adatok helyreállításának hibáiért, vagy ennek lehetetlenségéért a felhasználó a felelős. A hivatal által kiadott notebook-ok adatainak mentését az informatikus kérésre elvégzi, a felhasználókkal történt előzetes egyeztetés után. A felhasználók adatainak DVD-re írását, - ha az iroda nem rendelkezik saját DVD-íróval, - kérésre az informatikus végzi. A felhasználók által írt adathordozókon található adatok jogtisztaságáért a felhasználó a felelős.

A munkaállomások a felhasználó munkakörétől és jogosultságtól függően tartalmazhatnak adat be- és kiviteli eszközöket (FDD, CD, DVD, USB), de ezek használata korlátozott, az eddigiekben leírtak szerint történik. A mobil adathordozók használatát kerülni kell! A már nem használt, megrongálódott vagy selejtezendő adathordozókat a felhasználók kötelesek leadni.

4.6.2. A szervereken tárolt adatok mentése

A központi szervereken tárolt elektronikus információvagyont a biztonsági káresemények ellen szintén mentéssel védi az üzemeltetői csoport. A rendszer egészéről a *B37 Mentési rend* című dokumentumban leírtaknak megfelelően teljes mentést kell készíteni. A mentéseket minden mentési rendet érintő (fizikai, logikai, vagy adminisztratív) változáskor, de legalább évente egyszer ellenőrizni kell aszerint, hogy visszatöltésük, helyreállításuk valóban működik-e. Az ellenőrzéseket dokumentálni kell a *B37 Mentési rend* dokumentumon.

A mentések rendjét, valamint az esetleges helyreállítási tervet a rendszerszintű leírásoknak, illetve *B37 Mentési rend*nek kell tartalmaznia.

4.7. Az elektronikus információs rendszer helyreállítása és újraindítása

A hivatal informatikusa a *B36 Informatikai Működésfolytonossági- és Katasztrófa Terv*ben leírtaknak megfelelően gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

4.8. Karbantartás

4.8.1. Rendszer karbantartási eljárásrend

A hivatal...

- megfogalmazza, és a hivatalra érvényes követelmények szerint dokumentálja, valamint a hivatalon belül kihirdeti a rendszer karbantartási eljárásrendet (*B39 Karbantartási rend*), mely a rendszer karbantartási kezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- a fizikai védelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a rendszer karbantartási eljárásrendet.
- kialakít egy folyamatot a karbantartók munkavégzési engedélyének kezelésére, és nyilvántartást vezet a karbantartó szervezetekről vagy személyekről;
- megköveteli a hozzáférési jogosultság igazolását az elektronikus információs rendszeren karbantartást végzőktől;
- felhatalmazást ad a hivatalhoz tartozó, a kívánt hozzáférési jogosultságokkal és műszaki szakértelemmel rendelkező személyeknek arra, hogy felügyeljék a kívánt jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.

4.8.2. Rendszeres karbantartás

A hivatal...

- a karbantartásokat és javításokat ütemezetten hajtja végre (B39 Karbantartási rend), dokumentálja és felülvizsgálja a karbantartásokról és javításokról készült feljegyzéseket (*B40 Karbantartási napló*) a gyártó vagy a forgalmazó specifikációinak és a hivatali követelményeknek megfelelően;

- jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;
- az ezért felelős személyek jóváhagyásához köti az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a hivatali létesítményből (*B22 IT eszköz kiviteli-behozatali engedélye*);
- az elszállítás előtt minden adatot és információt – mentést követően – töröl a berendezésről;
- ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;
- csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási nyilvántartáshoz (*B40 Karbantartási napló*);

5. RENDSZER- ÉS INFORMÁCIÓ SÉRTETLENSÉG

Ezeket a rendelkezéseket egy adott elektronikus információs rendszer tekintetében abban az esetben kell alkalmazni, ha az adott elektronikus információs rendszert a hivatal üzemelteti. Üzemeltetési szolgáltatási szerződés esetén szerződéses kötelemként kell az alábbiakat érvényesíteni, és azokat a szolgáltatónak kell biztosítania.

5.1. Rendszer- és információsértetlenségre vonatkozó eljárásrend

A hivatal...

- megfogalmazza, és a hivatalra érvényes követelmények szerint dokumentálja, valamint a hivatalon belül kihirdeti a rendszer- és információsértetlenségre vonatkozó eljárásrendet, mely a hivatal informatikai biztonsági szabályzatának részét képező, rendszer- és információsértetlenségre vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- a rendszer- és információsértetlenségre vonatkozó eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a rendszer- és információsértetlenségre vonatkozó eljárásrendet.

5.2. Felügyelet

A biztonsági események olyan események, melyek eltérnek a megszokott ügymenettől, zavarokat okozhatnak és fenyegethetik az információk, illetve az információ feldolgozó eszközök bizalmasságát, sértetlenségét és rendelkezésre állását.

Az információbiztonsági incidensek az IBF vagy a hivatal vezetője által minősített olyan biztonsági események, melyek ténylegesen fenyegetik az információk, illetve az információfeldolgozó eszközök bizalmasságát, sértetlenségét és rendelkezésre állását.

Minősített incidens a hibás működés, mely a rendszerelemek (hardverek, szoftverek, adathordozók) rendeltetésszerű használata közben fellépő, normál működéstől eltérő viselkedését jelenti.

A védelem gyenge pontjai a rendszer, a folyamatok, illetve az abban részt vevő személyek olyan tulajdonságai, hiányosságai, melyek biztonsági incidensek kialakulásához vezethetnek.

Biztonsági eseményt, illetve a védelem gyenge pontjait a hivatal minden munkatársa, a rendszereket használó szerződött partnere és a projektekbe bevont harmadik felek észlelhetik, illetve annak létét feltételezhetik. Biztonsági eseményre utaló jelek lehetnek többek között:

- Adatok, információk, fájlok eltűnése, módosulása;
- Információ feldolgozó eszközök, adattárolók eltűnése, rongálódása;
- Információ feldolgozó eszközök megszokottól eltérő működése;
- Adatátvitel szokásostól eltérő lelassulása;
- Bizalmas információk nem ellenőrzött, külső csatornából történő visszahallása.

Elsődleges szabály, hogy az információbiztonsági incidensek gyanújának felmerülésekor (incidens észlelésekor) azonnal értesíteni kell az információbiztonsági felelőst (IBF) és az informatikust. TILOS az incidens körülményeit vizsgálni, illetve megkísérelni elhárítani azt!

5.2.1. Felügyeleti eszközök

A hivatal az információs rendszerei meghatározott alapvető attribútumainak (pl. merevlemez telítettség, CPU használat) gyűjtésére és elemzésére automata felügyeleti eszközöket alkalmaz. A gyűjtendő információkat az érintett rendszer dokumentációja tartalmazza. Az elektronikus információs rendszerben üzemelő aktív elemek üzemállapotának megfigyelése, forgalmának nyomon követése csak az informatikai vezető engedélye és az érvényes törvények betartása mellett lehetséges, az általa kijelölt hardver- és szoftvereszközökkel. A diagnosztikai megfigyelő tevékenységet csak az informatikai vezető által felhatalmazott személyek végezhetnek. Minden egyéb állapot-, illetve forgalomfigyelő tevékenység gyakorlása szigorúan tilos.

Az elektronikus információs rendszer felügyeleti információt az IBF havi vagy negyedéves rendszerességgel elemzi, igény esetén jelentést készít azokról. Fokozott kockázatra utaló jelek észlelése esetén javaslatokkal él *(B41 Rendszerfelügyeleti információs jelentés)*.

5.2.2. Biztonsági riasztások és tájékoztatások

A hivatal...

- folyamatosan figyeli a Kormányzati Eseménykezelő Központ (GovCERT-Hungary) által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;
- folyamatosan figyelemmel kíséri a Nemzeti Elektronikus Információbiztonsági Hatóságtól (NEIH) érkező értesítéseket;
- szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki (*B46 IT biztonsági riasztási napló*)
- a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez;
- kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, és kapcsolatot tart az érintett, jogszabályban meghatározott szervekkel;
- megfelelő ellenintézkedéseket és válaszlépéseket tesz.

5.3. Incidensek kezelése

Az incidensek kezelése során a hivatal vezetője és az IBF döntenek a szükséges lépésekről, de döntésük során figyelembe kell venniük az alábbi főbb irányelveket. A döntésekről írásban értesítik az informatikust, aki felelősséggel tartozik azok haladéktalan végrehajtásáért.

A biztonsági incidensek érintett rendszerelemeit, a minősítést követően lokalizálni kell és megakadályozni az esetleges tovább terjedést (hálózatról leválasztani, internet kapcsolatot megszüntetni, hardverelemet kiemelni stb.).

Be kell gyűjteni az összes releváns adatot és bizonyítékot a biztonsági incidensről (naplóbejegyzések, okozott jelenségek stb.) és az okozott fennakadásokról, károkról.

Gondoskodni kell a károk enyhítéséről. Biztosítani kell a hivatali funkcionalitás minimálisan elvárt szintű (az érintett vezetők határozzák meg) visszaállítását (ha az sérült) a biztonsági incidens megismétlődését kizáró, vagy a megismétlődést elfogadható kockázatúra csökkentő módon.

Biztosítani kell a hivatali funkcionalitás teljes körű visszaállítását.

5.3.1. Tanulás az incidensekből

Az IBF az Incidens nyilvántartást *(B10 IT biztonsági események naplója)* minden évben a vezetőségi átvizsgálás előtt felülvizsgálja. Ezen felülvizsgálat során különös figyelmet fordít...

- az ismétlődő incidensek azonosítására;
- az incidensek megfelelő kezelésének vizsgálatára;
- az incidensek előfordulási valószínűségét csökkentő, átfogó, az elektronikus információs rendszert érintő fejlesztési lehetőségek azonosítására.

A felülvizsgálatokról jelentést készít a hivatal vezetésének, melyben értékeli az incidenseket és ha szükséges, megelőző, helyesbítő intézkedéseket kezdeményez *(B42 Incidens-felülvizsgálati jelentés)*.

5.4. Naplózás

A hivatal informatikai rendszereinek tervezésekor rögzített naplózási szabályokat kell alkalmazni. Ennek során az alábbi alapelveknek kell megfelelni:

- A hivatal az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.
- Az egyedi elszámoltathatóság érdekében a naplózási funkciókat úgy kell beállítani, hogy a felhasználói tevékenységek személyre szólóan nyomon követhetők legyenek (*B45 Naplófájlok listája*).
- Az események és problémák azonosítása érdekében a napló tartalmazza a problémák megoldásához szükséges adatokat.
- A visszaélések felderítése érdekében a jogosult felhasználói tevékenységek és jogosulatlan tevékenységekre irányuló kísérletek naplózásra kerülnek.
- A hivatal minden rendszerében megbízható módon védeni kell az ott keletkezett naplóállományokat a jogosulatlan felfedés, módosítás és törlés ellen.
- A naplóállományok ellenőrzését az informatikus végzi. Az ellenőrzéseknek rendszeresen, legalább kéthetente kell megtörténnie. Az ellenőrzések hatékonyságának növelésére automata ellenőrzőszoftvert is lehet alkalmazni, amennyiben ez az adott rendszeren technológiailag lehetséges.
- Az Informatikuson túl a naplóállományok adattartalmába betekinthetnek:
  - IBF;
  - az informatikus vagy az IBF által írásban felhatalmazott szakember.

Az elektronikus információs rendszer:

- naplózási hiba esetén riasztást küld a meghatározott személyeknek vagy szerepköröknek;
- elvégzi a meghatározott végrehajtandó tevékenységeket, így például a rendszer leállítását, a legrégebbi naplóbejegyzések felülírását, a naplózási folyamat leállítását;
- belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához;
- időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz – úgynevezett UTC – vagy a Greenwichi középidőhöz – úgynevezett GMT – rendelhető módon, megfelelve a hivatal által meghatározott időmérési pontosságnak.

5.4.1. Naplózható események

A hivatal...

- meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét;
- egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő hivatali egységgel, hogy növelje a kölcsönös támogatást, és hogy iránymutatással segítse a naplózható események kiválasztását;
- megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

5.4.2. Naplóinformációk védelme

Az elektronikus információs rendszert úgy kell felépíteni, hogy az megvédje a naplóinformációkat és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

5.4.3. Napló tárkapacitás

A hivatal a naplózásra elegendő méretű tárkapacitást biztosít, a biztonsági osztályba sorolásból következő naplózási funkciók figyelembevételével.

5.4.4. Naplózási hiba kezelése

Az elektronikus információs rendszer...

- naplózási hiba esetén riasztást küld a meghatározott személyeknek vagy szerepköröknek;
- elvégzi a meghatározott végrehajtandó tevékenységeket, így például a rendszer leállítását, a legrégebbi naplóbejegyzések felülírását, a naplózási folyamat leállítását.

5.4.5. Naplóvizsgálat és jelentéskészítés

A hivatal...

- rendszeresen felülvizsgálja és elemzi a naplóbejegyzéseket (*B45 Naplófájlok listája*) nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából (*B43 Naplóelemzés-jelentés*);
- jelenti ezeket a meghatározott személyeknek vagy szerepköröknek.

5.5. Kártékony kódok elleni védelem

A lehetséges információbiztonsági fenyegetések közül igen jelentős kockázatot jelentenek a rosszindulatú programok és kódok, a levélszemetek (spam) és a káros Internet tartalmak. A felsorolt negatív elemek ellen számos technológiai eszközzel lehet védekezni, ilyenek a biztonságos átjárók, tűzfalak, vírusvédelmi eszközök, levélszemét szűrő szoftverek, IDS-ek és IPS-ek.

A hálózati határvédelem elsősorban a megelőzésre, másodsorban az elhárításra szolgál. A vírustámadások nagy része az internet, és a levelező rendszerek közreműködésével valósul meg.

A hivatal számítógépes hálózatát, szervereit és munkaállomásait folyamatosan, illetve egy adott számítástechnikai eszközt a felhasználó jelzése alapján vírusvédelmi szempontból figyelni kell. A vírusfertőzés ellenőrzéséről és annak eredményéről nyilvántartást kell vezetni (a legtöbb vírusvédelmi rendszer ezt magától megteszi).

A preventív vírusvédelmet, a tartalom- és spamszűrést és a hálózati határvédelmet hardvereszközök és szoftveres megoldások biztosítják. Ezek kiszűrik a vírusos üzeneteket és a kéretlen leveleket, valamint *letiltják meghatározott weblapok megnyitását*. A honlapok megnyitásának korlátozását elsősorban a Nemzeti Kibervédelmi Intézet (GovCERT-Hungary) által közzétett tiltólistákból, másodsorban helyi tiltólistákból kell előállítani.

A hálózati határvédelem eszközeinek működését folyamatosan ellenőrizni kell, a szoftverrendszer elemeinek (programok, szabályrendszerek, vírusdefiníciós adatbázisok, listák) frissítéséről automatizált módszerrel gondoskodni kell. A frissítések hiba nélküli megtörténtét ellenőrizni kell.

Valamennyi felhasználónak kötelessége minden tőle telhetőt megtenni annak érdekében, hogy olyan fájl (szoftver, dokumentum stb.), amely rosszindulatú kódot, tartalmat tartalmaz, ne kerüljön fel a felhasználók munkaállomásaira, hordozható számítógépeire (laptop), sem pedig a hálózati adattárolókra.

A fentiek miatt mind a munkaállomásokon, mind a szervereken védelmi szoftvereket kell alkalmazni. A hivatalban a hálózati határvédelmi illetve vírusvédelmi funkciókat a hivatal *B36 Informatikai működésfolytonossági- és katasztrófaterv*ben felsorolt szoftverek valósítják meg.

A határvédelem folyamatára az alábbi szabályok érvényesek:

- A határvédelmi programoknak folyamatosan kell működniük. A programoknak folyamatosan vizsgálniuk kell a bejövő és kimenő hálózati forgalmat (pl. levelezés, web).
- A vírusvédelemnek a klienseken rezidens módon kell futniuk, azaz a rendszer indulásakor automatikusan indul a program, illetve rendszeres időközönként vírusellenőrzést kell végrehajtani a klienseken, amely vizsgálatok eredményét ellenőrizni kell. A vírusvédelemnek a rendszer alábbi komponenseire kell kiterjednie: fájlok, rendszeradatok, hálózati web- és emailforgalom.
- A felhasználóknak a vírusvédelmi alkalmazások működését tilos leállítani!
- A felhasználónak tilos vírusirtót, személyes tűzfalat vagy egyéb biztonsági szoftvert telepíteni.
- A határvédelmi szoftverrendszer elemeinek (programok, szabályrendszerek, vírusdefiníciós adatbázisok) frissítéséről automatizált módszerrel kell gondoskodni. A frissítések hiba nélküli megtörténtét ellenőrizni kell.
- Külső helyekről származó adattárolókat csak hivatali okból szabad használni és a használat előtt vírusellenőrzésnek kell alávetni. Az adattárolók csak akkor használhatók, ha az ellenőrzés vírusfertőzést nem jelez.

- Vírusfertőzés gyanúja vagy nem üzemszerű működés esetén a felhasználóknak haladéktalanul értesíteni kell az informatikust, aki megvizsgálja az eseményt és hiba esetén elhárítja azt.
- Vírusfertőzés gyanúja esetén az informatikus és/vagy az IBF a fertőzött gépet lezárhatja, annak használatát a hiba elhárításáig felfüggesztheti.

5.6. Hibajavítás, biztonsági frissítések

A hivatal által használt szoftverek hibáinak napvilágra kerülése esetén számítani lehet arra, hogy az ártó szándékú támadók ezeket a biztonsági réseket kihasználva próbálnak az információs rendszerbe behatolni, ezért elengedhetetlen, hogy a szoftver gyártója által készített javítások (frissítések) a lehető leghamarabb telepítésre kerüljenek.

A hivatal informatikusa a fentiek megvalósulása érdekében...

- azonosítja, belső eljárásrendje alapján jelenti és kijavítja vagy kijavíttatja az elektronikus információs rendszer hibáit;
- telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket az érintett hivatali egység feladatellátásának hatékonysága, a szóba jöhető következmények szempontjából;
- a biztonságkritikus szoftvereket a frissítésük kiadását követően a lehető legrövidebb időn belül telepíti vagy telepítteti;
- beépíti a hibajavítást a konfigurációkezelési folyamatba.

6. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

6.1. Rendszer- és kommunikációvédelmi eljárásrend

A hivatal...

- megfogalmazza, és a hivatalra érvényes követelmények szerint dokumentálja, valamint a hivatalon belüli szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a rendszer- és kommunikációvédelmi eljárásrendet, mely a rendszer- és kommunikációvédelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- a rendszer- és kommunikációvédelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a rendszer- és kommunikációvédelmére vonatkozó eljárásrendet.

6.2. Határok védelme

Az elektronikus információs rendszer felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt. A zónák közötti kommunikáció csak szabályozott formában, határvédelmi rendszer beiktatásával biztosítható. Jelen fejezetben rögzített szabályok betartása alapvető követelmény, megszegése súlyos biztonsági eseménynek tekintendő.

A hivatal belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán, valamint engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.

