Informatikai Biztonsági Szabályzat

Tartalom

1 Általános rész

1.1. A szabályzat célja

A Nyőgéri Közös Önkormányzati Hivatal (a továbbiakban: Hivatal) Informatikai Biztonsági Szabályzatának (a továbbiakban: szabályzat) célja, hogy a hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában biztosítsa az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét. Ennek érdekében meghatározza a szervezetnek a jogszabályban előírt adminisztratív, fizikai és logikai védelmi intézkedéseket, amelyek támogatják:

a) a megelőzést és a korai figyelmeztetést,

b) az észlelést,

c) a reagálást,

d) a biztonsági események kezelését.

A szabályzat céljainak megvalósítását annak figyelembe vételével kell megszervezni, hogy az önkormányzat Hivatala informatikai szakrendszerei az önkormányzati ASP központban üzemelnek. Ennek megfelelően:

- Az önkormányzati ASP rendszer szakrendszereinek biztonsági osztályba sorolását a Magyar Államkincstártól kapja meg, azokat a nem kell biztonsági osztályba sorolni.
- A védelmi intézkedéseket a jogszabály alapján kijelölt szolgáltató követelményeinek megfelelően kell meghatározni és alkalmazni.
- A Hivatal információbiztonsági tevékenysége elsődlegesen az elektronikus információs rendszerrel kapcsolatba kerülő személyek információbiztonsággal kapcsolatos kötelezettségeinek szabályozására, számonkérésére terjed ki, addig a mértékig, ameddig a szervezet vagy az egyes személyek tevékenysége az elektronikus információs rendszerre hatást tud gyakorolni.

1.2. A szabályzat hatálya

1.2.1. Személyi hatály

A szabályzat személyi hatálya kiterjed a Hivatal informatikai rendszereit használó, valamint azzal egyéb céllal kapcsolatba kerülő természetes és jogi személyekre:

- a választott tisztségviselőkre,
- köztisztviselőire, ügykezelőire, munkavállalóira, (a továbbiakban együtt: munkatárs),
- a Hivatal elektronikus információs rendszerével, szolgáltatásaival szerződéses vagy más módon kapcsolatba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (a továbbiakban együtt: külső személy) a velük kötött szerződésben rögzített mértékben, illetve megállapodás szerint.

1.2.2. Tárgyi hatály

A szabályzat tárgyi hatálya a Hivatal használatában lévő vagy általa üzemeltetett valamennyi meglévő és a jövőben bevezetendő elektronikus információs rendszerre és azok környezetét alkotó rendszerelemekre terjed ki, azok teljes életciklusában (az előkészítéstől a rendszerből történő kivonásig), kivéve a minősített adatokat kezelő rendszereket.

1.2.3. Területi hatálya

A szabályzat területi hatálya kiterjed a Hivatal székhelyére, továbbá a Hivatal kirendeltségeire (Bejcgyertyános, Bögöte, Káld, Meggyeskovácsi, Sótony), és a Sárvári Kistérségi Irodára.

1.2.4. Időbeli hatálya

A szabályzat a kihirdetése napján lép hatályba és visszavonásig érvényes.

1.3. A szabályzat felülvizsgálata

A szabályzatot az alábbi esetekben kell felülvizsgálni:

- a szabályzatot érintő jogszabályokban a módosítást előíró vagy azt indokló változás következett be;
- ha új elektronikus informatikai rendszer bevezetésére kerül sor;
- ha a szabályzat hatálya alá eső szervezetben, elektronikus információs rendszerekben a biztonsági követelményeket érintő változás következett be;
- ha olyan biztonsági esemény következett be, amelynek kivizsgálása során a szabályozás módosításának szükségessége merült fel;
- egyéb esetben a hatályba lépést követő három éven belül.

A szabályzat felülvizsgálatát az elektronikus informatikai rendszer biztonságáért felelős személy (a továbbiakban: biztonsági felelős) kezdeményezi és készíti elő.

1.4. Értelmező rendelkezések

A szabályzatban az alábbi jogszabályokban meghatározott fogalmakat alkalmazzuk:

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (1 §)
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
- 185/2015. (VII. 13.) Korm. rendelet a Kormányzati Eseménykezelő Központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól
- 186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről

- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
- 257/2016. (VIII. 31.) Korm. rendelet az önkormányzati ASP rendszerről
- 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről

A jelen szabályzatban használt fontosabb fogalmakat az 5.1 Fogalmak jegyzéke ismerteti.

1.5. Az elektronikus információbiztonsággal kapcsolatos szerepkörök és feladatok

Az elektronikus információbiztonsággal kapcsolatos tevékenységek, feladatok és felelősségek az alábbi szerepkörökhöz vannak rendelve:

- A szervezet vezetője, a jegyző
- Az elektronikus információs rendszer biztonságáért felelős személy
- A felhasználó
- Kulcsfelhasználók (önkormányzati ASP adminisztrátor, szakrendszeri ASP adminisztrátor, ASP és helyi kulcsfelhasználó)
- A rendszergazda
- A szolgáltató

Az egyes szerepkörökhöz rendelt feladatok és felelősségek a következők:

1.5.1. Jegyző

Mint a szervezet vezetője az elektronikus információs rendszerek védelméről a következők szerint gondoskodik:

a. biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
b. biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
c. az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,
d. meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az Informatikai Biztonsági Szabályzatot,
e. gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,

f. rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
g. gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
h. biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,
i. ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy a törvényben foglaltak szerződéses kötelemként teljesüljenek,
j. ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy a törvényben foglaltak szerződéses kötelemként teljesüljenek,
k. felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,
l. megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

Felelőssége: felelős a vonatkozó jogszabályok és szabályzat követelményeinek megvalósulásáért.

1.5.2. Elektronikus információs rendszer biztonságáért felelős személy

Az elektronikus információs rendszer biztonságáért felelős személy (röviden informatikai biztonsági felelős, IBF) közvetlenül a jegyzőnek alárendelten végzi munkáját.

a. A jegyző előzetes jóváhagyásával ellenőrzi az Informatikai Biztonsági Szabályzatban foglaltak végrehajtását a Hivatal szervezeti egységeinél.
b. Együttműködik a belső ellenőrrel az informatikai biztonságot érintő ellenőrzési feladatok ellátásában (kockázatelemzés, vagyonvédelem, FEUV, stb.)
c. Együttműködik az informatikai biztonsággal kapcsolatos szakterületek felelőseivel, így különösen az informatika, a hivatal-üzemeltetés, a vagyonvédelem, a tűzvédelem és a munkavédelem területén.
d. Éves munkatervet, szükség szerint cselekvési tervet készít az informatikai biztonsági feladatok végrehajtására.
e. Szükség szerint, de legalább évente egy alkalommal, összefoglaló értékelést készít a jegyző részére a hivatal informatikai biztonsági helyzetéről, a további szükséges intézkedésekről. Részt vesz az e jelentést megvitató hivatalvezetői értekezleten.
f. Rendkívüli események esetén soron kívül elvégzi az Informatikai Biztonsági Szabályzatban meghatározott feladatait.
g. Folyamatosan figyelemmel kíséri a szabályzat felülvizsgálatára, módosítására okot adó körülményeket (jogszabályváltozás, új informatikai rendszer bevezetése, szervezeti változások, stb.), előkészíti a szükséges módosításokat.
h. Három évente kezdeményezi a szabályzat felülvizsgálatát, előkészíti a szükséges módosításokat.

i. Folyamatosan figyelemmel kíséri a biztonsági osztályba sorolás és a szervezeti szint felülvizsgálatára, módosítására okot adó körülményeket, kezdeményezi és előkészíti a módosított besorolásokat.
j. Három évente, illetve a jogszabály által meghatározott egyéb esetekben kezdeményezi a besorolások felülvizsgálatát, előkészíti a szükséges módosításokat.
k. Véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit.
l. Kapcsolatot tart a hatósággal és a Kormányzati Eseménykezelő Központtal.

Felelőssége: felelős a jogszabályokban és jelen szabályzatban meghatározott feladatainak végrehajtásáért.

1.5.3. Felhasználó

a. A Hivatal elektronikus informatikai rendszereinek felhasználója munkaköri leírásában szereplő feladatai és az egyedi vezetői munkautasítások alapján használhatja a számára engedélyezett informatikai eszközöket és szolgáltatásokat. Ennek során az információvédelem területén az adott helyzetben általában elvárható magatartást köteles tanúsítani, és tartózkodni minden károkozó tevékenységtől.
b. Felelősséggel tartozik a munkavégzés céljából átvett eszközért, köteles megőrizni annak hardver- és szoftverintegritását. Az integritás sérelmének minősül a rendeltetésellenes használat, hardveres vagy szoftveres módosítás.
c. A részére kiadott azonosítókat és hitelesítő eszközöket bizalmasan kell kezelnie, nem szabad kiadni azokat más személynek, illetve nem szabad felhasználnia másik felhasználó azonosítóját és hitelesítő eszközét, az erre irányuló esetleges kérést vagy utasítást meg kell tagadnia.
d. Köteles azonnal értesíteni munkahelyi vezetőjét, ha az informatikai rendszer rendelkezésre állása, a kezelt adatok bizalmassága és sértetlensége sérült, vagy ennek közvetlen veszélye fennáll.

Felelőssége: felelős a jelen szabályzatban és a vezetői utasításokban meghatározott szabályok betartásáért, az informatikai rendszerben végzett műveleteiért.

1.5.4. Kulcsfelhasználó

Feladatai:

a. Beállítja, karbantartja, illetve törli a felhasználói fiókokat, jogosultságokat a helyi hozzáférésekre vonatkozóan.
b. Segítséget nyújt a felhasználóknak a jelszavak beállításához és időszakos vagy eseti cseréje során.
c. Az önkormányzati ASP adminisztrátori és/vagy szakrendszer adminisztrátori feladatait az ASP rendszerben meghatározott szabályok szerint végzi.

Felelőssége: felelős azért, hogy a felhasználók kizárólag a jegyző által engedélyezett hozzáférési jogosultságokat kapják meg, a visszavont fiókokat és jogosultságokat pedig haladéktalanul törölje.

1.5.5. Rendszergazda

A Hivatalban a rendszergazdai feladatokat vállalkozási szerződés alapján külső személy (vállalkozás) látja el.

