Sárbogárdi Polgármesteri Hivatal Jegyzője
A-297-1/ 2019.

SÁRBOGÁRDI POLGÁRMESTERI HIVATAL

Informatikai Biztonsági Szabályzata

Sárbogárd Város Jegyzője

.....

Dr. Venicz Anita
jegyző

Verzió	Dátum	Módosította/létrehozta	Módosítás
0.1	2017.12.29.	Misák István	első verzió
1.0	2019.03.18.	Misák István	véglegezett verzió
2.0	2019.07.17.	Misák István	2. sz. melléklet módosítása (ASP tervezett)

Sárbogárd, 2019.

Tartalomjegyzék

I. Általános rész

I.1. Az IBSZ célja

Az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) biztonságkezelési elveket, követelményeket és szabályokat tartalmaz aSárbogárdi Polgármesteri Hivatal(továbbiakban: a Hivatal) tevékenykedő személyek (bizonyos feltételek esetén külső közreműködők) számára, akik felelősek az információbiztonság fejlesztéséért, megvalósításáért és megtartásáért. Az IBSZ hatékonyan támogatja a Hivatal biztonságkezelésének mindennapi gyakorlatát, illetve megfelelő kereteket biztosít a Hivatal teljes körű biztonsági szabályozásához.

Az IBSZ-ben szereplő követelményeket, rendelkezéseket és ajánlásokat a hatályos jogszabályok keretei között kell használni.A biztonsági szabályozás célja a következő:

a) A jogkövető magatartásés a jó hírnév érdekében védeni a szervezet értékeit,

b) A tudatosság,a szervezettség, a hatékonyság és a technikai megoldások használata segítségével növelni az információbiztonságot,

c) A megelőzés, a tájékoztatás, az oktatás, a felderítés és a szankcionálás eszközeivel segíteni az intézkedések érvényesítését.

A jelen IBSZ a Hivatal szervezeti szintű információbiztonsági szabályozó rendszerének egyik alapvető eleme.Az IBSZ a hatályos jogszabályokkal, a Hivatal működési és ügyrendi előírásaival összhangban megteremti az elektronikus információs rendszerek és az azokban kezelt adatok biztonságát. Tartalmazza a Hivatal elektronikus információs rendszereivel kapcsolatba kerülő személyek felé támasztott minimum információbiztonsági követelményeket, továbbá meghatározza azokat az elvárásokat, kötelezettségeket és a felelősséget, amelyekre a biztonságos információellátás érdekében szükség van.

A Hivatal informatikai szolgáltatóival kötött szolgáltatási szerződéseknek és azok mellékleteinek összhangban kell lenniük jelen IBSZ-szel.

I.2. Hatály

I.2.1. Szervezeti-személyi hatály

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

Az IBSZ személyi hatálya kiterjed a Hivatal munkavégzésre irányuló bármely jogviszonyban álló természetes és jogi személyre, tehát azokra, akik kapcsolatba kerülnek a Hivatal elektronikus információs rendszereivel (használják, fejlesztik, telepítik, üzemeltetik, javítják stb.), így:

a) a választott tisztségviselőkre (polgármester, alpolgármester, képviselők),

b) a közszolgálatijogviszony alapján foglalkoztatott munkatársakra,

c) a közalkalmazotti jogviszony alapján foglalkoztatott munkatársakra,

d) a munkaviszony alapján foglalkoztatott munkatársakra,

e) a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyekre,

f) más szervezetek képviseletében a Hivatal munkahelyein tartózkodó személyekre.

I.2.2. Tárgyi hatály

Az IBSZ tárgyi hatálya kiterjed a Hivatal adataival és adatainak kezelésével összefüggésben használt bármilyen adatrögzítésre, tárolásra, feldolgozásra vagy továbbításra képes elektronikus információs rendszerre és ezek működési környezetére.

A tárgyi hatály kiterjed továbbá azezenrendszerek működéséhez alkalmazott szoftverekre, illetve az ezekkel rögzített, tárolt, feldolgozott vagy továbbított adatokra és információkra.

A tárgyi hatály kiterjed az önkormányzati ASP által nyújtott szakrendszerek felhasználó oldali komponenseireis.

I.2.3. Területi hatály

Az IBSZ területi hatálya kiterjed a Hivatal sárbogárdi székhelyére, illetve bizonyos feltételek mellett az elektronikus információs rendszerek szolgáltatóinak telephelyeire is.

I.2.4. Időbeni hatály

Jelen IBSZ a kiadás napján lép hatályba.

I.3. Az IBSZ felülvizsgálata

Az IBSZ eseti módosítására kerül sor, ha a benne szereplő adatok megváltoztak, illetve ha az IBSZ olyan kisebb mértékű kiegészítésekre szorul, amelyek nem érintik az aktuális biztonsági követelményeket.

Az IBSZ módosítására van szükség, ha a Hivatal elektronikus információs rendszereinek működésében vagy a Hivatal elektronikus információs rendszereinek működését meghatározó jogszabályi környezetben jelentős változások következnek be.

Az IBSZ-t legalább évente egy alkalommal felül kell vizsgálni.

Az IBSZ eseti módosításának, felülvizsgálatának kezdeményezése és a felülvizsgálat, valamint a módosítás elvégzése az elektronikus információs rendszerek biztonságáért felelős személy (továbbiakban: információbiztonsági felelős, rövidítve IBF) feladata. A módosítások engedélyezése és az újabb változat jóváhagyása a jegyző hatásköre.

I.3.1. Hatásköri és illetékességi szabályok

Az IBSZ belső használatú dokumentum: a Hivatal elektronikus információs rendszerének felhasználói, illetve egyéb érintettek (a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyek,más szervezetek képviseletében a Hivatal munkahelyein tartózkodó személyek) megismerhetik és birtokolhatják, de illetékteleneknek nem adhatják tovább.

I.4. Kapcsolódó dokumentumok

I.4.1. Jogszabályok

a) AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg)

b) AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről

c) 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről

d) 2012. évi I. törvény a munka törvénykönyvéről

e) 2012. évi C. törvény a Büntető Törvénykönyvről

f) 2013. évi V. törvény a Polgári Törvénykönyvről

g) 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Info tv.)

h) 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról

i) 1995. évi LXVI. törvény a közokiratokról, a közlevéltárakról, és a magánlevéltári anyag védelméről

j) 1999. évi LXXII. törvény a polgárok személyi adatainak kezelésével összefüggő egyes törvények módosításáról

k) 1999. évi LXXVI. törvény a szerzői jogról

l) 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól

m) 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (továbbiakban: Ibtv.)

n) 257/2016. (VIII. 31.) Korm. rendelet az önkormányzati ASP rendszerről

o) 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenység vizsgálat lefolytatásának szabályairól

p) 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

q) 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről (továbbiakban: technológiai vhr)

r) 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról (továbbiakban: képzési rendelet)

s)

t)

u)

v)

w)

x) 146/1993. (X. 26.) Korm. rendelet a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény végrehajtásáról

I.4.2. Kapcsolódó szabványok, ajánlások

a) MSZ ISO/IEC 27002:2017: Az információbiztonság irányítási gyakorlatának kézikönyve

b) MSZ ISO/IEC 27001:2014: Az információbiztonság irányítási rendszerei. Követelmények

c) NIST SpecialPublication 800-53 Revision 4 Security and PrivacyControlsforFederalInformation Systems and Organizations

d) NIST SpecialPublication 800-53A Revision 4 AssessingSecurity and PrivacyControlsinFederalInformation Systems and Organizations

e) A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások

f) Tájékoztatás az önkormányzati ASP rendszerhez csatlakozáshoz megvalósítandó informatikai biztonsági követelményekről 2.0 (2018.11.19)

I.4.3. Az IBSZ-hez kapcsolódó belső dokumentumok

a) Szervezeti és Működési Szabályzat
b) Iratkezelési Szabályzat
c) Selejtezési Szabályzat
d) Cselekvési terv a Sárbogárdi Polgármesteri Hivatal elektronikus információs rendszereinek elvárt biztonsági osztályainak, illetve a Hivatal elvárt biztonsági szintjének elérésére
e) Információbiztonsági kockázatelemzés

I.5. Az IBSZ általános követelményei

Az IBSZ és a jelen IBSZ *{7. számú melléklet – Felhasználói Informatikai Biztonsági Házirend}*melléklete (továbbiakban: FIBH)előírásainak alkalmazása, betartása, illetve betartatása, a *{I.2.1.Szervezeti-személyi hatály}* pontban megjelöltek számára kötelező.

Az információbiztonsági előírások betartása megvédi a Hivatalt és a *{I.2.1.Szervezeti-személyi hatály}* pontban kifejtett személyi hatály alá eső felhasználóit, ügyfeleit, partnereit, adataik ésinformációik jogosulatlan vagy véletlenszerű nyilvánosságra jutásától, módosításától, megrongálódásától, megsemmisülésétől.

A felhasználók részére a FIBH tartalmaz egy kivonatot, melynek megismeréséről és betartásáról írásban nyilatkozniuk kell.

A szabályok be nem tartása jogi, munkaügyi, illetve szerződésben meghatározott következményeket vonhat maga után. Az IBSZ és a FIBH el nem olvasása nem mentesít a felelősség alól.

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

A Hivatal elektronikus információs rendszereit csak a jelen IBSZ *{8. számú melléklet – Felhasználói Nyilatkozat}*mellékletében található nyilatkozat aláírása után lehet használatba venni.

II. A Hivatal és az elektronikus információs rendszereinekinformációbiztonsági követelményei

A Hivatalnak nincsen 2-es biztonsági osztálynál magasabb elektronikus információs rendszere.

Jelen IBSZ a 2-es biztonsági osztály követelményeit veszi figyelembe.

A Hivatalnak a jelen IBSZ kiadását követően 90 napon belül cselekvési tervet kell készítenie a következő biztonsági szintre, illetve a 2-es biztonsági osztályra vonatkozó követelmények teljesítése érdekében.

A biztonsági szint és a biztonsági osztályok különbségeire nézve irányadó, hogy addig is törekedni kell az IBSZ-ben foglalt követelmények lehető legnagyobb mértékben történő teljesítésére.

Az önkormányzati ASP rendszer használatára nézve irányadó a *{Tájékoztatás az önkormányzati ASP rendszerhez csatlakozáshoz megvalósítandó informatikai biztonsági követelményekről 2.0 (2018.11.19)}* elnevezésű dokumentum, mely tartalmazza a Hivatal oldalán teljesítendő biztonsági követelményeket. A nem megfelelősségek kezelésére cselekvési tervet kell készíteni határidő és felelős megjelölésével.

III. Adminisztratív védelmi intézkedések

Az ebben a fejezetben leírt adminisztratív védelmi intézkedéseket egységesen kell, valamenynyi elektronikus információs rendszerre vonatkozóan megvalósítani.

III.1. Kockázatelemzés

III.1.1. Kockázatelemzési és kockázatkezelési eljárásrend

Az információbiztonsági kockázatelemzés célja, hogy feltárja a Hivatal elektronikus információs rendszereire és az azokban kezelt adatokra ható fenyegető tényezőket, veszélyforrásokat (fenyegetettség elemzés), vizsgálja az elektronikus információs rendszer gyenge pontjait (sérülékenység vizsgálat), elemezze a veszélyforrások által a gyenge pontokon keresztül bekövetkező sikeres támadások bekövetkezési valószínűségét és az általuk okozott kár nagyságát (kockázatelemzés), valamint kezelje a Hivatal által el nem fogadható kockázatokat (kockázatkezelés).

A kockázatarányos védelem kialakításához rendszeres és tervszerű informatikai kockázatkezelésre van szükség. Annak érdekében, hogy a kockázatkezelési folyamata a Hivatal számára jól követhető, megismételhető és ellenőrizhető legyen, írásos kockázatkezelési módszertanra van szükség, mely mind a kockázatelemzés, mind a kockázatkezelés területén lefekteti az alapvető végrehajtási módszereket.

A Hivatal kockázatelemzési és kezelési eljárásrendjét az*(4. számú melléklet – Kockázatelemzési és kezelési módszertan)*tartalmazza.

III.1.2. Biztonsági osztályba sorolás

A Hivatalnak az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 7. § (3) bekezdésében meghatározottak figyelembevételével, 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 a 41/2015. (VII. 15.) BM rendelet 1. számú melléklete alapján biztonsági osztályba kell sorolnia az elektronikus információs rendszereit, illetve biztonsági szintbe kell sorolnia a szervezetét biztonsági szintbe kell sorolnia.

III.1.2.1. Biztonsági osztályba sorolás követelménye

A Hivatal elektronikus információs rendszereit a technológiai vhr által előírt módon, különkülön a bizalmasság, a sértetlenség és a rendelkezésre állás alapfenyegetésségek vonatkozásában egy 5 fokozatú skálán biztonsági osztályba kell sorolni.

A biztonsági osztályba sorolást az elektronikus információs rendszerben kezelt adat bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint az elektronikus információs rendszer sértetlenségének és rendelkezésre állásának sérülése esetén bekövetkező kár mértéke alapján kell elvégezni.