Alapvető szabályok:

- A különböző zónák (pl. intranet -> internet) közötti kommunikáció tűzfal által kontrollált.
- Ha egy kommunikációs csatorna nincs külön engedélyezve, az tiltott.
- Az egyes hálózati zónák közötti kapcsolat létrehozásakor az alábbiakat kell figyelembe venni:
  - a kapcsolat legyen megfelelő erősségű titkosítással biztosítva;
  - a kapcsolat legyen megfelelő erősségű azonosítási algoritmussal ellátva.
- A kapcsolat megvalósításához ajánlott technológiák (ebben a sorrendben):
  - VPN kapcsolat kiépítése
  - SSL/TLS kapcsolat kiépítése
  - egyedi, titkosított és azonosított kapcsolat kiépítése

Az alkalmazott tűzfal beállításainak meghatározása a rendszergazda hatáskörébe tartozik, melyet az IBF véleményezhet. A tűzfal-konfiguráció módosításának igényét, valamint annak jóváhagyását és végrehajtását dokumentálni kell. A módosítás végrehajtása a kijelölt rendszergazda feladata.

A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban kell elhelyezni, elkülönítve a belső hivatali hálózattól.

A hálózati határvédelem eszközeinek működését folyamatosan ellenőrizni kell, annak rendszeres frissítéséről kiemelt figyelemmel kell gondoskodni!

6.3. Kriptográfiai kulcsok előállítása és kezelése

Az elektronikus információs rendszer szabványos, a jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg.

Az elektronikus információs rendszer meggátolja az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha a hivatal engedélyezte azt, és közvetlen jelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

Az elektronikus információs rendszer elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.

6.4. Hitelesítés szolgáltatók tanúsítványának elfogadása

Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság (NMHH) elektronikus aláírással kapcsolatos nyilvántartásában szereplőhitelesítés szolgáltatók által kibocsátott tanúsítványokat fogadhatja el a hivatalon kívüli felhasználók hitelesítéséhez.

Az elektronikus információs rendszer egy adott kriptográfiai modulhoz való hitelesítésre olyan mechanizmusokat használ, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának.

6.5. Biztonságos név/cím feloldó szolgáltatások

Az elektronikus információs rendszer a név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó kiegészítő adatokat is biztosít, és ha egy elosztott, hierarchikus névtár részeként működik, akkor jelzi az utódtartományok biztonsági állapotát is,

és (ha azok támogatják a biztonságos feloldási szolgáltatásokat) hitelesíti az utód- és elődtartományok közötti bizalmi láncot.

Biztonságos név/cím feloldó szolgáltatás (úgynevezett rekurzív- vagy gyorsítótárat használó feloldás). Az elektronikus információs rendszer eredethitelesítést és adatsértetlenség ellenőrzést kér és hajt végre a hiteles forrásból származó név/cím feloldó válaszokra.

Architektúra és tartalékok név/cím feloldási szolgáltatás esetén azok az elektronikus információs rendszerek, amelyek együttesen biztosítanak név/cím feloldási szolgáltatást egy hivatal számára, hibatűrők és belső/külső szerepkör szétválasztást valósítanak meg.

6.6. Túlterheléses (szolgáltatás megtagadás alapú) támadás elleni védelem

Az elektronikus információs rendszer véd a túlterheléses (úgynevezett „szolgáltatás megtagadás") jellegű támadásokkal szemben, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján, a meghatározott biztonsági intézkedések bevezetésével.

6.7. Záró rendelkezések

Ez a szabályzat 2017. december 14-étől lép hatályba, ettől az időponttól kezdődően a korábban hatályos Informatikai Biztonsági Szabályzat hatályát veszti.

7. MELLÉKLETEK

IBSZ 1. számú melléklet - Biztonsági osztályba sorolás

Adatbiztonság szempontjából a hivatal kezelésében lévő elektronikus formában tárolt információkat, eszközöket, erőforrásokat és szolgáltatásokat a kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából 1-től 5-ig terjedő skálán – a kockázat növekedésével arányosan növekvő - biztonsági osztályokba kell sorolni. A besorolás eredményét melléklet formában rögzíteni kell a *B07 Informatikai Biztonsági Szabályzat*ban is.

A hivatal NEIH által megadott besorolása: 3. biztonsági osztály

A besorolást minimum 2 évente, vagy az elektronikus információs rendszereket érintő változások után felül kell vizsgálni és szükség esetén ismételten el kell végezni.

Az ASP szakrendszert használó helyiségek besorolása a NEIH tájékoztatása alapján: 4. biztonsági osztály

A hivatal besorolása: 3. biztonsági szint

A hivatal vagy hivatali egység szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt. A hivatal kritikus adatot, nem minősített, de nem közérdekű, illetve közérdekből nyilvános adatot kezel.

Bodajk, 2017. december 14.

BODAJK VÁROS JEGYZŐJE

Nagy Csilla
jegyző

Bodajki Polgármesteri Hivatal

B38 IRATKEZELÉSI SZABÁLYZATA

Bodajki Polgármesteri Hivatal

a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény alapján készített, a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló, többször módosított 335/2005. (XII. 29.) Korm. rendeletben előírtaknak megfelelő

EGYEDI IRATKEZELÉSI SZABÁLYZATA

A köziratokról, közlevéltáraktól, és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény 10. § (1) bekezdés a) pontjában biztosított jogkörömben eljárva a Bodajki Polgármesteri Hivatal egyedi iratkezelési szabályzatának 2018. január 1-jével történő bevezetésével egyetértek.

Székesfehérvár, 2018. .....

.....
igazgató
MNL Fejér Megyei Levéltára

A köziratokról, közlevéltáraktól, és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény 10. § (1) bekezdés a) pontjában biztosított jogkörömben eljárva a Bodajki Polgármesteri Hivatal egyedi iratkezelési szabályzatának 2018. január 1-jével történő bevezetésével egyetértek.

Székesfehérvár, 2018. .....

.....
főigazgató/igazgató
Fejér Megyei Kormányhivatal

Bodajk Város Önkormányzat jegyzője 1/2018. (VIII. 10.) utasítása a Bodajki Polgármesteri Hivatal Iratkezelési Szabályzatáról

IRATKEZELÉSI SZABÁLYZAT

Hatályos: 2018. január 1-jétől

Nagy Csilla
jegyző

I. FEJEZET
AZ IRATKEZELÉS SORÁN HASZNÁLT ÉRTELMEZŐ RENDELKEZÉSEK

ÁNYK űrlap benyújtás támogatás szolgáltatás: a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról szóló kormányrendelet szerinti szolgáltatás;

Átadás: irat, ügyirat vagy irategyüttes kezelési jogosultságának dokumentált átruházása;

Átmeneti irattár: a polgármesteri hivatal által az iktatóhelyhez kapcsolódóan kialakított olyan irattár, amelyben az irattári anyag meghatározott időtartamú átmeneti, selejtezés vagy központi irattárba adás előtti őrzése történik;

Biztonságos kézbesítési szolgáltatás: a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról szóló kormányrendelet szerinti szabályozott biztonságos kézbesítési szolgáltatás;

Csatolás: iratok, ügyiratok átmeneti jellegű összekapcsolása;

Elektronikus archiválás: elektronikus iktatókönyvek és adatállományaik, valamint elektronikus dokumentumok hosszú távú biztonságos és olvashatóságát biztosító megőrzése elektronikus adathordozón;

Elektronikus érkeztető nyilvántartás: elektronikus iratkezelés esetén az iratkezelési szoftver azon szolgáltatás-együttese, amely az érkeztetési információk rögzítését, megőrzését és visszakereshetőségét biztosítja;

Elektronikus iktatókönyv: elektronikus iratkezelés esetén az iratkezelési szoftver azon szolgáltatás-együttese, amely az iktatási információk rögzítését, végleges megőrzését és visszakereshetőségét biztosítja;

Elektronikus irattár: a polgármesteri hivatal által használt iratkezelési szoftver - ideértve az erre vonatkozó elektronikus dokumentumtárolási szolgáltatás útján történő biztosítást is - azon része, vagy olyan adatbázis, amelyben az elektronikusan tárolt irattári anyag meghatározott időtartamú elektronikus őrzése történik;

Elektronikus tájékoztatás: az információs önrendelkezési jogról és az információszabadságról szóló törvény szerint előírt elektronikus közzétételi kötelezettség;

Elektronikus ügyintézés: a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló törvény szerinti elektronikus ügyintézés;

Elektronikus űrlap: minden olyan elektronikus formában adatszolgáltatásra szolgáló felület, amelynél a megadandó adatok formája és tartalmi köre előre rögzített, és a kitöltést követően a megadott tartalommal elektronikus dokumentum jön létre;

Elektronikus visszaigazolás: olyan - kiadmánynak nem minősülő - elektronikus dokumentum, amely az elektronikus úton érkezett irat átvételéről és az érkeztetés azonosítójáról, valamint a külön jogszabályban meghatározott egyéb adatokról is értesíti annak küldőjét;

Előadói ív: az üggyel, a szignálással, a kiadmányozással, az ügyintézéssel és az iratkezeléssel kapcsolatos információkat hordozó, az ügyirat elválaszthatatlan részét képező, illetve azzal közös adatbázisban kezelt iratkezelési segédeszköz;

Előzményezés: az iratkezelési alapfolyamat azon művelete, amely során megállapításra kerül, hogy az új irat egy már meglévő ügyirattal kapcsolatban áll-e vagy sem, vagy az új iratot új ügy első irataként kell-e nyilvántartásba venni;

Expediálás: az irat kézbesítésének előkészítése, ügyintézői vagy vezetői utasítás alapján a küldemény címzettjének (címzettjeinek), adathordozójának, fajtájának, a kézbesítés és küldés módjának és időpontjának meghatározása, a küldemény küldési mód szerinti összeállítása;

Érkeztetés: a beérkezett küldemény érkeztetési azonosítóval, valamint beérkezési dátummal történő ellátása és nyilvántartásba vétele;

Eseménynapló: olyan speciális adatok strukturált összessége, amely a számítógépen történő alkalmazással, biztonsággal, telepítéssel vagy rendszerrel kapcsolatos minden eseményt rögzít;

Hiteles elektronikus másolat: valamely nem elektronikus dokumentumról e rendelet szabályai szerint készült, azzal képileg vagy tartalmilag egyező, joghatás kiváltására alkalmas elektronikus eszköz útján értelmezhető adategyüttes;

Iktatás: az irat iktatószámmal történő nyilvántartásba vétele az irat beérkezésével vagy az érkeztetéssel egy időben vagy az érkeztetést, keletkezést követően;

Iktatószám: olyan egyedi azonosító, amellyel a polgármesteri hivatal látja el az iktatandó iratot;

Iratkezelési szoftver: az iratkezelési alapfolyamatot támogató olyan informatikai alkalmazás, amely alapfunkcióját tekintve az e rendeletben foglalt iratkezelési műveleteket vagy azok egy részének végrehajtását támogatja, függetlenül attól, hogy ezek mellett egyéb funkciókat is ellát;

Irat: valamely szerv működése vagy személy tevékenysége során keletkezett vagy hozzá érkezett, egy egységként kezelendő rögzített információ, adategyüttes, amely megjelenhet papíron, mikrofilmen, mágneses, elektronikus vagy bármilyen más adathordozón; tartalma lehet szöveg, adat, grafikon, hang, kép, mozgókép vagy bármely más formában lévő információ vagy ezek kombinációja;

Iratkölcsönzés: a papír alapú ügyirat visszahozatali kötelezettség melletti kiadása az átmeneti vagy a központi irattárból, elektronikus irattár alkalmazása esetén az elektronikusan tárolt irathoz történő hozzáférés biztosítása;

Irattár: az irattári anyag szakszerű és biztonságos őrzése, valamint kezelésének biztosítása céljából létrehozott és működtetett fizikai, illetve elektronikus tárolóhely;

Iratkezelés: az irat készítését, nyilvántartását, rendszerezését és a selejtezhetőség szempontjából történő válogatását, segédletekkel való ellátását, szakszerű és biztonságos megőrzését, használatra bocsátását, selejtezését, illetve levéltárba adását együttesen magába foglaló tevékenység;

Irattárba helyezés: az irattári tételszámmal ellátott ügyirat átmeneti vagy központi irattárban történő dokumentált elhelyezése - elektronikus irattár esetén archiválása -, illetve kezelési jogának átadása az irattárnak az ügyintézés befejezését követő időre;

Irattári terv: a köziratok rendszerezésének és a selejtezhetőség szempontjából történő válogatásának alapjául szolgáló jegyzék, amely az irattári anyagot tételekre (tárgyi csoportokra, indokolt esetben iratfajtákra) tagolva, a közfeladatot ellátó szerv feladat- és hatásköréhez, valamint szervezetéhez igazodó rendszerezésében sorolja fel, s meghatározza a kiselejtezhető irattári tételekbe tartozó iratok ügyviteli célú megőrzésének időtartamát, továbbá a nem selejtezhető iratok levéltárba adásának határidejét

Irattári tétel: a polgármesteri hivatal ügykörének és szervezetének megfelelően kialakított legkisebb - egyéni irattári őrzési idővel rendelkező - irattári egység, amelybe több egyedi ügy iratai tartozhatnak;

Irattári tételszám: az iratnak az irattári tervben meghatározott, címmel ellátott tárgyi csoportba és iratfajtába sorolását, selejtezhetőség szerinti csoportosítását meghatározó, az irattári tervben elfoglalt helyüknek megfelelő azonosító;

Kezdőirat: az ügyben keletkezett első irat, az ügy indító irata;

Kezelési feljegyzések: az ügyirat vagy az egyes irat kezelésével kapcsolatos, ügykezelőnek szóló vezetői vagy ügyintézői utasítások;

Kézbesítés: a küldeménynek kézbesítő szervezet, személy, adatátviteli eszköz útján történő eljuttatása a címzetthez;

Kézbesítési szolgáltatás: a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról szóló kormányrendelet szerinti kézbesítési szolgáltatás;

Központi irattár: a polgármesteri hivatal irattári anyagának selejtezés vagy levéltárba adás előtti, valamint a maradandó értékű nem selejtezhető és levéltárba nem adott iratok, továbbá a nem selejtezhető és levéltárba átadásra nem kerülő iratok őrzésére szolgáló irattár, ideértve az erre vonatkozó elektronikus dokumentumtárolási szolgáltatás útján történő biztosítást is;

Küldemény: papír alapú irat vagy tárgy, továbbá elektronikus irat - kivéve a reklámanyag, sajtótermék, elektronikus szemét -, amelyet kézbesítés céljából burkolatán, a hozzá tartozó listán vagy egyéb, egyértelműen az irathoz vagy tárgyhoz rendelt felismerhető módon címzéssel láttak el;

Küldemény bontása: az érkezett küldemény felnyitása, olvashatóvá tétele;

Küldő: a küldemény tartalmából, vagy a küldeményhez kapcsolódó azonosító adatokból a küldemény benyújtójaként azonosítható személy vagy szervezet;

Levéltárba adás: a lejárt irattári őrzési idejű, maradandó értékű iratok teljes és lezárt évfolyamainak átadása az illetékes közlevéltárnak;

Másodlat: az eredeti irat egyik hiteles példánya, amelyet az első példánnyal azonos módon hitelesítettek;

Másolat: az eredeti iratról szöveg-azonos és alakhű formában, utólag készült egyszerű (nem hitelesített) vagy hiteles (hitelesítési záradékkal ellátott) irat;

Megsemmisítés: a kiselejtezett irat végleges megsemmisítése, a benne foglalt információ helyreállításának lehetőségét kizáró módon történő hozzáférhetetlenné tétele, törlése, amely következtében az irat tartalma nem rekonstruálható;

Mellékelt irat: az iratnak nem szerves része, tartozéka, attól - mint kísérő irattól - elválasztható;

Melléklet: valamely irat szerves tartozéka, annak kiegészítő része, amely elválaszthatatlan attól;

Naplózás: az iratkezelési szoftverben és az általa kezelt adatállományokban bekövetkezett események meghatározott körének regisztrálása;

Önkormányzati ASP rendszer: a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 114. § (2) bekezdése szerinti, a helyi önkormányzatok feladatellátását támogató, számítástechnikai hálózaton keresztül távoli alkalmazásszolgáltatást (Application Service Provider, ASP) nyújtó elektronikus információs rendszer;

Papíralapú érkeztető könyv: hitelesített iratkezelési segédeszköz, amelyben a küldeményeknek a polgármesteri hivatalhoz történő beérkezésének a nyilvántartásba vétele az üzemzavar idején megtörténik;

Papíralapú iktatókönyv: olyan nem selejtezhető, hitelesített iratkezelési segédeszköz, amelyben az iratok iktatása az üzemzavar idején történik;

Savmentes doboz: lignint, savas adalékanyagot és színezéket nem tartalmazó, papírból készített tárolóeszköz;

Selejtezés: a lejárt megőrzési határidejű iratok vagy e rendelet alapján selejtezési eljárás alá vonható iratok kiemelése az irattári anyagból és megsemmisítésre történő előkészítése;

Szerelés: ügyiratok végleges jellegű összekapcsolása, amelynek következtében az összekapcsolt ügyiratok a továbbiakban kizárólag együtt kezelhetőek;

Szignálás: az ügyben eljárni illetékes szervezeti egység és/vagy ügyintéző személy kijelölése, az elintézési határidő és a feladat meghatározása;

Továbbítás: az ügyintézés során az irat eljuttatása az egyik ügyintézési ponttól a másikhoz, amely elektronikusan tárolt irat esetén megvalósulhat az irathoz való hozzáférés lehetőségének biztosításával is;

Ügyfél ügyintézési rendelkezésének nyilvántartása: a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról szóló kormányrendelet szerinti nyilvántartás;

Ügyintéző: az ügy intézésére kijelölt személy, az ügy előadója, aki az ügyet döntésre előkészíti;

Ügyirat: egy ügyben keletkezett valamennyi irat;

Ügykezelő: iratkezelési feladatokat végző személy;

Ügykör: a polgármesteri hivatal vagy valamely, a polgármesteri hivatallal munkaviszonyban álló személy feladat- és hatáskörébe tartozó ügyek meghatározott csoportja;

Vegyes ügyirat: papír alapú és elektronikus iratokat egyaránt tartalmazó ügyirat.

II. FEJEZET
ÁLTALÁNOS RENDELKEZÉSEK

A Bodajki Polgármesteri Hivatal egyedi iratkezelési szabályzata (a továbbiakban: Iratkezelési Szabályzat)

- a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény,
- az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény,
- a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló, többször módosított 335/2005. (XII. 29.) Korm. rendelet,
- az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet,
- a Bodajki Polgármesteri Hivatal Szervezeti és Működési Szabályzat rendelkezéseinek figyelembevételével,
- az MNL Fejér Megyei Levéltára és a Fejér Megyei Kormányhivatal egyetértésével készült.

Az Iratkezelési Szabályzat hatálya

1. Az Iratkezelési Szabályzat hatálya kiterjed a Bodajki Polgármesteri Hivatalnál (a továbbiakban: Hivatal) keletkező, oda érkező, illetve onnan kimenő valamennyi iratra, az ügyvitel valamennyi területére és résztvevőjére. Az Iratkezelési Szabályzat hatálya kiterjed a Hivatal testületeire és bizottságaira, valamint a kisebbségi önkormányzatokra, az e testületek által keletkeztetett iratokra.

Az Iratkezelési Szabályzat rendelkezéseit a minősített iratokra és azok kezelési rendjére a minősített adat védelméről szóló 2009. évi CLV. törvényben és a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III.26.) Korm. rendeletben foglalt eltérésekkel kell alkalmazni.

Az iratkezelés szabályozása

2. Az Iratkezelési Szabályzat a köziratok biztonságos őrzésének módját, rendszerezését, nyilvántartását, segédletekkel ellátását, irattározását, selejtezését és levéltárba történő átadását szabályozza.