Feladatai:

a. A szerződésben rögzített gyakorisággal ellenőrzi a helyi hálózat, számítógépek, nyomtatók és egyéb berendezések üzemképességét, elvégzi az esedékes diagnosztikai és karbantartási munkákat.
b. Elvégzi a fenti eszközökön működő alapszoftverek (firmware, operációs rendszer, irodai szoftverek stb.) frissítését.
c. Gondoskodik a konfigurációk mentéséről, a feladatkörébe tartozó hardver és szoftver elemek nyilvántartásáról.
d. Ellenőrzi a biztonsági beállításokat, a mentési és naplózó alrendszerek működését.
e. Szükség szerint elvégzi a meghibásodott eszközök javítását, javaslatot tesz a nem javítható eszközök cseréjére.

Felelőssége: felelős a jelen szabályzatban meghatározott szabályok betartásáért, a munkája során megismert bizalmas információk titokban tartásáért, valamint a szerződésben vállalt egyéb kötelezettségek teljesítéséért.

1.5.6. Az IBSZ-hez kapcsolódó szabályzatok

Az IBSZ előírásait az alábbi szabályzatokkal összhangban kell értelmezni és alkalmazni:

- Szervezeti és Működési Szabályzat
- Iratkezelési Szabályzat
- Kockázatkezelési szabályzat
- Leltározási és selejtezési szabályzat
- Tűzvédelmi szabályzat
- Munkavédelmi szabályzat
- Közzétételi szabályzat

1.5.7. Biztonsági osztályba sorolás

Az önkormányzati ASP rendszer szakrendszereinek biztonsági osztályba sorolását a Magyar Államkincstártól kapja meg, azokat a nem kell biztonsági osztályba sorolni.

A Hivatal egyéb informatikai rendszert nem üzemeltet, ide nem értve a papíralapú szöveges iratok előkészítését, szerkesztését, nyilvántartását támogató irodai és egyéb, archiválást nem igénylő alkalmazásokat, mivel ezek adatainak hitelességét kizárólag a papír alapú dokumentumok biztosítják.

1.5.8. Biztonsági szintbe sorolás

A Hivatal elvárt biztonsági szintje a 41/2015. (VII. 15.) BM rendelet alapján 2., mivel olyan elektronikus információs rendszert használ, amely személyes adatokat kezel, és a Hivatal jogszabály alapján (önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet) kijelölt szolgáltatót vesz igénybe. A Hivatal szervezeti egységekre nem tagolódik, így szervezeti egységekre vonatkozóan a biztonsági szintbe sorolás nem értelmezhető.

A Hivatal jelenlegi biztonsági szintje az elvárt 2. szintet a legutóbbi felülvizsgálat alapján eléri.

1.5.9. Védelmi intézkedések

A szabályzat 2.-4. fejezete a Hivatal a 41/2015. (VII. 15.) BM rendelet és a Magyar Államkincstár által kiadott, az önkormányzati ASP rendszerekhez történő csatlakozáshoz megvalósítandó informatikai biztonsági követelmények teljesítését szolgáló védelmi intézkedéseket, eljárásokat és szabályokat rögzíti.

2 Adminisztratív védelmi intézkedések

2.1 Szervezeti szintű alapfeladatok

2.1.1 Informatikai Biztonsági Szabályzat

A Hivatal jelen szabályzatban megfogalmazta a szervezetre érvényes követelményeket, melyet jegyzői utasítással kihirdet.

2.1.2 Az elektronikus információs rendszerek biztonságáért felelős személy

Az elektronikus információs rendszerek biztonságáért felelős személy (IBF) kijelölése vagy megbízása a jegyző feladata.

Amennyiben átmenetileg a Hivatal nem rendelkezik IBF-fel, a jegyző gondoskodik az IBF feladatkörébe tartozó tevékenységek elvégzéséről.

Az IBF feladatait és felelősségét jelen szabályzat általános része tartalmazza.

2.1.3 Az intézkedési terv és mérföldkövei

A Hivatal informatikai biztonsági helyzetét évente kell ellenőrizni (belső audit) és értékelni. Ennek eredményeképpen meg kell határozni, hogy szükséges-e intézkedési tervet készíteni a hiányosságok megszüntetése, az informatikai biztonsági politika és stratégia megvalósítása érdekében.

- ha az adott elektronikus információs rendszerére követelmények értékelése során hiányosságokat állapít meg, a vizsgálatot követő 90 napon belül kell a hiányosságok megszüntetésére intézkedési tervet elkészíteni;
- ha a meghatározott biztonsági szint alacsonyabb, mint az érintett szervezetre érvényes szint, a vizsgálatot követő 90 napon belül kell az intézkedési tervet elkészíteni, az előírt biztonsági szint elérése érdekében.

Az intézkedési tervet az IBF készíti elő és – a szükséges önkormányzati egyeztetések és döntések után - a jegyző hagyja jóvá.

Az intézkedési tervben mérföldköveket kell meghatározni, melyek elérését a meghatározott határidőben, de legalább évente kell ellenőrizni.

2.1.4 Az elektronikus információs rendszerek nyilvántartása

A Hivatal az elektronikus információs rendszereiről nyilvántartást vezet, melyet folyamatosan aktualizál. A nyilvántartás minden rendszerre nézve tartalmazza:

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

A Hivatal az előírt nyilvántartásokat elektronikusan, az erre kialakított IBF portálon vezeti. A nyilvántartásban a változásokat 5 munkanapon belül át kell vezetni.

2.1.5 Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, a Hivatal hatás körébe tartozó emberi, fizikai és logikai erőforrásra, eljárási és védelmi követelményszintre és folyamatra. Az ezekkel kapcsolatos engedélyeket – ha jogszabály vagy a Hivatalra vonatkozó utasítás ettől eltérően nem rendelkezik - a jegyző, illetve a helyettesítésével megbízott személy adhatja ki.

Az emberi, fizikai és logikai erőforrásra, eljárási és védelmi követelményszintre és folyamatra vonatkozó engedélyezési eljárások speciális szabályait a szabályzat vonatkozó fizikai és logikai védelmi intézkedéseinek meghatározása tartalmazza.

2.2 Kockázatelemzés

2.2.1 Kockázatelemzési és kockázatkezelési eljárásrend

A Hivatal egységes kockázatkezelési módszertant és eljárásrendet alkalmaz, melyet a Hivatal Kockázatkezelési szabályzata tartalmaz.

2.2.2 Biztonsági osztályba sorolás

Az önkormányzati ASP rendszer szakrendszereinek biztonsági osztályba sorolását a Magyar Államkincstártól kapja meg, azokat a nem kell biztonsági osztályba sorolni.

A Hivatal egyéb informatikai szakrendszert nem üzemeltet, ide nem értve a szakrendszernek nem minősülő, a papíralapú szöveges iratok előkészítését, szerkesztését, valamint nyilvántartását támogató irodai és egyéb, jogszabály alapján archiválást nem igénylő alkalmazásokat.

2.2.3 Kockázat elemzés

Kockázatelemzést évente kell végezni. A kockázatelemzés dokumentumai nem nyilvános iratok.

Az IBF a Kockázatkezelési szabályzatban meghatározottak szerint együttműködik a belső ellenőrrel, részt vesz az évente kötelezően elvégzendő kockázatelemzésben. Ennek eredményeképpen meghatározza a következő belső audit szempontjait, melyet a jegyző hagy jóvá.

A kockázatelemzés eredményét, a szükséges intézkedéseket az érintett önkormányzatok polgármesterei, szükség szerint az önkormányzatok képviselő testületei számára, a jegyző ismerteti. Amennyiben a kockázatkezelés anyagi ráfordítással járó intézkedéseket tesz szükségessé, a jegyző – az IBF és más kijelölt munkatársak bevonásával – elkészíti az ehhez szükséges előterjesztést, gondoskodik az önkormányzati döntés végrehajtásról.

A kockázatelemzés eredményeképpen megállapított szervezeti szintű intézkedésekről a jegyző munkaértekezleten tájékoztatja az érintett munkatársakat.

2.3 Rendszer és szolgáltatás beszerzés

A Hivatal saját hatókörében nem végez, vagy végeztet rendszerfejlesztési tevékenységet. Az ASP rendszerhez történt csatlakozással a Hivatalban a rendszer- és szolgáltatásbeszerzéssel összefüggő eljárások szabályozása szükségtelenné vált. A vonatkozó rendelkezések szerint ezeket az *„eljárásokat abban az esetben nem kell bevezetni az érintett szervezetnél, ha saját hatókörében informatikai szolgáltatást, vagy eszközöket nem szerez be, és nem végez, vagy végeztet rendszerfejlesztési tevékenységet (ide nem értve a jellemzően kis értékű, kereskedelmi forgalomban kapható általában irodai alkalmazásokat, szoftvereket, vagy azokat a hardver beszerzéseket, amelyek jellemzően a tönkrement eszközök pótlása, vagy az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából történnek, valamint a javítás, karbantartás céljára történő beszerzéseket). Jelen fejezet alkalmazása szempontjából nem minősül fejlesztésnek a kereskedelmi forgalomban kapható szoftverek beszerzése és frissítése*[1]*."*

A Hivatal informatikai eszközökre és szolgáltatásokra irányuló beszerzési tevékenysége a következőkre korlátozódik:

- az önkormányzati ASP rendszer használatához szükséges, jogszabályban meghatározott paraméterekkel rendelkező eszközök és hálózati infrastruktúra,
- a Hivatal ügyviteli tevékenységéhez kapcsolódó, általános célú irodai eszközök (jellemzően kis értékű, kereskedelmi forgalomban kapható irodai alkalmazások, szoftverek, illetve olyan hardver beszerzések, amelyek jellemzően a tönkrement eszközök pótlása, vagy az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából történnek),
- az informatikai rendszerelemek karbantartására, javítására irányuló szolgáltatások, valamint a javítás, karbantartás céljára történő tartalék eszközök beszerzése,
- távközlési szolgáltatások.

A Hivatalban a fentiekre vonatkozóan a beszerzési javaslatot a jegyző által kijelölt munkatárs állítja össze, melyet az IBF véleményez. A beszerzést az SZMSZ-ben meghatározott hatáskör szerint engedélyezik.

Rendszer és szolgáltatás beszerzés vonatkozásában a szabályzat - a jogszabályban meghatározottak szerint - a logikai védelmi intézkedések között további követelményeket határoz meg.