Az önkormányzati ASP rendszer szakrendszereit az ASP működtetője sorolja biztonsági osztályba. Az önkormányzat oldali szükséges védelmi intézkedéseket a csatlakozási szerződésben megfogalmazottak szerint kell végrehajtani.

A biztonsági osztályba sorolást mindig kockázatelemzéssel együtt kell végezni.

A biztonsági osztályba sorolást újra el kell végezni, hogy ha

a) jelentős változás következik be Hivatal szervezeti felépítésében;

b) az elektronikus információs rendszerben kezelt adatok bővülnek vagy az adatok köre változik;

c) változnak a hatályos információbiztonságra vonatkozó jogszabályok.

Ha nem történik lényegi változás, a biztonsági osztályba sorolástháromévente felül kell vizsgálni.

A biztonsági osztályba sorolást az IBF készíti elő az adatgazdákkal együttműködve és a jegyző hagyja jóvá.

A felhasználóknak az információ kezelése során tisztában kell lennie az adott információ védelmi igényével és ennek megfelelően kell kezelniük azt.

III.1.2.2. A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása

A Hivatal a technológiai vhr alapján elvégezte az elektronikus információs rendszerek biztonsági osztályba sorolását.

A biztonsági osztályba sorolás eredményét a jelen IBSZ*{2. számú melléklet – A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása}*melléklete tartalmazza.

III.1.3. Biztonsági szintbe sorolás

Az Ibtv. 9. §-ának (1) és (2) bekezdései alapján a kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet, valamint az elektronikus információs rendszer

a) fejlesztését végző,

b) üzemeltetését végző,

c) üzemeltetéséért felelős vagy

d) információbiztonságáért felelős

szervezeti egységeket az elektronikus információs rendszerek védelmére való felkészültségük alapján a szervezettől elvárt, eltérő biztonsági szintekbe kell sorolni jogszabályban meghatározott szempontok szerint.

III.1.3.1. A Hivatal biztonsági szintbe sorolása

Az Ibtv. 9. §-ának (4) bekezdése alapján a szervezet vagy szervezeti egységek biztonsági szintjének meghatározását az elektronikus információs rendszer felhasználásának módja határozza meg, jogszabályban meghatározott szempontok szerint.

A technológiai vhr alapján

a Hivatal elvárt biztonsági szintje 4-es,

mivel

a) szakfeladatait támogató elektronikus információs rendszert használ (3-as szint)

b) személyes adatok és adótitok formájában kritikus adatokat[1] kezel (3-as szint)

c) elektronikus információs rendszert üzemeltet (4-es szint)[2].

III.1.3.2. Szervezeti egységek biztonsági szintbe sorolása

A Hivatal hatályban lévő Szervezeti és Működési Szabályzata alapján a Hivatalban nem működnekaz elektronikus információs rendszer

a) fejlesztését végző,

b) üzemeltetését végző,

c) üzemeltetéséért felelős vagy

---

[1] *Ibtv. 1. §. 32.a kritikus adat: az Infotv. szerinti személyes adat, különleges adat vagy valamely jogszabállyal védett adat;*

[2] *2018. január 1-ével nem kerülnek kivezetésre azon hivatal által működtetett elektronikus információs rendszerek, melyek új megfelelőit az önkormányzati ASP rendszerben 2018. január 1-ével a Hivatal használatba vesz.*

d) információbiztonságáért felelős

szervezeti egységek, ezért azok biztonsági szintbe sorolása nem értelmezhető.

III.1.4. Kockázatelemzés

A kockázataránYos védelem kialakításához rendszeres és tervszerű informatikai kockázatelemzésre van szükség. A kockázatelemzést a jelen IBSZ *{4. számú melléklet – Kockázatelemzési és kezelési módszertan}*mellékletében leírt módszertan alapján az IBF végzi el.

A kockázatelemzést évente el kell végezni, melynek során felül kell vizsgálni az előző évi kockázatelemzés eredményét. A kockázatelemzést soron kívül el kell végezni, hogy ha

a) változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését),

b) olyan körülmények következnek be, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát.

A kockázatelemzés eredményét IBF-nek dokumentálnia kell, majd meg kell ismertetnie a jegyzővel.

A nem tolerálható kockázatok kezelésére intézkedési tervet kell készíteni, melynek tartalmaznia kell a kockázat kezelésére javasolt intézkedéseket, felelős, határidő és költségvonzat megjelölésével.

A kockázatkezelési tervet az IBF-nek kell előkészítenie és a jegyző hagyja jóvá.

A kockázatelemzéssel és kezeléssel kapcsolatos dokumentumok bizalmasnak minősülnek, ezért azok megismerésére az IBF, a rendszergazda, a jegyző, valamint a jegyző által írásban kijelölt személyek jogosultak.

III.2. Rendszer és szolgáltatás beszerzés – Beszerzési eljárásrend

A Hivatalnak a jelen fejezetben foglalt követelmények alapján kell az elektronikus információs rendszereire vonatkozó beszerzéseit elvégeznie.

III.2.1. Erőforrás igény felmérés

Az éves költségvetési tervezési folyamatban ki kell térni az elektronikus információs rendszerek biztonsági beruházásainak tervezésére, oly módon, hogy az a Hivatal költségvetésében elkülönítetten szerepeljen.

A biztonsági beruházások tervezését az informatikai biztonsági stratégiai célok, valamint a cselekvési tervekben megfogalmazottak alapján kell elkészíteni.

A tervezési dokumentumot az információbiztonsági felelős készíti el az informatikai vezetővel együttműködve.

A tervezési dokumentumban legalább a következőket kell feltüntetni:

a) beruházás megnevezése;

b) beruházás indoka, célja, kezelt kockázat;

c) költség-hasznon elemzés;

d) a beruházás elhagyásának következményei (jogi, információbiztonsági kockázat).

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

III.2.2. Beszerzések

III.2.2.1. Funkcionális biztonsági követelmények

A kockázatokkal arányos védelem kialakítása érdekében az IBF-et még a tervezés (ajánlatkérés) fázis elejétől kezdve be kell vonni a projektbe.

Az IBF bevonása a szerződést kezdeményező szervezeti egység vezetőjének feladata és felelőssége.

A tervezés fázisában az adatgazdának az IBF-el együttműködve biztonsági osztályba kell sorolni az alkalmazni kívánt EIR-t.

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

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

Az IBF-fel a tervezés fázisában el kell fogadtatni a funkcionális biztonsági követelményeket, anélkül az EIR fejlesztése nem kezdhető meg.

III.2.2.2. Garanciális biztonsági követelmények

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

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

III.2.2.3. Biztonsággal kapcsolatos dokumentációs követelmények

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

a) a szállítandó termék/fejlesztés biztonsági intézkedéseinek funkcionális biztonsági leírása;

b) adminisztrátori dokumentáció;

c) felhasználói dokumentáció.

Dokumentálásformai követelmények
Az EIR dokumentálása során az alábbi pontokban részletezett formai elemeket minden dokumentumban értelemszerűen kell szerepeltetni.

a) Dokumentum adatlap:
    a. a Dokumentum címe,
    b. tárgya,
    c. fájl neve és verziója,
    d. Dokumentum típusa,
    e. Dokumentum verziószáma,
    f. Dokumentum státusza,
    g. Dátum,
    h. Készítő, Ellenőr,
    i. Verziószám,
    j. Státusz,
    k. Minősítés.
b) lapszámozás,
c) tartalomjegyzék,
d) tárgymutató.

Dokumentumok rendelkezésre állása

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

III.2.2.4. A biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelmények

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

A biztonsággal kapcsolatos dokumentumokat a következő szerepkörök ismerhetik meg:

a) fejlesztő;
b) rendszergazda;
c) IBF;
d) jegyző.

III.2.2.5. Fejlesztési szerződések biztonsági követelményei

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

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

Elő kell írni a jelen IBSZ *{III.2.3Az elektronikus információs rendszerre vonatkozó dokumentáció}* fejezetében megkövetelt biztonsági dokumentációk elkészítését.

A szerződésben meg kell követelni, hogy a fejlesztő, szállító hozza létre és bocsássa rendelkezésére jelen IBSZ *{III.2.2.1Funkcionális biztonsági követelmények}*fejezetében megkövetelt, az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak a leírását.

Fejlesztett komponensek esetében a szerződésben rögzíteni kell, hogy a leszállított szoftver megfelelően biztonságos környezetben, auditálható körülmények között készült, így nem tartalmaz kártékony kódot. Amennyiben mégis tartalmazna, és ebből adódóan a Hivatalnak bármilyen kára keletkezne, akkor azért a Szállító felelősséggel tartozik.

III.2.2.6. Rendszerkövetés (támogatás)

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

a) azinfokommunikációs rendszerben felmerülő hibák javítása,

b) aHivatal fejlesztési igényeinek ellátása,

c) azinfokommunikációs rendszer futtató környezetének (operációs rendszer, adatbázis rendszerek) frissítése.

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

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

III.2.3. Az elektronikus információs rendszerre vonatkozó dokumentáció

A szállítónak következő dokumentációkat kell készítenie a fejlesztés során:

III.2.3.1. Adminisztrátoridokumentáció

Az adminisztrátori dokumentációnak tartalmaznia kell:

a) a technikai környezet ismertetését,

b) a kapacitástervezési leírást,

c) az alkalmazott portok, szolgáltatások, és protokollok részletes ismertetése,

d) a kommunikációs környezet ismertetését,

e) a szerepköröket és hozzájuk tartozó feladatok ismertetését,

f) a jogosultsági rendszer részletes ismertetését,

g) a feldolgozások részletes ismertetését üzemeltetési szempontból,

h) a mentés, archiválás, monitorozás ismertetését,

i) az időszaki teendők ismertetését,

j) a hibaüzenetek, hibaelhárítással kapcsolatos feladatok ismertetését,

k) rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,

l) a biztonsági funkciók hatékony alkalmazását és fenntartását,

m) a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket.

III.2.3.2. Felhasználói dokumentáció

A felhasználói dokumentáció tartalmazza:

a) a funkciók felhasználói leírása képekkel illusztrálva,

b) a kezelési felületek, menürendszer ismertetését,

c) az interfész leírásokat,

d) a funkcióleírásokat, a funkciójegyzéket,

e) a kapcsolódó rendszerelemek pontos hivatkozását,

f) az ellenőrzési és hibakezelési eljárásokat / hibajegyzéket,

g) logikai kontrollok ismertetése.

III.2.4. A védelem szempontjainak érvényesítése a beszerzés során

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

A sikeres átadás-átvétel feltétele

a) a jelen IBSZ-ben meghatározott dokumentációk Hivatal általi elfogadása,

b) a funkcionális biztonsági követelmények IBF általi, tesztrendszerben történő ellenőrzése.

III.2.5. Külső elektronikus információs rendszerek szolgáltatásai

Külső elektronikus információs rendszerek igénybevétele esetén a jelen IBSZ *{III.5.16. Harmadik felekkel kapcsolatos előírások}* pontjában foglaltakon kívül szerződésben kell rögzíteni az érintett EIR biztonsági osztályát, a szolgáltató és a Hivatal által külön-külön, illetve együttesen teljesítendő, az érintett EIR biztonsági osztályából fakadó adminisztratív, fizikai és logikai védelmi intézkedéseket.

A szerződésben ki kell térni a Hivatal felhasználóinak feladataira az igénybe vett külső elektronikus információs rendszerek szolgáltatásával kapcsolatban.

A szerződésben ki kell kötni a jogot arra, hogy a Hivatal az IBF útján auditálhassa a szolgáltatónál kialakított, szerződésben meghatározott védelmi intézkedéseket.

III.3. Elektronikus információs rendszerek ügymenet folytonosságának tervezése

A Hivatal elektronikus információs rendszereinek folyamatos működésének biztosítása érdekében, valamint a katasztrófa-helyzetek bekövetkezte során a jelen fejezetben foglaltak szerint kell eljárni.

III.3.1. Ügymenet folytonossági terv informatikai erőforrás kiesésekre

Az IBF-nek az érintett területek bevonásával ki kell dolgoznia és jóvá kell hagyatnia az elektronikus információs rendszerekre vonatkozó ügymenet-folytonossági tervet (továbbiakban: ÜFT).

A folyamatos működés tervezésére vonatkozó tevékenységeket össze kell hangolni a biztonsági események és vészhelyzeti/katasztrófa helyzetek kezelésével.

A tervezés során meg kell határozni a Hivatal által biztosítandó szolgáltatásokat és alapfunkciókat, valamint az ezekhez kapcsolódó és a Hivatal részéről elvárt vészhelyzeti követelményeket.

Meg kell határozni az elektronikus információs rendszer kiesése esetére a helyreállítási feladatokat, a helyreállítási prioritásokat és azok mértékét.

Ki kell jelölni a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket.