Az iratkezelési szabályzatban az iratkezelés minden fázisára meg kell határozni azokat az előírásokat, amelyek biztosítják a papíralapú és az elektronikus ügyiratok egységének megőrzését, kezelhetőségét, használhatóságát és megakadályozzák az illetéktelen hozzáférést.

3. Jelen Iratkezelési Szabályzat kötelező mellékletét képezi az önkormányzati hivatalok egységes irattári tervének kiadásáról rendelkező 78/2012. (XII. 28.) BM rendelet mellékletében kiadott irattári terv.

Az iratkezelés szervezete

4. A Hivatal a Szervezeti és Működési Szabályzatában és az egyes munkaköri leírásokban határozza meg az iratkezelés szervezeti rendjét, az iratkezelésre, valamint az azzal összefüggő tevékenységekre vonatkozó feladat- és hatásköröket, és kijelöli az iratkezelés felügyeletét ellátó vezetőt.

5. A Hivatal az iratkezelést központi iratkezelési szervezettel látja el.

6. Az iratkezelés szervezetét, az iratok nyilvántartásának módját, rendszerét, az egyes ügyviteli területek kezelését megváltoztatni, módosítani csak a naptári év kezdetén az MNL Fejér Megyei Levéltár és a Fejér Megyei Kormányhivatal egyetértésével lehet.

Az iratkezelés felügyelete

7. Az egységes és szabályszerű iratkezelési gyakorlat általános felügyeletét a Hivatal jegyzője felügyeli. Az iratkezelési feladatok felügyeletének egyes részfeladatait az iktatással, irattározással megbízott köztisztviselő látja el.

8. A jegyző közvetlenül felelős az Iratkezelési Szabályzatban foglaltak végrehajtásáért, a szervezeti, működési és ügyrendi szabályok, az alkalmazott informatikai eszközök és eljárások, valamint az irattári tervek és iratkezelési előírások folyamatos összhangjáért, az iratok jogszerű, szakszerű, és biztonságos megőrzésére, kezelésére alkalmas irattár kialakításáért és működtetéséért, továbbá az iratkezeléshez szükséges tárgyi, technikai és személyi feltételek biztosításáért, felügyeletéért.

9. A jegyző az iratkezelés felügyeletével megbízott vezetőként gondoskodik:
   - az elektronikus ügyintézés végrehajtásához szükséges részletszabályok meghatározásáról,
   - az elektronikus ügyintézés megvalósításához szükséges feltételek biztosításáról,
   - az iratkezelési szabályzat elkészítéséről, évenkénti felülvizsgálatáról, szükség szerinti módosításáról, az illetékes közlevéltár egyetértésének beszerzéséről,
   - az iratkezelésben résztvevők feladatainak meghatározásáról, az iratkezelési szabályzat végrehajtásának rendszeres ellenőrzéséről, intézkedik a szabálytalanságok megszüntetéséről,
   - az iratkezelést végző, vagy azért felelős személyek szakmai képzéséről és továbbképzéséről.
   - a szabályzatban foglaltak végrehajtásának ellenőrzéséért,
   - az iratkezelési segédeszközök, iratminták és formanyomtatványok, számítástechnikai programok, adathordozók stb. biztosításáért,
   - az elektronikus iratkezelési szoftver hozzáférési jogosultságainak, az egyedi azonosítóknak, a helyettesítési jogoknak, a külső és a belső név- és címtáraknak naprakészen tartásáért.
   - az iratok szakszerű és biztonságos megőrzésére alkalmas elektronikus iktatási rendszer kialakításáért.

A jogosultságok kezelésének szabályai

10. Az iratkezelő szoftverhez való hozzáférési jogosultságokat névre szólóan kell dokumentálni. A dokumentumok tárolása és kezelése a rendszergazda feladata.

11. Azon természetes személyekről, akik részére a Hivatal elektronikus aláírást biztosít, valamint a Hivatal által használt aláírás bélyegzőkről az illetékes szervezeti egység nyilvántartást köteles vezetni.

12. A hivatalos célra felhasználható elektronikus aláírásokról az iktatással megbízott ügyintéző vezet nyilvántartást.

13. A jogosultsági beállítást igazoló dokumentumot az iratkezelő szoftver alkalmazásával iktatni kell.

III. FEJEZET
AZ IRATOK KEZELÉSÉNEK ÁLTALÁNOS KÖVETELMÉNYEI

Az iratok rendszerezése

14. A Hivatal feladat- és hatáskörébe tartozó ügyek intézésének áttekinthetősége érdekében az azonos ügyre – egy adott (egyedi) tárgyra – vonatkozó iratokat egy irategységként, ügyiratként kell kezelni. A több fázisban intézett ügyek egyes fázisaiban keletkezett iratok ügyiraton belüli irategységnek, ügyiratdarabnak (ügydarabnak) minősülnek.

15. A papíralapú ügyirat fizikai együttkezelése az előadói ívben történik. Az előadói ívben a kezdőirat a legalsó, a legnagyobb alszámú irat a legfelső.

16. Az elektronikus ügyirathoz tartozó ügyiratdarabok nyilvántartását ügyirattérkép segítségével az elektronikus rendszer biztosítja.

17. Az ügyiratokat, és a nem iktatással nyilvántartott egyéb irategyütteseket, valamint a Hivatal irattári anyagába tartozó egyéb iratokat – még irattárba helyezésük előtt – az irattári terv alapján kell az irattári tételekbe sorolni, és irattári tételszámmal ellátni.

18. Az ügyvitelhez már nem szükséges, irattározási utasítással ellátott ügyiratokat az irattárban, az irattári tételszám szerinti rendszerben kell elhelyezni.

Az iratok nyilvántartása és az iratforgalom dokumentálása

19. A Hivatalhoz érkező, ott keletkező, illetve az onnan kimenő iratokat az azonosításhoz szükséges, és az ügy intézésére vonatkozó legfontosabb adatok rögzítésével, az e célra rendszeresített iratkezelő szoftverrel vezérelt adatbázisban kell nyilvántartani.

20. Az iratkezelési szabályzatban meghatározottak kivételével az iratokat iktatással kell nyilvántartásba venni. Az iktatást olyan módon kell végezni, hogy mind az elektronikus iktató adatbázist, mind az abból kinyerhető papíralapú iktatókönyvet az ügyintézés hiteles dokumentumaként lehessen használni.

21. Az iratforgalom keretében az iratok átadását-átvételét minden esetben úgy kell végezni, hogy egyértelműen bizonyítható legyen az átadó, átvevő személye, az átadás időpontja és módja.

22. Az iratok nyilvántartásba vételével, iktatásával és az iratforgalom dokumentálásával biztosítani kell, hogy az ügyintézés folyamata, és az iratok szervezeten belüli útja pontosan követhető és ellenőrizhető, az iratok holléte pedig naprakészen megállapítható legyen.

Hozzáférés az iratokhoz, az iratok védelme

23. Az iktatásnak külön helyiséget kell kijelölni, illetőleg a helyiséget úgy kell kialakítani, hogy az iratok tárolása az egyéb tevékenységtől (átadás-átvétel stb.) elkülönítetten történjen.

24. A Hivatal irattári anyaga használható belső ügyviteli célból és külső szerv vagy személy megkeresésére. A használat módjai: betekintés, kölcsönzés, másolat készítése.

25. A Hivatal dolgozói csak azokhoz az iratokhoz, illetőleg adatokhoz férhetnek hozzá, amelyekre munkakörük ellátásához szükségük van, vagy amelyre az illetékes vezető felhatalmazást ad. A hozzáférési jogosultságról naprakész nyilvántartást kell vezetni.

26. Az ügyintézők és ügykezelők fegyelmi felelősséggel tartoznak a rájuk bízott iratokért és azok adattartalmáért egyaránt.

27. Az ügyfélnek és képviselőjének a rá vonatkozó iratba való betekintést és a másolatkészítést úgy kell biztosítani, hogy azzal mások személyiségi jogai ne sérüljenek.

28. A papíralapú dokumentumról történő elektronikus másolatkészítés során a másolatkészítő biztosítja a papíralapú dokumentum és az elektronikus másolat képi vagy tartalmi megfelelését, és azt, hogy minden az aláírás elhelyezését követően az elektronikus másolaton tett módosítás érzékelhető legyen.

29. A betekintéseket, kölcsönzéseket, másolatok készítését utólagosan is ellenőrizhető módon, papíralapon és az elektronikus iratkezelő rendszerben egyaránt dokumentálni kell.

30. Az iratokhoz a kiadmányozó döntése alapján az alábbi, a hozzáférést korlátozó, kezelési utasítások alkalmazhatók:

- „Saját kezű felbontásra!",
- „Más szervnek nem adható át!",
- „Nem másolható!",
- „Kivonat nem készíthető!",
- „Elolvasás után visszaküldendő!",
- „Zárt borítékban tárolandó!" (a kezelésére vonatkozó utasítások megjelölésével),
- valamint más, az adathordozó sajátosságától függő egyéb szükséges utasítás.

A kezelési utasítások nem korlátozhatják a közérdekű adatok megismerését.

31. Az iratokkal és az azok kezeléséhez alkalmazott gépi adathordozókkal kapcsolatban minden esetben rendelkezni kell a szükséges védelmi intézkedésekről.

32. Az elektronikus dokumentumokat oly módon kell megőrizni, amely kizárja az utólagos módosítás lehetőségét, a megőrzési kötelezettség lejártáig folyamatosan biztosítja a jogosultak részére a hozzáférést, a dokumentum létrehozójának és archiválójának egyértelmű azonosíthatóságát, valamint az elektronikus dokumentumok értelmezhetőségét (olvashatóságát). Az elektronikus dokumentumokat védeni kell a jogosulatlan hozzáférés, módosítás, törlés vagy megsemmisítés ellen.

33. Az iratkezelő szoftver elemeiről (alkalmazások, adatok, operációs rendszer és környezetük) olyan mentési renddel és biztonsági mentésekkel kell rendelkezni, amelyek biztosítják azok helyreállítását.

34. Az elektronikus iktatórendszer minden felhasználójának személy szerint azonosítottnak kell lennie. Az azonosított hozzáférést és a hozzáférési jogosultság változtatását naplózni kell.

35. Gondoskodni kell az iratkezelési rendszer valamennyi eseményének naplózásáról.

Ügyiratok iktatási szabályai az elektronikus iktatórendszer üzemzavara esetén

36. Papíralapú iktatókönyvet (a továbbiakban: iktatókönyv) kell felfektetni, arra az esetre, ha bármely oknál fogva az iratkezelők számára az iktatórendszerhez való hozzáférés több órán keresztül akadályba ütközik.

37. A „sürgős", „azonnal", „soron kívül" jelöléssel ellátott – mind a bejövő, mind a kimenő és belső iratforgalom esetében – iratokat, az adott évben 1-től kezdődő iktatószámmal erre a célra, a hitelesítés szabályai szerint megnyitott, ÜZ egyedi azonosítási jellel ellátott papíralapú iktatókönyvbe kell iktatni, ha az üzemzavar a 4 órát meghaladja, továbbá a megkülönböztetett jelölés nélküli iratokat is, ha az iktatás akadályoztatása meghaladja a 24 órát.

38. Az előző pont szerint nyilvántartásba vett iratokon az iktatószám feltüntetésénél „ÜZ" egyedi azonosítási jelölést kell alkalmazni. (Pl. 233-1/2008/ÜZ). Az „ÜZ" egyedi azonosító jelöléssel ellátott papíralapú iktatókönyvek beszerzéséről és nyilvántartásáról, valamint az ÜZ iktatókönyvek, egyéb azonosítók nyilvántartásáról az iratkezelés felügyeletét ellátó vezető intézkedik, azok hitelesítésére, vezetésére az iratkezelési segédletekre vonatkozó szabályokat kell alkalmazni.

39. Az iktatás során, amennyiben ismert az iktatórendszerben használt iktatószám, akkor azt minden esetben fel kell tüntetni a papíralapú iktatókönyv 'Megjegyzés' rovatában.

40. Az üzemzavar megszűnését követően minden ügyiratot, az önkormányzati iktatórendszerbe át kell iktatni. Az átvezetés tényét a két nyilvántartásban a kölcsönösen hivatkozott iktatószámokkal jelezni kell.

41. Az üzemzavar esetén használt iktatókönyvben az év végén az iktatásra felhasznált utolsó számot követő aláhúzással kell a zárást elvégezni, majd azt a keltezést követően aláírással és a szervezeti egység körbélyegzőjének lenyomatával kell hitelesíteni. A lap alján vízszintes vonallal le kell zárni, ha a lapon fennmaradtak számok, a lezárás átlós vonallal történik. A lapra rá kell vezetni, hogy mely iktatószámmal zárul a könyv, és mikor történt a lezárás. Az iktatókönyv lezárását – úgy, mint a megnyitását – a szervezeti egység vezetőjének aláírása és a hivatalos bélyegző lenyomat hitelesíti. Az üzemzavar esetén használt iktatókönyvet az aktuális év iratai mellett kell tartani. Papíralapú iktatókönyvben ceruzával írni, sorszámot üresen hagyni, a felhasznált lapokat összeragasztani, a bejegyzett adatokat kiradírozni, vagy bármely más módon olvashatatlanná tenni nem szabad. Ha helyesbítés szükséges, a téves adatot vagy számot egy vonallal úgy kell áthúzni, hogy az eredeti feljegyzés olvasható maradjon. A javítást keltezéssel és kézjeggyel kell igazolni.

IV. FEJEZET
AZ IRATKEZELÉS FOLYAMATA

A küldemények átvétele

42. A küldemény átvételére a Hivatallal alkalmazotti jogviszonyban álló, munkaköri leírásában erre felhatalmazott személyek jogosultak.

43. Ha az ügyfél az iratot személyesen vagy képviselő útján nyújtja be, az iratot átvevő dolgozó az átvétel tényéről az iratkezelő szoftver által generált elismervényt ad.

44. Munkaidőn túl érkezett küldemények átvételére a Hivatallal alkalmazotti jogviszonyban álló, munkaköri leírásában erre felhatalmazott személyek jogosultak.

45. Küldemény átvételére sor kerülhet a Hivatal Hivatali Kapuján keresztül érkező elektronikus dokumentum iratkezelő szoftverben való átvételével és automatikus érkeztetésével.

46. Elektronikus küldemények esetében az átvevő automatikusan elküldi a feladónak a küldemény átvételét igazoló és az érkezés sorszámát is tartalmazó elektronikus visszaigazolást (átvételi nyugtát).

47. Az átvétel időpontját rögzíteni kell a küldeményen. Az „azonnal" és „sürgős" jelzésű hatósági küldemények átvételi idejét óra, perc pontossággal kell megjelölni. A küldeményt azonnal az érintettnek, vagy a postabontásért felelős szervezeti egységnek kell továbbítani.

48. Az átvétel során ellenőrizni kell:
- a címzés alapján a küldemény átvételére való jogosultságot,
- a kézbesítő okmányon és a küldeményen lévő azonosító jel megegyezőségét,
- az iratot tartalmazó boríték, illetve egyéb csomagolás sértetlenségét.

49. Elektronikus dokumentum átvétele során, a Hivatalnak vizsgálnia kell az alábbiakat:
- a Rendelkezési Nyilvántartás alapján az ügyfél ügyintézési rendelkezéseinek egyezőségét,
- a dokumentum megnyithatóságát és olvashatóságát,
- továbbá azt, hogy a dokumentum az elektronikus tájékoztatásra vonatkozó szabályok alapján közzétett címre és formátumban érkezett-e.

50. A Hivatal az elektronikus dokumentum sikeres benyújtásáról a természetes személy ügyfelet a Rendelkezési Nyilvántartásban meghatározottak szerint értesíti.

51. Téves címzés vagy helytelen kézbesítés esetén a küldeményt azonnal továbbítani kell az illetékeshez, vagy ha ez nem lehetséges, vissza kell küldeni a feladónak.

Amennyiben a feladó nem állapítható meg, a küldeményt irattározni és az irattári tervben meghatározott idő után selejtezni kell.

52. Sérült küldemény esetén a sérülés tényét az átvételi okmányon jelölni kell, és soron kívül ellenőrizni kell a küldemény tartalmának meglétét. A hiányzó iratokról vagy mellékletekről a küldő szervet, személyt értesíteni kell.

53. Ha az elektronikus irat benyújtása az elektronikus tájékoztatásra vonatkozó szabályok alapján közzétett formátumban lehetséges, és a benyújtott elektronikus irat nem a közzétett formátumban van, vagy a Hivatal által az elektronikus tájékoztatásra vonatkozó szabályok alapján közzétett elérhetőségi címre és nem biztonságos elektronikus kézbesítési szolgáltatáson keresztül történt, abban az esetben az iratot be nem nyújtottnak kell tekinteni, amit érkeztetni sem szükséges. A küldőt erről, az 57. pontban részletezettek szerint értesíteni kell.

54. Az elektronikus tájékoztatásra vonatkozó szabályok értelmezésekor az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény., illetve az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről rendelkező 137/2016. (VI.13.) Korm. rendelet értelmezései az irányadók.

55. Ha a benyújtott elektronikus irat az elektronikus tájékoztatásra vonatkozó szabályok alapján közzétett formátumot kezelő programokkal nem nyitható meg, úgy a küldőt - amennyiben elektronikus válaszcíme ismert - az érkezéstől számított legkésőbb három munkanapon belül elektronikus úton értesíteni kell a küldemény értelmezhetetlenségéről és az általa használt és elvárt formátumokról.

56. Az elektronikusan érkezett irat átvételét meg kell tagadni, ha az biztonsági kockázatot jelent a Polgármesteri Hivatal számítástechnikai rendszerére.

57. Az átvett, de az átvételt követő ellenőrzés alapján biztonsági kockázatot jelentő elektronikus küldemények esetében a fogadó szerv a további feldolgozást megszakítja, és a küldőt a biztonsági kockázat miatti feldolgozás elutasításról az alábbiak szerint értesíti:

- ha a küldő az azonosításához szükséges adatait megadta, az ügyintézési rendelkezésében megadott elektronikus elérhetőségén, az ott előírt módon,
- ennek hiányában, ha a küldő közölte a válaszadási elektronikus postafiók címét, úgy elektronikus levélben,
- egyéb esetben papír alapon.

58. Nem köteles a Hivatal értesíteni a feladót, ha korábban már érkezett azonos jellegű biztonsági kockázatot tartalmazó beadvány vagy ismétlődés az adott küldőtől.

59. Nem köteles a fogadó szerv értesíteni a feladót, ha korábban már érkezett azonos jellegű biztonsági kockázatot tartalmazó beadvány vagy ismétlődés az adott küldőtől.

A küldemények felbontása

60. A Hivatalhoz érkezett küldeményeket a polgármester bontja fel, majd látja el érkeztető bélyegzővel, Távollétében a jegyző helyettesíti.

61. Felbontás nélkül dokumentáltan a címzettnek kell továbbítani:

- a minősített iratokat,
- az „s.k." felbontásra, a képviselők, nem képviselő bizottsági tagok, a kisebbségi önkormányzatok és tagjaik nevére szóló küldeményeket,
- azokat, amelyek egyébként névre szólók és megállapíthatóan magánjellegűek.

62. A felbontás nélkül átvett küldemények címzettje soron kívül köteles gondoskodni az általa átvett hivatalos küldemény Iratkezelési Szabályzat szerinti további kezeléséről.