2.4 Üzletmenet (ügymenet) folytonosság tervezése

2.4.1 Üzletmenet folytonosságra vonatkozó eljárásrend

Az üzletmenet folytonosságot veszélyeztető körülmények esetén a jegyző - szükség szerint az IBF és más munkatársak, valamint az érintett szolgáltatók bevonásával, a hivatal székhelye szerinti polgármester egyidejű tájékoztatása mellett – értékeli a kialakult helyzetet. Ennek eredményeképpen az alábbi intézkedéseket teszi:

[1] *4. melléklet a 41/2015. (VII. 15.) BM rendelethez*

- Az önkormányzat veszélyelhárítási tervében meghatározott estekben végrehajtja a Hivatal részére kijelölt feladatokat.
- A Hivatal ügymenetét tartósan akadályozó káresemény, vészhelyzet esetén a jogszabályban meghatározottak szerint igazgatási szünetet rendel el, intézkedik a helyreállítás és az újraindítás érdekében szükséges feladatok végrehajtására.
- A Hivatal ügymenetét részlegesen és/vagy csak munkanapon belüli rövid időre akadályozó káresemény, vészhelyzet esetén intézkedik a helyreállítás és az újraindítás érdekében szükséges feladatok végrehajtására.
- A bekövetkezett káresemény, vészhelyzet jellegétől függően értesíti az illetékes hatóságokat.

2.4.2 Üzletmenet folytonossági terv informatikai erőforrás kiesésekre

Az informatikai erőforrások kiesése esetén a jegyző az IBF bevonásával értékeli a kialakult helyzetet és meghatározza a kisesés miatt végrehajtandó intézkedéseket.

- Az internet szolgáltatás hivatali épületre, kirendeltségre kiterjedő kiesése esetén a halaszthatatlan adatfeldolgozást igénylő ügyek (banki utalások, határidős jelentések) tekintetében a jegyző intézkedik, hogy az érintett dolgozók átmenetileg a kieséssel nem érintett intézményben vagy kirendeltségen folytatják a munkát.
- A belső hálózatot és egyedi számítógépeket érintő átmeneti és korlátozott kiesés esetén értesíti a javítást végző szolgáltatót a hiba elhárítása érdekében, szükség szerint az előző pontban leírtak szerint gondoskodik a halaszthatatlan feladatok végrehajtásáról.
- Ha az erőforrás kiesés visszavezethető kártékony kódra vagy illetéktelen külső beavatkozásra, a kárelhárítással egyidejűleg az IBF értesíti az illetékes hatóságot.

Az üzletmenet folytonosságának sérülését okozó káresemények helyreállítását követően az IBF soron kívül ellenőrzést végez, és javaslatot tesz a hasonló jellegű veszélyhelyzetek megelőzésére, a kiesések következményeinek hatékony felszámolását biztosító feladatok tervezésére.

2.4.3 Kritikus rendszerelemek meghatározása

A Hivatal informatikai rendszereinek kritikus elemei:

- Az önkormányzati ASP rendszer, mint szolgáltatás.
- Az önkormányzati ASP rendszer elérését biztosító hálózat (WAN/LAN, internet szolgáltatás, NTG hálózat) és az ehhez kapcsolódó számítógépek (kliensek).

Nem kritikus rendszerelemek: az irodai munkát támogató egyéb elektronikus berendezések, nyomtatók, szkennerek stb.

2.4.4 A folyamatos működésre felkészítő képzés

A felhasználók a szokásos informatikai biztonsági oktatás keretében kapnak felkészítést az ügymenet folyamatosságának fenntartását biztosító feladataikról.

Az IBF soron kívüli oktatást tart az üzletmenet folytonosságot érintő káreseményt követően, ha az visszavezethető felhasználói mulasztásra, illetve, ha megfelelő felhasználói magatartással megelőzhető lett volna.

A Hivatal éves beszámolója keretében tájékoztatja az érintett önkormányzati képviselő testületeket, polgármestereket az üzletmenet folyamatosságának fenntartására irányúló tevékenységéről, az esetleges rendkívüli önkormányzati intézkedések szükségességéről.

2.4.5 Üzletmenet folytonosság elérhetőség

Az üzletmenet folytonosság megszakítását előidéző események során jellemzően nem elérhetők vagy nem használhatók a szokásos informatikai eszközök, ezért a jegyzőnél kinyomtatott formában kell tárolni a vészhelyzeti eljárások során szükséges információkat:

- a vészhelyzet kezelésébe bevonandó személyek, szolgáltatók és hatóságok elérési adatait (név, telefonszám);
- a helyreállítás és újraindítás érdekében szükséges szolgáltatói szerződések adatait;
- a hálózat konfigurálásához és az ASP kliensek helyreállításához szükséges telepítési dokumentációkat.

2.4.6 Infokommunikációs szolgáltatások

A Hivatal a Nemzeti Távközlési Gerinchálózat kiesése esetére kereskedelmi internet szolgáltatásra fizet elő a hivatali központra és kirendeltségeire vonatkozóan.

További infokommunikációs tartalékként a Hivatal szükség szerint igénybe veszi az intézményi internet előfizetéseket is.

2.5 Emberi tényezőket figyelembe vevő – személy – biztonság

2.5.1 Személybiztonsági eljárásrend

A Hivatal személyes adatokat és egyéb, nem nyilvános adatokat tartalmazó, az önkormányzati ASP központban üzemeltetett adatbázisaihoz köztisztviselői jogállású munkatársak férhetnek hozzá. Más jogviszony alapján foglalkoztatott személyek a jegyző egyedi engedélye alapján csak korlátozottan, köztisztviselő munkatárs felügyeletével végezhetnek a rendszerben adatkezelést.

A munkakör betöltésének feltétele a köztisztviselő kinevezése, melynek szabályait a közszolgálati tisztviselőkről szóló 2011.évi CXCIX. tv. és a kapcsolódó jogszabályok tartalmazzák. A munkaköri leírásban rögzíteni kell, hogy az adott munkakör ellátásához

- melyik informatikai rendszerben,
- milyen rendszerfunkciókhoz,
- milyen szerepkört, illetve milyen szintű jogosultságot kell biztosítani.

Az egyes rendszerelemek javítása, karbantartása, rendszergazda feladatok ellátása során az ezzel megbízott személy, vállalkozó a Hivatal központi adatbázisaihoz nem férhet hozzá.

2.5.2 Munkakörök, feladatok biztonsági szempontú besorolása

A Hivatalban az egyes munkakörök biztonsági szempontból az elektronikus információs rendszerek tekintetében azonos besorolásúak.

A Hivatalban nincs nemzetbiztonsági ellenőrzéshez kötött munkakör.

A munkakörök és feladatok biztonsági szempontú besorolását az IBSZ módosításának szükségessége esetén felül kell vizsgálni.

2.5.3 A személyek ellenőrzése

A jegyző a köztisztviselőt a kinevezés előtt a vonatkozó jogszabályok alapján ellenőrzi. Az elektronikus információs rendszerhez való hozzáférés jogosságát - az alkalmazási feltételeknek való megfelelés és a köztisztviselő kinevezése esetén - a betöltött munkakörnek megfelelő mértékben igazoltnak kell tekinteni.

Az egyes rendszerelemek karbantartásával, javításával és a rendszergazda feladatok ellátásával megbízott személytől, ha az nem köztisztviselő, a büntetlen előélet igazolására vonatkozóan a megbízáskor (szerződéskötéskor) 3 hónapnál nem régebbi erkölcsi bizonyítványt, illetve szakmai életútját bemutató referenciaigazolást kell kérni.

2.5.4 Eljárás a jogviszony megszűnésekor

A Hivatal munkavégzésre irányuló jogviszony megszűnésekor az alábbi feladatokat végzi el:

- legkésőbb a jogviszony fennállásának utolsó napján megszünteti a hozzáférési jogosultságot az elektronikus információs rendszerhez, és – ha volt ilyen – a riasztó rendszerhez;
- megszünteti vagy visszaveszi a személy egyéni hitelesítő eszközeit;
- visszaveszi a fizikai belépéshez használt kulcsokat;
- tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről;
- visszaveszi az érintett szervezet elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt;
- megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz;
- e-mailben értesíti az IBF-t és a rendszergazdát a jogviszony megszűnéséről;
- a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik;
- a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzi.

2.5.5 Az áthelyezések, átirányítások és kirendelések kezelése

A Hivatalban nem különülnek el a szervezeti egységek, ezért az áthelyezések, átirányítások és kirendelések kezelése nem igényel szabályozást.

A munkakör megváltozása, pl. helyettesítés esetén a jegyző, mint önkormányzati ASP adminisztrátor gondoskodik az elektronikus információs rendszerhez való hozzáférési jogosultságok beállításáról az új munkakörnek megfelelően, vagy intézkedik, hogy a szakrendszeri adminisztrátor ezeket állítsa be. Egyidejűleg a már szükségtelenné váló jogosultságokat vissza kell vonni.

Ha az új munkakörben a korábbitól eltérő számítástechnikai eszközöket kell az érintett munkatársnak használni, a jegyző intézkedik a belépést, hozzáférést biztosító fiókok, azonosítók létrehozására, illetve a szükségtelenné válók törlésére.

2.5.6 Az érintett szervezettel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények

A Hivatallal a számítástechnikai eszközök javítására, karbantartására és rendszergazda feladatok ellátására külső szolgáltatóval köt szerződést.

A szerződésnek a személybiztonságra vonatkozóan tartalmaznia kell:

- a szolgáltató információbiztonsági felelősségét, az ezzel kapcsolatos megrendelői elvárásokat;
- a szolgáltató azon munkatársaira vonatkozó személyi adatokat és személybiztonsági követelményeket, akik a Hivatalban munkát végeznek;
- a szolgáltató azonnali értesítési kötelezettségét arra vonatkozóan, ha a Hivatalban korábban munkát végző munkatársának a munkaviszonya megszűnt.

A jegyző folyamatosan ellenőrzi, hogy a szolgáltató a személybiztonsági követelményeknek megfelel.

2.5.7 Fegyelmi intézkedések

A jegyző fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket súlyosan megsértő személyekkel szemben.

Amennyiben az elektronikus információbiztonsági szabályokat nem a Hivatal személyi állományába tartozó személy sérti meg, a jegyző érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések lehetőségét, szükségességét.

2.5.8 Belső egyeztetés

A Hivatalban a biztonságot érintő intézkedéseket a munkahelyi értekezletek keretében ismertetni kell. Ennek során figyelembe kell venni a munkatársak észrevételeit, javaslatait annak érdekében, hogy a munkaköri feladatok ellátását a biztonsági intézkedések ne tegyék aránytalanul terhesebbé.

2.5.9 Viselkedési szabályok az interneten

A Hivatal felhasználói munkaköri feladataik teljesítéséhez kizárólag a Hivatal által meghatározott eszközöket és internetes szolgáltatásokat használhatják.

A Hivatal felhasználói számára tilos:

- a hivatali (nem nyilvános) információk nyilvános internetes oldalakon való jogtalan közzététele;
- munkaköri feladatokhoz kapcsolódóan magáncélú e-mail fiókot, üzenőszolgáltatást vagy bármilyen egyéb, nem engedélyezett szolgáltatást használni;
- a munkaköri feladatokon kívül bármilyen, internet használatával megvalósuló tevékenységet végezni (magáncélú fájlletöltés, böngészés, közösségi oldalak és fórumok látogatása, magáncélú levelezés stb.).