Az ügymenet-folytonosságot úgy kell kialakítani, hogy az biztosítsa a Hivatal által előzetesen definiált alapszolgáltatások fenntartását, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is.

Ki kell dolgozni a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

III.3.1.1. Az ÜFT felülvizsgálata

Az Ügymenet-folytonossági tervet évente felül kell vizsgálni.

Az Ügymenet-folytonossági tervet soron kívül felül kell vizsgálni

a) az elektronikus információs rendszer vagy a működtetési környezet jelentős változása,

b) az ügymenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémák esetén.

Az Ügymenet-folytonossági terv változásairól képzés formájában tájékoztatni kell az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket.

III.3.1.2. Az ÜFT kezelése

Az Ügymenet-folytonossági terv jóváhagyott példányának páncélszekrényben történő őrzéséről a rendszergazda gondoskodik.

Az Ügymenet-folytonossági terv bizalmas dokumentumnak tekinthető, ezért csak az abban megjelölt személyek számára hozzáférhető, illetékteleneknek nem adhatják tovább.

III.3.2. Kritikus rendszerelemek meghatározása

Az ÜFT-ben meg kell határozni a Hivatal elektronikus információs rendszereinek alapfunkcióit támogató kritikus rendszerelemeket.

III.3.3. Folyamatos működésre felkészítő képzés

Évente folyamatos működésre felkészítő képzést kell tartani, melynek során képezni kell a felhasználókat az ÜFT-ben foglaltakról. A képzést az IBF-nek kell megtartania. A képzésen a részvétel kötelező.

III.3.4. Infokommunikációs szolgáltatások

Tartalék internet vonalat kell biztosítani az önkormányzati ASP rendszer folyamatos elérése érdekében. Amennyiben az elsődleges vonal nem áll rendelkezésre, úgy a rendszergazdának gondoskodnia kell a tartalék vonal beüzemeléséről. Olyan tartalék szolgáltatást kell biztosítani, mely az éles vonaltól elkülönülő vonalon biztosítja az internetelérést.

III.3.5. Szolgáltatás-prioritási rendelkezések

Az internet szolgáltatókkal kötött szerződéseknek tartalmazniuk kell az elvárt

a) szolgáltatási időszakot,

b) szolgáltatási szintet,

c) helyreállítási időket.

III.3.6. Az elektronikus információs rendszer mentései

Az elektronikus információs rendszerek és az azokban kezelt adatok az adatgazdák és a jogszabályok által elvárt, megfelelő rendelkezésre állásának biztosítása érdekében mentési eljárás-rendet kell kidolgozni a következők figyelembevételével:

Rendszeres mentéseket kell készíteni a legalább 2-es biztonsági osztályba sorolt elektronikus információs rendszerekről és az azokban kezelt adatokról. A mentések során a következő adat-fajták mentését kell biztosítani:

a) felhasználói szintű adatok (ügyviteli adatok)

b) rendszerszintű információk

c) naplóinformációk

d) a rendszerrel kapcsolatos dokumentációk.

Biztosítani kell a háttérkörnyezetet, annak érdekében, hogy a lényeges adatok és szoftverek esetleges adathordozó hiba, az elektronikus információs rendszerek összeomlása vagy megsemmisülése esetén visszaállíthatóak legyenek.

A mentési eljárásrendet úgy kell kialakítani, hogy az egyrészt megfeleljen az üzembiztonsági elvárásoknak, másrészt minél biztonságosabb védelmet nyújtson az esetlegesen előforduló hibák ellen.

Az EIR-ek fizikai védelme érdekében, gondoskodni kell arról, hogy a telepítő állományok ne károsodjanak, ezért az eredeti példányukról biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag elkülönítve, biztonságos helyen elzárva kell tárolni. Az eredeti hordozókról készített másolatokat kell a napi tevékenység során használni. Az olvasási biztonság fenntartása érdekében az eredeti adathordozókról rendszeres időközönként frissítő mentést kell készíteni.

Az ügymenet folytonosság fenntartása érdekében a mentéseket tartalmazó adathordozókat szerverhelyiségtől elkülönítve, páncélszekrényben kell tárolni.

III.3.7.

III.3.8.

d)

e)

f)

III.3.9. Az elektronikus információs rendszer helyreállítása és újraindítása

Az ügymenet-folytonosság tervezése során ki kell dolgozni az elektronikus információs rendszerek helyreállítási terveit, melyek a katasztrófahelyzetek kezelésére vonatkozóan a következőket kell tartalmaznia:

a) katasztrófát követő helyreállítandó célállapot;

b) a katasztrófa események definíciója;

c) a katasztrófa tényét eldöntő, a folyamat inicializálásáért felelős személyt, személyeket;

d) a helyreállítási terv hatóköre;

e) a megelőzés érdekében végzett tevékenységeket;

f) felkészülés a katasztrófa elhárítására;

g) katasztrófa esetén végrehajtandó tevékenységek;

h) elektronikus információs rendszerek vészleállításának és újraindításának folyamatát leíró dokumentumot;

i) a helyreállítási terv tesztelése, karbantartása.

Az elektronikus információs rendszerekre vonatkozóhelyreállítási tervek elkészítéséről, teszteléséről és folyamatos karbantartásáról a rendszergazda gondoskodik. A terv készítési tevékenységeket az IBF-nek információbiztonsági szempontból támogatnia és rendszeresen ellenőriznie kell.

A terveket minden olyan esetben aktualizálni kell, amikor jelentősen megváltozik az infokommunikációs infrastruktúra (pl.: új elektronikus információs rendszer bevezetése, új nagyteljesítményű hardverelemek változása).

A rendszergazdának - mindezeken túl - gondoskodnia kell az elektronikus információs rendszer helyreállításához szükséges mentések meglétéről, elérhetőségéről.

III.4. Biztonsági események kezelése

A Hivatal az elektronikus információs rendszerek biztonsági eseményeinek kezelésekor a következők szerint ját el:

III.4.1. Jelentés a biztonsági eseményekről

A biztonságot érintő eseményekről, a felfedezésük után, haladéktalanul tájékoztatni kell a felfedező közvetlen munkahelyi vezetőjét és a rendszergazdát.

A biztonságot érintő eseményekről szóló jelentések elkészítésére a jelen IBSZ *{3. számú melléklet –Biztonsági események jelentése}* mellékletében található űrlapot kell használni.

Amennyiben a rendszergazda úgy ítéli meg, hogy a bejelentett probléma biztonsági eseményre utal, úgy jelentenie kell az IBF-nek.

Biztonsági esemény esetén az IBF látja el a biztonságiesemény-kezelési megbízott feladatait.

Az IBF-nek a saját Ügyfélkapuján keresztül haladéktalanul jelentenie kell a biztonsági eseményt a Kormányzati Eseménykezelő Központ (továbbiakban: GovCert) részére. Amennyiben a biztonsági esemény érinti az önkormányzati ASP rendszert, úgy a biztonsági eseményt az önkormányzati ASP rendszer működtetőjének is jelenteni kell.

Az IBF-nek csatolnia kell a bejelentéshez a biztonsági eseményhez kapcsolódó valamennyi bizonyítékot.

Az IBF-nek és a Hivatalnak együtt kell működnie a GovCert-tel a biztonsági esemény kezelésében és a GovCert által javasolt intézkedéseket végre kell hajtania.

Az IBF-nek kivizsgálást kell kezdeményeznie a beérkezett jelentés alapján és javaslatot kell tennie a jegyző részére az esemény előfordulási esélyének csökkentése, illetve az okozott kár mérséklése érdekében.

Amennyiben a biztonsági esemény igazoltan a szabályok megsértéséből adódik, úgy az IBF-nek javaslatot kell tennie a jegyző részére a fegyelmi eljárások lefolytatása érdekében.

III.4.2. Jelentés a biztonság gyenge oldalairól

A rendszergazda köteles azonnal jelenteni az IBF-nek, amennyiben munkája során biztonsági veszélyeket, vagy az elektronikus információs rendszerben valamilyen gyenge pontot fedeztek fel.

A biztonságot érintő gyenge pontokról szóló jelentések elkészítésére a jelen IBSZ *{3. számú melléklet –Biztonsági események jelentése}* mellékletében található űrlapot kell használni.

III.4.3. Jelentés a szoftverzavarokról

Az elektronikus információs rendszerekben tapasztalt szoftverzavarokat jelenteni kell a rendszergazdának. Szoftverzavarok esetén legalább a következő feladatokat végre kell hajtani:

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

b) be kell szüntetni az adott számítógép használatát.

A felhasználóknak tilos a hibásnak feltételezett szoftvert eltávolítaniuk az elektronikus információs rendszerből. A hibaelhárítást és helyreállítást a rendszergazda hajthatja végre.

Abban az esetben, hogy ha feltételezhető az információbiztonság sérülése, akkor az eseményt a rendszergazda jelenti az IBF-nek, aki a jelen *IBSZ{III.4. Biztonsági események kezelése}* pontjának megfelelően kivizsgálja az eseményt.

III.4.4. Tanulságok levonása a biztonsági eseményekből

Az IBF-nek a bejelentett biztonsági eseményekről, veszélyes helyzetekről, illetve a működési zavarokról, azok előfordulási gyakoriságáról, és kezelésükre tett intézkedések eredményéről háromhavonta jelentést kell készítenie jegyző számára.

Az IBF feladata a biztonsági események kezelése során nyert tapasztalatok felhasználásával a meglévő biztonsági rendszer – így a szabályozó elemek és technikai megoldások felülvizsgálata és szükség esetén tökéletesítése.

Szükség esetén (nagy kár, vagy várható jelentős potenciális kár, illetve gyorsan szaporodó előfordulás esetén) az egyes eseményeket, illetve esemény típusokat az IBF-nek soron kívül jelentenie kell a jegyző részére.

III.5. Emberi tényezőket figyelembe vevő – személy – biztonság

III.5.1. Információbiztonsági tevékenységek

A Hivatalban a következő információbiztonsági tevékenységeket kell ellátni:

a) informatikai kockázatelemzés és kezelés,

b) elektronikus információs rendszerek biztonsági felügyelete,

c) új elektronikus információs rendszerek információbiztonsági véleményezése és elfogadása,

d) szervezetek közötti információbiztonsági együttműködés,

e) az információbiztonság független felülvizsgálata.

III.5.2. Az információbiztonsági felelősségi rend meghatározása

Az információbiztonság megteremtése és fenntartása olyan alapvető felelősség, amely szerint nem tartozhat egyszemélyi felelősségi és hatáskörbe az elektronikus információs rendszerek tervezése, fejlesztése, üzemeltetése és felügyelete.

Az információbiztonság megvalósítását, fenntartását és ellenőrzését a Hivatal a feladatok és felelősség szempontjából egymástól elhatárolt szervezeti keretek között valósítja meg.

A Hivatal információbiztonsági feladatainak ellátása során a következő szerepkörök érintettek:

a) a jegyző,

b) az információbiztonsági felelős,

c) a rendszergazda,

d) az adatgazdák,

e) a szervezeti egység vezetője,

f) önkormányzati ASP adminisztrátor,

g) önkormányzat szakrendszeri adminisztrátor,

h) a felhasználók.

III.5.3. A jegyző

A jegyző az Ibtv. alapján gondoskodik az elektronikus információs rendszerek védelméről a következők szerint:

III.5.3.1. A jegyző feladatai

A jegyző

a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,

b) biztosítja a Hivatalra irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,

c) az elektronikus információs rendszer biztonsági osztálya és a Hivatal biztonsági szintje alapján előírt követelményeknek megfelelően az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg, aki azonos lehet a minősített adat védelméről szóló 2009. évi CLV. törvény szerinti biztonsági vezetővel,

d) meghatározza a Hivatal elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az információbiztonsági szabályzatot,

e) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a Hivatal munkatársai információbiztonsági ismereteinek szinten tartásáról,

f) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a Hivatal 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 az e törvényben foglaltak szerződéses kötelemként teljesüljenek,

j) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy a jelen IBSZ-ben 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.

A jegyző köteles együttműködni a jogszabályban meghatározott hatóságokkal. Ennek során

a) az IBF személyéről tájékoztatást nyújt,

b) a Hivatal információbiztonsági szabályzatát tájékoztatás céljából megküldi,

c) megküldi a Hivatal elvárt biztonsági szintjének és az elektronikus információs rendszereinek elvárt biztonsági osztályának elérésére készített cselekvési tervet,

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

III.5.3.2. A jegyző felelőssége

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

III.5.4. Az IBF

A jegyző által megbízott IBF-nek a következők a feladatai, felelősségei és felelősségei:

III.5.4.1. Az IBF feladatai

Az IBFa Hivatal információbiztonsági irányítási rendszerének működtetése és ellenőrzésével kapcsolatos feladatai a következők:

a) gondoskodik a Hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,

b) elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,

c) előkészíti a Hivatal elektronikus információs rendszereire vonatkozó információbiztonsági politikát, információbiztonsági stratégiát és azinformációbiztonsági szabályzatot,

d) intézkedési tervet készít az elektronikus információbiztonsági stratégia megvalósításához, ebben mérföldköveket határoz meg, azokat meghatározott időközönként felülvizsgálja, valamint karbantartja az intézkedési tervet,

e) előkészíti a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását és a Hivatal biztonsági szintbe történő besorolását,

f) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a Hivatal e tárgykört érintő szabályzatait és szerződéseit,

g) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.