63. A küldemény felbontásakor ellenőrizni kell a jelzett mellékletek meglétét és olvashatóságát. Az esetlegesen felmerülő problémák tényét jegyzőkönyvben, az iraton vagy az előadói íven – a keltezés pontos megjelölésével – rögzíteni kell.

64. Amennyiben az érkezett elektronikus küldemény a rendelkezésre álló eszközzel nem nyitható meg, úgy a küldőt az érkezéstől számított három napon belül értesíteni kell a küldemény értelmezhetetlenségéről, és a Hivatal által használt elektronikus úton történő fogadás szabályairól.

Ilyen esetben az érkezés időpontjának a Hivatal által is értelmezhető küldemény megérkezését kell tekinteni.

65. Ha a felbontás alkalmával kiderül, hogy a küldemény pénzt vagy egyéb értéket tartalmaz, a felbontó az összeget illetőleg a küldemény értékét köteles az iratokon vagy feljegyzés formájában az irathoz csatoltan feltüntetni, és a pénzt, illetékbélyeget és egyéb értéket – elismervény ellenében – a pénzkezeléssel megbízott dolgozónak átadni. Az elismervényt az irathoz kell csatolni.

66. Amennyiben az irat benyújtásának időpontjához jogkövetkezmény fűződik vagy fűződhet, gondoskodni kell arról, hogy annak időpontja harmadik fél által megállapítható legyen. Papíralapú irat esetében a benyújtás időpontjának megállapítása a boríték csatolásával is biztosítható. Elektronikus úton érkezett irat esetében az elektronikus rendszer által automatikusan generált, az elektronikus visszaigazolásban meghatározott időpont az irányadó.

67. A küldemények téves felbontásakor, valamint, ha később derül ki, hogy a küldeményben minősített irat van, a borítékot újból le kell ragasztani, rá kell vezetni a felbontó nevét, majd a küldeményt a felvett jegyzőkönyvvel együtt sürgősen el kell juttatni a címzetthez, illetve a minősített iratokat az illetékes iratkezelőhöz, és a minősítőt – mivel az iratot az annak megismerésére nem jogosult látta – értesíteni kell a betekintésről. (A felbontó a kézbesítőkönyvben az átvétel és a felbontás tényét köteles rögzíteni az átvétel dátumának megjelölésével.)

68. A küldemény borítékját minden esetben véglegesen az ügyirathoz kell csatolni.

A küldemények érkeztetése

69. Minden papíralapú és elektronikus küldemény átvételét érkeztető nyilvántartás segítségével hitelesen dokumentálni, érkeztetni kell. Az érkeztetés minimálisan az érkezett küldemény sorszámának, küldőjének, az érkeztetés dátumának és könyvelt postai küldeménynél a küldemény postai azonosítójának (különösen kód, ragszám) nyilvántartásba vétele.

70. Az érkeztetés nyilvántartása – függetlenül az irat adathordozójától – az iratkezelő szoftverben történik. Az érkeztetési sorszám évente eggyel kezdődően folyamatos.

Az üzemzavar esetén alkalmazandó papíralapú iktatás esetén az érkeztetés külön érkeztető könyvben történik.

71. Az elektronikus küldeményeket a Hivatal központi e-mail címén, illetve a jegyző által külön utasításban megállapított egyéb hivatali e-mail címeken keresztül lehet fogadni.

72. A Hivatal központi e-mail címére és a jegyző által külön utasításban megállapított e-mail címre érkezett elektronikus küldeményeket az ügyintéző kinyomtatja, majd az iratkezelő szoftverben érkezteti. Ezt követően az elektronikus iratokat a továbbiakban a papír alapú iratoknak megfelelően kezelik.

73. A nem a központi e-mail címre és a jegyző által külön utasításban megállapított e-mail címre érkező hivatalos elektronikus küldeményeket az ügyintézők kötelesek továbbítani a 72. pontban meghatározott e-mail címekre.

Az ügyintéző kijelölése (szignálás)

74. Az érkezett ügyiratok szignálására a jegyző jogosult. A szignálási jogosultságot átmeneti vagy tartós időtartamra a jegyző átruházhatja.

75. Automatikus szignálás valósítható meg abban az esetben, ha automatikus szignálási jegyzékek állnak rendelkezésre.

76. Az automatikus szignálás esetében a szignálásra jogosultak állítják össze az egyes ügyintézők által használatos ügykörök, más azonosítók és az ügyintézők nevének egymáshoz rendelésével, a Hivatalnál kialakított munkamegosztáshoz igazodva.

77. Az automatikus szignálási jegyzéket évente kötelezően felül kell vizsgálni. Az ügyintézés szervezetében történt változások esetén a jegyzéket haladéktalanul módosítani kell.

78. A szignálásra jogosultsággal rendelkező vezető az automatikus szignálást felülbírálhatja és módosíthatja.

79. Az irat szignálására jogosult
- kijelöli az ügyintézőt (szervezeti egységet, vagy személyt),
- közli az elintézéssel, kiadmányozással kapcsolatos esetleges külön utasításait, melyeket a szignálás idejének megjelölésével előadói íven (írásban) rögzít.

80. Az iratkezelés során az üggyel és az ügyirattal kapcsolatos fontos utasításokat, kezelési feljegyzéseket minden esetben az iratkezelő szoftverben és az előadói íven kell rögzíteni.

Az iktatás

81. A Hivatalhoz érkező, illetve ott keletkező iratokat – a 82-83. pontban felsoroltak kivételével – ha jogszabály másként nem rendelkezik, iktatással kell nyilvántartani.

82. Nem kell iktatni, de külön jogszabályban meghatározott módon kell nyilvántartani és kezelni:
- pénzügyi bizonylatokat és számlákat,
- anyagkezeléssel kapcsolatos nyilvántartásokat,
- munkaügyi nyilvántartásokat,
- bérszámfejtési iratokat,
- a visszaérkezett tértivevényeket és elektronikus visszaigazolásokat,
- a visszavárólag érkezett, ún. átfutó iratokat.

83. Nem kell iktatni, és más módon sem kell nyilvántartásba venni:
- a tananyagokat, a tájékoztatókat,
- az üdvözlő lapokat,
- az előfizetési felhívásokat, a reklám anyagokat, az árajánlatokat, az árjegyzékeket,
- ügyintézést nem igénylő meghívókat.

84. Az iratkezelőnek az iratokat a beérkezés napján, de legkésőbb az azt követő munkanapon be kell iktatni.

Soron kívül kell iktatni és továbbítani a rövid határidős iratokat, táviratokat, elsőbbségi küldeményeket, a hivatalból tett intézkedéseket tartalmazó „sürgős" jelzésű iratokat.

Ha az irat munkaidőn kívüli időben érkezik, azt a következő munkanapon iktatni kell, s a tényleges érkezési, átvételi időpontot a megjegyzés rovatban minden esetben jelezni kell.

Az iktatószám

85. Az iktatásra kijelölt iratokat, az ügyiratra, az ügyirathoz tartozó iratokra, illetve az ügy intézésére vonatkozó legfontosabb adatok rögzítésével, egyedi azonosító számon, iktatószámon kell nyilvántartani és kezelni.

86. Az iktatást minden évben 1-gyes sorszámmal – számkeret alkalmazása esetén a számkeret egyes sorszámával – kell kezdeni.

87. A sorszámok felhasználása folyamatos, egy iktatószámra csak egy irat iktatható. Téves iktatás esetén az iktatószám nem használható fel újra.

88. Az iktatás során kötelező a sorszámos és alszámos iktatás alkalmazása. Az alszámokra tagolódó sorszámos iktatásnál az egyedi ügyben keletkezett első irat önálló sorszámot, azaz főszámot kap. Az ügyben érkező, keletkező további iratok a főszám alszámain kerülnek nyilvántartásba. Egy főszámhoz korlátlan számú alszám tartozhat.

89. Új alszámra kell iktatni – mint hivatalból keletkezett iratot, a hatósági határozatokat. A határozatra érkező fellebbezés – mint beérkező irat – ugyancsak új alszámra kerül.

90. Az iktatószám felépítése:
iktatóhely vagy iktatókönyv azonosítója, perjel, főszám, kötőjel, alszám, perjel, négyjegyű évszám, (Pl. Bod/324-17/2018.)
Az iktatószámot az iraton fel kell tüntetni.

91. Az iktatóhely azonosítókat az iratkezelési feladatok közvetlen felügyeletét ellátó jegyző adja ki és tartja nyilván.

92. Az ugyanazon ügyben, ugyanabban az évben keletkezett iratokat egy főszámon kell nyilvántartani. Egy iktatókönyvön belül a főszámokat folyamatos sorszámos rendszerben kell kiadni. Az ügyirathoz tartozó iratokat az iktatási főszám alatt folyamatosan kiadott alszámokon kell nyilvántartani.

Iktatókönyv

93. A Hivatal iktatás céljára az ún. ASP iratkezelő szoftvert használja. Az iktatókönyv az ASP iratkezelő szoftver adatállománya.

94. Az iktatókönyvnek kötelezően kell tartalmaznia az alábbi adatokat:

- iktatószám,
- iktatás időpontja,
- küldemény érkezésének időpontja, módja, érkeztető száma,
- küldemény elküldésének időpontja, módja,
- küldemény adathordozójának típusa (papíralapú, elektronikus), adathordozója,
- küldő megnevezése, azonosító adatai,
- címzett megnevezése, azonosító adatai,
- érkezett irat iktatószáma (idegen szám),
- mellékletek száma,
- ügyintéző szervezeti egység és az ügyintéző megnevezése,
- irat tárgya,
- elő- és utóiratok iktatószáma,
- kezelési feljegyzések,
- ügyintézés határideje, és végrehajtásának időpontja,
- irattári tételszám,
- irattárba helyezés időpontja.

95. Az iratkezelő szoftverben a módosításokat, tartalmuk megőrzésével, a jogosultsággal rendelkező ügyintéző azonosítójával és a javítás idejének megjelölésével, naplózással dokumentálni kell.

96. A téves iktatás, illetőleg az automatikus iktatásnál hibásan a rendszerbe került iktatás iktatószáma nem használható fel újra, azt az utólagos módosítás szabályainak megfelelően használaton kívül kell helyezni.

97. Az elektronikus iktatókönyvet (adatbázist) az év utolsó munkanapján, az utolsó irat iktatása után hitelesen le kell zárni.

98. A lezárást követően gépi adathordozóra el kell készíteni az elektronikus iktatókönyv (adatbázis) minősített elektronikus aláírással és időbélyegzővel ellátott másolatát, illetve papírra kell nyomtatni és azt kell hitelesíteni.

Előzményezés

99. Iktatás előtt az ügykezelőnek meg kell állapítania, hogy az iratnak van-e előirata. Amennyiben az irat iktatása nem lehetséges az előzmény főszámára, rögzíteni kell az iktatókönyvben az előirat iktatószámát, és az előzménynél a jelen irat iktatószámát, mint az utóirat iktatószámát.

100. Az előzményt ideiglenesen (csatolás), szükség esetén véglegesen (szerelés) az iktatott irathoz kell kapcsolni.

Az irat határidő – nyilvántartásba helyezése

101. Határidő-nyilvántartásba kell helyezni azt az iratot, amelynek végleges elintézése valamilyen közbeeső intézkedés elvégzése, feltétel bekövetkezése, vagy megszűnése után válik lehetővé.

102. Az iratot határidő-nyilvántartásba az ügyben érdemben eljáró ügyintéző helyezi. A határidőt az előadói íven év, hó, nap megjelölésével kell meghatározni.

Továbbítás az ügyintézőhöz

103. A szignált és nyilvántartásba vett iratokat az átvétel igazolása mellett az ügyintézőhöz kell továbbítani. Az elektronikus dokumentum (irat) elektronikus úton történő továbbítását a Hivatal szervezetén belül az iratkezelő szoftver biztosítja. Az átadás-átvétel igazolása az iratkezelő szoftverben történik.

Kiadmányozás (aláírás, hitelesítés)

104. Külső szervhez vagy személyhez csak hiteles kiadmányt lehet továbbítani.

105. Nem minősül kiadmánynak:
- az elektronikus visszaigazolás,
- a fizetési azonosítóról és az iktatószámról szóló elektronikus tájékoztatás, valamint
- az iratkezelési szabályzatban meghatározott egyéb iratok.

106. A papírlapú kiadmányokat (válaszleveleket és hivatalból kezdeményezett iratokat egyaránt) a helyi önkormányzat hivatalos levélpapírján és/vagy nyomtatványán kell elkészíteni.

107. A papíralapú kiadmány hitelesítésére az önkormányzat hivatalos körbélyegzőjét kell használni.

108. Külső szervhez vagy személyhez küldendő iratot kiadmányként csak a Szervezeti és Működési Szabályzatban meghatározott, kiadmányozási joggal rendelkező személy írhat alá.

109. A papíralapú irat akkor hiteles kiadmány, ha:
- azt az illetékes kiadmányozó saját kezűleg aláírja, vagy a kiadmányozó neve mellett az „s.k." jelzés szerepel, a hitelesítéssel felhatalmazott személy azt aláírásával igazolja, valamint

- a kiadmányozó, illetve a felhatalmazott személy aláírása mellett a szerv hivatalos bélyegzőlenyomata szerepel.

110. Hiteles elektronikus kiadmánynak csak az az elektronikus irat minősül, amelyet az arra jogosult személy fokozott biztonságú elektronikus aláírás vagy minősített elektronikus aláírással látott el.

111. A Hivatalnál keletkezett iratokról az iratot őrző szervezeti egység vezetője vagy ügyintézője – figyelemmel az iratok másolására, hitelesítésére vonatkozó szabályokra – a jogosult részére hitelesítési záradékkal ellátott papíralapú és elektronikus másolatot is kiadhat.

112. A kiadmányozáshoz használt bélyegzőkről nyilvántartást kell vezetni.

Expediálás és az iratok továbbítása

113. A kiadmányozott iratokat az érintett címzetthez, címzettekhez továbbítani kell.

114. Elektronikus iratok esetében a Hivatal a Rendelkezési Nyilvántartásban szereplő adatok alapján vizsgálja a címzett elérhetőségét, valamint a küldés és a kézbesítés módját.

115. Az elintézett, kiadmányozott irat továbbításra történő előkészítéséről, az expediálásról és az iratok továbbításáról az ügyintéző gondoskodik.

116. A küldeményeket lehetőleg még az átvétel napján kell továbbítani.

117. A kimenő iratnak minden esetben tartalmaznia kell:
- az önkormányzat/hivatal nevét, azonosító adatait (cím, telefon, fax, e-mail),
- az ügyintéző nevét,
- a kiadmányozó nevét, beosztását,
- az irat tárgyát,
- az irat iktatószámát,
- a mellékletek számát,
- a címzett nevét, azonosító adatait,
- az ügyet indító beadvány hivatkozási számát.

118. Az elküldés tényét és dátumát az irat tértivevénye vagy a postakönyv igazolja.

119. A küldeményeket a továbbítás módja szerint kell kezelni:
- személyes átvétel esetén elegendő a kézbesítési időpont, és az átvétel aláírással történő igazolása a kiadmány irattári példányán,
- postai feladás esetén postakönyv vagy kísérőjegyzék alkalmazásával,
- külön kézbesítő, futárszolgálat igénybevétele esetén a szerződésben rögzített szabályoknak megfelelően,
- elektronikus úton történő kézbesítés esetén a visszaigazolás biztosításával,
- elektronikus ügyintézés esetén a rendszer automatikusan tájékoztatja a címzettet az ügyintézés befejezéséről, a letöltési lehetőségekről, és hitelesen naplózza a letöltést.

120. A postai kézbesítésnél használt tértivevényeket – iktatás nélkül, de érkeztetve – az ügyirathoz kell mellékelni.

121. Ha a postára adott küldemények valamilyen okból visszaérkeznek, nem lehet az ügyet befejezettnek tekinteni. A visszaérkezett küldeményt az irattal együtt vissza kell adni az ügyintézőnek, aki rendelkezik a visszaérkezett irat további kezeléséről.

122. Ha a küldemény kézbesítésére biztonságos kézbesítési szolgáltaton keresztül kerül sor, abban az esetben az ügyfél részére a küldemény kézbesítése
- ügyfélkapun keresztül (természetes személy esetén),
- cégkapun keresztül (jogi személy esetén),

- hivatali kapun keresztül (közigazgatási szervezet részére)

történhet meg.

V. FEJEZET
IRATTÁROZÁS

Irattárba helyezés, irattár

123. Az elintézett ügyek iratait, amelyeknek kiadmányait, egyéb kimenő iratait továbbították, vagy amelyeknek irattározását elrendelték, irattárba kell helyezni.

124. Az irattárba helyezést a kiadmányozásra jogosult engedélyezi. Irattárba helyezés előtt az ügyintéző:
- megvizsgálja, hogy az előírt kezelési és kiadási utasítások teljesültek-e,
- az ügyirathoz hozzárendeli az irattári tételszámot, illetőleg a nyilvántartásba vétel során adott irattári tételszámot jóváhagyja, vagy felülbírálja, és azt saját nyilvántartó könyvében (munkakönyv, átadókönyv stb.) rögzíti (papíralapú irat esetén rávezeti az iratra is),
- a feleslegessé vált munkapéldányokat és másolatokat az ügyiratból kiemeli, és a selejtezési eljárás mellőzésével, az erre vonatkozó, külön szabályzatban megfogalmazott szabályok betartásával megsemmisíti.

125. Az irattárba helyezés alkalmával az iratkezelő köteles ellenőrizni, hogy az iratkezelés szabályainak eleget tettek-e. Amennyiben az iratkezelő hiányosságot észlel az iraton, visszaadja az ügyintézőnek, aki gondoskodik annak kijavításáról.

126. Az irattárba adást és az irattári anyag kezelését – papíralapú, más adathordozón tárolt és elektronikus iratok esetében egyaránt – dokumentáltan, visszakereshetően kell végezni.

127. Az iratokról el kell távolítani az összefűzésükhöz használt anyagokat, pl. fémből készült iratkapcsoló, zsineg, műanyag borító stb.

128. A Hivatalnál kijelölhető papíralapú iratokat őrző helyiség akkor felel meg céljának, ha száraz, portól és más szennyeződéstől tisztán tartható, megfelelően megvilágítható, levegője cserélhető, ha benne a tűz keletkezése a legbiztosabban elkerülhető, nem veszélyeztetik közművezetékek, a kívül támadt tűztől és erőszakos behatolástól védett.

129. Az iratok elhelyezésére nyitott, stabilan, vagy mobil rendszerben telepített – felületi festékkel ellátott fémből készült – állványokkal kell az irattári helyiséget berendezni. Az irattári berendezés kialakításakor a tűz- és balesetvédelem mellett a kezelés célszerűségi szempontjait is figyelembe kell venni.

130. Az iratanyag tárolására az ügyintézés során és az irattárban az iratok együttkezelését, portól való védelmét és az állványokon történő szakszerű elhelyezését egyaránt szolgáló tároló eszközöket kell használni. Erre a célra a Hivatal speciális irattároló dobozokat használ.

131. A nem papíralapú iratok tárolását az adathordozó időtállóságát biztosító paramétereknek megfelelően kialakított tároló rendszerekben kell biztosítani. A Hivatalnál a tárolásból adódható adatvesztés előtt gondoskodni kell az adathordozón található információk hiteles másolásáról, konvertálásáról, átjátszásáról.

Átmeneti és központi irattár

132. A Hivatal átmeneti és központi irattárakat működtet.

133. Átmeneti irattárba helyezhetők az elintézett, és a határidőbe helyezett ügyiratok. Az átmeneti irattár az iratkezelést végző ügyintéző irodájában található.