A Hivatal az önkormányzati ASP rendszert elérő számítógépeken az interneten elérhető tartalmakat indokolt esetben szűri, erről az érintett munkatársakat tájékoztatja.

2.6 Tudatosság és képzés

2.6.1 Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és az e célt szolgáló ágazati szervezetekkel

A jegyző és az IBF a jogszabályokban meghatározottak szerint kapcsolatot tart a Nemzeti Elektronikus Információbiztonsági Hatósággal, a Magyar Államkincstárral, a NISZ Zrt.-vel, a Kormányhivatallal, valamint a jogszabályokban kijelölt más illetékes szervezetekkel, ennek során kölcsönösen tájékoztatják egymást a hatáskörükbe tartozóan megtett intézkedésekről.

2.6.2 Képzési eljárásrend

Az elektronikus információs rendszerek biztonságával összefüggő oktatásra az IBF évente készít tervet, melyet a jegyző hagy jóvá.

Az oktatást lehetőség szerint úgy kell megtartani, hogy minden munkatárs részt tudjon venni rajta, pl. on-line videoelőadás formájában. Az oktatás során kapott ismeretekről kérdőív kitöltetésével vagy más megfelelő formában meg kell győződni.

Az új belépő dolgozóknak meg kell ismerni jelen szabályzatot, illetve annak a felhasználói ismereteket tartalmazó kivonatát, és erről a munkatársat nyilatkoztatni szükséges.

A képzés helyzetét az IBF az éves jelentés keretében felülvizsgálja, és javaslatot tesz a szükséges intézkedésekre.

2.6.3 Biztonság tudatosság képzés

A lehetséges belső fenyegetések felismerése érdekében az IBF gondoskodik a felhasználók biztonsággal kapcsolatos rendszeres tájékoztatásáról, felkészítéséről. Ennek keretében:

- Felhívja a figyelmet az informatikai rendszereket fenyegető aktuális veszélyekről, a megelőzés, az észlelés és a szükséges jelzés érdekében teendő felhasználói feladatokról.
- Az új belépő munkatársak részére évente aktualizálja a jelen szabályzatból a felhasználók oktatásához készített kivonatot.
- Az elektronikus rendszerben bekövetkezett változásokhoz kapcsolódóan tájékoztatja a felhasználókat a megváltozott követelményekről, intézkedésekről.

2.6.4 Belső fenyegetés

Minden felhasználónak kötelessége jelenteni a jegyzőnek, ha az informatikai rendszert érintő belső fenyegetést észlel. A munkahelyi értekezletek keretében fel kell a felhasználók figyelmét hívni arra, hogy az informatikai rendszer biztonsága a Hivatal működésének előfeltétele, ezért minden olyan körülményt, magatartást (mulasztást) időben fel kell tárni, ami a rendszer rendelkezésre állását, az adatok bizalmasságát és sértetlenségét veszélyezteti.

Az IBF a belső fenyegetések felismerése érdekében közvetlen (on-line) kapcsolatot tart minden felhasználóval, és konzultációs lehetőséget biztosít kérdéseik megválaszolására annak érdekében, hogy a belső fenyegetések gyanúja minden esetben kivizsgálásra kerüljön.

2.6.5 Szerepkör vagy feladatalapú képzés

A jegyző gondoskodik arról, hogy az önkormányzati ASP rendszerben kiemelt felhasználók (szakrendszeri adminisztrátor, kulcsfelhasználó) az üzemeltető által szervezett, előírt képzéseken részt vegyenek.

Az önkormányzati ASP rendszerben szakrendszeri adminisztrátor és kulcsfelhasználó szerepkört betöltő munkatárs feladata, hogy azon munkatársakat a szükséges rendszerbiztonsági funkciókat illetően eligazítsa, akiknek jogosultságot adott az adott rendszermodulhoz.

A jegyzőnek és az informatikai rendszer biztonságáért felelős személynek a jogszabályban rögzített továbbképzéseken kell részt venni.

2.6.6 A biztonsági képzésre vonatkozó dokumentációk

A biztonságtudatossága vonatkozó képzést minden esetben dokumentálni szükséges:

- Az új belépő munkatársakat illetően a jelen szabályzat megismerését igazoló nyilatkozattal.
- A rendszeres (éves, havi) oktatáson történt részvételt az oktatási formához igazodóan, tantermi képzés esetén jelenléti ívvel, on-line távoktatás esetén a felhasználói belépést, valamint – ha része az oktatásnak – a teszt kérdőív kitöltését igazoló naplóval.
- Hivatalon kívül szervezett továbbképzések esetén a képzésről (helye, ideje, tematikája) és a résztvevőkről készített feljegyzéssel. A feljegyzést a résztvevő, többes részvétel esetén a résztvevők közül jegyző által megbízott munkatárs készíti el.

A biztonságtudatossági képzés dokumentumait– eltérő rendelkezés hiányában – az IBF három évig elektronikus formában megőrzi.

3 Fizikai védelmi intézkedések

3.1 Fizikai védelmi eljárásrend

A Hivatal elektronikus információs rendszereinek fizikai védelmét a tűzvédelmi, vagyonvédelmi, munkavédelmi és más kapcsolódó jogszabályok, önkormányzati és hivatali szabályzatok figyelembe vételével kell megszervezni.

A fizikai védelmi szabályok kialakítása, módosítása és ellenőrzése során az egyes szakterületek felelőseinek (IBF, tűzvédelmi felelős stb.) együttműködését a jegyző koordinálja.

A Hivatalban végrehajtandó, a fizikai védelmet érintő felújítás, karbantartás előkészítésébe az IBF-t a szükséges mértékben be kell vonni.

A fizikai védelem helyzetét az IBF évente ellenőrzi, értékeli és javaslatot tesz a szükséges intézkedésekre.

3.2 Fizikai belépési engedélyek

A Hivatal épületeibe a belépést és ott tartózkodást a jegyző engedélyezi.

A Hivatal épületeiben, hivatali időben külön engedély nélkül tartózkodhatnak:

- a polgármester;
- a hivatal köztisztviselő jogállású munkatársai;
- egyéb munkavégzésre irányuló jogviszony alapján munkát végző személyek, akiknek kijelölt munkahelyük a hivatalban van;
- a szolgáltatók a szerződésben meghatározott feltételeknek (kísérő, előzetes bejelentés stb.) megfelelően.

A hivatali időn kívül belépésre jogosultakról, a belépés esetleges külön feltételeiről (riasztó, kulcs használat) a jegyző nyilvántartást vezet.

3.3 A fizikai belépés ellenőrzése

A Hivatali épületbe munkavégzés céljából belépő munkatársak jelenléti ívet vezetnek. A munkaidőn kívüli belépést, épületnyitást a riasztórendszer naplózza.

A Hivatalba ügyintézés céljából belépő ügyfelek szabad mozgását az ügyfélvárónak kijelölt területre kell korlátozni. A Hivatal ügyintézésre kijelölt irodáiba ügyfél csak az illetékes munkatárs engedélyével és felügyelete mellett léphet be, és tartózkodhat ott.

Az ügyfelet vagy más látogatót nem szabad felügyelet nélkül hagyni olyan helyiségben, ahol aktív informatikai eszközök működnek, illetve ahol az informatikai infrastruktúra kritikus elemei hozzáférhetők (pl. kapcsoló szekrény, kábelelosztó, szünetmentes táp stb.).

A Hivatal minden munkatársának kötelessége jelenteni a jegyzőnek, ha az épületben vagy annak valamely helyiségében illetéktelen személy tartózkodik, vagy a belépési rendet veszélyeztető egyéb körülményt (riasztó, zár meghibásodás, kulcs elvesztése stb.) észlelt.

3.4 Hozzáférés az adatátviteli eszközökhöz és csatornákhoz

Azokat a helyiségeket, amelyekben az elektronikus információs rendszer adatátviteli eszközei, kapcsolódási pontjai vannak elhelyezve, a bárki által látogatható hivatali részektől elzártan kell tartani. Ezekbe a helyiségekbe csak a kijelölt munkatársaknak, illetve az ő felügyeletük mellett szabad belépni.

Az elektronikus információs rendszer azon adatátviteli eszközeit, kapcsolódási pontjait, melyek nem elzárható hivatali helyiségben vannak, megfelelő fizikai védelemmel kell ellátni az illetéktelen hozzáférés megakadályozása érdekében.

3.5 A kimeneti eszközök hozzáférés ellenőrzése

A számítógépeket az ügyintézésre kijelölt irodákban úgy kell elhelyezni, hogy az ügyfél a képernyőt ne láthassa.

A hálózati nyomtatókat nem szabad elhelyezni és üzemeltetni olyan helyiségben, ahol ügyfél felügyelet nélkül tartózkodhat.

A helyi nyomtatók használata esetén ügyelni kell arra, hogy a nyomtatóhoz ügyfél ne férjen hozzá, illetve, ha ez az adott irodában nem megoldható, ügyfél jelenlétében ne kerüljön nyomtatásra olyan irat, melynek megismerésére az adott ügyfél nem jogosult.

3.6 A fizikai hozzáférések felügyelete

A fizikai hozzáférés szabályainak betartását hivatali időben a Hivatal munkatársai kötelesek felügyelni, és a hivatalba ügyintézés vagy szolgáltatás céljából érkezett személyektől ezek betartását megkövetelni. Indokolt esetben a szabályokat erőszakosan megsértőkkel szembeni intézkedéshez a rendőrség vagy a polgárőrség segítségét kell kérni.

A Hivatalba hivatali időn kívül történt belépéseket, azok indokoltságát és jogosságát a jegyző ellenőrzi.

3.7 Behatolás riasztás, felügyeleti berendezések

A Hivatalba telepített riasztó rendszert az épület zárásakor élesíteni kell, ezért az épület zárására kijelölt dolgozó a felelős.

A riasztó rendszer meghibásodása, üzemképtelensége esetén a jegyző soron kívül intézkedik a javításra, és gondoskodik az átmeneti kiegészítő őrzés-védelmi intézkedésekről.

3.8 A látogatók ellenőrzése

A Hivatalba ügyintézés céljából érkező ügyfelek személyazonosságának ellenőrzése az ügyintézés jellegének megfelelően a hivatalos eljárás részeként történik.

Nem szükséges a látogatót azonosítani:

- ha csupán felvilágosítást kér,
- a választott tisztségviselőkhöz érkezőket,
- a munkatársak által személyesen ismert, nem hivatalos ügyben érkező vendégeket.