Az IBF biztosítja a jogszabályokban meghatározott követelmények teljesülését

a) a Hivatal valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők,

b) ha a Hivatal adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők,

az IBSZ hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

III.5.4.2. Az IBF jogai

Az IBF a Hivatal információbiztonságának fenntartása érdekében, illetve információbiztonsági incidens esetében jogosult:

a) külön engedély nélkül a Hivatal bármely helyiségébe belépni, amennyiben ott az információbiztonságot érintő munkavégzés folyik,

b) bármelyik számítógép, adathordozó vagy számítógépes lista tartalmába betekinteni, függetlenül annak minősítésétől (a vonatkozó jogszabályok betartásával), amennyiben az adott ügyben, illetve témában vizsgálat folyik,

c) minden értekezleten részt venni, észrevételeit és javaslatait megtenni, amelynek számítástechnikai, illetve információbiztonsági vonatkozása van, és ez az értekezlet összehívásakor ismert.

III.5.4.3. Az IBF felelőssége

Az IBF felelős a Hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról.

III.5.5. A rendszergazda

A rendszergazda információbiztonsággal kapcsolatos feladata és kötelessége a következő:

III.5.5.1. A rendszergazda feladata

A rendszergazda feladata, hogy

a) az IBF-fel közösen meghatározza az információbiztonsági követelmények megvalósításához szükséges informatikai eszközöket;

b) kidolgozza a hatáskörébe tartozó üzemeltetési eljárásokat,

c) biztosítja a rendszerfelügyeletet;

d) üzemelteti a rá bízott elektronikus információs rendszereket;

e) vezeti az IBSZ-ben előírt nyilvántartásokat.

f) gondoskodik a jelen IBSZ *{2. számú melléklet – A Hivatal elektronikus információs rendszereinek biztonsági osztályba* sorolása*}*mellékletében felsorolt elektronikus információs rendszerek naprakész nyilvántartásáról.

III.5.5.2. A rendszergazda felelőssége

A rendszergazda felelőssége az általa a jelen IBSZ *{2. számú melléklet – A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása}*mellékletében felsorolt elektronikus információs rendszerek jelen IBSZ-ben foglaltak szerinti biztonságos üzemeltetése.

III.5.6. Az adatgazda

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

Az adatgazdák a jelen IBSZ *{2. számú melléklet – A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása}*mellékletében kerültek kijelölésre.

III.5.6.1. Az adatgazda feladatai

Az adatgazda információbiztonsággal kapcsolatos feladatai a következők:

a) az IBF-el közreműködve biztonsági osztályba sorolja a hozzá rendelt elektronikus információs rendszereket;

b) meghatározza az adatokhoz / tevékenységekhez hozzáférőket, a szükséges-elégséges hozzáférési elv alapján, azaz mindenki csak annyi jogot kapjon, amennyi a munkája elvégzéséhez feltétlenül szükséges;

c) Az ügymenet folytonosság tervezése során meghatározza az érintett EIR maximális kiesési idejét és az EIR-ben elfogadható maximális adatvesztés mértékét.

III.5.6.2. Az adatgazda felelőssége

Az adatgazda felelős a hatáskörébe tartozó elektronikus információs rendszerek hozzáférési jogosultságainak - a lehetőségek szerint - a „szükséges, minimális jogosultságok" elve alapján történő engedélyezéséért.

III.5.7. A szervezeti egység vezetője

A szervezeti egység vezetőjének feladata és felelőssége, hogy az általa irányított szervezeti egység munkatársai megismerjék és betartsák a rájuk vonatkozó információbiztonsági előírásokat.

III.5.8. Önkormányzati ASP adminisztrátor

Az önkormányzati ASP adminisztrátor feladata a bérlő fiók, tenant (önkormányzat, intézmény, nemzetiségi önkormányzat) szintű felhasználó kezelés, azaz

a) az adott tenant felhasználóinak felvétele és szakrendszeri szerepkör(ök)höz rendelése, annak adminisztrációja és karbantartása;

b) intézményi kapcsolattartóként az adott tenant felhasználók tanúsítvány igénylésének adminisztrációja és karbantartása, illetve a tanúsítványokat hordozó tokenek csoportos átvétele és felhasználók közötti kiosztása.

III.5.9. Önkormányzat szakrendszeri adminisztrátor

Az önkormányzat szakrendszeri adminisztrátor(ok) feladata a szakrendszer szintű jogosultságkezelés, azaz a szolgáltatást igénybe vevő felhasználók számára a szakrendszeri jogosultságok beállítása, adminisztrációja és karbantartása.

III.5.10. A felhasználó

A Hivatal felhasználóinak az elektronikus információs rendszerek biztonságával kapcsolatban a következők a jogai, a kötelességei és a felelőssége:

III.5.10.1. A felhasználó jogai

A felhasználó jogosult:

a) a számára biztosított infokommunikációs eszközök, szoftverek üzemszerű használatára,

b) a beállított jogosultságának megfelelően, a munkájához szükséges adatállományok elérésére,

c) információbiztonsági képzésre,

d) a működtetéshez szükséges támogatás igénylésére, a munkavégzéshez szükséges általa nem ismert szoftverek használatához támogatást kérni,

e) meghibásodás, üzemzavar esetén az elhárítás igénylésére.

III.5.10.2. A felhasználó kötelessége

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

Valamennyi felhasználó köteles azonnal értesíteni felettesét a következő eseményekről, körülményekről:

a) az informatikához kapcsolódó tevékenység fennakadása, megszakadása,

b) ha olyan adatokhoz fér hozzá, melynek kezelésében nem illetékes,

c) információbiztonsági esemény.

Az munkahelyi vezetőnek jeleznie kell a tapasztaltakat a rendszergazda részére, aki információbiztonsági incidens esetén értesíti az IBF-et.

Minden felhasználónak bizalmasan kell kezelnie valamennyi felhasználói azonosítót, jelszót, eToken-t, kulcsot, vagy bárminemű egyéb, a Hivatal erőforrásaihoz hozzáférést biztosító eszközt.

A személyi azonosító kódokat, jelszavakat szigorúan titokban kell tartani. Még a közeli munkakapcsolatban álló, egymást jól ismerő kollégák sem közölhetik ezeket egymással. Az információbiztonsági hiányosságok megelőzése céljából a felhasználók kötelesek rámutatni az információbiztonsági szint romlására, illetve annak lehetőségére, és a tapasztalatokat a további problémák elkerülésében felhasználni.

Az információbiztonságot veszélyeztető események kivizsgálására irányuló felülvizsgálatokban a felhasználó köteles együttműködni a kivizsgálókkal.

A felhasználó számára büntetőjogi, illetve munkajogi felelősségre vonás terhe mellett tilos illetéktelenül más felhasználó jogosultságainak használata, a hálózat monitorozása, felderítése, jelszavak kipróbálása, illetve ezek kísérlete is.

III.5.10.3. A felhasználó felelőssége

A felhasználó felelősséggel tartozik:

a) a jelen IBSZ *{7. számú melléklet – Felhasználói Informatikai Biztonsági Házirend}* mellékletének megismeréséért és az abban foglalt szabályok betartásáért,

b) az önkormányzati ASP központ működtetője által közzétett felhasználói biztonsági követelmények betartásáért,

c) a birtokában lévő, vagy tudomására jutott információk bizalmasságának megfelelő kezeléséért,

d) a személyre szóló és védett területre belépést biztosító kártyájának/kártyáinak védelméért és át nem ruházásáért,

e) az elektronikus információs rendszerben végzett műveletekért,

f) a Hivatalelektronikus információs rendszereinek szakszerű kezeléséért és

f) a személyi használatra átvett eszközök megfelelő fizikai védelméért.

III.5.11. A munkaköri felelősség és az alkalmazás feltételei

A munkaköri leírásokban meg kell határozni az általános és az adott munkakörhöz tartozó információbiztonsági feladatokat és felelősségeket.

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

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

A Hivatal elektronikus információs rendszereit csak a jelen IBSZ *{8. számú melléklet – Felhasználói Nyilatkozat}* mellékletében található nyilatkozat és az ASP titoktartási nyilatkozat aláírása után lehet használatba venni.

III.5.12. Munkakörök, feladatok biztonsági szempontú besorolása

A Hivatal az információbiztonsági szempontból alap és kiemelt munkaköröket állapított meg.

A Hivatalban nincsenek nemzetbiztonsági ellenőrzés alá eső munkakörök és feladatok.

III.5.12.1. Alap biztonsági osztály

Az alap biztonsági osztályba a következő munkakörök kerültek besorolásra:

a) Adatgazda,
b) Önkormányzati ASP adminisztrátor,
c) Önkormányzati szakrendszeri adminisztrátor,
d) Felhasználó.

Az alap munkakör betöltésének követelményei:

a) Erkölcsi bizonyítvány,
b) Szakirányú végzettség,
c) Informatikai alapismeretek,
d) Önkormányzati szakrendszerek használatában szerzett jártasság.

III.5.12.2. Kiemelt biztonsági osztály

A kiemelt biztonsági osztályba a következő munkakörök tartoznak:

a) Jegyző,
b) Helyi rendszergazda,
c) Információbiztonsági felelős.

A kiemelt biztonsági osztályba a következő munkakörök kerültek besorolásra:

a) Erkölcsi bizonyítvány,
b) Szakirányú végzettség,
c) 2 év szakmai tapasztalat,
d) Alapfokú angol nyelvtudás.

III.5.13. A személyek ellenőrzése

A Hivatal személyügyekért felelős vezetőjének a feladata, hogy az elektronikus információs rendszerekhez való hozzáférési jogosultság megadása előtt ellenőrizze, hogy az érintett személy a *{III.5.12. Munkakörök, feladatok biztonsági szempontú besorolása}*fejezetben meghatározott feltételeknek megfelel-e. A vizsgálat magában foglalja az alábbiakat:

a) referenciák ellenőrzése,

b) a felvételre jelentkező életrajzának ellenőrzése a teljességre és pontosságra vonatkozóan,

c) a legmagasabb iskolai végzettség (szakképzettség) ellenőrzése,

d) nyelvtudást igazoló okiratok ellenőrzése,

e) hatóság által kibocsátott azonosító irat ellenőrzése,

f) erkölcsi bizonyítvány ellenőrzése.

Külső szerződő felek esetében az szerződést kezdeményező feladata a szerződésben előírni a személybiztonsági feltételeket.

III.5.14. Eljárás jogviszony megszűnésekor

A jogviszony megszüntetésekor a következő feladatok végrehajtása szükséges:

a) Jogosultságok dokumentált formában történő megszüntetése.

b) A felhasználó elektronikusan tárolt információit, e-mailjeit és egyéb általa létrehozott adatot menteni, archiválni kell az általa használt informatikai eszközről, szerver tárhelyről, illetve bármely egyéb adathordozóról.

c) Az így archivált adatokat a törvényi előírásoknak megfelelően tárolni kell, illetve 1 év után törölni kell a rendszerből.

A fentiek végrehajtását a jogviszony megszűnésével egy időben, kockázatot jelentő esetekben a jogviszony megszűnését megelőzőn kell végrehajtani. A végrehajtás elrendeléséért a jegyző, a végrehajtásért a rendszergazda a felelős.

Kiemelt biztonsági osztályba tartozó munkakörök esetén a jogviszony megszüntetését információbiztonsági szempontból az IBF koordinálja.

III.5.14.1. Vagyontárgyak visszaszolgáltatása

Valamennyi felhasználónak, a szerződőknek és a felhasználó harmadik félnek vissza kell szolgáltatnia a Hivatal valamennyi használatra átvett vagyontárgyát, amikor alkalmazásuk, szerződésük, illetve megállapodásuk lejár, illetve megszűnik.

A rendszergazdának az eszköz leadásakor ellenőriznie kell, hogy a felhasználó az átvételi elismervényben rögzített hardver-, szoftver specifikációval adja-e vissza a munkaállomást.

III.5.14.2. Hozzáférési jogok megszüntetése

Valamennyi alkalmazottnak, a szerződőknek és a felhasználó harmadik feleknek információkhoz és információ-feldolgozó eszközökhöz való hozzáférési jogosultságát meg kell szüntetni, amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár.

A fentiektől eltérni a jegyző írásos engedélyével lehetséges.

A feladatok végrehajtásáért a rendszergazda a felelős.