134. Az átmeneti irattárból az ügyiratokat két év után a központi irattári kezelésbe kell átadni.

135. A központi irattár a lezárt évfolyamú ügyiratokat eredeti alakjukban, előadói ívben elhelyezve, irattároló dobozokban, nyilvántartásaikkal együtt, az irattári tervben meghatározott tételszámok szerint csoportosítva veszi át.

136. Az elektronikusan tárolt adatok, iratok utólagos olvashatóságát, használatát a selejtezési idő lejáratáig vagy levéltárba adásáig biztosítani kell.

137. A központi irattárba helyezés módját az adathordozó határozza meg:

- a papíralapú iratokat a központi irattári helyiségben kell elhelyezni,
- az elektronikus iratokat háttérállományban kell archiválni az irattárba helyezés szabályainak megfelelően,
- az archivált, két éven túl selejtezhető, elektronikus iratokról a 2. év végén gépi adathordozóra – a központi irattár rendszerének megfelelő csoportosításban – hitelesített másolatot kell készíteni,
- vegyes ügyiratok esetében a selejtezhetőnek minősített iratokat az adathordozónak megfelelő módszerrel kell irattározni, az ügyirat egységét ebben az esetben az ügyviteli rendszer által generált módszerrel kell biztosítani,
- a nem selejtezhető, levéltári átadásra kerülő vegyes ügyiratok esetében az ügyiratba az elektronikus iratokról készült papíralapú hiteles másolatot kell elhelyezni (további intézkedésig).

138. Az irattárban elhelyezett iratokról naprakész nyilvántartást, irattári jegyzéket kell vezetni. Az irattári jegyzék a raktári, tárolási egységek szintjén készül, tartalmazza a raktári egységben elhelyezett iratok irattári jeleit, ezen belül a kezdő és záró iktatószámokat, a tételek megnevezését, valamint a raktári egység irattári helyének azonosítóját. Az irattári jegyzékbe be kell vezetni a kiselejtezett és a levéltári átadásra került iratokat.

Az irattári jegyzék számítástechnikai program segítségével, elektronikus adatbázisban is készíthető.

139. Az ügyintézők a munkakörük ellátásához szükséges, illetve a vezetők felhatalmazása alapján munkájukhoz szükséges iratokat az irattárból hivatalos használatra iratkikérővel kérhetnek ki. Az iratkikérést utólagosan is ellenőrizhető módon, dokumentáltan kell elvégezni. Az iratkölcsönzések dokumentálására nyilvántartást kell vezetni (kölcsönzési napló). Az átvételt igazoló iratkikérőket az irattárban kell tárolni.

140. Az irattárból kiadott ügyiratról ügyiratpótló lapot kell készíteni, amelyet mint elismervényt az átvevő aláír. Az aláírt ügyiratpótló lapot a kölcsönzés ideje alatt az ügyirat helyén kell tárolni.

141. Elektronikus iratok esetében a jogosult felhasználók naplózás mellett tekinthetik meg az iratot. Amennyiben a felhasználó a saját gépéről nem éri el a megtekintendő iratot, akkor az irattár kezeléséért felelős ügyintézőnek kell gondoskodnia arról, hogy a jogosult felhasználó elektronikus úton – az iratkölcsönzés szabályainak betartásával - megkapja a kért irat másolatát.

Selejtezés, megsemmisítés

142. A Hivatal valamennyi irattárában, az irattári tervben rögzített őrzési idő leteltével, szabályszerű eljárás keretében, iratselejtezést kell végezni, az illetékes közlevéltár egyidejű értesítésével. A selejtezést célszerű évente elvégezni. A szervezeti egységeknél a selejtezést a központi irattár tudomásával és közreműködésével kell elvégezni. Az irat selejtezését az irat keletkezésekor érvényben volt irattári terv szerint (figyelemmel a vonatkozó jogszabályra is) kell végrehajtani az Iratkezelési Szabályzatban foglaltak szerint.

143. Az iratselejtezést az iratkezelésért felelős vezető által kijelölt legalább 3 tagú selejtezési bizottság javaslata alapján lehet elvégezni.

144. Az iratselejtezésről a selejtezési bizottság tagjai által aláírt és a szerv körbélyegzőjének lenyomatával ellátott selejtezési jegyzőkönyvet kell készíteni 2 példányban, amelyeket iktatás után az illetékes levéltárhoz kell továbbítani a selejtezés engedélyeztetése végett.

A selejtezési jegyzőkönyv melléklete a selejtezett iratok tételszámát, tárgyát, évkörét felsoroló tételszintű iratjegyzék.

145. A levéltár az iratok megsemmisítését, a szükséges ellenőrzés után, a selejtezési jegyzőkönyv visszaküldött példányára írt záradékkal engedélyezi. A selejtezésre kijelölt iratokból a levéltár mintavétel vagy iratértékelés céljára visszatarthat vagy levéltári átadásra kijelölhet iratokat, egyes irattári tételeket.

146. A selejtezés tényét és időpontját a nyilvántartás megfelelő rovatába be kell vezetni.

147. Az irat megsemmisítéséről a jegyző az adatvédelmi és biztonsági előírások figyelembevételével gondoskodik.

148. A selejtezés során gondoskodni kell arról, hogy a több példányban megtalálható iratokból – az előírt megőrzési időig – csak az ügyet intéző szervezeti egység példánya kerüljön megőrzésre.

149. Az elektronikus adathordozón tárolt iratok és az elektronikus iratok selejtezése esetén az eljárás azonos a fentiekben leírtakkal.

Levéltárba adás

150. A Hivatal a nem selejtezhető iratait a hatályos vonatkozó jogszabályi előírásoknak megfelelően (általában 15 évi őrzési idő után), előzetes egyeztetéssel – az illetékes levéltárnak adja át. A levéltárnak csak lezárt, teljes évfolyamok iratai adhatók át.

151. Az irattári terv szerint a levéltár számára átadandó ügyiratokat az ügyviteli segédletekkel együtt, nem fertőzött állapotban, savmentes dobozokban az átadó költségére, átadás-átvételi jegyzőkönyv kíséretében, annak mellékletét képező raktári egység szerinti (doboz, kötet stb.) tételjegyzékkel együtt, teljes, lezárt évfolyamokban kell átadni. A visszatartott ügyiratokról külön darabszintű jegyzéket kell készíteni. Az átadási jegyzéket és a visszatartott ügyiratokról szóló jegyzéket a levéltárral egyeztetett formátumban elektronikusan is át kell adni.

152. Elektronikus iratokat az elektronikus formában tárolt iratok közlevéltári átvételének eljárásrendjéről és műszaki követelményeiről szóló 34/2016. (XI.30.) EMMI rendeletben meghatározott eljárásrend szerint kell levéltárba adni.

153. Az iratok levéltári átadásának tényét és idejét az iktatási és az irattári segédleteken is át kell vezetni.

VI. FEJEZET
INTÉZKEDÉSEK A HIVATAL FELADATKÖRÉNEK MEGVÁLTOZÁSA, HIVATAL- VAGY MUNKAKÖR ÁTADÁSA ESETÉN

154. A Hivatal feladatkörének megváltozása, hivatalának átadása esetén intézkednie kell az irattári anyagának további elhelyezéséről, biztonságos megőrzéséről, kezeléséről és további használhatóságáról. Az iratanyag elhelyezéséről az illetékes közlevéltára(ka)t írásban értesíteni kell.

155. Hivatalátadás esetén az erről felvett és iktatott jegyzőkönyvben fel kell tüntetni az utolsó iktatószámot (számokat) és tételesen fel kell sorolni az átadott, illetőleg átvett ügyiratokat és az ügyiratháttalékot.

156. Az iratkezelési folyamat szereplőit (szervezeti egység, szignáló, kiadmányozó, ügyintéző, iratkezelő) megszűnés, átszervezés és személyi változás esetén a kezelésükben lévő iratokkal, a nyilvántartások alapján ügyirat szinten el kell számoltatni, az elszámoltatásról jegyzőkönyvet kell felvenni.

VII. FEJEZET
ZÁRÓ RENDELKEZÉSEK

157. Jelen Iratkezelési Szabályzat 2018. január 1-jén lép hatályba.

158. Ezen Iratkezelési Szabályzat hatályba lépésével egyidejűleg a 918/2013. számú, 2013. február hó 20-án kiadott, az Iratkezelés Rendjéről szóló szabályzat hatályát veszti.

melléklet

Egységes irattári terv

Az irattári terv az egységes iratkezelés érdekében az irattári anyagot tételekre (tárgyi csoportokra, indokolt esetben iratfajtákra) tagolva, az önkormányzat szervezetéhez, feladat- és hatásköréhez igazodó rendszerezésben sorolja fel, és meghatározza a kiselejtezhető irattári tételekbe tartozó iratok ügyviteli célú megőrzésének időtartamát, továbbá a nem selejtezhető iratok levéltárba adásának határidejét. Az irattári terv általános és különös részre oszlik.

Az ügy típusát, ágazati hovatartozását, az irat selejtezhetőség szerinti csoportosítását és a levéltári átadás időpontját az irattári tervben rögzített irattári tételszám mutatja, amely egyúttal meghatározza az irat irattári helyét is.

Az irattári tételszám és kód összetevői:

1. irattári tételszám: az iratnak az irattári tervben meghatározott tárgyi csoportba és iratfajtába sorolását, selejtezhetőség szerint csoportosítását az önkormányzati hivatal szervezetéhez és feladatköréhez igazodó rendszerezésben meghatározó négyjegyű kód; első karaktere az ágazat betűjel, amelyet a tétel ágazaton belüli háromjegyű sorszáma követ;
2. megőrzési idő: szám, amely meghatározza a kiselejtezendő irattári tételekbe tartozó iratok ügyviteli célú megőrzésének időtartamát években, vagy „NS" jel, amely meghatározza a nem selejtezendő tételeket;
3. Lt.: a levéltári átadás határideje években, a tényleges átadás időpontjáról az önkormányzati hivatal és az illetékes levéltár esetenként állapodik meg (illetve „HN" jel, amely ügyviteli érdekből határidő nélkül az önkormányzat irattárában maradó iratok jelzésére szolgál).

A „lejárat után" kiegészítéssel ellátott tételeknél a selejtezés, illetve a levéltári átadás ideje a tételbe tartozó ügyiratok érvényességének lejártakor kezdődik.

MEGŐRZÉS			
ÁLTLÁNOS RÉSZ			
TÉTEL SZÁMKERETE		ÁGAZAT MEGNEVEZÉSE	
	U	ÖNKORMÁNYZATI ÉS ÁLTALÁNOS IGAZGATÁSI ÜGYEK	
U101-		U.1.	Képviselőtestület iratai
U201-		U.2.	Nemzetiségi önkormányzat iratai
		A polgármesteri hivatalnak, a közös önkormányzati hivatalnak, az önkormányzat gazdálkodó szervezeteinek, közalapítványainak és intézményeinek (a továbbiakban: intézményeinek) ügyei	
U301-		U.3.	Szervezet, működés
U401-		U.4.	Iratkezelés, ügyvitel
U501-		U.5.	Személyzeti, bér- és munkaügyek
U601-		U.6.	Pénz- és vagyonkezelés
KÜLÖNÖS RÉSZ			
TÉTEL SZÁMKERETE		ÁGAZAT MEGNEVEZÉSE	
	A	PÉNZÜGYEK	
A101-		A.1.	Adóigazgatási ügyek
A201-		A.2.	Egyéb pénzügyek

B101-	B	EGESZSÉGÜGYI IGAZGATÁS	
C101-	C	SZOCIÁLS IGAZGATÁS	
	E	KÖRNYEZETVÉDELMI, ÉPITÉSI ÜGYEK, TELEPÜLÉSRENDEZÉS, TERÜLETRENDEZÉS KOMMUNÁLIS IGAZGATÁS	
E101-		E.1.	Környezet- és természetvédelem
E201-		E.2.	Településrendezés, területrendezés
E301-		E.3.	Építési ügyek
E401-		E.4.	Kommunális ügyek
F101-	F	KÖZLEKEDÉS ÉS HÍRKÖZLÉSI IGAZGATÁS	
G101-	G	VÍZÜGYI IGAZGATÁS	
	H	ÖNKORMÁNYZATI, IGAZSÁGÜGYI ÉS RENDÉSZETI IGAZGATÁS	
H101-		H.1.	Anyakönyvi és állampolgársági ügyek
H201-		H.2.	A polgárok személyi adatainak, lakcímének nyilvántartásával kapcsolatos ügyek
H301-		H.3.	Választásokkal kapcsolatos ügyek
H401-		H.4.	Rendőrségi ügyek
H501-		H.5.	A helyi tűzvédelemmel kapcsolatos ügyek
H601-		H.6.	Menedékjogi ügyek
H701-		H.7.	Igazságügyi igazgatás
H801-		H.8.	Egyéb igazgatási ügyek
I101-	I	LAKÁSÜGYEK	
J101-	J	GYERMEKVÉDELMI ÉS GYÁMÜGYI IGAZGATÁS	
K101-	K	IPARI IGAZGATÁS	
L101-	L	KERESKEDELMI IGAZGATÁS, TURISZTIKA	
M101-	M	FÖLDMŰVELÉSÜGY, ÁLLAT- ÉS NÖVÉNYEGÉSZSÉGÜGYI IGAZGATÁS	
N101-	N	MUNKAÜGYI IGAZGATÁS, MUNKAVÉDELEM	
P101-	P	KÖZNEVELÉSI ÉS KÖZMŰVELŐDÉSÜGYI IGAZGATÁS	
R101-	R	SPORTÜGYEK	
	X	HONVÉDELMI, KATASZTRÓFAVÉDELMI IGAZGATÁS, FEGYVERES BIZTONSÁGI ŐRSÉG	
X101-		X.1.	Honvédelmi igazgatás
X201-		X.2.	Katasztrófavédelmi igazgatás
X301-		X.3.	Fegyveres biztonsági őrség
U.1. Képviselő-testület iratai			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
U101	Polgármesteri, főpolgármesteri, alpolgármesteri tisztség átadás-átvételével, egyéb feladat- és hatáskör átadás-átvételével kapcsolatos iratok	NS	15

U102	Képviselő-testületi jegyzőkönyv és mellékletei (előterjesztések, sürgősségi indítványok, tájékoztatók, közmeghallgatás, interpellációk, egyéb döntés-előkészítő iratok stb.)	NS	15
U103	Képviselő-testületi zárt ülések jegyzőkönyvei és mellékletei, zárt ülésekről készült hanganyagok	NS	15
U104	Képviselő-testületi bizottságok, részönkormányzatok üléseinek, falugyűlések, járási tanácskozások, lakossági fórum jegyzőkönyvei és mellékletei	NS	15
U105	Képviselő-testületi, képviselő-testületi bizottsági, részönkormányzati ülésekről készült hang- és képanyag	NS	15
U106	Képviselő-testületi bizottságok, részönkormányzatok zárt üléseiről készült jegyzőkönyvek, hang- és képanyagok	NS	15
U107	Önkormányzati biztos kirendelése, iratai	NS	15
U108	Tanácsnoki iratok	NS	15
U109	Okmánytár (címer és zászlórajz, díszpolgári cím, helyi kitüntetés adományozása stb.)	NS	15
U110	Önkormányzati érdek-képviseleti tagsági ügyek	NS	15
U111	Önkormányzati rendeletek, határozatok, szabályzatok, együttműködési szerződések/megállapodások eredeti példánya	NS	15
U.2. Nemzetiségi önkormányzat iratai			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
U201	Együttműködési megállapodások	NS	15
U202	Feladatellátási, intézményhálózat-működtetési és fejlesztési terv nemzetiségi önkormányzati véleményezése	NS	15
U203	Nemzetiségi gazdálkodó szervezetek, intézmények alapítása, átszervezése, megszűnése	NS	15
U204	Nemzetiségi oktatást is folytató iskolákban az érettségi vizsga előkészítésének, megszervezésének, lebonyolításának figyelemmel kísérésével kapcsolatos iratok	2	-

U205	Nemzetiségi óvodai, iskolai döntések véleményezése, szakmai ellenőrzése	NS	15
U206	Nemzetiségi önkormányzat, nemzetiségi önkormányzati bizottságok üléseinek jegyzőkönyvei, mellékletei, előterjesztések, egyéb döntés-előkészítő iratok	NS	15
U207	Nemzetiségi önkormányzat, nemzetiségi önkormányzati bizottságok üléseinek hang- és képanyaga	NS	15
U208	Nemzetiségi önkormányzat, nemzetiségi önkormányzati bizottságok zárt ülések jegyzőkönyvei és mellékletei, zárt ülésekről készült hanganyagok	NS	15
U209	Nemzetiségi önkormányzatok társulási megállapodásai	NS	15
U210	Nemzetiségi önkormányzat költségvetési és vagyonkezelési ügyei	NS	15
U211	Közoktatási megállapodás nemzetiségi oktatásról	NS	15
U212	Nemzetiségi önkormányzat ellenőrzése	NS	15
U213	Nemzetközi kapcsolattartás iratai	NS	15
U214	Nemzetiségi önkormányzat szabályzatai	NS	15
U215	Nemzetiségi önkormányzat törvényességi felügyeletével kapcsolatos iratok	NS	15
U216	Oktatási, nevelési, kulturális, művészeti célú pályázatok, támogatások, ösztöndíjak iratai	5	-
A polgármesteri hivatalnak, a közös önkormányzati hivatalnak, az önkormányzat gazdálkodó szervezeteinek, közalapítványainak és intézményeinek (a továbbiakban: intézményeinek) ügyei			
U.3. Szervezet, működés			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
U301	Belső ellenőrzési jelentések	10	-
U302	Biztonsági és egészségvédelmi intézkedések	2	-
U303	Érdekegyeztetés a szakszervezetekkel, érdekvédelmi és érdekképviseleti szervezetekkel, érdek-képviseleti fórumok alapítása, működtetése	NS	15
U304	Érintésvédelmi vizsgálati jegyzőkönyvek	15	-
U305	Hírlap-, folyóirat- és könyvrendelés	2	-

U306	Intézmények, érdekeltségi körbe tartozó gazdasági társaságok alapítása, alapító okiratok, tevékenység változása, megszüntetése, irányítással és működéssel kapcsolatos elvi ügyek, szervezeti és működési szabályzat, fejlesztési tervek, ellenőrzési jegyzőkönyvek, minőségirányítási program	NS	15
U307	Intézmények, érdekeltségi körbe tartozó gazdasági társaságok irányításával és működésével kapcsolatos felügyeleti, ellenőrzési, operatív ügyek	5	-
U308	Kártérítések	10	-
U309	Kollektív szerződés	NS	15
U310	Közalkalmazotti Tanács ügyei	NS	15
U311	Közérdekű kérelmek, panaszok, javaslatok, bejelentések	2	-
U312	Külföldi kapcsolatok bonyolítása	10	-
U313	Külföldi kapcsolatokra vonatkozó két- és többoldalú megállapodások, éves értékelések	NS	15
U314	Külföldi kiküldetés, tapasztalatcsere, úti jelentések	10	-
U315	Külső szervek, Állami Számvevőszék, a fővárosi és megyei kormányhivatal ellenőrzése, átvilágítás, fenntartói, szakfelügyeleti vizsgálatok, törvényességi felhívások, törvényességi felügyeleti bírsággal kapcsolatos iratok, ügyészi intézkedések, a helyi önkormányzat helyett a fővárosi és megyei kormányhivatal vezetője által megalkotott önkormányzati rendeletekkel kapcsolatos iratok, a fővárosi és megyei kormányhivatal által pótolt helyi önkormányzati határozatok, a helyi önkormányzat által pótolt feladat-ellátási kötelezettséggel kapcsolatos iratok	NS	15
U316	Munkabalesetek és foglalkozási betegségek nyilvántartása	75	-
U317	Munkáltatói juttatások elvi ügyei	NS	15
U318	Munkavédelmi ügyek (munkahelyek kialakítása, rovar-rágcsálóirtás, dohányzóhelyek kijelölése stb.)	10	-