A fenti látogatók fizikai hozzáférésének korlátozására az ügyfelekre vonatkozó szabályokat kell alkalmazni.

3.9 Áramellátó berendezések és kábelezés

Az informatikai infrastruktúra elektromos ellátását biztosító technikai eszközöket (kapcsoló- és biztosíték tábla, szünetmentes táp, hosszabbítók, stb.) védeni kell az illetéktelen hozzáféréstől, sérüléstől és rongálástól. Ennek során figyelembe kell venni a vonatkozó műszaki, tűzvédelmi, érintésvédelmi és egyéb előírásokat. Az áramellátó berendezések és kábelek telepítését, karbantartását és javítását csak megfelelő szakképesítéssel és engedéllyel rendelkező személy végezheti.

A munkatársak figyelmét fel kell hívni arra, hogy az irodai elosztók, csatlakozók, hosszabbítók épségére ügyeljenek, a meghibásodott, sérült eszközöket ne használják tovább.

3.10 Tűzvédelem

A Hivatalban a tűzvédelmi feladatokat az ezzel megbízott külső személy látja el. A Hivatalnak az informatikai rendszerek tekintetében is meg kell felelni a hatályos tűzvédelmi előírásoknak.

3.11 Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem

Az elektronikus információs rendszer elemeit meg kell védeni a víz-, és más, csővezetéken szállított anyag okozta károkkal szemben. Ennek érdekében nem szabad csővezeték, víztározó, vízmelegítő és hasonló funkciójú, folyadékot, gázt vagy gőzt tartalmazó berendezés közelében aktív informatikai eszközöket elhelyezni.

A munkatársakat munkavédelmi, tűzvédelmi és egyéb oktatás keretében tájékoztatni kell az elzárószelepek helyéről, vészhelyzetben történő használatának szabályairól, a vészhelyzetben teendő halaszthatatlan intézkedésekről.

3.12 Be- és kiszállítás

Az informatikai eszközök javítására, karbantartására a jegyző által kijelölt szakszervíz, vállalkozó jogosult a szerződésben, megrendelésben rögzített feltételeknek megfelelően.

A Hivatal épületéből személyes adatokat tároló eszközt kivételesen, csak a jegyző vagy kijelölt munkatársának felügyelete mellett szabad kivinni. Egyéb esetben az adattároló eszközt a javítandó berendezésből, annak kiszállítása előtt, el kell távolítani, és illetéktelen hozzáféréstől védett, biztonságos helyen kell tárolni.

A kiszállított eszközökről a jegyző nyilvántartást vezet.

3.13 Az elektronikus információs rendszer elemeinek elhelyezése

A Hivatalban az informatikai eszközöket – a helyi adottságok keretein belül – úgy kell elhelyezni, hogy a lehető legnagyobb mértékben védve legyenek a jogosulatlan fizikai hozzáféréstől és az üzemi működési feltételeket veszélyeztető fizikai hatásoktól (hő-, nap-, elektromágneses sugárzás, rezgés, stb.).

Az informatikai eszközök elhelyezése, az irodák berendezése során figyelembe kell venni az alapvető ergonómiai és munkavédelmi követelményeket annak érdekében, hogy napi munkavégzést, ügyintézést az irodában elhelyezett eszközök, kábelek ne akadályozzák.

3.14 Karbantartók

A Hivatal informatikai eszközeinek karbantartását kizárólag önkormányzati vagy hivatali szintű vállalkozási (szolgáltatási) szerződés keretében megbízott személyek végezhetik, akik szerződésben vállalják a jelen szabályzatban részükre meghatározott követelmények teljesítését. Karbantartást csak a szerződésben nevesített és személyi adataikkal azonosított személyek végezhetnek.

A karbantartási munkákra jogosult személyekről a jegyző nyilvántartást vezet.

3.15 Időben történő javítás

A Hivatal – a helyi lehetőségek függvényében – átalánydíjas karbantartási szerződéssel biztosítja az informatikai eszközök rendszeres átvizsgálását, tisztítását, az elhasználódott eszközök időben történő cseréjét.

Ennek keretében a szerződésben meghatározott gyakorisággal, de legalább évente egyszer, szükséges a számítógépek és tartozékaik átfogó műszaki tesztelése, portalanítása, a beviteli eszközök (billentyűzet, egér) ellenőrzése, szükség szerinti cseréje.

4 Logikai védelmi intézkedések

4.1 Általános védelmi intézkedések

A jegyző megfogalmazza, dokumentálja, és kihirdeti az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárási folyamatokat, amelyek kiterjednek minden emberi, fizikai és logikai erőforrásra. Felügyeli az elektronikus biztonsági rendszer és környezet biztonsági állapotát, meghatározza az információbiztonsággal összefüggő szerepköröket és felelősségi köröket.

Az információbiztonsággal összefüggő szerepköröket jelen szabályzat Általános része ismerteti. Az egyes szerepköröket betöltő személyeket a jegyző a munkaköri leírásokban, illetve az IBF, a szolgáltatók és a rendszergazda szerepkört illetően a szerződéskötéssel jelöli ki.

4.1.1 Az elektronikus információs rendszer kapcsolódásai

A Hivatalban nem engedélyezett az információs rendszerek összekapcsolása más elektronikus információs rendszerekkel, ide nem értve az önkormányzati ASP rendszer használatával összefüggő, jogszabályban meghatározott központi szolgáltatóhoz történő kapcsolódást.

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

4.1.2 Belső rendszer kapcsolatok

A Hivatal belső információs rendszereinek összekapcsolását a jegyző engedélyezheti.

Nem minősül rendszerösszekapcsolásnak az általános célú irodai szoftverekkel előállított fájlok megosztása a helyi operációs rendszer és/vagy helyi hálózati kiszolgáló szolgáltatásain keresztül.

4.1.3 Külső kapcsolódásokra vonatkozó korlátozások

A Hivatalban engedélyezett a kapcsolódás a jogszabályban meghatározott központi szolgáltatásokhoz, illetve a munkakör ellátásához szükséges adatbázisokhoz és információs forrásokhoz. Nem engedélyezett a munkakör ellátásával közvetlenül össze nem függő hálózatokhoz és szolgáltatásokhoz történő kapcsolódás.

4.1.4 Személybiztonság

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. Jelen szabályzat személyi hatálya ennek megfelelően

került meghatározásra. A szabályzat felülvizsgálata során figyelembe kell venni azokat a körülményeket, melyek a személyi hatály módosítását indokolhatják.

Azokban az esetekben, amikor a Hivatal elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem az érintett szervezet tagja, a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot). A jegyző gondoskodik arról, hogy a szerződések, megállapodások e követelményeknek megfeleljenek.

4.2 Tervezés

4.2.1 Cselekvési terv

A jegyző - az IBF javaslata alapján, valamint az esetleg szükséges önkormányzati döntéseknek megfelelően - cselekvési tervet fogad el, amennyiben az IBF vagy más, ellenőrzésre jogosult szerv megállapítása szerint a biztonsági helyzet nem felel meg a jelen szabályzat bármely pontja kapcsán a követelményeknek.

A cselekvési tervben dokumentálni kell a megállapított hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeket, ezek pénzügyi forrását, a felelősöket és a határidőket. A cselekvési tervet a Hivatal a tervben meghatározott mérföldkövek szerint, de legalább évente felülvizsgálja.

4.2.2 Személyi biztonság

A Hivatalban az informatikai rendszerekhez hozzáférési jogosultságot csak a munkakör ellátásához szükséges mértékben, a legkisebb funkcionalitás elvének szem előtt tartásával szabad kiosztani.

A jogosultságot szerzett felhasználónak az informatikai rendszer használata előtt meg kell ismernie a vele szemben támasztott elvárásokat, magatartási szabályokat és felelősséget, és erről írásban nyilatkoztatni kell őt.

Az önkormányzati ASP rendszerben jogosultsággal rendelkező felhasználóknak a hozzáférés előtt a vonatkozó központi követelményeknek megfelelő titoktartási nyilatkozatot kell tenniük.

A helyi informatikai rendszerelemekhez történő hozzáféréshez nem kell külön titoktartási nyilatkozatot tenni a köztisztviselő jogállású felhasználóknak és a választott tisztségviselőknek. A munkavégzésre kijelölt számítógépeken az érintett felhasználó külön engedély nélkül jogosult általános célú felhasználói fiókot használni.

A személyi biztonsági követelményeket a jegyző évente, biztonsági incidens esetén soron kívül, felülvizsgálja.

4.3 Konfigurációkezelés

4.3.1 Konfigurációkezelési eljárásrend

A Hivatal nyilvántartást vezet a tulajdonában lévő informatikai rendszerelemekről. A nyilvántartás kiterjed – ha ez az adott esetben értelmezhető - a rendszerelem szoftver konfigurációjára, a szoftverek verziójára is. Az IBF folyamatosan ellenőrzi a konfigurációk nyilvántartását. A nyilvántartás vezetéséhez a rendszergazda, a szolgáltató köteles támogatást nyújtani, e kötelezettségét a vonatkozó szerződésnek tartalmaznia kell.

A Hivatalban csak az önkormányzati ASP rendszerhez előírt hardver és szoftver konfigurációnak megfelelő számítógépeket és egyéb eszközöket szabad használni. Az ezen követelményeket nem sértő konfigurációs eltéréseket a jegyző engedélyezi.

A Hivatal helyi rendszereinek hardver és szoftver konfigurációját a szállítói alapbeállításoknak megfelelően kell üzembe állítani. Az alapkonfigurációk dokumentációit, telepítő készleteit a jegyző által kijelölt tárolási helyen kell tartani úgy, hogy egy esetleges biztonsági incidens után a helyreállítást a lehető legrövidebb időn belül el lehessen végezni.

4.3.2 Legszűkebb funkcionalitás

A Hivatal informatikai eszközeinek meg kell felelni a munkakör ellátásához szükséges funkcionális követelményeknek, ezen túl azonban további szolgáltatásokat az informatikai rendszerben nem szabad engedélyezni. Tilos olyan programtermékek telepítése, melyek a munkakör ellátásához nem szükségesek. A nem használt protokollokat, portokat a rendszergazdának kell letiltani.

4.3.3 Duplikálás elleni védelem

A Hivatal nem veszi nyilvántartásba azokat az informatikai eszközöket, melyek más, jellemzően központi szerv nyilvántartásában szerepelnek.

4.3.4 A szoftver használat korlátozásai

A Hivatalban tilos olyan szoftvereket, digitális szellemi termékeket telepíteni és használni, melyek felhasználási jogával a Hivatal nem rendelkezik.