III.5.14.3. Információbiztonsági kötelmek a jogviszony megszűnése után

A személyügyi referensnek a jelen IBSZ *{9. számú melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén}*mellékletében foglaltak szerint tájékoztatnia kell a dolgozót arról, hogy

a) legkésőbb a jogviszony megszűnése napján köteles a Hivatal elektronikus információs rendszerével kapcsolatos valamennyi eszközt hiánytalanul, sértetlenül munkáltatója részére visszaszolgáltatni;

b) a Hivatalban működő elektronikus információs rendszereket a Hivatal kizárólag hivatali munkavégzés céljából biztosítja a munkatársak részére, az elektronikus információs rendszerekben keletkező és ott tárolt, kezelt adatok, információk vonatkozásában a Hivatal fenntartja magának a tulajdonjogot;

c) a Hivatalnak továbbra is hozzáférési lehetősége van az általa korábban használt, kezelt elektronikus információs rendszerekhez és az azokban kezelt adatokhoz;

d) a titoktartási kötelezettsége a jogviszonya megszűnését követően is fennáll.

A fentiek megsértése jogi következményeket von maga után.

III.5.15. Áthelyezések, átirányítások és kirendelések kezelése

Az áthelyezés során, szükség esetén el kell végezni az érintett munkatárs ellenőrzését a jelen IBSZ *{III.5.13.A személyek ellenőrzése}*pontjában foglaltak alapján.

Az érintett munkatárs részére az elektronikus információs rendszerhez történő logikai és fizikai hozzáférések engedélyezését a jelen IBSZ *{V.7.3Hozzáférési jogok igénylésének eljárásrendje}* pontjában foglaltaknak megfelelően kell elvégezni.

Szükség esetén el kell végezni az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését.

A jogviszony megváltozásáról a jegyző értesíti a munkatárs régi, valamint új vezetőjét.

III.5.16. Harmadik felekkel kapcsolatos előírások

Harmadik fél csak egyedi esetben, meghatározott időre és meghatározott feladat ellátásához látható el jogosultsággal, amit szerződésben kell dokumentálni. A hozzáférést az elektronikus információs rendszer adatgazdájának kell engedélyezni.

A Hivatal és szerződéses partnerei szerződésben rögzített, a jelen IBSZ-nek megfelelő biztonsági intézkedéseket kötelesek foganatosítani annak érdekében, hogy a kicserélt (átadott/átvett) adatok és dokumentumok véletlen vagy szándékos kompromittálódását megakadályozzák.

A harmadik félnek a Hivatal elektronikus információs rendszereihez történő hozzáférése esetében – figyelembe véve a szükséges hozzáférési típusokat, az információ értékét, a harmadik fél által alkalmazott biztosítékokat, valamint a hozzáférés mélységét – törekedni kell a kockázatok minimalizálására.

Azokban az esetekben, amelyekben az információ feldolgozása vagy kezelése kiszervezéssel történik, a harmadik féllel kötött szerződésnek a betartandó biztonsági követelményeket is tartalmaznia kell.

Harmadik fél hozzáférése a Hivatal adataihoz és információihoz, a munkájához elengedhetetlenül szükséges minimum szintre kell korlátozni. A hozzáférések feltételeit szerződésben kell

részletezni. A szerződés csak a Hivatal jelen IBSZ-ével összhangban lévő követelményeket tartalmazhat.

A szerződésnek tartalmaznia kell továbbá a bizalmasságra, a szellemi tulajdonjogokra, a szerzői jogok átruházására és minden közösen végzett munkálatok védelmére vonatkozó nem nyilvános garanciákat is.

A szerződésben elő kell írni, hogy a Hivatal információs vagyonelemei a szerződés lejártát követően kerüljenek vissza a Hivatal birtokába, a szerződött félnél – valamint annak partnereinél, alvállalkozóinál – pedig kerüljenek megsemmisítésre.

A szerződéses partnernek a Hivatallal egyeztetnie kell a számára nyújtott szolgáltatásokkal kapcsolatos minden részdöntést.

A szerződésben a Hivatal számára jogot kell biztosítani arra, hogy a már kölcsönösen elfogadott szerződéses felelősséget felülvizsgálja, szükség esetén harmadik féllel felülvizsgáltassa.

Harmadik fél a Hivatal adatait és az elektronikus információs rendszereit a hozzáférést rögzítő szerződés és a jelen IBSZ *{10. számú melléklet – Titoktartási Nyilatkozat}* mellékletében található titoktartási nyilatkozat aláírása előtt nem ismerheti meg.

III.5.16.1. A harmadik fél hozzáférési kockázatának azonosítása

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

A kockázatok felmérése a jelen IBSZ *{4. számú melléklet – Kockázatelemzési és kezelési módszertan}* melléklete szerint történik. A kockázatkezeléshez, a megfelelő óvintézkedések kialakításához és a hozzáférések engedélyezéséhez a hozzáférés igénylésben pontosan meg kell határozni a hozzáférések típusát és azt, hogy milyen okból történik a hozzáférés.

A kockázat meghatározásért a harmadik féllel kötött szerződés teljesítésében elsődlegesen érintett szervezeti egység vezetője a felelős, és a szerződés megkötése előtt köteles az informatikai biztonsági felelőst bevonni a szerződéskészítés folyamatába.

III.5.16.2. A harmadik féllel kötött szerződés biztonsági követelményei

A szerződésekben, amennyiben az értelmezhető az alábbiakat kell előírni:

a) a külső szervezetnek meg kell határoznia a Hivatallal kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat;
b) meg kell követelni, hogy a szerződő fél feleljen meg a Hivatal által meghatározott személybiztonsági követelményeknek;
c) meg kell követelni, hogy a szerződő fél dokumentálja a személybiztonsági követelményeket;
d) elő kell írni, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik a Hivatal elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést a Hivatalnak;

e) az informatikai biztonság fő szabályait;

f) az információs vagyon bizalmasságának, sértetlenségének és rendelkezésre állásának meghatározását, illetve a védelem érdekében meghatározott eljárásokat;

g) az információk másolásának és nyilvánosságra hozatalának feltételeit;

h) a szolgáltatás elvárt szintjének és a szolgáltatási időszaknak a meghatározását;

i) a felek felelősségének meghatározását;

j) a szellemi tulajdon védelmére és másolására vonatkozó jogokat és kötelezettségeket;

k) a teljesítések ellenőrizhetőségét, monitorozását és jelentések készítését;

l) a felmerülő problémák kezelését;

m) a hardver- és szoftvertelepítésből és karbantartásokból eredő felelősséget;

n) világos és egyértelmű jelentéskészítési struktúrát és rendszert;

o) a változáskezelések egyértelmű és meghatározott folyamatát;

p) óvintézkedések meghatározását a kártékony kódok ellen;

q) biztonsági események kivizsgálására és jelentésére vonatkozó intézkedések meghatározását;

r) az alvállalkozók bevonására vonatkozó szabályokat.

Abban az esetben, ha a feladat elvégzésére a harmadik fél alvállalkozót is igénybe vesz, a szerződésben pontosan meg kell nevezni az alvállalkozót, s meg kell határozni a rá vonatkozó hozzáférési jogosultságokat. A titoktartási kötelezettség a harmadik fél alvállalkozójára is vonatkozik, és a szerződésnek titoktartási nyilatkozat részt is kell tartalmaznia.

III.5.17. Fegyelmi intézkedések

A jelen IBSZ-ben előírt szabályok megszegéséről az észlelő haladéktalanul köteles tájékoztatni az IBF-et. Az IBF a tudomására jutott események súlyosságát mérlegeli, és szükség esetén jelenti a jegyzőnek.

A biztonsági előírások megsértőivel szemben fegyelmi felelősségre vonásra kerülhet sor, amelyet az IBF által felterjesztett jelentés alapján a jegyző kezdeményez. Az eljárás a jogszabályok és a Hivatal belső szabályai szerint történik.

Külső szerződő fél által elkövetett szabályszegés esetében a szerződésben foglaltak szerint, illetve a vonatkozó jogszabályok alapján kell eljárni.

III.5.18. Belső egyeztetés

A Hivatalnak a cselekvési tervében foglaltaknak megfelelően terveznie és egyeztetnie kell az elektronikus információs rendszerei biztonságát érintő következő tevékenységeit annak érdekében, hogy csökkentse annak a nem érintett szervezeti egységeire gyakorolt hatását:

a) információbiztonsági értékelések;

b) információbiztonsági auditok;

c) hardver vagy szoftverkarbantartások;

d) biztonsági frissítések telepítése;

e) vészhelyzeti tervek tesztelése.

III.5.19. Viselkedési szabályok az interneten

A Hivatal által nyújtott internetkapcsolat és elektronikus levelezési szolgáltatás igénybevételének a következők a szabályai.

III.5.19.1. A web böngészés szabályai

Az Internethez való kapcsolódás csak és kizárólag a munkavégzést szolgálja! A felhasználók kizárólag jóváhagyott szoftvereket használhatnak az Internet elérésére.

A nem munkavégzést szolgáló hálózati sávszélesség foglalása (pl. nagyméretű állományok letöltése), és adatok kiszolgálón történő tárolása esetén a felhasználó figyelmeztetésben részesül. Ismételt előfordulás esetén az rendszergazda jelentést tesz az IBF-nek, aki eljár az ügyben a jegyző felé.

Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, kiiktatása. Ebbe a körbe tartoznak a vírusellenőrző és Internet böngésző kontrollok is.

Tilos az IBF engedélye nélkül külső féllel nem web alapú hálózati kapcsolat kialakítása (pl.: FTP).

Tilos az elektronikus információs rendszerek használata a hivatali értékekkel összhangban nem álló célokra, vagyis pl. szexuális jellegű fájlok fogadására, küldésére, fenyegetésre vagy megfélemlítésre, megkülönböztetésre, gyűlölködésre, fegyverekkel és illegális drogokkal való kereskedésre, erőszakra, internetes- illetve szerencsejátékokra, bármilyen kereskedelmi illetve jogellenes tevékenységre.

Tilos nem a munkavégzést szolgáló közösségi oldalak látogatása.

Tilos a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele.

Főszabály szerint tilos hivatali adatok tárolására külföldi felhő-alapú tárhely-szolgáltatást igénybe venni. Amennyiben külföldi felhő-alapú tárhely-szolgáltatás igénybe vételére van szükség, úgy előzetesen engedélyeztetni kell a Nemzeti Elektronikus Információbiztonsági Hatósággal, de ebben az esetben is csak EGT tagállamon belüli adatkezelés, illetve adatfeldolgozás lehetséges.

Az internetről csak hivatali célból lehet fájlokat letölteni! Tilos fájlletöltő szolgáltatások használata. Különösen tilos jogvédett, illetve illegális tartalmak, fájlok letöltése, tárolása!

Az internetes oldalak elérése monitorozásra és naplózásra kerülhet, a munkával összefüggésbe nem hozható oldalak elérhetőségét az informatikai üzemeltetés jogosult korlátozni.

III.5.19.2. E-mail használat

A Hivatal által biztosított elektronikus levél cím és az elektronikus levelezési szolgáltatás kizárólag hivatali munkavégzés céljára biztosított, ezért a felhasználóknak tilos a hivatali e-mail címüket nem hivatali minőségben használni (pl.: regisztráció letöltési weboldalakra, online játék oldalakra, közösségi oldalakra, az Interneten elérhető nyilvános chat-és fórum oldalakon hivatali email címmel hozzászólni stb.)!

A Hivatal által nem támogatott levelezőrendszer (pl.: Gmail, Freemail) használata munkavégzésre nem engedélyezett.

Az e-mail a munkavégzéssel kapcsolatos levelezést szolgálja, ahol az egy felhasználóra eső tárterület korlátozott, és ennek túllépése esetén a rendszer figyelmeztetést küld, további figyelmeztetési határok átlépése esetén pedig megszűnhet a további levelezési lehetőség.

Az elektronikus levelek és csatolmányok védelmi előírásai megegyeznek az egyéb dokumentumok védelmének előírásaival.

A Hivatal elektronikus levelező rendszeréből elküldött elektronikus levél önmagában nem használható kötelezettség vállalására, illetve annak visszaigazolására.

A Hivatal elektronikus levelező rendszeréből csak akkor lehet bizalmas, jogszabály által védett adatot, titkot (személyes adatok, különleges adatok, adótitok stb.) elküldeni, hogy ha szabványos, sérülékenységektől mentes kriptográfiai algoritmussal az adat titkosításra került.

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

A felhasználónak tilos a postafiókjában kezelt elektronikus levelek automatikus vagy manuális továbbítása más, külső elektronikus levelező rendszerbe (pl.: a saját magán email címére).

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

Ismeretlen helyről származó e-mail-ek esetében fokozott óvatossággal kell eljárni, mert maga a levél vagy annak csatolmánya kártékony lehet.

III.6. Tudatosság és képzés

III.6.1. Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel

A Hivatal a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megosztása érdekében kapcsolatot alakít ki és tart fenn akövetkező, elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és e célt szolgáló ágazati szervezetekkel:

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet által működtetett

a) Hatóság,
b) és Eseménykezelő Központ.