U319	Jogi ügyek (peres és nem peres ügyek, jogi képviseleti tevékenység)	15	-
U320	Sajtóügyek, településmarketing, reprezentációs, PR tevékenység	2	-
U321	Statisztika (éves)	NS	15
U322	Statisztika (időszaki)	5	-
U323	Társulási megállapodások, társulási tanács üléseinek előterjesztései, jegyzőkönyvei, határozatai	NS	15
U324	Társulási tanács zárt üléseinek előterjesztései, jegyzőkönyvei, határozatai	NS	15
U3252	Kapcsolattartás civil és ifjúsági szervezetekkel, vallási közösségekkel	5	-
U326	Népszámlálás, egyéb összeírások lebonyolításával kapcsolatos ügyek	5	-
U327	Önkormányzatok együttműködésére vonatkozó iratok	NS	15
U328	Európai Uniós csatlakozás jogharmonizáció iratai	NS	15
U329	Közigazgatási reform előkészítésére vonatkozó iratok	NS	15
U330	Alapítványokkal, nonprofit szervezetekkel kapcsolatos ügyek	NS	15
U331	Önkormányzati feladatokat érintő stratégia, koncepció, program, terv	NS	15
U332	Társulások területének, településeinek összehangolt fejlesztésével kapcsolatos ügyek	10	-
U333	Társulási közszolgáltatások biztosítása, fejlesztése és szervezése	10	-
U334	Társulások által fenntartott intézmények ügyei	10	-
U335	Társulások egyéb operatív ügyei, területfejlesztési önkormányzati társulás ügyei	10	-
U336	Önkormányzati (fejlesztési, működési célú) elnyert pályázatok	NS	15
U337	Jegyzői hatáskörbe tartozó szabályzatok	NS	15
U338	Képviselő-testületi, képviselő-testületi bizottságok, részönkormányzatok rendeleteinek, határozatainak utólagos normakontrolljával kapcsolatos iratok	NS	15
U339	Polgármesteri, jegyzői fogadónap jegyzőkönyvei, emlékeztetői	2	-

U340	Jogszabálytervezetek, szerződések, megállapodások előzetes jogi véleményezése	2	-
U341	Önkormányzati (fejlesztési, működési célú) sikertelen pályázatok	5	-
U342	Informatikai üzemeltetés és karbantartási operatív ügyek	5	-
U343	Állásfoglalások kérése	5	-
U344	A hivatal működtetésével, karbantartásával kapcsolatos ügyek	5	-
U345	Adatvédelemmel kapcsolatos ügyek	10	-
U346	Területszervezés	NS	15
U347	Település átcsatolása másik megyéhez, területrész átadása, átvétele, cseréje	NS	15
U348	Településegyesítés, településegyesítés megszüntetése, új község alakítása	NS	15
U349	Várossá, megyei jogú várossá nyilvánítás, fővárost érintő területszervezési ügyek	NS	15
U350	Vállalkozási szerződések	5	-
U351	Munka-, szakmai értekezleti jegyzőkönyvek	5	-
U352	Beszámolók, jelentések, munkatervek (éves polgármesteri, jegyzői, szakigazgatási, intézményi)	NS	15
U353	Beszámolók, jelentések, munkatervek (időszaki jegyzői, polgármesteri, intézményi)	5	-
U354	Munkarend, ügyrend és ügyfélfogadási rend	5	-
U355	Vezetői értekezletek jegyzőkönyvei, emlékeztetői	NS	15
U356	Utasítások (jegyzői, polgármesteri)	NS	15
U357	Lobbitevékenység	10	-
U358	Hivatal, munkakör átadás-átvételi jegyzőkönyvek	10	-
U359	Körlevelek (intézkedést igénylő)	2	-
U360	Minőségbiztosítási, minőségirányítási rendszer, teljesítménykövetelmény célmeghatározása, teljesítményértékelés általános iratai	NS	15
U361	Intézkedést nem igénylő, de vezetői utasítás alapján iktatott körlevelek, meghívók, tájékoztatók	1	-

U362	Tájékoztatások, adatszolgáltatások	1	-
U363	Önkormányzati rendezvények előkészítésével és lebonyolításával kapcsolatos ügyek	1	-
U364	Társulás törvényességi felügyeletével kapcsolatos iratok	NS	15
U.4. Iratkezelés, ügyvitel			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
U401	Iratkezelési szabályzattal és irattári tervvel kapcsolatos ügyek	NS	HN
U402	Ügyvitelszervezés (saját fejlesztésű/megrendelésű elektronikus programleírások, programrendszer, védelem szabályozás stb.)	NS	15
U403	Belső ügyviteli segédkönyvek (előadói munkakönyv, érkeztető könyv, iratátadó könyv, postakönyv stb.)	5	-
U404	Kiadmányozásra használt és más, joghatás kiváltására alkalmas bélyegzők nyilvántartása, selejtezésükről, visszavonásukról készült jegyzőkönyvek	NS	HN
U405	Elektronikus aláírások nyilvántartása	NS	HN
U406	Iktató- és mutatókönyv, főnyilvántartó könyv, irattári segédkönyvek	NS	15
U407	Főnyilvántartó könyv, irattári segédkönyvek	NS	HN
U408	Iratselejtezési, iratmegsemmisítési jegyzőkönyvek	NS	HN
U409	Átmeneti irattárból a központi irattárba történő iratátadás-átvétel jegyzőkönyvei	15	-
U410	Iratátadás-átvételi jegyzőkönyvek	NS	HN
U411	Minősített adat továbbítására vonatkozó lezárt nyilvántartás (belső átadókönyv vagy más belső átadóokmány, külső kézbesítő könyv, futárjegyzék stb.)	NS	HN
U412	Irat megismerési engedélyek iratai minősített iratok esetén	NS	HN
U413	Munkakör átadás-átvétel során keletkezett iratok	5	-
U414	Nemzeti minősített adatra érvényes személyi biztonsági tanúsítvány	visszavonását követően haladéktalanul	-
U415	Felhasználói engedély és titoktartási nyilatkozat	15 (vissza-vonását	-

		követően)	
U.5. Személyzeti, bér- és munkaügyek			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
U501	Bér- és munkaügyi kimutatások, nyilvántartások, jelentések	10	-
U502	Létszám- és bérgazdálkodási ügyek (éves)	NS	15
U503	Bérnyilvántartás (bérkarton)	75	-
U504	A foglalkoztatottak illetményügyei (bérjegyzék, illetménykiegészítés, illetménypótlékok, személyi illetmény megállapítása, illetményeltérítés, járulékelszámolás, jutalom, munkáltatói kölcsön, távolléti díj, letelepedési támogatás, köztisztviselői, közalkalmazotti juttatások stb.)	50 (a jog-viszony megszű-nésétől)	-
U505	Fizetési előleg, helyettesítések, kereseti igazolás, személyzeti tárgyú pályázati kiírások és beadott pályázatok, üres álláshelyekről tájékoztatás, tartalékállománnyal, betöltetlen álláshelyekkel, pályázatokkal kapcsolatos iratok	2	-
U506	Jelenléti ívek, munkába járás költségeinek térítése, utazási utalványok ügyei, napidíjak, szabadságolási rend, szabadságügyek, egy hónapnál rövidebb fizetés nélküli szabadság	5	-
U507	Képviselők nyilvántartása, összeférhetetlensége, juttatásai, tiszteletdíjai	5	-
U508	Kinevezés, megbízás, besorolás, átsorolás, áthelyezés, minősítés, egyéni teljesítményértékelés iratai, munkaköri leírás, felmentés a képesítési előírás alól, esküokmányok, hatósági bizonyítványok, címek, kitüntetések adományozása, közszolgálati munkaviszony igazolása, rendelkezési, tartalékállományba helyezés (erről tájékoztatás) és megszüntetés, felmentés, munkavégzés alóli felmentés, nyugdíjazás, végkielégítés, eseti megbízások, összeférhetetlenség, kirendelés, prémium évek programba helyezés	50 (a jog-viszony megszű-nésétől)	-

U509	Közigazgatási alap-, és szakvizsga-kötelezettséggel kapcsolatos ügyek, ügykezelői alapvizsga-kötelezettséggel kapcsolatos ügyek	5	-
U510	Eltartói nyilatkozat	5	-
U511	Fegyelmi és kártérítési ügyek	10	-
U512	Egy hónapot meghaladó fizetés nélküli szabadság ügyek	75	-
U513	Baleseti, rokkantsági ügyek	50	-
U514	Köztisztviselők, közalkalmazottak egyéb jogviszonyainak engedélyezése	10	-
U515	Vagyonnyilatkozat (lejárat után)	*	*
U516	Megbízási szerződések	5	-
U517	Köztisztviselői, közalkalmazotti nyilvántartások	NS	HN
U518	Közhasznú, közcélú alkalmazások, távmunka egyedi ügyei	75	-
U519	Kitüntetések, kitüntető címek, díjak adományozásának előkészítése, lebonyolítása	5	-
U520	A foglalkoztatottak szociális helyzetével, munkakörülményeinek alakulásával és az esélyegyenlőség érvényesülésével kapcsolatos értékelések, jelentések, tervek, programok	NS	15
U521	Munkáltató által biztosított egyedi szociális támogatások ügyei	5	-
U522	Magánnyugdíjpénztárral, önkéntes kiegészítő nyugdíjpénztárral, önkéntes egészségpénztárral kötött szerződés	NS	HN
U523	Közszolgálati jogviták	30	-
U524	Tanulmányi szerződés	10	-
U525	Továbbképzés, átképzés egyedi ügyei, szakmai gyakorlat, egyetemi, főiskolai hallgatók szakmai gyakorlata (konzulens kérése)	2	-
U526	Továbbképzési éves és középtávú terv	10	-
* A vagyonnyilatkozat-tételi kötelezettség megszűnését vagy a kötelezett által új vagyonnyilatkozat tételét követően 8 napon belül vissza kell adni a kötelezettnek.			
U.6. Pénz- és vagyonkezelés			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
U601	Adóügyek (saját)	5	-

U602	Analitikus nyilvántartások (eszköznyilvántartás, könyvelési naplók, leltár, selejtezés)	8	-
U603	Anyag- és készletnyilvántartás, kisebb beszerzések, megrendelések	8	-
U604	Banki és pénzügyi levelezés, átutalási megbízások, bankszámlakivonat, bankszámlanyitás	5	-
U605	Közbeszerzéssel járó beruházások, építési koncessziók szervezése és pénzügyi lebonyolítása, épületfenntartás, felújítási terv, felújítások szervezése és pénzügyi lebonyolítása, közbeszerzés lebonyolítása, településüzemeltetéssel, fejlesztéssel kapcsolatos feladatok	5	-
U606	Közbeszerzéssel nem járó beruházások szervezése és pénzügyi lebonyolítása, épületfenntartás, felújítási terv, felújítások szervezése és pénzügyi lebonyolítása, településüzemeltetéssel, fejlesztéssel kapcsolatos feladatok	5	-
U607	Bizonylatok (bevétel-kiadási bizonylatok, pénztárbizonylatok, pénztárnaplók, számlák, számlatömbök tőpéldányai, készpénzellátmány bizonylatai)	8	-
U608	Fizetési felszólítás, számlareklamáció, számlarendezés, számlaegyeztetés, követelés érvényesítése, adósságelengedés	5	-
U609	Gépkocsik üzemeltetése (biztosítás a lejárat után, menetlevél, szerviz, üzemanyag stb.)	2	-
U610	Illetményszámfejtés	10	-
U611	Ingatlan- és vagyonnyilvántartás; tulajdonjog-, szolgalmi jog, vezetékjog-rendezés, nyilvántartás	NS	HN
U612	Költségvetési beszámoló (éves)	NS	15
U613	Költségvetési beszámoló (időszaki)	10	-
U614	Költségvetéssel és pénzkezeléssel kapcsolatos ügyek (adósságrendezés,	15	-

	átcsoportosítás, céltartalékok felhasználása, pénzmaradvány elszámolása, pótelőirányzat, reorganizáció, számviteli rend, intézmények közüzemi számlájának rendezése)		
U615	Céltámogatások igénylése és lebonyolítása, pályázatok pénzkezelése	15	-
U616	Hitelfelvétel és lebonyolítás, hitelnyilvántartás	15	-
U617	Költségvetés és beszámoló előkészítése, költségvetési koncepció	15	-
U618	Leltárfelvételi ívek	8	-
U619	Önkormányzati vagyon kezelésére, elidegenítésére, bérletére, cseréjére, jelzálogjaira, vásárlására, haszonbérletére, vagyonkezelői jog létesítésére vonatkozó alapiratok, szerződések, beruházási terv, tervpályázat, tulajdonosi hozzájárulás, törzskönyvi nyilvántartás	NS	HN
U620	Munkáltatói segélyek, támogatások pénzügyi lebonyolítása	5	-
U621	Szállítólevél	2	-
U622	Térségi fejlesztési program, ipari park ügyek, térségi fejlesztési tanács ügyei	NS	15
U623	Kisajátítás, kisajátítási kérelmek	NS	15
U624	Vagyonbiztonsági rendszer működtetése	10	-
U625	Vagyonbiztosítás (lejárat után)	2	-
U626	Vagyonhasznosítás pénzügyi lebonyolítása (bérlet, elidegenítés stb.)	10	-
U627	Térségi fejlesztési menedzsment ügyek	10	-
U628	Közbeszerzési ügyek (árubeszerzés, szolgáltatások megrendelése)	5	-
U629	Önkormányzati ingatlanok fenntartása, karbantartása	5	-
U630	Gazdasági program	NS	15
U631	Könyvvizsgálói jelentések	10	-
U632	Területi vagy regionális nyugdíjpénztár alakítása	NS	15
KÜLÖNÖS RÉSZ			
(ÁGAZATI IRÁNYÍTÁS, SZAKIGAZGATÁS)			
***A)* PÉNZÜGYEK**			

A.1. Adóigazgatási ügyek			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
A101	Adó- és értékbizonyítványok	8	-
A102	Adóbevételi terv és teljesítés	10	-
A103	Adóellenőrzés, adategyeztetés, adókedvezményi-mentességi ügyek, adókivetés elleni jogorvoslatok, adóbevallás és adókivetés, adóhátralék, túlfizetés, téves befizetés	15	-
A104	Adóösszesítő, valamint a számítógépes éves feldolgozás adattartalmáról év végén készített lista	5	-
A105	Adózók egyéni törzsadatai (nyilvántartás)	NS	HN
A106	Adók módjára behajtandó köztartozások iratai	10	-
A107	Vagyoni igazolások, adóigazolások	5	-
A108	Adótartozások behajtása, végrehajtása	10	-
A.2. Egyéb pénzügyek			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
A201	Általános és céltartalékok felhasználása	10	-
A202	Átmeneti gazdálkodással kapcsolatos iratok	10	-
A203	Betéti kamatügyek	5	-
A204	Decentralizált támogatások felhasználása	10	-
A205	Fejlesztési alapterv	10	-
A206	Feladatmutatókhoz kapcsolódó állami hozzájárulás előirányzata, visszaigénylés	10	-
A207	Feladatmutató-növekedés miatti pótigény	5	-
A208	Intézményi térítési díjak megállapítása, elengedése (egészségügyi, gyermekjóléti, művelődési, nevelési-oktatási, szociális)	5	-
A209	Kötvény-, részvénykibocsátás (lejárat után)	5	-
A210	Különféle célú pénzalapok, közműfejlesztési hozzájárulás visszatérítés	10	-
A211	Pénzügyi szabálysértések, bírságok	5	-
A212	Mezőőri járulék kivetése	5	-
***B)* EGÉSZSÉGÜGYI IGAZGATÁS**			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.

B101	Egészségügyi alapellátás helyzetfelmérése és megszervezése	NS	15
B102	Egészségügyi alapellátás fejlesztésének iratai	5	-
B103	Egészségügyi szűrővizsgálatok megszervezése	2	-
B104	Iskola-egészségügyi szolgálat szervezése	NS	15
B105	Körzeti egészségügyi, háziorvosi, házi gyermekorvosi, fogorvosi, gyógyszerészi, védőnői, ügyeleti ellátás megszervezése	NS	15
B106	Foglalkozás-egészségügyi ellátás megszervezése	10	-
B107	Egészségügyi ellátást támogató pályázatok	10	-
B108	Rehabilitációs Bizottság iratai	10	-
B109	Finanszírozási szerződés az egészségbiztosítási szervvel (lejárat után)	10	-
B110	Gyógyszertár felállításának kezdeményezése és véleményezése	5	-
B111	Egészségügyi szolgáltatások ÁNTSZ-től érkezett engedélyek (lejárat után)	2	-
B112	Betegek panaszügyei, betegjogi képviselő észrevételei	2	-
B113	Háziorvosi, házi gyermekorvosi, fogorvosi, gyógyszerészi, védőnői, ügyeleti pályázatok, szerződések (lejárat után)	5	-
B114	Háziorvosoknál bejelentkezett biztosítottakról havi jelentés	2	-
B115	Ifjúsági orvos (iskolaorvos) kijelölése (középfokú oktatási intézményekben)	5	-
B116	Járványügyi intézkedések	10	-
B117	Köztisztasági és településtisztasági feladatok	10	-
B118	Betegellátási díj (külföldi állampolgárok, nem biztosított magyar állampolgárok ügyei)	5	-
B119	Nyilvántartás a bejelentett biztosítottakról	10	-
B120	Társadalombiztosítási járulékügyek	75	-
B121	Szenvedélybetegek (alkohol- és kábítószer-használók, egyéb függőségben szenvedők) kötelező gondozásba vétele	30	-
B122	Házi szakápolási szolgálat, járó- és fekvőbeteg-szakellátás, óraszám, ügyeletek	NS	15

B123	Bölcsődék működésével kapcsolatos iratok	NS	15
B124	Gyógyhely, gyógyfürdőintézmény, kitermelt ásványvíz, gyógyvíz, gyógyiszap és gyógyforrástermék törzskönyvi adatai változásának bejelentése	5	-
B125	Gyógyiszap és gyógyforrástermék kitermelésének, kezelésének és forgalmazásának engedélyezése	NS	15
B126	Rágcsálómentesítés, szúnyoggyérítés, rovarirtás	2	-
B127	Az egészséges életmód segítését célzó szolgáltatások iratai	10	-
***C)* SZOCIÁLIS IGAZGATÁS**			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
C101	Személyes gondoskodás körébe tartozó alapszolgáltatások és szakosított ellátási formák megszervezése	NS	15
C102	Személyes gondoskodás körébe tartozó alapszolgáltatást, szakosított ellátásokat biztosító intézmény vagy vállalkozás működésének engedélyezése, ellenőrzése, nyilvántartása	NS	HN
C103	Személyes gondoskodás körébe tartozó szociális alapszolgáltatási ügyek	2	-
C104	Személyes gondoskodás körébe tartozó szakosított ellátást igénybevevők ügyei	2	-
C105	Személyes gondoskodás körébe tartozó szociális szolgáltatásokhoz jövedelemigazolás kiállítása	2	-
C106	Szociális ellátást támogató pályázatok	10	-
C107	Szerződés a szociális feladatok átvállalásáról	NS	15
C108	Szociálpolitikai kerekasztal működésével kapcsolatos iratok	5	-
C109	Szociális szakértői bizottság működésével kapcsolatos iratok	5	-
C110	Helyi rendeletben szabályozott rendszeres segélyek (saját ellátások)	5	-
C111	Helyi rendeletben szabályozott átmeneti ellátások (saját ellátások)	2	-
C112	Átmeneti segélyezés	2	-
C113	Árvízkárosultak állami támogatása	5	-
C114	Közüzemi kompenzációs ügyek, lakbér-hozzájárulás	2	-