A kereskedelmi forgalomban beszerzett szoftverek licenceit nyilván kell tartani, és kizárólag a licencfeltételekben meghatározott terjedelemben és feltételekkel szabad a terméket használni.

A szerzői joggal védett állományok megosztását a jegyző engedélyezi, ennek során vizsgálja, hogy a megosztást nem használják-e fel a szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

4.3.5 A felhasználó által telepített szoftverek

A Hivatalban nem engedélyezett a felhasználók számára a szoftverek telepítése.

Szoftver telepítését a jegyző utasítására, illetve engedélye alapján a rendszergazda, vagy más, a jegyző által kijelölt munkatárs végzi el.

4.4 Karbantartás

4.4.1 Rendszer karbantartási eljárásrend

Az információs rendszereket, aktív rendszerelemeket legalább félévente ellenőrizni és szükség szerint karbantartani szükséges. A karbantartás diagnosztikai programok futtatásával, szoftverkomponensek frissítésével, indokolt esetben az operációs rendszer és más komponensek újratelepítésével, a konfigurációs beállítások ellenőrzésével és a szükséges módosítások elvégzésével kell végrehajtani.

A rendszerkarbantartás rendjét az erre vonatkozó szolgáltatási szerződésnek kell tartalmazni.

4.4.2 Adathordozó ellenőrzés

A rendszergazda köteles ellenőrizni a diagnosztikai és teszt programokat tartalmazó adathordozókat a kártékony kódok tekintetében, mielőtt azokat az elektronikus információs rendszerben felhasználná.

4.4.3 Távoli karbantartás

A karbantartást távfelügyelettel csak úgy szabad elvégezni, ha biztosított, hogy az önkormányzati ASP központhoz csatlakozó számítógépek vezérlését (képernyő- és billentyűzet átvétel) ezáltal nem lehet elérni.

A távoli karbantartás kizárólag a rendszerkarbantartást rögzítő szerződésben, munkautasításban meghatározott módszerekkel, eszközökkel és egyéb feltételekkel szabad végezni. A távoli karbantartás során biztonságos hitelesítési eljárásokat kell használni, a munkaszakaszt és a hálózati kapcsolatokat a karbantartás végén le kell zárni.

A távoli karbantartási tevékenységet rögzítő naplóállományokat a karbantartás elvégzését követően egy évig meg kell őrizni.

4.5 Adathordozók védelme

4.5.1 Adathordozók védelmére vonatkozó eljárásrend

Az adathordozók (USB kulcs, külső HDD, memóriakártya, CD/DVD) beszerzését és használatát a jegyző engedélyezi.

A felhasználók felelősek a részükre kiadott adathordozók kezeléséért, jelen szabályzatban meghatározott korlátozások és követelmények maradéktalan betartásáért. A jegyző - az IBF és a rendszergazda támogatásával – rendszeresen ellenőrzi a használatban lévő adathordozók kezelési szabályainak betartását.

4.5.2 Hozzáférés az adathordozókhoz

Az adathordozók használatát a kijelölt munkatársak részére a jegyző engedélyezi. A személyi használatra kiadott adathordozó esetén a használathoz további engedély – a jelen szabályzatban meghatározott használati korlátozások keretein belül - nem szükséges.

A hivatali használatra rendszeresített adathordozót külső, harmadik személynek átadni nem szabad.

4.5.3 Adathordozók tárolása

A még felhasználásra ki nem adott adathordozók tárolására, nyilvántartására a gazdálkodási szabályok az irányadók.

A mentésre használatba vett adathordozókat olyan biztonságos, zárt helyen kell tárolni, ahol a hozzáférés kizárólag az arra jogosult munkatársak részére lehetséges.

A személyi használatban lévő adathordozók tárolása során a felhasználó felelőssége, hogy az adathordozó átmenetileg se kerüljön illetéktelen személyhez.

4.5.4 Adathordozók szállítása

A Hivatal szokásos működése során nincs adathordozó szállításával összefüggő feladat.

Rendkívüli esetben, ha személyes adatokat tartalmazó adathordozó szállítására lenne szükség, az eseti részletszabályokat a jegyző határozza meg. Ennek során dokumentálni kell a szállítás célját és körülményeit, az adathordozón tárolt adatbázis megnevezését, terjedelmét, a szükséges kriptográfiai eljárást, ki kell jelölni a szállításért felelős személyt. A feladat végrehajtásába be kell vonni az IBF-t.

4.5.5 Kriptográfiai védelem

Kriptográfiai védelmet a Hivatal saját hatáskörében nem alkalmaz.

Jogszabályban előírt, kriptográfiai védelemmel összefüggő hivatali feladatok végrehajtása során maradéktalanul be kell tartani a kijelölt központi szolgáltató által előírt eljárásokat és szabályokat.

4.5.6 Adathordozók törlése

A Hivatal kijelölt munkatársai vagy szerződött műszaki partnerei támogatásával gondoskodik arról, hogy helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törölje az elektronikus információs rendszer adathordozóit a leselejtezés, a használatból történő kivonás vagy újrafelhasználásra való kibocsátás előtt.

A törlési eljárások megválasztása során figyelembe kell venni, hogy az adott adathordozón milyen adatok tárolása történt.

4.5.7 Adathordozók használata

A Hivatalban kizárólag a jegyző által engedélyezett, a Hivatal által beszerzett alábbi adathordozókat szabad használni:

- USB kulcs,
- memóriakártya,
- külső HDD.

Adathordozókat csak a jegyző által engedélyezett célra, pl. mentések készítésére és általános célú irodai alkalmazásokkal készült állományok átmeneti tárolására szabad használni.

A Hivatal adathordozón tesz eleget adatszolgáltatási kötelezettségének, ha ezt jogszabály előírja.

Tilos magán, illetve idegen tulajdonban lévő bármilyen adathordozó és adathordozóként használható eszköz (pl. mobil eszköz) csatlakoztatása a Hivatal informatikai eszközeihez, kivéve, ha ez szerződésben vállalt kötelezettség teljesítésének a részét képezi (pl. rendszergazda, karbantartó, IBF feladatok ellátása során).

4.5.8 Ismeretlen tulajdonos

Tilos bármilyen adathordozó és adathordozóként használható eszköz csatlakoztatása a Hivatal informatikai eszközeihez, ha tulajdonos nem azonosítható.

4.6 Azonosítás és hitelesítés

4.6.1 Azonosítási és hitelesítési eljárásrend

A Hivatalban az azonosítással kapcsolatos engedélyeket a jegyző adja ki.

Engedélyezettnek kell tekinteni egyedi azonosító használatát a munkakör ellátásához rendszeresített számítógépeken, a hivatali (önkormányzati) tartományban létrehozott e-mail fiókhoz, a munkakörhöz rendelt önkormányzati ASP rendszer moduljaihoz, funkcióihoz.

4.6.2 Azonosító kezelés

Az azonosítók kezelését az önkormányzati ASP rendszerben a szolgáltatási szerződésben és a központi szolgáltatók által kiadott rendelkezéseknek megfelelően kell végezni.

A Hivatal helyi rendszereiben és eszközein az azonosítók létrehozását a kijelölt munkatársak, illetve a szolgáltatók végzik, a jegyző intézkedései alapján. Ennek során kerülni kell a korábban felhasznált azonosító ismételt használatba vételét, és gondoskodni kell a nem használt azonosítók inaktiválásáról.

4.6.3 A hitelesítésre szolgáló eszközök kezelése

Az önkormányzati ASP rendszerben a felhasználók kizárólag elektronikus személyazonosító okmánnyal hitelesítik magukat.

A Hivatalban egyéb hitelesítést szolgáló eszköz nincs rendszeresítve.

4.6.4 Jelszó (tudás) alapú hitelesítés

A Hivatal a felhasználók jelszavát nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hasító érték tárolást), és nem továbbítja. Kivételt képez a számítógépek és egyéb aktív eszközök adminisztrációjához szükséges rendszergazda jelszó, melynek aktuálisan érvényes verzióját zárt borítékban a jegyzőnél kell elhelyezni.

Tilos a felhasználói jelszavakat leírva vagy elektronikusan olvasható formában tárolni, más személlyel szóban vagy írásban közölni.

4.6.5 Birtoklás alapú hitelesítés

A Hivatalban hardver token és nyilvános kulcsú infrastruktúra alapú hitelesítés saját hatáskörben nincs rendszeresítve.

4.6.6 Személyes vagy megbízható harmadik fél általi regisztráció

A Hivatalban regisztrációs eljárást igénylő hitelesítő eszköz nincs rendszeresítve.

4.7 Hozzáférés ellenőrzése

4.7.1 Hozzáférés ellenőrzési eljárásrend

A Hivatal elektronikus informatikai rendszeréhez és a Hivatalon belül elérhető, nem nyilvános külső rendszerekhez csak a jegyző által engedélyezett személyek férhetnek hozzá. A hozzáférés ellenőrzése érdekében a felhasználók részére felhasználói fiókok kerülnek létrehozásra. Minden felhasználó köteles a hozzáférés során a saját fiókját használni.

Az ASP Központtól kapott szoftveres tanúsítványt és annak jelszavát tilos átadni az ASP Központ által nem feljogosított személynek.

4.7.2 Felhasználói fiókok kezelése

A Hivatalban – a jogszabály alapján kijelölt központi szolgáltatóknál létrehozott felhasználói fiókokon kívül – az alábbi fióktípusok vannak rendszeresítve:

- a munkakör ellátásához biztosított számítógépen normál (nem rendszergazda) fiók,
- a Hivatal (önkormányzat) internetes tartományába bejegyzett e-mail fiók,
- a hivatali számítógépekhez és más aktív eszközök adminisztrációjához szükséges rendszergazda fiók.

A fiókokok kezelését a jegyző, illetve kijelölt munkatársa szolgáltatói támogatással végzi.

A helyi felhasználói fiókok csoport, illetve szerepköri alapon nincsenek elkülönítve.

A felhasználói fiókok létrehozására, módosítására, tiltására, törlésére a munkáltatói intézkedésekhez kapcsolódóan a jegyző ad utasítást.

A felhasználói fiókok rendeltetésszerű használatát a jegyző a szolgáltatók bevonásával is ellenőrizheti.

4.7.3 A felelősségek szétválasztása

A Hivatal minden felhasználója felelős a felhasználói fiókja jelen szabályzatban meghatározott követelményeknek megfelelő használatáért.

A rendszergazda feladatokkal megbízott személy köteles a felhasználói fiókok használatával kapcsolatosan visszaélésre utaló naplóbejegyzések, rendszeresemények észlelése esetén a jegyzőnek a tapasztaltakról soron kívül jelentést tenni.