III.6.2. Képzési eljárásrend

Rendszeres belső oktatásokkal gondoskodni kell arról, hogy a felhasználókban tudatosodjanak az alapvető információbiztonsági fogalmak, illetve ismerjék meg a munkájuk során felmerülő információbiztonsági fenyegetettségeket. Gondoskodni kell arról is, hogy a napi feladatok végzése során a felhasználók kellőképpen felkészültek legyenek a jelen IBSZ-ben foglaltak betartására.

III.6.2.1. Biztonságtudatosság képzés

Minden felhasználó részére alap biztonság tudatosság képzéseket kell tartani. A képzésen a következő témaköröket kell érinteni:

- információbiztonságra vonatkozó jogszabályok;
- információbiztonsági alapfogalmak;
- felhasználók napi munkavégzése során jelentkező fenyegetettségek;
- fenyegetettségekkel szembeni védekezési lehetőségek;
- Hivatal információbiztonsági szabályozó rendszerének ismertetése.

Új dolgozó munkába lépésekor a dolgozóval a munkába állás előtt az információbiztonsági előírásokat meg kell ismertetni. A dolgozók információbiztonsági tudatosságának fenntartása érdekében évente frissítő oktatást kell szervezni.

Azinformációbiztonsági oktatások és továbbképzések tematikájának kidolgozása, a szükséges szakirodalom és tájékoztató anyagok biztosítása, valamint a képzés megtartása az IBF feladata.

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

III.6.2.2. Belső fenyegetés

A biztonsági képzések tematikáját úgy kell kidolgozni, hogy a felhasználó képes legyen felismerni a belső fenyegetéseket és legyen tudatában annak, hogy jelentenie kell a szabálysértéseket és egyéb belső fenyegetésből fakadó biztonsági incidenseket.

III.6.2.3. Szerepkör vagy feladat alapú biztonsági képzés

A jegyzőnek, a rendszergazdának és az IBF-nek a következő, külön jogszabályban előírt továbbképzésen és éves továbbképzésen kell részt venniük:

Szerepkör megnevezése	Képzés megnevezése
Jegyző	elektronikus információs rendszerek védelméért felelős vezető (Nemzeti Közszolgálati Egyetem)
Rendszergazda	elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy (Nemzeti Közszolgálati Egyetem)
IBF	NKE végzettség esetén elektronikus információbiztonsági vezető
	A képzési rendelet 7. § (2) bekezdése szerinti nemzetközi minősítések esetében az adott minősítés fenntartásának biztosítása

III.7. Az elektronikus információs rendszerek nyilvántartása

Nyilvántartást kell vezetni az általa működtetett valamennyi elektronikus információs rendszerről. A nyilvántartásnak minden elektronikus információs rendszerre nézve a következőket kell tartalmaznia:

a) az EIR nevét;

b) annak alapfeladatait;

c) a rendszerek által biztosítandó szolgáltatásokat;

d) az érintett rendszerekhez tartozó licenc számot;

e) a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;

f) a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

A nyilvántartást a rendszergazdának kell vezetnieés évente felülvizsgálnia.

IV. Fizikai védelmi intézkedések

IV.1. Alapelvek

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

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

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

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

IV.2. A területek fizikai biztonsági követelményei

IV.2.1. Fizikai biztonság védősávja

A védett helyiségeket, illetve területeket a fenyegetettség és kockázat mértéke szerint biztonsági zónákba kell besorolni. Héjszerű, többlépcsős fizikai védelmet kell kialakítani.

A jelen IBSZ *{I.2.2Tárgyi hatály}* pontja alá eső területeket az alábbi kategóriák egyikébe kell besorolni:

a) belső terület;

b) védett terület;

c) érzékeny terület.

További védett terület kategóriákat az IBF határozhat meg.

IV.2.2. Belső terület

Belső területnek tekintendők a Hivatal bejárata utáni közös használatú helyiségei és folyosói.

A belső terekben infokommunikációs eszközök nem telepíthetők, a kivételek jóváhagyása az IBF feladata.

IV.2.3. Védett terület

Védett terület valamennyi iroda és tárgyaló helyiség.

A védett területeken a következő védelmi intézkedéseket kell alkalmazni:

a) a kulcsokat nem szabad nyilvános, idegenek számára is könnyen hozzáférhető helyen tárolni;

b) a fénymásoló és nyomtató berendezéseket, a fax készülékeket védett területen belül kell elhelyezni. Gondoskodni kell arról, hogy a belső területen elhelyezett eszköz esetében csak egyedi azonosítás és hitelesítés után lehessen a nyomtatást az eszközön elindítani;

c) a dokumentumok tárolása védett területen történjen;

d) azokban az időszakokban, amikor a helyiségek felügyelet nélkül maradnak, az ajtókat és ablakokat zárva kell tartani;

e) a védett területek bejárati ajtajában a kulcsokat nem szabad a zárban hagyni, illetve ha az ajtó nyitva van, a helyiséget nem szabad őrizetlenül hagyni.

f) munkaidőn kívül, amikor az épületben senki sem tartózkodik a belső és a védett területeken elektronikus riasztórendszert kell alkalmazni.

g) ügyfelet és más külsős személyt nem szabad felügyelet nélkül hagyni.

IV.2.4. Érzékeny terület

Érzékeny terület a Hivatal

a) szerverszobája és

b) a strukturált kábelezés rendező központjai.

Az érzékeny területekre vonatkozóan a következő védelmi intézkedéseket kell megvalósítani:

Látogatók belépése az érzékeny területre csak hivatalos célból, ellenőrzötten és kísérővel történhet. A látogatóknak a figyelmét fel kell hívni az érvényben lévő biztonsági előírásokra.

Az érzékeny területeken a jogosulatlan belépések kizárása, a belépések engedélyezése, figyelése, dokumentálása és ellenőrzése érdekében belépési naplót kell vezetni.

A belépési naplót a jegyzői titkárságon kell tárolni.

Az érzékeny területek elérésére a jegyző, a rendszergazda és az IBF jogosultak. Minden más személy részére csak a jegyző engedélyezheti a belépést az érzékeny területekre.

Az érzékeny területek belépési naplóit, valamint a kiosztott jogosultságokat az IBF-nek évente ellenőriznie kell.

Az érzékeny területekre az ideiglenes jellegű munkát végző harmadik fél számára csak korlátozott mértékben és ellenőrzés mellett szabad biztosítani a hozzáférést. A felügyeletet a rendszergazda biztosítja.

A szerverszobában munkanapokon 18 órától 06 óráig, munkaszüneti napokon 0-24 óráig, illetve az utolsó rendszergazda távozása után elektronikus riasztórendszert kell alkalmazni.

A nyilvános helyen elhelyezett rack szekrényekben nyitásérzékelővel ellátott elektronikus riasztórendszert kell alkalmazni.

IV.3. Fizikai belépési engedélyek

El kell készíteni és napra készen kell tartani a Hivatalba belépésre jogosultak listáját. A listát a jegyző hagyja jóvá.

A jogosultságot igazoló dokumentumként az elektronikus beléptető rendszerhez tartozó beléptető kártya szolgál.A belépésre jogosultak listáját a Hivatal elektronikus beléptető rendszere tárolja.

A belépésre jogosultakat a személyügyi referens félévente dokumentáltan felülvizsgálja és törli a rendszerből a belépési jogosultsággal már nem rendelkező személyeket.

Amennyiben valakinek megszűnik a munkavégzésre irányuló jogviszonya, a személyügyi referensnek soron kívül törölnie kell a listáról.

IV.4. Fizikai belépés ellenőrzése

IV.4.1. Fizikai belépések

A Hivatal épületébe a belépés kizárólag a Hivatal főbejáratán lehetséges.

IV.4.2. Fizikai belépések naplózása

A Hivatalba történő fizikai be- és kilépések tényét naplózni kell.

A Hivatalba történő be- és kilépések naplózására a Hivatal portáján elhelyezett jelenléti ív szolgál.

A jelenléti íven rögzíteni kell a munkatárs nevét, illetve a ki- és belépések idejét.

A jelenléti ívet munkaidőben a portaszolgálatot teljesítő munkatárs vezeti. Munkaidőn kívül minden munkatárs köteles a jelenléti ívet saját maga kitölteni.

Ügyfélszolgálati időn kívül a Hivatal főbejárati ajtaját zárva kell tartani.

IV.4.3. Vendégek kísérete

Biztosítani kell a Hivatalba érkező vendégek, ügyfelek kíséretét és regisztrációját, amennyiben védett munkaterületre lépnek be. A regisztrációt a portaszolgálat végzi. A regisztráció során rögzíteni kell a vendég nevét, a látogatás célját, az ügyintéző nevét, valamint a ki-és belépés időtartamát. A kíséretet annak a munkatársnak kell biztosítani, akihez a vendég érkezik.

A látogatói naplókat 1 évig meg kell őrizni.

IV.4.4. Kulcsok megóvása

Gondoskodni kell a védett munkaterületek ajtóinak kulcsainak megőrzéséről. Amennyiben a kulcsot a birtokosa elveszti, azonnal jelentenie kell a jegyzőnek, aki gondoskodik az ajtó zárjának a cseréjéről.

IV.4.5. Belépések ellenőrzése, felügyelete

A Hivatalba történő be-és kilépések felügyeletét az elektronikus beléptető rendszer, illetve a portaszolgálat végzi.

IV.4.6. Rendellenességek jelentése

Valamennyi hivatali dolgozó kötelessége, hogy jelentse a jelen fejezetben leírt szabályokkal ellentétes viselkedést a jegyzőnek, aki kivizsgálja az eseményt és dönt a szükséges további intézkedésekről.

IV.5. Az infokommunikációs eszközök biztonsága

Az információs vagyon – lopás, veszélyeztetés, egyéb károsodás elleni – védelmének és a működési folyamatok folytonosságának biztosítása érdekében a Hivatal infokommunikációs eszközeit, azok megfelelő fizikai elhelyezésével és kezelésével is biztosítani kell.

Az infokommunikációs eszközök elhelyezése és védelme

Az infokommunikációs eszközöket úgy kell elhelyezni, és védelmüket úgy kell kialakítani, hogy minimálisra csökkenjenek a környezeti hatások következtében megjelenő kockázatok, és minimálisra csökkenjen az illetéktelen hozzáférések lehetősége, de a munkavégzés hatékonysága ne romoljon.

A védelmi intézkedések biztosítsák, hogy a különböző környezeti hatás miatt keletkező meghibásodások csökkenjenek. Ezért:

a) be kell tartani a tűzvédelmi előírásokat;

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

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

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

IV.5.1. „Üres asztal – üres képernyő" szabály

Az elektronikus formában tárolt adatokhoz, információkhoz való illetéktelen hozzáférés megakadályozása és azok jogosulatlan eltulajdonításának elkerülése érdekében minden dolgozónak ismernie és alkalmaznia kell a jelen pontban leírtakat:

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

b) a felhasználó a munkaállomását zárolni köteles (a Ctrl +Alt +Del billentyűk, majd Zárolás), ha azt őrizetlenül hagyja;

c) a zárolás elfelejtésének esetére jelszóvédett, automatikus zárolást kell beállítani, úgy, hogy az maximum 10 perc várakozást követően zárolja a számítógépet;

d) a munkafázis végeztével ki kell jelentkezni az alkalmazásokból, majd leállítani a munkaállomást;

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

f) ügyfelet irodában felügyelet nélkül hagyni tilos.

IV.6. Felügyelet alól kikerülő eszközök

Szerviz részére eszközt csak a rendszergazda adhat át. Szervizbe történő szállítás esetén a szerviz által adott szállítólevelet a rendszergazda őrzi meg.

Szervizbe történő szállításkor vagy garanciális javítás esetén – jegyzőkönyv felvétele mellett – a rendszergazdának gondoskodnia kellaz adatokat tartalmazó adathordozók törléséről.

A munkatársak részére hosszú távú használatra kiadott nagy értékű eszközökről (pl.: laptop) a Hivatalnak nyilvántartást kell vezetnie. Ezen eszközöket a munkatársak korlátozás nélkül ki- és beszállíthatják.

Minden más esetben eszközt kiszállítani csak a rendszergazda írásos engedélyével lehet.

A ki- és beszállítások ellenőrzése arendszergazda feladata. Infokommunikációs eszközök és berendezések írásos engedély nélküli ki- és beszállításának kísérlete esetét jelenteni kell az IBF-nek a szabálysértést elkövető személy felettes vezetőjének egyidejű értesítése mellett.

Az információbiztonsági tudatosság fokozását célzó oktatások keretében a felhasználókat tájékoztatni kell az ezzel kapcsolatos ellenőrzési feladatokról és jogokról.

IV.7. Áramellátó berendezések és kábelezés

A kritikus infokommunikációs eszközök (kiszolgáló, tűzfal, router, switch) működését szünetmentes áramforrásról kell biztosítani. Intézkedéseket kell foganatosítani, hogy a kiszolgálók az áthidalási időn belül szabályosan leállíthatók legyenek.

Biztosítani kell az elektromos és adatvezetékek megszakadás és a rongálások elleni megfelelő védelmét.