C115	Lakásfenntartási támogatási ügyek	2	-
C116	Aktív korúak ellátása	10	-
C117	Temetési segély	2	-
C118	Krízishelyzetbe került személyek támogatása	5	-
C119	Szociális kölcsön egyedi ügyek (lejárat után)	5	-
C120	Adósságkezelési szolgáltatás (lakhatást segítő ellátás, adósságcsökkentési támogatás)	2	-
C121	Nyugdíjasházi elhelyezés	5	-
C122	Köztemetés	25	-
C123	Megváltozott munkaképességű dolgozók ügyei	10	-
C124	Segítséggel élők érdekvédelme, támogatása, közlekedési kedvezményei	10	-
C125	Személyi térítési díj megállapítása	10	-
C126	Gondozási szükséglet vizsgálata	15	-
C127	Behajtás, végrehajtás kezdeményezésével kapcsolatos ügyek (pl. gondozási díj)	30	-
C128	Helyi utazási támogatás megállapítása	5	-
C129	„Sikeres Magyarországért Panel Plusz" hitelprogramhoz kapcsolódó szociális támogatás	NS	HN
C130	Társhatósági megkeresések (idegen környezettanulmány, igazolások)	2	-
C131	Közgyógyellátási ügyek (méltányosság)	5	-
C132	Ápolási díj ügyek (méltányosság)	5	-
C133	Szociális ellátásra jogosultak nyilvántartásai	NS	HN
C134	Települési támogatás	5	-
***E)* KÖRNYEZETVÉDELMI, ÉPÍTÉSI ÜGYEK, TELEPÜLÉSRENDEZÉS, TERÜLETRENDEZÉS ÉS KOMMUNÁLIS IGAZGATÁS**			
E.1. Környezet- és természetvédelem			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
E101	Helyi természeti érték védetté nyilvánítása	NS	15
E102	Környezet- és természetvédelmi hatósági feladatok	10	-
E103	Környezet- és természetvédelmi program	NS	15
E104	Környezet- és természetvédelmi program végrehajtása, akcióprogramok	5	-
E105	Környezetvédelmi hatásvizsgálati eszközök telepítése	2	-

E106	Környezetvédelmi hatásvizsgálati tanulmány	NS	15
E107	A helyi természeti területek védetté nyilvánításával kapcsolatos ügyek	NS	15
E108	Védetté nyilvánított területekés védett természeti területek hasznosításának, kezelésének ügyei	5	-
E109	Zaj- és természetvédelmi, egyéb környezetvédelmi ellenőrzés és bírság	5	-
E110	Légszennyezési vizsgálatok, mérések	NS	15
E111	Légszennyező források nyilvántartása	NS	HN
E112	Levegőtisztaság-védelmi (rendkívüli) intézkedési terv (füstköd-riadóterv)	NS	15
E113	Lakóhelyi környezet állapotfelmérése	NS	15
E114	Szolgáltató tevékenységet ellátó üzemi építmény energiahordozó- és/vagy üzemmódváltásra kötelezése, tevékenységének korlátozása, felfüggesztése, illetőleg feloldása	10	-
E115	Környezetvédelmi alappal, célelőirányzattal kapcsolatos ügyek	10	-
E116	Zaj- és rezgésvédelmi szempontból fokozottan védett övezet kijelölése	30	-
E117	Stratégiai zajtérkép, ezzel összefüggő intézkedési terv	30	-
E118	Szolgáltató tevékenységet ellátók zajkibocsátással kapcsolatos ügyintézése	5	-
E.2. Településrendezési és területrendezési ügyek			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
E201	Helyi építészeti örökség védetté nyilvánítása és megszüntetése	NS	15
E202	Helyi építészeti örökség védelmének biztosítása (fenntartás, fejlesztés, őrzés, védett épületek támogatása stb.)	10	-
E203	Kulturális örökség védelmével kapcsolatos önkormányzati feladatok (pl. régészeti lelőhelyek védetté nyilvánításával összefüggésben hirdetmény elhelyezés, mentő feltárás, elővásárlási jog gyakorlása stb.)	75	-

E204	Településfejlesztési menedzsment ügyek, pályázatok	10	-
E205	Városrehabilitációs program	NS	15
E206	Városrehabilitációs pályázatok, megállapodások, ehhez kapcsolódó operatív ügyek	10	-
E207	Építészeti-műszaki tervtanács iratai (a tanácsot működtető önkormányzatnál) főépítészi szakmai vélemények, állásfoglalások	NS	15
E208	Átnézeti nyilvántartási térkép, földmérési alaptérkép	NS	HN
E209	Pincebeomlások, támfal, partfal által veszélyeztetett területek felmérése	NS	15
E210	Területfejlesztési koncepció, területrendezési terv, településfejlesztési koncepció, településfejlesztési stratégia, településszerkezeti terv, helyi építési szabályzat	NS	15
E211	Elővásárlási jog	NS	15
E212	Útépítési és közművesítési hozzájárulás	NS	15
E213	Területrendezési hatósági eljárások	15	-
E214	Vis maior ügyek	5	-
E215	Repülőterek zajgátló védőövezetének kialakítása	10	-
E216	Kiszolgáló és lakóút céljára történő lejegyzés	NS	15
E217	Településrendezési kötelezések	NS	15
E218	Településrendezési szerződés	NS	15
E219	Településképi véleményezési eljárás	15	-
E220	Településképi bejelentési eljárás	15	-
E221	Közterület-alakítás	15	-
E222	Közműnyilvántartás ügyei	NS	15
E.3. Építési ügyek			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
E301	Bontási-, építési-, összevont-, használatbavételi-, fennmaradási engedélyezési eljárások, építésügyi vagy eljárási bírság kiszabása, bontási vagy átalakítási kötelezettség, végrehajtási eljárás, engedély hatályának meghosszabbítása iránti engedélyezési eljárás	NS	15
E302	Felvonóval, illetve mozgólépcsővel kapcsolatos építésügyi hatósági engedélyezési eljárás	15	-

E303	Építésügyi hatósági tudomásulvételi eljárások (jogutódlás tudomásul vétele, használatbavétel tudomásul vétele)	10	-
E304	Az országos építési követelményektől való eltérés engedélyezési eljárása	10	-
E305	Építésügyi hatósági bizonyítványok, igazolások, adatkérés, adatszolgáltatás	10	-
E306	Egyéb építésügyi hatósági kötelezési ügyek	10	-
E307	Építésügyi hatósági ellenőrzés	10	-
E308	Bauxitcementtel vagy más építőanyag-hibával kapcsolatos hatósági eljárások	NS	HN
E309	Építésüggyel kapcsolatos panaszok és egyéb észrevételek intézése, tájékoztatások, szolgáltatás körében kiadott szakmai nyilatkozat	5	-
E.4. Kommunális ügyek			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
E401	Hulladéklerakó-helyek (szilárd, állati eredetű, folyékony) kijelölése, létesítése, hulladékkezelési szerződések, hulladékgazdálkodási program	NS	15
E402	Közcélú ártalmatlanító telep létesítése	NS	15
E403	Kéményseprő-ipari szolgáltatás ügyei	15	-
E404	Zöldterületek létesítése, fenntartása (parkok, játszóterek)	NS	15
E405	Energiagazdálkodás, szélerőmű létesítése	NS	15
E406	Köztemetők létesítése, lezárása, megszüntetése, nyilvántartásai, térképei, újbóli használatba vétele	NS	HN
E407	Sírboltkönyv, síremlékek és sírboltok terve	NS	HN
E408	Hozzájárulás temetkezési szolgáltatást végző gazdálkodó szervezet alapításához	5	-
E409	Hulladékká vált járművek ügyei, gépjármű elszállítási és értékesítési ügyek	5	-
E410	Közműfejlesztés, ingatlanok közműellátása, közműfejlesztési hozzájárulás visszafizetésének ügyei	NS	15

E411	Közterületi felújítás, karbantartás, hibaelhárítás	5	-
E412	Közterület tisztán tartása, felügyelete, hulladék elhelyezése, gyűjtése, szállítása, hulladékártalmatlanítás, hulladékújrahasznosítás, hulladékgazdálkodási bírság ügyek	5	-
***F)* KÖZLEKEDÉS ÉS HÍRKÖZLÉSI IGAZGATÁS**			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
F101	Közutak, helyi vasutak műszaki, minőségi, baleseti, forgalmi adatainak, valamint forgalmi rendjét meghatározó jelzéseinek nyilvántartása	NS	HN
F102	Közutak, helyi vasutak tisztán tartása, síkosság elleni védekezés	2	-
F103	Közterület-foglalási, -használati megállapodások és díjak	5	-
F104	Közterület-bontási hozzájárulás	5	-
F105	Külterületi közút, helyi vasút menti építmény elhelyezési és nyersanyag-kitermelési hozzájárulás	5	-
F106	Külterületi közút, helyi vasút menti fakivágási és ültetési hozzájárulás	5	-
F107	Belterületi közútkezelői hozzájárulások	5	-
F108	Közúton, helyi vasúton történő építési munkákhoz való hozzájárulás	2	-
F109	Vasúti átkelőhelyek, gépkocsibehajtók, gyalogutak, járdák, kerékpárutak, közutak fenntartása, parkolók kialakítása, fenntartása	10	-
F110	Egyéb közútkezelői hozzájárulás	1	-
F111	Utcabútorok, utca névtáblák, házszámtáblák kihelyezése, karbantartása, javítása	5	-
F112	Repülőtér létesítésének és megszüntetésének véleményezése	5	-
F113	Kikötők, (közforgalmú) kompok és révek létesítése	NS	15
F114	Közforgalmú kikötők, kompok, révek működtetése	10	-
F115	Hidak, aluljárók és felüljárók létesítése	NS	15
F116	Hidak, aluljárók és felüljárók működtetése	10	-

F117	Hídtörzskönyv	NS	HN
F118	Közvilágítási berendezés létesítése	NS	15
F119	Közvilágítási berendezés működtetése	10	-
F120	Forgalomszabályozás, forgalomtechnika	5	-
F121	Helyi tömegközlekedés fejlesztési koncepciója	NS	15
F122	Helyi közforgalmú vasúti társasággal kapcsolatos ügyek	10	-
F123	Hatósági árak megállapítása (helyi tömegközlekedés, taxi, vasút), menetrend	5	-
F124	Helyi tömegközlekedési pályázat	10	-
F125	Postai, távközlő, elektromos, valamint más nagyfrekvenciás jelet vagy mellékhatást keltő berendezések létesítése, üzemeltetése, rongálása, hírközlési szabálysértések	10	-
F126	Távközlési és egyéb nyomvonaljellegű építmények létesítéséhez való hozzájárulás	NS	15
F127	Útellenőri szolgálat megszervezése	5	-
F128	Útvonalengedélyek	1	-
F129	Parkolási, eseti behajtási, egyéb eseti közlekedési engedély	2	-
F130	Közlekedési kártérítések	5	-
F131	Kerékbilincs alkalmazásának ügyei	2	-
F132	Behajtási engedélyek	2	-
***G)* VÍZÜGYI IGAZGATÁS**			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
G101	Árvíz és belvízzel, helyi vízkárelhárítással kapcsolatos operatív ügyek	5	-
G102	Árvíz- és belvíz-védekezési terv	NS	15
G103	Védművek létesítése és fejlesztése	NS	15
G104	Védművek működtetése	5	-
G105	Patakok, csatornák áradásai elleni védekezés, csapadékvízelvezetés	NS	15
G106	Vízi közüzemi tevékenység koncepciója, vízrendezési programok	NS	15
G107	Ivóvíz, szennyvízdíjak megállapítása	10	-
G108	Közműves vízszolgáltatási korlátozási terv, vízkorlátozás ügyei	5	-
G109	Vízjogi létesítési, fennmaradási és üzemeltetési engedély	NS	HN

G110	Ivóvíz-, szennyvíztisztító berendezés létesítésének engedélyezése	NS	15
G111	Ivóvíz-, szennyvízhálózat, csapadékcsatorna-hálózat létesítése, üzemeltetőjének kijelölése	NS	15
G112	Ivóvíz-, szennyvízhálózat, csapadékcsatorna-hálózat üzemeltetése	5	-
G113	Vízmérőhely, tisztítóakna ügyei	15	-
G114	Közkifolyókkal, tűzcsapokkal kapcsolatos ügyek	2	-
G115	Kutak létesítési, fennmaradási és üzemeltetési engedélye	NS	15
G116	Vízvezetési és szennyvízelvezetési szolgalmi ügyek	5	-
G117	Azonos telken több ívóvízbekötő vezeték létesítése	2	-
G118	Víziközmű-használattal kapcsolatos iratok	NS	15
G119	Víziközmű-társulat, érdekeltségi hozzájárulással kapcsolatos iratok	15	-
G120	Vizek és vízi létesítmények nyilvántartása	NS	HN
G121	Közműfejlesztési támogatáshoz kapcsolódó iratok	15	-
G122	Talajterhelési ügyek	5	-
G123	Vízszennyezési, vízvédelmi és csatornabírság ügyek	5	-
G124	Folyékonyhulladék-bebocsátási pontok kijelölése	15	-
G125	Vízi állással kapcsolatos ügyek	2	-
***H)* ÖNKORMÁNYZATI, IGAZSÁGÜGYI ÉS RENDÉSZETI IGAZGATÁS**			
H.1. Anyakönyvi és állampolgársági ügyek			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
H101	Állampolgársági eskü jegyzőkönyv	NS	HN
H102	Anyakönyv, anyakönyvi alapirat, betűrendes névmutató, családi jogállás rendezésével kapcsolatos irat, apa adatai nélkül anyakönyvezett születések nyilvántartása, házasságkötéssel, bejegyzett élettársi kapcsolat létesítésével kapcsolatos jegyzői engedély, felmentés	NS	HN
H103	Nyilvántartás a helyi anyakönyvvezetői megbízásokról és jogosultságokról, valamint a helyettesítéssel kapcsolatos iratok	NS	HN
H104	Anyakönyvi okirat kiállítása iránti kérelem, belföldi és külföldi	5	-

	jogsegély iránti kérelem, anyakönyvi kivonat átvételi elismervénye, anyakönyvi adatszolgáltatás iratai, anyakönyvbe történő betekintés iratai, anyakönyvi események egyeztetése		
H105	Anyakönyvi Szolgáltató Rendszer működésével kapcsolatos egyéb ügyek	10	-
H106	Állampolgársági egyéb ügyek, hazai anyakönyvezési kérelem, névváltoztatási kérelem felterjesztésével, továbbá házassági névmódosítási kérelem áttételével kapcsolatos iratok, családi események polgári szertartása	2	-
H107	Külföldön történő házasságkötéshez, bejegyzett élettársi kapcsolat létesítéséhez szükséges tanúsítvány kiállításával kapcsolatos iratok	5	-
H.2. A polgárok személyi adatainak, lakcímének nyilvántartásával kapcsolatos ügyek			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
H201	Adategyeztetés	5	-
H202	A polgárok személyi adatainak és lakcímének nyilvántartásával kapcsolatos ügyek	5	-
H203	A címnyilvántartással kapcsolatos ügyek	15	-
H.3. Választásokkal kapcsolatos ügyek			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
H301	Választási jegyzőkönyvek (szavazóköri és eredményjegyzőkönyvek) első eredeti példánya	NS	#90 nap
H302	Választási jegyzőkönyvek (szavazóköri és eredményjegyzőkönyvek) második eredeti példánya	NS	5
H303	Szavazókörök, helyi önkormányzati választókerületek megállapítása	NS	15
H304	Választási szervek (választási irodák, választási bizottságok) létrehozása és tevékenysége	NS	15
H305	Választások lebonyolításával kapcsolatos kisebb jelentőségű ügyek	5	-
H306	Népszavazás, népi kezdeményezés iratai	NS	15

H307	Választójogosultság nyilvántartásával kapcsolatos ügyek (kifogás, felvételi kérelem, igazolás stb)	5	-
# A jegyzőkönyvek első példányának illetékes levéltárba történő átadása érdekében a külön jogszabályi előírások alapján kell intézkedni.			
H.4. Rendőrségi ügyek			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
H401	Rendőrfőkapitány, rendőrkapitány és rendőrőrs vezetője kinevezésének véleményezése, felmentésről szóló tájékoztatás	10	-
H402	Rendőrkapitányság, rendőrőrs, körzeti megbízotti állomás létesítésének, megszüntetésének véleményezése	10	-
H403	Rendőrségi munkával kapcsolatos észrevételek, éves beszámoló elfogadása	2	-
H404	Együttműködési szerződés a rendőri feladatok ellátásának segítésére, támogatására, bűnmegelőzési önkormányzati feladatok	NS	15
H405	Polgárőrség megalakítása	NS	15
H406	Bűnmegelőzési és közbiztonsági bizottság létrehozásával, működésével kapcsolatos iratok	5	-
H.5. A helyi tűzvédelemmel kapcsolatos ügyek			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
H501	Fenntartási, fejlesztési és működési ügyek	10	-
H502	Önkéntes tűzoltóság alapításával, működésével kapcsolatos iratok	NS	15
H503	Tűz- és műszaki mentés jelzés, oltóvíz-nyerés ügyei	5	-
H504	Tűzvédelmi kötelezettség megállapítása	NS	15
H505	Tűzoltók képzésével, továbbképzésével kapcsolatos iratok	10	-
H506	Önkéntes tűzoltó jövedelmének megtérítése, kár megtérítése, kártalanítás	5	-
H507	Készenléti szolgálatot, tűzoltás irányítását ellátó tagok részére élet- és balesetbiztosítás megkötése	5	-
H508	Tűzvédelmi kötelezettség megsértése miatti tevékenységtől eltiltás	2	-

H509	Lakosság tűzvédelmi felvilágosítása	5	-
H510	Éves beszámoló elfogadása	2	-
H.6. Menedékjogi ügyek			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
H601	Együttműködés a menekültügyi szervekkel	15	-
H.7. Igazságügyi igazgatás			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
H701	Bírósági ülnökök jelölése, megválasztása és visszahívása	5	-
H702	Birtokvédelmi ügyek	5	-
H7034	Vallási közösség tulajdonában lévő ingatlanok tulajdoni helyzetének rendezése	NS	15
H704	Eltartási szerződési ügyek (lejárat után)	5	-
H705	Közalapítvány létrehozása	NS	15
H.8. Egyéb igazgatási ügyek			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
H801	Címerhasználat, névhasználat, turisztikai logó engedélyezése, zászló (lobogó) kitűzésével kapcsolatos iratok	5	-
H802	Hagyatéki ügyek	NS	HN
H803	Hatósági bizonyítványok, igazolások, adatkérés, adatszolgáltatás	5	-
H804	Jelzálogügyek (lejárat után)	5	-
H805	Közigazgatási bírság	5	-
H806	Tűzszerészeti mentesítés, fel nem robbant lövedékek, rendkívüli események (bombariadó stb.) bejelentése, helyszíni mentesítése	5	-
H807	Talált tárgyak ügyei	1	-
H808	Utcanévváltozások, házszámrendezés	NS	15
H809	Ingatlanforgalom (elidegenítési tilalom elrendelése, törlése)	5	-
H810	Tolmács és szakfordító igazolvány kiadása	5	-
H811	Tolmács és szakfordítói nyilvántartás	NS	HN
H812	Hirdetmények (ingatlan bérleti, vételi ajánlat, haszonbérlet is) kifüggesztéséről igazolás	2	-
H813	Külföldiek ingatlanszerzésével kapcsolatos nyilatkozatok	5	-
H814	Ingatlanközvetítői, ingatlanvagyon-értékelő és közvetítői névjegyzék vezetése	NS	HN
H815	Közüzemi fogyasztók szerződéséhez kapcsolódó ügyek (szerződéskötés, -szegés stb.)	5	-