4.7.4 Legkisebb jogosultság elve

A Hivatal az elektronikus információs rendszerhez történő hozzáférés engedélyezése során a legkisebb jogosultság elvét alkalmazza, azaz a felhasználók - vagy a felhasználók tevékenysége - számára csak a számukra kijelölt munkaköri feladatok végrehajtásához feltétlenül szükséges jogosultságokat engedélyezi.

4.7.5 Jogosult hozzáférés a biztonsági funkciókhoz

A Hivatal a jegyző által kijelölt munkatársaknak és szolgáltatóknak hozzáférési jogosultságot biztosít azon rendszerelemekhez és biztonsági funkciókhoz, melyek feladataik ellátásához szükségesek.

4.7.6 Nem privilegizált hozzáférés a biztonsági funkciókhoz

A Hivatal meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező felhasználói a nem biztonsági funkciók használatához nem használhatják a különleges jogosultsághoz kötött - úgynevezett privilegizált - fiókjukat vagy szerepkörüket.

Ennek biztosítása érdekében azon felhasználók részére, akik meghatározott biztonsági funkciókhoz privilegizált fiókkal rendelkeznek, létre kell hozni a munkakörük, feladataik ellátása során egyébként használandó, nem privilegizált fiókot.

4.7.7 Privilegizált fiókok

Privilegizált fiókok létrehozása kizárólag a jegyző engedélyével történhet azon személyek részére, akik meghatározott feladataikat csak ezen fiókok használatával tudják ellátni.

Privilegizált fiókkal rendelkezhet a helyi rendszerelemeket illetően:

- a jegyző és a helyettesítésére jogosult személy,
- a rendszergazda, illetve kulcsfelhasználó feladatokkal megbízott munkatárs,
- a szolgáltató a szerződésben meghatározott feltételekkel.

Az önkormányzati ASP rendszerben privilegizált fiókkal a jegyző által kijelölt személyek rendelkezhetnek:

- az önkormányzati (tenant) adminisztrátor,
- a szakrendszeri adminisztrátor,
- a kulcsfelhasználó.

A privilegizált fiókokat használó személyek kijelölése írásos megbízással, szerződéssel, a jogosultságnak a munkaköri leírásban való rögzítésével vagy az ASP rendszer szolgáltatója által meghatározott eljárással történhet.

4.7.8 A munkaszakasz zárolása

Az önkormányzati ASP rendszerben a munkaszakaszok zárolására és annak feloldására a szolgáltató által megadott szabályok érvényesek.

A helyi munkaállomások operációs rendszereit úgy kell konfigurálni, hogy

- meghatározott időtartamú inaktivitás vagy a felhasználó erre irányuló lépése esetén a képernyő zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést;
- megtartsa a munkaállomás zárolását mindaddig, amíg a felhasználó a bejelentkezési eljárással nem azonosítja és hitelesíti magát újra.

A zárolás feloldásának könnyebbé tétele érdekében – ha azt az operációs rendszer lehetővé teszi - a bejelentkezéshez PIN kód használata engedélyezett.

4.7.9 Képernyőtakarás

A munkaszakasz zárolásakor a képernyőn korábban látható információt egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a zároló személy nevét is tartalmazhatja - kell eltakarni.

4.7.10 A munkaszakasz lezárása

Az önkormányzati ASP rendszerben a munkaszakasz lezárására a szolgáltató által megadott szabályok érvényesek.

A helyi rendszerelemek lezárását kijelentkezéssel és a készülék kikapcsolásával kell biztosítani.

4.7.11 Vezeték nélküli hozzáférés

Az önkormányzati ASP rendszerhez használt számítógépeket nem szabad vezeték nélküli hálózathoz csatlakoztatni. Ez alól a jegyző engedélyével olyan esetekben szabad csak átmenetileg kivételt tenni, amikor a vezetékes kapcsolatra technikai lehetőség nincs, és a munkaköri feladatok ellátását más módon nem lehet biztosítani.

A vezeték nélküli hálózathoz történő hozzáférést úgy kell korlátozni a hálózati eszközök megfelelő konfigurálásával, hogy illetéktelen személy a hálózaton üzemelő hivatali számítógépekhez ne férhessen hozzá.

Külső személyeknek, illetve magáncélú eszközöknek a Hivatalban vezeték nélküli kapcsolatot biztosító hálózati eszközökhöz csak úgy szabad hozzáférést engedélyezni, ha a hálózat külső személyek által látható szegmense a hivatali számítógépek által használt szegmenstől biztonságosan el van választva.

4.7.12 Mobil eszközök hozzáférés ellenőrzése

A Hivatal hálózatához – a Hivatal (önkormányzat) tulajdonában lévő laptop számítógépek kivételével - mobil eszközökkel nem szabad csatlakozni, ennek lehetőségét a hálózati eszközök megfelelő konfigurálásával ki kell zárni.

4.7.13 Titkosítás

A Hivatalban eszköztitkosítást biztosító eljárások nincsenek rendszeresítve, ezért a Hivatal mobil eszközein védett információt nem szabad tárolni.

4.7.14 Külső elektronikus információs rendszerek használata

A Hivatalban kizárólag a jogszabályban meghatározott és központi szolgáltatók által üzemeltett külső információs rendszerek használata engedélyezett.

Nem minősül külső információs rendszer használatnak a munkaköri feladatok ellátása érdekében igénybe vett, azonosítást nem igénylő, nyilvános, böngésző alapú információs szolgáltatások (keresők, portálok) használata.

4.7.15 Korlátozott használat

A jogszabályban meghatározott és központi szolgáltatók által üzemeltett külső információs rendszerek használata során maradéktalanul be kell tartani a szolgáltató által előírt és megkövetelt biztonsági szabályokat, korlátozásokat.

A külső elektronikus információs rendszerek eléréséhez nem szabad olyan hálózati kapcsolatot, eszközt felhasználni, melyet az üzemeltető szervezet nem hagyott jóvá, vagy amelyet megállapodás, szolgáltatási szerződés nem rögzített.

4.7.16 Hordozható adattároló eszközök

A jogszabályban meghatározott és központi szolgáltatók által üzemeltett külső információs rendszerek használata során nem szabad a munkaállomáshoz hordozható tároló eszközt csatlakoztatni, a rendszerből adatokat kimásolni, vagy oda betölteni. Ez alól csak a központi szolgáltató által jóváhagyott, kifejezetten hordozható adattároló használatát igénylő műveletek lehetnek kivételek (pl. adatmigrálás).

4.7.17 Információ megosztás

A Hivatalban információmegosztásra vonatkozó döntést csak a jegyző, valamint a helyettesítésére jogosult hozhat.

Nem szükséges engedély az elektronikus információs rendszerben olyan dokumentumok hivatali belső megosztásához, melyeket a szokásos ügymenet során a munkatársak feladataik elvégzése érdekében egymásnak átadnak.

4.7.18 Nyilvánosan elérhető tartalom

Az információk nyilvános közzétételének feltételeit a Hivatal külön szabályzatban rögzítette.

4.8 Rendszer és információ sértetlenség

4.8.1 Rendszer és információ sértetlenségre vonatkozó eljárásrend

A rendszer- és információ sértetlenséget érintő rendellenességeket, hibákat minden felhasználó köteles jelenteni a jegyzőnek, aki megteszi a szükséges intézkedéseket.

A helyi rendszerelemeket érintő rendellenesség, hiba kivizsgálásába bevonja a rendszergazdát, biztonsági incidensre utaló körülmények esetén az IBF-t, akik a megállapításaikat, intézkedési javaslataikat dokumentálják.

Az önkormányzati ASP-t ért incidensek észlelését a jegyző jelenti az ASP Központ felé, az IBF pedig a Kormányzati Eseménykezelő Központnak. A jelentés nem tartalmazhat olyan szenzitív adatot (pl. személyes adatot), elemeket, amelyet harmadik fél nem ismerhet meg.

4.8.2 Hibajavítás

Az arra kijelölt felhasználók az ASP rendszerben észlelt hibákat a hibabejelentő rendszeren keresztül jelentik be. Az ASP Központ a bejelentéseket fogadja, továbbítja az illetékes terület felé és a jogszabály szerinti lépéseket megteszi. Az ASP Központ az elhárítási határidőről a Tájékoztatási

Portálon közleményt helyez el, amely alapján a jegyző dönt a szükséges munkaszervezési intézkedéseket illetően.

A helyi hardver rendszerelemek meghibásodása esetén a jegyző gondoskodik a javítás megrendeléséről.

A hibajavítással kapcsolatos szoftverfrissítéseket a rendszergazda a szerződésben, megrendelésben rögzített feltételekkel köteles telepíteni. A jegyző soron kívüli szoftvertelepítésre intézkedik, ha az IBF tájékoztatása szerint ennek hiányában a biztonságos munkavégzés feltételei a Hivatalban nem adottak, és a veszélyhelyzet elhárítása nélkül nagy valószínűséggel káresemény következne be.

A konfigurációk nyilvántartásának ki kell terjedni a telepített szoftverek verziójára is annak érdekében, hogy a szükséges frissítések végrehajtása ellenőrizhető legyen.

4.8.3 Kártékony kódok elleni védelem

A Hivatal számítógépein vírusvédelmi szoftvert kell használni. Azokon a számítógépeken, ahol az operációs rendszer tartalmaz vírusok és más veszélyforrások elleni védelmi funkciókat (pl. Windows Defender), ott más vírusvédelmi programot nem kötelező alkalmazni. Az operációs rendszer védelmi funkcióit ebben az esetben teljes körűen engedélyezni kell.

A védelmi funkciókat úgy kell konfigurálni, hogy:

- rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren, és hajtsa végre a külső forrásokból származó fájlok valós idejű ellenőrzését amikor a fájlokat letöltik, megnyitják vagy elindítják,
- kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt, és erről értesítse a felhasználót, aki köteles ezt biztonsági incidensként kezelni és jelenteni.

A téves riasztásokról, ennek várható megismétlődéséről és a szükséges teendőkről a rendszergazda és az IBF szükség szerint tájékoztatja a felhasználókat.

4.8.4 Automatikus frissítés

A kártékony kódok elleni védelmi szoftvereket úgy kell konfigurálni, hogy az elektronikus információs rendszer automatikusan frissítse azokat.