A hálózati zavarok okozta hibák elkerülése érdekében az erősáramú vezetékeket el kell különíteni a kommunikációs hálózattól. A kábelstruktúra legyen érzéketlen az elektromos hálózati zavarokra.

IV.8. Tűzvédelem

A szerverhelyiségben független áramellátással ellátott tűzjelző készüléket, valamint elektromos tüzek oltására alkalmas tűzoltó készüléket kell alkalmazni.

IV.9. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem

Biztosítani kell, hogy víz- és más csővezetéken szállított anyag esetében a jegyző által kijelölt személyek részére hozzáférhetőek legyenek a főelzáró szelepek.

A jegyző felelőssége gondoskodni a főelzáró szelepek működőképességének fenntartásáról.

A szerverhelyiségben vízbetörés érzékelő szenzorokat kell telepíteni, mely vízbetörés esetén riasztja (pl.: SMS, email) a rendszergazdát.

IV.10. Hőmérséklet és páratartalom ellenőrzés

A szerverhelyiségben elhelyezett központi kiszolgáló egységek biztonságos működése érdekében a hőmérsékletet 20-21 Celsius fok között kell tartani.

A hőmérsékletet az elhelyezett eszközök hő leadását figyelembevevő teljesítménnyel rendelkező klímaberendezéssel kell biztosítani.

A klímaberendezés által termelt kondenzvizet erre rendszeresített zárt csatornán ki kell vezetni a szerverhelyiségből.

A relatív páratartalom szintjét 40-60% között kell tartani.

A hőmérsékletet és a relatív páratartalom szintjét arra alkalmas eszközzel folyamatosan mérni kell. Az eszköznek riasztást kell adnia (pl.: SMS, email) a rendszergazdának, hogy ha a hőmérséklet 10 Celsius fok alá csökken vagy meghaladja a 28 Celsius fokot, illetve ha a relatív páratartalom szintje eléri a fent megadott határértéket.

V. Logikai védelmi intézkedések

V.1. Általános védelmi intézkedések

V.1.1. Engedélyezés

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

a) az elektronikus információs rendszer és annak környezete biztonsági állapotának felügyelete,

b) meghatározásra kerüljenek az információbiztonsággal összefüggő szerepkörök és felelősségi körök,

c) kijelölésre kerüljenek az ezeket betöltő személyek,

d) az elektronikus információbiztonsági engedélyezési folyamatok kerüljenek integrálásra a Hivatali szintű kockázatkezelési eljárásba, összhangban az informatikai biztonsági szabályzattal.

e) az elektronikus információbiztonsággal kapcsolatos engedélyezés terjedjen ki minden, a Hivatal hatókörébe tartozó:

f) emberi, fizikai és logikai erőforrásra;

g) eljárási és védelmi szintre és folyamatra.

V.1.2. Elektronikus információs rendszer kapcsolódásai

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

Az összekapcsolást mind a jegyzőnek, mind a rendszergazdának, mind pedig az IBF-nek is jóvá kell hagynia.

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

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

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

Információbiztonsági incidens esetén a Hivatal jogosult a kapcsolatot felfüggeszteni.

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

IP szinten korlátozni kell a kapcsolódást.

Az összekapcsolás feltételeinek fennállását legalább évente ellenőrizni kell.

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

V.1.3. Belső rendszerkapcsolatok

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

V.1.4. Külső kapcsolódásokra vonatkozó korlátozások

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

Minden kapcsolatot előzetesen jóvá kell hagyatni az IBF-fel.

V.2. Tervezés – Biztonságtervezési eljárásrend

V.2.1. Rendszerbiztonsági terv

El kell készíteni az elektronikus információs rendszerek rendszerbiztonsági tervét, mely a következőket tartalmazza:

a) az elektronikus információs rendszer hatóköre, alap feladatai (biztosítandó szolgáltatásait), biztonságkritikus elemei és alap funkciói,

b) az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztálya,

c) az elektronikus információs rendszer működési körülményei és más elektronikus információs rendszerrel való kapcsolatai.

Az elektronikus információs rendszer biztonsági követelményeit a vonatkozó rendszerdokumentációban kell rögzíteni.

Meg kell határozni a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedésbővítéseket, illetve végre kell hajtani a jogszabály szerinti biztonsági feladatokat.

A rendszerbiztonsági tervet meg kell ismertetni a Hivatal érintett munkatársaival illetve a fejlesztővel.

Az elektronikus információs rendszerek rendszerbiztonsági tervét kétévente felül kell vizsgálni.

Soron kívül felül kell vizsgálni a rendszerbiztonsági terveket az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások, illetve a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén.

Az elektronikus információs rendszerek rendszerbiztonsági tervét az érintettek bevonásával az IBF készíti el.

A rendszerbiztonsági tervek bizalmasnak minősülnek, ezért azok megismerésére az IBF, a rendszergazda, a jegyző, valamint a jegyző által írásban kijelölt személyek jogosultak.

V.2.2. Cselekvési terv

A cselekvési tervre vonatkozó követelményeket a jelen IBSZ *{II.A Hivatal és az elektronikus információs rendszereinekinformációbiztonsági követelményei}* fejezete tartalmazza.

V.2.3. Személybiztonság

A személybiztonságra vonatkozó követelményeket a jelen IBSZ *{I.5Az IBSZ általános követelményei}* pontja tartalmazza.

V.3. Konfigurációkezelési eljárásrend

V.3.1. Alap konfiguráció

A Hivatal valamennyi elektronikus információs rendszeréhez elkészíti az alapkonfigurációt, amelyet dokumentált formában biztonságos helyen tárolni szükséges.

A dokumentációnak minimálisan a következő elemeket kell magában foglalnia a munkaállomásokra, kiszolgálókra, a hálózati eszközökre és egyéb mobil eszközök telepített operációs rendszerek és egyéb szoftverek verzióit, patch szintjét, továbbá az egyes szoftverkomponensek biztonságosnak ítélt konfigurációs beállításait.

Vázolni kell az érintett EIR elhelyezkedését a logikai topológiában.

Az egyes elektronikus információs rendszerek alapkonfigurációját a rendszergazda hathavonta felülvizsgálja, és a módosításokat átvezeti.

V.3.2. Legszűkebb funkcionalitás

A Hivatal elektronikus információs rendszereiben csak a szükséges portokat, protokollokat és szolgáltatásokat szabad engedélyezni. Az engedélyezett portokat, protokollokat és szolgáltatásokat dokumentálni kell a rendszer alapkonfigurációjában.

Az önkormányzati ASP rendszert elérő munkaállomásokon tilos olyan alkalmazást futtatni, amely a munkaállomást harmadik féllel köti össze, és amelynek segítségével lehetőség van távoli támogatásra, vezérlésre, képernyő átvételére.

V.3.3. Elektronikus információs rendszerelem leltár

Az elektronikus információs rendszerek valamennyi hardver/szoftver eleméről a rendszergazdának nyilvántartást kell vezetni. A nyilvántartásnak tartalmaznia kell a kiszolgálók és munkaállomások pontos és naprakész hardver konfigurációját, az elhelyezkedésüket, a működő alkalmazások egyedi beállításait és az értük felelős személy nevét.

V.3.4.

V.3.5. Duplikálás elleni védelem

A Hivatalnak ellenőriznie kell, hogy az elektronikus információs rendszer hatókörén belüli elemek nincsenek-e felvéve más elektronikus információs rendszerek leltárában.

V.3.6. A szoftver használat korlátozásai

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

Az alkalmazott szoftverekről leltárt kell vezetni.

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

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

A szerzői jogokkal védett szellemi termékek felhasználását nyomon kell követni.

V.3.7. A felhasználó által telepített szoftverek

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

A felhasználók munkaállomásain telepített alkalmazások megfelelőségét az IBF szúrópróbaszerűen ellenőrzi.

V.4. Rendszer karbantartási eljárásrend

Az elektronikus információs rendszerek karbantartására vonatkozóan a jelen fejezetben leírtak az irányadók:

V.4.1. Rendszeres karbantartás

A folyamatos működés érdekében a Hivatal elektronikus információs rendszereit a gyártó ajánlása alapján rendszeresen karban kell tartani. A karbantartások ütemezése, végrehajtása és az ellenőrzés megszervezése a rendszergazda feladata.

V.4.2. A karbantartások engedélyezése

A tervezett karbantartásokat dokumentált formában a jegyző engedélyezi. Amennyiben ez az elektronikus információs rendszerek leállításával jár, akkor a felhasználókat a karbantartás megkezdése előtt legalább 1 héttel értesíteni szükséges.

V.4.3. A karbantartások dokumentálása, nyilvántartása

Az elvégzett munkákat jegyzőkönyvezni kell, valamint a karbantartás tényét karbantartási nyilvántartásban kell dokumentálni, illetve nyilvántartani. A nyilvántartásba a következő adatokat kell minimálisan rögzíteni:

a) az elvégzett karbantartás megnevezése,

b) az érintett eszközök, szoftverek, elektronikus információs rendszerek,

c) a karbantartás engedélyezője,

d) a karbantartás elvégzője,

e) a karbantartás dátuma,

f) leállási idő (ha volt ilyen).

A jegyzőkönyveket csatolni kell a karbantartási nyilvántartáshoz.

V.4.4. A karbantartások ütemezése

Éves karbantartási tervet kell készíteni, melyben meg kell tervezni a karbantartások ütemezését. A terv elkészítése a rendszergazda, a terv jóváhagyása a jegyző feladata.

V.4.5. Kiszállítás

Amennyiben az adatot tartalmazó adathordozó kiszállítása válik szükségessé, akkor a jelen IBSZ*{V.5.3Adathordozók szállítása}*fejezetben leírtak szerint kell eljárni. A kiszállítást a rendszergazda engedélyezi.

V.4.6. A karbantartás ellenőrzése

Az elvégzett karbantartás után az eszköz fajtájától függően funkcionális és biztonsági teszteket kell végezni, melynek eredményét rögzíteni kell a karbantartási nyilvántartásban. Sikertelen teszt esetén az eszköz nem helyezhető újra éles üzembe.

V.4.7. Karbantartók

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

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

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

a) szervezet megnevezése,

b) szerződésszám,

c) szerződés időtartama,

d) szerződéses kapcsolattartó neve, elérhetősége,

e) karbantartás végzők neve, elérhetősége,

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

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

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

V.4.8. Adathordozók ellenőrzése

A karbantartás során igénybe vett adathordozókat használatba vétel előtt kártékony kód elleni ellenőrzésnek kell alávetni.

V.4.9. Távoli karbantartás

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

A távoli karbantartásokról a rendszergazdának nyilvántartást kell vezetni.

A távoli hozzáférésekre vonatkozó követelményeket a jelen IBSZ *{V.7.16. Külső elektronikus információs rendszerek használata}* fejezete tartalmazza.

V.5. Adathordozók védelmére vonatkozó eljárásrend

Az adathordozók védelmére a következő előírások vonatkoznak.

V.5.1. Hozzáférés az adathordozókhoz, adathordozók használata

A Hivatalban csak a Hivatal tulajdonában lévő, regisztrált adathordozót lehet használni. Adathordozó igénylését a rendszergazdához kell benyújtania a szervezeti egység vezetőjének.

Az eszközhasználatot, a Hivatal elektronikus információs rendszereihez történő csatlakoztatása után, a Hivatal minden előzetes értesítés nélkül figyelheti, monitorozhatja.

Otthoni munkavégzés és bármilyen más célból bármilyen adatot floppyn, CD-n, elektronikus levélben vagy egyéb más módon (Pl.: Pen drive) a Hivatal informatikai infrastruktúrájából kijuttatni csak az Adatgazda írásos engedélyével szabad. Az adatok kivitelét az Adatgazdának vagy a szervezeti egység vezetőjének kell engedélyeznie, minden esetben írásos formában.

A Hivatal az adathordozók használatát információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozhatja.

V.5.2. Adathordozók tárolása

A Hivatal elektronikus információs rendszereinek kiszolgáló oldali adathordozóit a szerverhelyiségben kell tárolni. A szerverhelyiség fizikai védelmét a jelen IBSZ *(IV.2.4. Érzékeny terület)*fejezetében foglaltaknak megfelelően kell kialakítani.

A felhasználók részére kiosztott mobil adathordozókat használaton kívül zárható irodabútorban kell tárolni.

V.5.3. Adathordozók szállítása

A felhasználók részére biztosított mobil adathordozók a felhasználók részéről korlátozás nélkül szállíthatóak.

A kiszolgáló oldali adathordozók szállítására a rendszergazda jogosult. Ebben az esetben a szállítást dokumentálni kell.

V.5.4. Kriptográfiai védelem

Szállítás során biztosítani kell az adathordozókon tárolt adatok bizalmasságát és sértetlenségét. Ennek érdekében a felhasználók részére kiosztott mobil adathordozókon tárolt adatokat szabványos, ismert sérülékenységektől mentes kriptográfiai módszerrel titkosítani kell.