H816	Tűzijáték engedélyezése	2	-
H817	2012. április 15. előtt elkövetett szabálysértések végrehajtással kapcsolatos iratai	5	-
***I)* LAKÁSÜGYEK**			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
I101	Önkormányzati bérlakásra várók ügyei, névjegyzéke	15	-
I102	Bérlakások nyilvántartása	NS	HN
I103	Jogcím nélküli lakáshasználat	5	-
I104	Lakásbérleti szerződés, lakáscsere, lakáshasznosítás (lejárat után), lakásbérleti szerződés megszűnése	5	-
I105	Lakás- és helyiségbérleti díjtartozás	5	-
I106	Társasházak alapítása, elidegenítés	NS	15
I107	Társasház-felújítási ügyek és társasház-felújítási pályázatok, társasházak operatív ügyei	10	-
I108	Helyiség-, garázsbérleti, - elidegenítési szerződés, helyiséggazdálkodási ügyek (lejárat után)	5	-
I109	Első lakáshoz jutás, lakásépítés, lakásvásárlás, egyéb lakáscélú támogatás egyedi ügyek (lejárat után)	15	-
I110	Lakásfelújítási, karbantartási támogatás	15	-
I111	Lakáscélú állami támogatásokkal kapcsolatos iratok (ingatlan-nyilvántartásba jelzálog, elidegenítési és terhelési tilalom bejegyeztetése, törlése, döntésekről és intézkedésekről adatszolgáltatás stb.)	NS	15
I112	Jegyzői igazolás lakásépítési kedvezményhez, pénzintézeti hitelhez	5	-
I113	Nyilvántartásba nem vett, elutasított kérelmek	5	-
***J)* GYERMEKVÉDELMI ÉS GYÁMÜGYI IGAZGATÁS**			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
J101	Szülő adatai nélkül anyakönyvezett gyermekek nyilvántartása	NS	HN
J102	Gyámhatósági és gyermekvédelmi munka szakmai, felügyeleti ellenőrzése (éves értékelés)	NS	15

J103	Rendszeres gyermekvédelmi kedvezmény	2	-
J104	Gyermekvédelmi kedvezmény nyilvántartása	NS	HN
J105	Rendkívüli gyermekvédelmi támogatás	2	-
J106	Kiegészítő gyermekvédelmi támogatás	2	-
J107	Személyes gondoskodás körébe tartozó gyermekvédelmi szakellátások	5	-
J108	Óvodáztatási támogatás megállapítása	5	-
J109	Halmozottan hátrányos helyzetű gyermekek nyilvántartása	NS	HN
J110	Halmozottan hátrányos helyzetű gyermekek részére kiadott igazolások	5	-
J112	Gyermekvédelmi intézkedést valószínűsítő lakossági vagy jelzőrendszeri jelzések	2	-
J113	Más hatóság megkeresésére készített környezettanulmányok, egyéb társhatósági megkeresések	2	-
J114	Helyettes szülői hálózat megszervezése	75	-
***K)* IPARI IGAZGATÁS**			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
K101	Atomerőmű, veszélyes ipari üzemek biztonsági, veszélyességi övezetének megállapítása	75	-
K102	Energiaellátási tanulmány	NS	15
K103	Földalatti tárolótérségek nyilvántartása	NS	HN
K104	Gazdasági érdek-képviseleti jogok gyakorlása	NS	15
K105	Telepengedélyezési eljárások, bejelentésköteles tevékenységek folytatásának bejelentése; telepengedélyhez, illetve bejelentéshez kötött tevékenységek folytatásának ellenőrzése és annak jogkövetkezményei	10	-
K106	Telepengedélyek, bejelentésköteles tevékenységek, nyilvántartása	NS	15
K107	Törzsvezetékek létesítése és vezetékjogi engedélyezési eljárása	5	-
***L)* KERESKEDELMI IGAZGATÁS, TURISZTIKA**			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.

L101	Turisztikai értékek fejlesztési koncepciója	NS	15
L102	Turisztikai értékek feltárása, bemutatása, fejlesztések, tanulmányok	10	-
L103	Turisztikai hivatal működtetése, turisztikai tervek, kapcsolódó operatív ügyek	10	-
L104	Turisztikai marketing, turisztikai rendezvények szervezése	2	-
L105	Turisztikai témájú pályázatok	10	-
L106	Turistatájékoztató berendezések, információs eszközök telepítése, fejlesztése, karbantartása	2	-
L107	Szálláshely-üzemeltetési engedély kiadása, a tevékenység folytatásának ellenőrzése és annak jogkövetkezményei	10	-
L108	Szálláshelyek, szálláshely-szolgáltatók nyilvántartása	NS	HN
L109	Nem üzleti célú közösségi, szabadidős szálláshely szolgáltatás végzésének bejelentése, a tevékenység folytatásának ellenőrzése és annak jogkövetkezményei	10	-
L110	Nem üzleti célú közösségi, szabadidős szálláshelyek nyilvántartása	NS	HN
L111	Vásár, piac rendezésének engedélyezése, bevásárlóközpont üzemeltetésének bejelentése, adatváltozások bejelentése, tevékenység folytatásának ellenőrzése és annak jogkövetkezményei	10	-
L112	Vásár, piac és bevásárlóközpontok nyilvántartása	NS	HN
L113	Működési engedély köteles kereskedelmi tevékenység folytatásának engedélyezése, bejelentésköteles kereskedelmi tevékenység folytatásának bejelentése, zenés, táncos rendezvények rendezvénytartási engedélyezése, adatváltozások bejelentése, tevékenység folytatásának ellenőrzése és annak jogkövetkezményei	10	-
L114	Bejelentéshez kötött kereskedelmi tevékenységek nyilvántartása, működési engedéllyel rendelkező üzletek nyilvántartása	NS	HN

L115	Szerencsejáték-szervező tevékenység végzéséhez szükséges okiratok kiállítása, játékterem működéséhez való hozzájárulás megadása; szerencsejáték-szervező tevékenység gyakorlásának átengedése tárgyában önkormányzat egyetértése koncessziós pályázat kiírásához	10	-
L116	Vásárlói panasz	2	-
L117	Fogyasztóvédelemmel kapcsolatos ügyek	5	-
***M)* FÖLDMŰVELÉSÜGY, ÁLLAT- ÉS NÖVÉNYEGÉSZSÉGÜGYI IGAZGATÁS**			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
M101	Állategészségügyi ellátással kapcsolatos ügyek	5	-
M102	Állati hulladékgyűjtő hellyel, gyűjtő-átrakó teleppel (gyepmesteri teleppel), kedvtelésből tartott állatok kegyeleti temetőjével kapcsolatos iratok	10	-
M103	Állatorvosi körzetek alakítása	10	-
M104	Állatszállítás és marhalevél kezelés	2	-
M105	Állattartási, állatvédelmi ügyek	5	-
M106	Állattartók és állatállomány nyilvántartása	NS	HN
M107	Marhalevél nyilvántartás	NS	HN
M108	Veszélyes állatok tartási engedélye	10	-
M109	Árutermelő ültetvény helyszíni szemléje, határszemle	5	-
M110	Belterületi növényvédelem és ellenőrzése	10	-
M111	Parlagfű elleni védekezés	5	-
M112	Borászati hatósági ügyek	5	-
M113	Járványügyi intézkedések, élelmiszerlánccal, élelmiszerbiztonsággal összefüggő intézkedések, veszélyes kártevők elleni védekezés	15	-
M114	Méhészekkel kapcsolatos egyedi ügyek	5	-
M115	Méhészek és méhvándorlás nyilvántartása	NS	HN
M116	Mezei őrszolgálattal kapcsolatos ügyek megszervezése	15	-
M117	Nyilvántartás az árutermelő szőlő és gyümölcs telepítéséről, kivágásáról	NS	HN

M118	Fás szárú és cserje kivágási bejelentések, engedélyek, közterületi fa- és cserjepótlás	5	-
M119	Tarló, avar, kerti hulladék-égetési ügyek	2	-
M120	Halászati jogok gyakorlása (holtágak, bányatavak)	15	-
M121	Vadászterületi résztulajdonosok közös képviseleti ügyei	10	-
M122	Vadkárral, halászati károkkal kapcsolatos iratok	5	-
M123	Állami tulajdonú földingatlan tulajdonjogának megszerzése	NS	15
M124	Belterületi és külterületi határvonalak megállapítása	NS	15
M125	Földkiadó bizottság, birtokhasznosítási bizottság iratai	NS	15
M126	Hivatalos földrajzi nevek megállapításával, megváltoztatásával kapcsolatos iratok (véleménykérés, javaslat, véleményezés)	NS	15
M127	Művelési ágváltozások	10	-
M128	Térképészeti határkiigazítás	NS	15
M129	Termőföld elővásárlási és előhaszonbérleti jog gyakorlásával kapcsolatos iratok	5	-
M130	Újrahasznosításra alkalmassá tett terület önkormányzati tulajdonba vétele	NS	15
***N)* MUNKAÜGYI IGAZGATÁS, MUNKAVÉDELEM**			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
N101	Foglalkoztatási érdekegyeztetés, tervek	NS	15
N102	Közfoglalkoztatási terv, közhasznú, közcélú foglalkoztatás szervezése, álláshelyek, közérdekű munkával kapcsolatos operatív ügyek	3	-
***P)* KÖZNEVELÉSI ÉS KÖZMŰVELŐDÉSÜGYI IGAZGATÁS**			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
P101	Közoktatási fejlesztési és intézkedési terv, esélyegyenlőségi intézkedési terv	NS	15
P102	Közoktatási intézmények jegyzéke	NS	15
P103	Nevelési és pedagógia program, minőségirányítási program	NS	15
P104	Iskolaszék alakítása, tagok delegálása, egyéb iskolaszéki ügyek	NS	15
P105	Óvodákkal és egységes óvoda-bölcsődékkel kapcsolatos iratok	15	-

P106	Általános iskolákkal és alapfokú művészetoktatási intézményekkel kapcsolatos iratok	15	-
P107	Szakiskolákkal kapcsolatos iratok	15	-
P108	Középiskolákkal (gimnáziumokkal és szakközépiskolákkal) kapcsolatos iratok	15	-
P109	Gyógypedagógiai, konduktív pedagógiai nevelési-oktatási intézménnyel kapcsolatos iratok	15	-
P110	Diákotthonokkal és kollégiumokkal kapcsolatos iratok	15	-
P111	Szakszolgáltatással, szakmai szolgáltatással kapcsolatos iratok	15	-
P112	Állandó pedagógus helyettesítési rendszer megszervezése	5	-
P113	Bizonyítványmásodlatok kiállítása	2	-
P114	Érettségi szervezési, érettségi vizsgabizottsági ügyek	5	-
P115	Gyermekek szakértői vizsgálata, iskolaérettséget tanúsító vizsgálat, szakvélemény	5	-
P116	Intézményi felvételi és fegyelmi ügyekben törvényességi kérelem	2	-
P117	Iskolai, óvodai felvételi eljárás szervezése	2	-
P118	Kötelező felvételt biztosító iskola kijelölése	10	-
P119	Tanuló- és gyermekbaleseti ügyek	5	-
P120	Tanköteles és fejlesztő iskolai oktatásra köteles tanulók nyilvántartása	NS	HN
P121	Pedagógus igazolvány ügyek	2	-
P122	Közoktatási, kulturális megállapodások	NS	15
P123	Integrált oktatás során keletkező iratok	5	-
P124	Tanulói jogviszony igazolása	2	-
P125	Közoktatási Információs Rendszer ügyei	5	-
P126	Felnőttoktatással kapcsolatos ügyek	15	-
P127	Közművelődési Tanács ügyei	NS	15
P128	Levéltári és muzeális értékek közgyűjteményi megőrzése, rendelkezési jog gyakorlása	NS	15
P129	Művészeti alkotások elhelyezésének véleményezése	5	-
P130	Nem helyi önkormányzat által alapított nevelési, oktatási, kulturális, művészeti intézmények működésének engedélyezése, működéssel kapcsolatos egyéb ügyek	NS	15
P131	Művészeti ügyek	NS	15

P132	Intézményi vezetők munkakör átadás-átvétele	5	-
P133	Intézmények beruházásával, felújításával kapcsolatos iratok	10	-
P134	Helyi önkormányzat által működtetett kulturális intézmények (közművelődési, közgyűjteményi intézmények, múzeumok, könyvtárak, levéltárak) létesítésének és közösségi színterek biztosításának iratai	NS	15
P135	A közművelődéssel kapcsolatos operatív ügyek iratai	5	-
P136	Nyilvános könyvtári ellátás biztosításával kapcsolatos iratok	NS	15
P137	Régészeti jelentőségű földterület védetté nyilvánítása	NS	15
P138	Műemléki és építészeti értékek felkutatása	5	-
P139	Szobrok, művészi alkotások, emlékművek, emléktáblák állítása, újraállítása, kialakítása	NS	15
P140	Szobrok, művészi alkotások, emlékművek, emléktáblák, helyi építészeti értékek védelme, fenntartása	10	-
P141	Oktatási, nevelési, kulturális, művészeti tárgyú pályázatok, támogatások, ösztöndíjak	10	-
P142	Ünnepségek, ünnepélyek, rendezvények szervezése	5	-
***R)* SPORTÜGYEK**			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
R101	Sportegyesületek, sportlétesítmények, sportolók támogatása, pályázatok, szponzori szerződések	10	-
R102	Sportlétesítményekre, versenyengedélyekre vonatkozó adatszolgáltatásokkal összefüggő iratok	10	-
R103	Testnevelési és sportfeladatok koncepciója	NS	15
R104	Sportfeladatokkal kapcsolatos operatív ügyek	5	-
R105	Sportrendezvények ügyei	5	-
***X)* HONVÉDELMI, KATASZTRÓFAVÉDELMI IGAZGATÁS, FEGYVERES BIZTONSÁGI ŐRSÉG**			
X.1. Honvédelmi igazgatás			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.

X101	Hadkötelesek tájékoztatási és bejelentési kötelezettségéhez tartozó ügyek	2	-
X102	Hadkötelesek sorozásával kapcsolatos ügyek	2	-
X103	Potenciális hadkötelesek, hadkötelesek nyilvántartásához kapcsolódó adatszolgáltatás	5	-
X104	Meghagyással kapcsolatos ügyek	3	-
X105	Gazdasági és anyagi szolgáltatások előkészítésével, elrendelésével, kártalanítással kapcsolatos ügyek	5	-
X106	A NATO Válságreagálási Rendszerrel, az Európai Unió válságkezelési mechanizmusaival összhangban álló nemzeti intézkedési rendszerrel kapcsolatos ügyek	30	-
X107	Rendkívüli intézkedésekkel kapcsolatos ügyek	NS	HN
X108	Honvédelmi célú terület-előkészítési ügyek	5	-
X109	Nemzetgazdaság honvédelmi célú felkészítésének ügyei	30	-
X110	Befogadó Nemzeti Támogatással kapcsolatos ügyek	30	-
X111	Honvédelemi szempontból létfontosságú (kritikus) infrastruktúra védelmével kapcsolatos ügyek	30	-
X112	Polgári veszélyhelyzeti tervezés honvédelmi feladataival kapcsolatos ügyek	30	-
X113	Védelmi bizottságok üléseivel kapcsolatos iratok	5	-
X114	Felkészítések, gyakorlatok	5	-
X115	Intézkedési tervek, munkajegyek	5	-
X116	Lakosság tájékoztatása	5	-
X117	Gazdaságfelkészítés és mozgósítási feladatok ellátásával kapcsolatos iratok	30	-
X118	Munkacsoportokkal, ügyeleti szolgálatokkal kapcsolatos iratok	5	-
X.2. Katasztrófavédelmi igazgatás			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
X201	Életvédelmi létesítmények (óvóhely) kijelölése	NS	HN
X202	Életvédelmi létesítmények fenntartása	10	-
X203	Életvédelmi létesítmények hasznosítása	10	-
X204	Rendkívüli intézkedések	NS	HN
X205	Polgári védelmi terv	NS	HN

X206	Polgári védelmi szervezet létrehozása (területi, települési, munkahelyi is)	NS	HN
X207	Polgári védelmi felkészítési követelmények	10	-
X208	Polgári védelmi készletgazdálkodási ügyek	10	-
X209	Polgári védelmi személyi állomány nyilvántartása	30	-
X210	Polgári védelmi kötelezettség teljesítése alóli mentesség igazolása	10	-
X211	Polgári védelmi ügyeleti és jelentési feladatok	10	-
X212	Önkéntesek nyilvántartása	30	-
X213	Katasztrófavédelmi terv	NS	HN
X214	Katasztrófariasztás elrendelése és végrehajtása	NS	HN
X215	Katasztrófavédelmi gyakorlatok	10	-
X216	Veszélyelhárítási terv	NS	HN
X217	Gazdasági-anyagi szolgáltatásokkal kapcsolatos vagyonelemek kijelölése, szolgáltatás elrendelése, átadás-átvételi jegyzőkönyv, kártalanítás	NS	HN
X218	Termelési, ellátási és szolgáltatási kötelezettségre vonatkozó szerződés	NS	HN
X219	Védelmi bizottságok iratai	NS	15
X220	Visszamaradó készletek	10	-
X221	Helyreállítási és újjáépítési ügyek	NS	15
X222	Veszélyes ipari üzemek külső védelmi tervének készítésével és gyakoroltatásával, valamint a lakossági tájékoztató kiadványok készítésével kapcsolatos iratok	NS	HN
X223	Települések veszélyeztetettségének felmérése	10	-
X224	Logisztikai feladatok ellátása	10	-
X225	Egyéni védőeszközökkel történő ellátási feladatok	10	-
X226	Létfontosságú anyagi javak védelme, kritikus infrastruktúra védelme	30	-
X227	A kulturális javak védelmével kapcsolatos feladatok	30	-
X228	Kitelepítéssel, kimenekítéssel, kiürítéssel, befogadással kapcsolatos iratok	NS	HN
X229	Menekültek elhelyezésével és ellátásával kapcsolatos feladatok	30	-
X230	Halálos áldozatokkal kapcsolatos halaszthatatlan intézkedések	30	-
X231	Nemzetközi kapcsolatok és katasztrófa segítségnyújtás	10	-

X232	Lakosság tájékoztatása	10	-
X.3. Fegyveres biztonsági őrség			
Irattári tételszám	Tétel megnevezése	Megőrzési idő (év)	Lt.
X301	Fegyveres biztonsági őrség létrehozása, működtetése, megszüntetése	15	-
X302	Rendészeti ügyek	2	-