4.8.5 Az elektronikus információs rendszer felügyelete

Az elektronikus információs rendszer felügyeletében a biztonságért felelős minden szereplőnek meghatározott felelőssége és feladata van:

- a felhasználók kötelesek minden olyan jelenséget, szokatlan rendszerviselkedést jelenteni a jegyzőnek, ami a rendszer jogosulatlan használatára, a kezelt adatok sértetlenségének, bizalmasságának sérülésére utal;
- a jegyző intézkedik minden észlelt rendellenesség dokumentálásáról, az érintett rendszertől függően a jelzés kivizsgálásának kezdeményezéséről az ASP Központ, a rendszergazda és az IBF felé;
- a rendszergazda a szerződésben meghatározott módon rendszeresen ellenőrzi az elektronikus információs rendszer naplózásait, kivizsgálja a felhasználók jelzéseit, elvégzi a felügyeleti eszközök konfigurálását;

- az IBF legalább évente ellenőrzi a felügyeleti eszközök beállításait, szükség esetén szakmai támogatást nyújt a bejelentett rendellenességek kivizsgálásához.

4.8.6 Biztonsági riasztások és tájékoztatások

A Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező, illetve a Kormányzati Eseménykezelő Központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket az IBF értékeli, meghatározza az ezzel összefüggésben javasolt vezetői intézkedéseket, felhasználói magatartási szabályokat, rendszergazda feladatokat, és erről az érintetteket haladéktalanul tájékoztatja.

A jegyző és az IBF kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, kapcsolatot tart a jogszabályban meghatározott szervekkel.

4.8.7 Bemeneti információ ellenőrzés

Az elektronikus információs rendszereket úgy kell konfigurálni, hogy a belépési pontok ellenőrzését biztosító funkciók teljes körűen engedélyezve legyenek.

4.8.8 A kimeneti információ kezelése és megőrzése

A Hivatal az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az ASP üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

Nyőgér, 2018. március 31.

NYŐGÉRI KÖZÖS ÖNKORMÁNYZATI HIVATAL * 1 *

(:Dr. Lendvai Róbert:)
jegyző

5 Mellékletek

5.1 A szabályzat alapján vezetendő nyilvántartások

A jegyző jelen szabályzat végrehajtása keretében nyilvántartást vezet, illetve ezek vezetésére intézkedik:

- Az elektronikus információs rendszerekről, mely tartalmazza
  - annak alapfeladatait;
  - a rendszerek által biztosítandó szolgáltatásokat;
  - az érintett rendszerekhez tartozó licenc számot (ha azok a Hivatal kezelésében vannak);
  - a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;
  - a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.
- az elektronikus rendszerelemekről
  - neve;
  - típusa;
  - gyártója;
  - felelős felhasználója;
  - felhasználói hozzáférések azonosítói;
  - hardver paraméterek, konfiguráció jellemzői (CPU, memória, stb.);
  - szoftver paraméterek (operációs rendszer, telepített programok neve, elérési útja, telepítés dátuma, verziója).
- a Hivatalba hivatali időben és azon kívül belépésre jogosultakról, a belépés esetleges külön feltételeiről (riasztó, kulcs használat);
- a kiszállított informatikai eszközökről;
- a beszerzett (raktáron lévő) és a személyi használatra kiadott adathordozókról;
- a karbantartási munkákra jogosult személyekről;
- a kereskedelmi forgalomban beszerzett szoftverek licencéről;
- a munkatársak elektronikus levelezési címéről;
- a felhasználóknak az informatikai oktatáson való részvételéről.

A nyilvántartásokat elektronikusan, az erre kialakított IBF portálon vezetik.

5.2 Informatikai Biztonsági Házirend

1. A Hivatal felhasználói munkaköri feladataik teljesítéséhez kizárólag a Hivatal által meghatározott eszközöket és internetes szolgáltatásokat használhatják.

   A Hivatal felhasználói számára tilos:

   - a hivatali (nem nyilvános) információk nyilvános internetes oldalakon való jogtalan közzététele;
   - munkaköri feladatokhoz kapcsolódóan magáncélú e-mail fiókot, üzenőszolgáltatást vagy bármilyen egyéb, nem engedélyezett szolgáltatást használni;
   - a munkaköri feladatokon kívül bármilyen, internet használatával megvalósuló tevékenységet végezni (magáncélú fájlletöltés, böngészés, közösségi oldalak és fórumok látogatása, magáncélú levelezés stb.).

2. A Hivatalban nem engedélyezett a felhasználók számára, hogy a számítógépükre szoftvereket telepítsenek.

3. A felhasználók felelősek a részükre kiadott adathordozók kezeléséért, jelen szabályzatban meghatározott korlátozások és követelmények maradéktalan betartásáért. A hivatali használatra rendszeresített adathordozót nem szabad külső, harmadik személynek átadni, hivatalon kívül őrizetlenül hagyni, valamint engedély nélkül nem hivatali eszközhöz csatlakoztatni.

4. Tilos a felhasználói jelszavakat leírva vagy elektronikusan olvasható formában tárolni, más személlyel szóban vagy írásban közölni.

5. A felhasználó köteles jelenteni a jegyzőnek, ha

   a. az informatikai rendszert érintő belső fenyegetést, pl. jogosulatlan rendszerhozzáférést, adatvesztést, bizalmas adatok kikerülését észleli;

   b. rendszer- és információ sértetlenséget érintő rendellenességeket észlel, biztonsági problémára utaló rendszerüzenetet kap, vagy szokatlan, hibás programviselkedést tapasztal;

   c. ha a hivatali épületben vagy annak valamely helyiségében illetéktelen személy tartózkodik, vagy a belépési rendet veszélyeztető egyéb körülményt (riasztó, zár meghibásodás, kulcs elvesztése stb.) észlelt.

6. Az ügyfelet vagy más látogatót nem szabad felügyelet nélkül hagyni olyan helyiségben, ahol aktív informatikai eszközök működnek, illetve ahol az informatikai infrastruktúra kritikus elemei hozzáférhetők (pl. kapcsoló szekrény, kábelelosztó, szünetmentes táp stb.).

7. Az ügyfélfogadás során ügyelni kell arra, hogy az ügyfél a számítógép képernyőjét ne láthassa, a nyomtatóban az adott ügyfélnek szánt iraton kívül más dokumentum ne készüljön, illetve a nyomtatóban ne maradjon.

8. A számítógépen minden alkalmazásból ki kell jelentkezni és az alkalmazásokat be kell zárni a munkaidő végén vagy hosszabb munkaközi szünet esetén. Karbantartást megelőzően a számítógépet le kell állítani, illetve újra kell indítani, a karbantartó a számítógépet csak a saját azonosítójával használhatja.

9. A Felhasználó köteles a számítástechnikai eszközökkel végzett munkája során a tűz—és munkavédelmi szabályokat maradéktalanul betartani. Ügyelni kell az elektromos berendezések, irodai elosztók, csatlakozók, hosszabbítók épségére, a meghibásodott, sérült eszközöket tovább használni tilos.

10. Minden felhasználó köteles az informatikai biztonsági oktatáson részt venni, az ott megismert ismereteket mindennapi munkájában hasznosítani.

5.3 Fogalmak jegyzéke

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

adatfeldolgozás: az adatkezeléshez kapcsolódó technikai feladatok elvégzése;

adatfeldolgozó: az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az adatkezelő részére adatfeldolgozást végez;

adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása;

adatkezelő: az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az adatkezelést végzi;

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

auditálás: előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;

bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

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

biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége;

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

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

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

elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese;

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

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

észlelés: a biztonsági esemény bekövetkezésének felismerése;

felhasználó: egy adott elektronikus információs rendszert igénybe vevők köre;

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

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

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

információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;

kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;

kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

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

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

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

központi szolgáltató: a NISZ Nemzeti Infokommunikációs Szolgáltató Zártkörűen Működő Részvénytársaság (a továbbiakban: NISZ Zrt.) és az IdomSoft Informatikai Zártkörűen Működő Részvénytársaság (a továbbiakban: IdomSoft Zrt.);

kritikus adat: az Infotv. szerinti személyes adat, különleges adat vagy valamely jogszabállyal védett adat;

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

megelőzés: a fenyegetés hatása bekövetkezésének elkerülése;

önkormányzati ASP rendszer: a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény (a továbbiakban: Mötv.) 114. § (2) bekezdése szerinti, a helyi önkormányzatok, valamint gazdálkodási szakrendszer esetében az önkormányzat által alapított költségvetési szerv feladatellátását támogató, számítástechnikai hálózaton keresztül távoli alkalmazásszolgáltatást (Application Service Provider, ASP) nyújtó elektronikus információs rendszer;

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

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

sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

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

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

szakrendszer: az önkormányzati ASP rendszer által nyújtott, igazgatási feladatokat támogató szakalkalmazás;

szervezet: az adatkezelést vagy adatfeldolgozást végző jogi személy, valamint jogi személyiséggel nem rendelkező gazdasági társaság, egyéni vállalkozó;

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

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

védelmi feladatok: megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;

zárt célú elektronikus információs rendszer: jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer;

zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.

Nyilatkozat a szabályzat megismeréséről

A Nyőgéri Közös Önkormányzati Hivatal Informatikai Biztonsági Szabályzatában foglaltakat megismertem, tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

Név	Beosztás	Kelt	Aláírás
Pallósi Csabáné	Nyőgéri KÖH/aljegyző	2018. 04. 06.	
Lengyel Árpád Csabáné	Nyőgéri KÖH Bögötei Kir./ig. ea.	2018. 04. 06.	
Komáromi Laura	Nyőgéri KÖH Bögötei Kir./püi.,	2018. 04. 06.	
Vajda Krisztina	Nyőgéri KÖH/ Káldi Kir./püi. ea.	2018. 04. 06.	
Mihályi Anna	Nyőgéri KÖH/Káldi Kir./ adóügyi. ea.	2018. 04. 06.	
Takóné Nagy Gabriella	Nyőgéri KÖH Káldi Kir./ig. ea.	2018. 04. 06.	
Kovács Annamária	Nyőgéri KÖH Sótonyi Kir./püi. ea.	2018. 04. 06.	
Antalné Klauzer Judit	Nyőgéri KÖH Sótonyi Kir./ig. ea.	2018. 04. 06.	
Szakos Károlyné	Nyőgéri KÖH/ ügykezelő	2018. 04. 06.	
Takács Ferencné	Nyőgéri KÖH/ig. ea.	2018. 04. 06.	
Bándoliné Máté Judit	Nyőgéri KÖH /püi. ea.	2018. 04. 06.	
Pintér Katalin	Nyőgéri KÖH Mkov. Kir./püi. adóüi. ea.	2018. 04. 06.	
Tamás Sándorné	Nyőgéri KÖH Mkov Kir./ig. ea.	2018. 04. 06.	
Szabó Ildikó	Nyőgéri KÖH /püi., adóügyi. ea.	2018. 04. 06.	
Bándoli Tímea	Nyőgéri KÖH/kistérségi üi.	2018. 04. 06.	