V.5.5. Az infokommunikációs eszközök biztonságos újrahasznosítása vagy mások rendelkezésére bocsátása

Az infokommunikációs eszközök újrahasznosítása vagy mások rendelkezésre bocsátása előtt minden esetben gondoskodni kell arról, hogy az infokommunikációs eszközökön tárolt információk visszaállíthatatlanul eltávolításra kerüljenek. Ennek érdekében

a) a rajtuk tárolt adatokat helyreállíthatatlanságot garantáló technikával törölni kell;

b) a törlést az adattárolón lévő adatok gazdájának jóvá kell hagynia;

c) garanciális eszközök esetén, ha az eszköz hibája miatt az adatok törlésére nincs mód, az IBF dönt az eszköz cserére történő kiadhatóságáról, vagy megsemmisítéséről.

Az adatok megfelelő módon történő eltávolításáért az adatgazda a felelős. Az adatok eltávolítását a rendszergazda végzi. Az adatok eltávolítását jegyzőkönyvezni kell.

V.5.6. Ismeretlen tulajdonos

A Hivatal elektronikus információs rendszereiben tilos nem a hivatal tulajdonát képező adathordozót csatlakoztatni, ezért alapértelmezésként technikai eszközökkel tiltani kell a CD/DVD olvasókat és az USB portokat.

A fentiek alól a felhasználó indoklása (munkavégzés) esetén a jegyző adhat felmentést.

V.5.7. A hordozható infokommunikációs eszközök védelme

A hordozható infokommunikációs eszközök használata során a munkaállomásokra vonatkozó előírásokon kívül az alábbi védelmi szabályokat kell betartani:

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

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

c) a mobilitás és a kis méret miatt a mobil infokommunikációs eszközök fokozottan vannak kitéve lopásveszélynek, emiatt nem szabad őrizetlenül hagyni autóban, szállodai szobában;

V.5.7.1. Mobil infokommunikációs eszközök ellopása

Mobil infokommunikációs eszköz ellopása esetén:

i. az ellopás tényét a lehető leggyorsabban jelenteni kell az IBF-nek;

ii. értesíteni kell a rendőrséget;

iii. értesíteni kell a szálloda vezetését, ha az eszközt a szállodai szobából vagy a szálloda területén álló kocsiból lopták el;

iv. valamennyi rendőrségi jelentést meg kell őrizni és a jegyző részére át kell adni.

V.5.7.2. Infokommunikációs eszköz elvesztése

Bármely infokommunikációs eszköz eltűnését a lehető leggyorsabban jelenteni kell a munkahelyi vezetőnek és az IBF-nek, valamint tájékoztatni kell őket arról, hogy az eszköz tartalmaze bárminemű érzékeny információt. (Előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban is megerősítve.)

V.6. Azonosítási és hitelesítési eljárásrend

V.6.1. Azonosítás és hitelesítés (szervezeten belüli felhasználók)

Valamennyi elektronikus információs rendszernek egyedileg kell azonosítania és hitelesítenie a Hivatal valamennyi felhasználóját és a felhasználók által végzett tevékenységeket.

Ennek érdekében egyénre szóló felhasználói azonosítókat kell képezni, a csoportos azonosítók használata nem engedélyezett.

V.6.2. Azonosító kezelés

Az elektronikus információs rendszerekhez történő hozzáférést biztosító azonosítókat a rendszergazda hozza létre. Az azonosítók ismételt felhasználása tilos.

90 nap inaktivitás után az azonosítókat a rendszergazdának le kell tiltania.

A fentiek háromhavi rendszerességgel történő végrehajtása az rendszergazdák feladata.

V.6.3. A hitelesítésre szolgáló eszközök kezelése

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

A Hivatal jelszókezelő rendszere:

a) tegye lehetővé a felhasználók számára jelszavuk kiválasztását és megváltoztatását;

b) kényszerítse ki az ideiglenes jelszavak megváltoztatását az első bejelentkezéskor;

c) kényszerítse ki a megfelelő minőségű jelszavak használatát;

d) kényszerítse ki a jelszóváltoztatást;

e) tiltsa meg a korábban használt jelszavak ismételt felhasználását;

f) beíráskor ne jelenítse meg a jelszavakat a képernyőn;

g) a jelszó állományokat rejtjelezve tárolja;

h) változtassa meg a szállító alapértelmezett jelszavát a szoftver installálása után.

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

a) szükség esetén a felhasználók kötelezhetők arra, hogy nyilatkozatban vállalják a számukra kiadott, vagy általuk képzett jelszavaik titokban tartását;

b) biztosítani, hogy a kezdeti jelszavak is biztonságos körülmények között kerüljenek a felhasználóknak átadásra.

A felhasználói jelszavak képzéséhez az alábbi szabályokat kell betartani:

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

b) a jelszavakat 90 naponta meg kell változtatni;

c) a jelszavakat két napon belül nem szabad megváltoztatni;

d) az előző jelszavak újra használatát 24 alkalomig kerülni kell;

e) 5 sikertelen bejelentkezési kísérlet esetére 30 percre zárolja a fiókot és a számlálót 30 perc után nullázza.

V.6.3.1. Technikai azonosítók kezelése

A technikai azonosítók elkülönített úton történő kezelését a jelen fejezetben foglaltak szerint kell megvalósítani:

A technikai azonosítókat a rendszergazda hozza létre. A technikai azonosítóknak nem adható automatikusan rendszergazda jog, törekedni kell a „szükséges, minimális jogok elve" alapján a minimális jog biztosítására.

Az azonosítók létrehozásánál biztosítani kell a nevükben futó alkalmazások, szolgáltatások egyedi azonosítását és hitelesítését a következő névkonvenció alapján: _svc_"futó szolgáltatás rövid neve".

A technikai azonosítók jelszavait jelszógenerátorral véletlenszerűen kell képezni, úgy hogy a jelszó hossza minimum 20 karakter legyen és feleljen meg a bonyolultsági kritériumnak.

Gondoskodni kell a technikai azonosítók jelszavainak évente történő megváltoztatásáról.

A jelszavakat vagy lezárt borítékban és páncélszekrényben vagy szabványos, kriptográfiai algoritmussal őrzött jelszókonténerben kell tárolni. A jelszókonténer mesterjelszavát lezárt borítékban, páncélszekrényben kell őrizni.

V.6.4. Jelszó (tudás) alapú hitelesítés

A Hivatalban csak olyan azonosítási rendszert lehet alkalmazni, mely nem tárolja a jelszót nyílt formában. Jelszavak védelmét mértékadó dokumentumban biztonságosnak mondott lenyomatoló algoritmussal, legalább 32 bit sózással és legalább 10000 alkalommal végrehajtott iterációval kell megvalósítani. A megfelelő, ismert sérülékenységektől mentes kriptográfiai algoritmus kiválasztásába be kell vonni az IBF-et.

V.6.5. Birtoklás alapú hitelesítés

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

Kiemelt figyelmet kell fordítani az e-személyi megőrzésére.

V.6.6. A felhasználó felelősségi körea jelszó használat során

A Hivatalelektronikus információs rendszereiben a jelszavak használatának és képzésének részletes szabályai a következők:

a) a felhasználó a jelszavát köteles titokban tartani;

b) a jelszószabályok betartása minden felhasználónak jól felfogott érdeke. A felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el az elektronikus információs rendszerben;

c) a felhasználói jelszót TILOS leírni;

d) ha bármilyen jel mutat arra, hogy a jelszó illetéktelen kézbe jutott, azonnal meg kell változtatni és értesíteni kell az IBF-et;

e) nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé, pl. makróra, vagy funkció billentyűre;

f) a jelszó minél komplexebb, annál kisebb a valószínűsége, hogy nevünkben visszaélést követnek el. Ennek érdekében az alábbi szempontokat kell betartani:

g) könnyen megjegyezhető, és nehezen kitalálható legyen;

h) semmi olyasmin ne alapuljon, aminek alapján valaki kitalálhatja, ilyenek a nevek, telefonszámok, születési dátumok, stb.;

i) ne legyen a gépnévre vagy a felhasználói névre utaló;

j) ne legyen sorozat.

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

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

V.6.7. A hitelesítésre szolgáló eszköz visszacsatolása

Az illetéktelen hozzáférések elkerülése érdekében olyan hitelesítési módszereket kell alkalmazni, amely a beütött jelszavak karaktereit valamilyen helyettesítő karakterrel ábrázolja (pl.: csillag karakter).

V.6.8. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

Az elektronikus információs rendszernek egyedileg kell azonosítania és hitelesítenie az érintett szervezeten kívüli felhasználókat, illetve a tevékenységüket.

V.6.9. Hitelesítésszolgáltatók tanúsítványának elfogadása

A Hivatal EIR-jeihez történő külső felhasználó általi hozzáférés esetén, amennyiben az azonosítás és hitelesítés kriptográfiai tanúsítvány felhasználásával történik, csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő bizalmi szolgáltatók által kibocsátott tanúsítványokat lehet felhasználni.

V.7. Hozzáférés ellenőrzési eljárásrend

A hozzáférési jogok kezelését jelen eljárásrendben foglaltak szerint kell megvalósítani a következő alapelvek alkalmazásával:

a) Minden felhasználó csak a feladatellátásához szükséges, minimális jogosultságot kapja meg.

b) A felhasználók a munkaállomásukon nem rendelkezhetnek rendszergazda jogokkal.

c) A rendszergazda a rendszerek adminisztrálásához használt adminisztrátori azonosítóját a napi munkavégzése során nem használhatja. A napi munkavégzéshez normál felhasználói jogú azonosítót kell használnia.

V.7.1. Felhasználói fiókok kezelése

Elektronikus információs rendszerenként meg kell határozni, hogy milyen típusú fiókok engedélyezettek (pl.: általános, megosztott, csoport, gyártói/fejlesztői/szállítói, ideiglenes, vendég, technikai).

Meg kell határozni azokat az alapfunkciókat (alapjogosultságokat) melyeket munkakörökhöz lehet rendelni és ezeket a jogosultságokat a felhasználók automatikusan megkaphatják a munkakör betöltésekor.

Elektronikus információs rendszerenként dokumentálni kell az érintett EIR-ben létrehozott szerepköröket és a szerepkörökhöz rendelt jogosultságokat (szerepkör-jogosultsági mátrix).

A Hivatal EIR-jeihez hozzáférési jogosultságokat vagy a Hivatal Szervezeti és Működési Szabályzata alapján meghatározott alapfunkciók alapján vagy egyedi igénylések alapján lehet biztosítani.

A beépített adminisztrátori és vendég fiókokat valamennyi eszközön tiltani kell.

A felhasználók csak jóváhagyott hozzáférés-védelmi megoldásokat alkalmazhatnak.

A jogosultságok és a hozzáférés menedzselésekor az alábbi alapelveket kell figyelembe venni:

a) A meghatározott jogosultságok alkalmazásával minimalizálható legyen a rosszindulatú vagy egyéb jogosulatlan hozzáférés kockázata.

b) Az elektronikus információs rendszerrel kapcsolatba kerülő személyeknek a munkájuk ellátásához szükséges minimális jogosultságokat kell biztosítani, a munkavégzésük időtartamára.

c) Az azonos tevékenységet ellátó felhasználók jogosultságai szerepkörök szintjén legyenek kialakítva, és a felhasználók a kialakított szerepkörökbe kerüljenek besorolásra.

d) Az összeférhetetlenségi szabályokat figyelembe kell venni.

e) Az elektronikus információs rendszerben alkalmazott hozzáférési jogosultságokat adminisztrálni kell.

f) Törekedni kell arra, hogy a jogosultságok automatizált módon kerüljenek nyilvántartásba, szükség esetén, papír alapon kell a nyilvántartást vezetni.

g) Minden egyes elektronikus információs rendszerhez, csak a megfelelő adminisztrálást követően lehet felhasználói jogosultságot adni, módosítani, és felfüggeszteni, illetve visszavonni.

h) Az éles elektronikus információs rendszerekben a fejlesztők hozzáférési jogosultságokkal nem rendelkezhetnek.

A felhasználók nyilvántartásba vételi szabályainak és a követendő eljárásrend kidolgozásakor a következőket kell figyelembe venni:

a) A felhasználói tevékenység ellenőrizhetősége és nyomon követhetősége érdekében a felhasználók elektronikus információs rendszerekben történő azonosítására egyedi felhasználó azonosítókat kell alkalmazni.

b) A csoportos felhasználó azonosítók használatát tiltani kell.

c) A felhasználói hozzáférési jogosultságokat a szervezeti egység vezetője határozza meg. A jogosultság meghatározása során figyelembe kell venni:

i. a felhasználó munkakörét és az azzal kapcsolatos feladatait;

ii. a munkaköri feladatok végrehajtásához minimálisan szükséges jogosultságok elvét;

iii. a felhasználó jogviszonyát;

iv. a felhasználó munkahelyét.

d) A jogosultság igénylését tartalmazó dokumentumnak tartalmaznia kell:

i. a felhasználó nevét, munkakörét, szervezeti egységét és munkahelyét;

ii. annak megjelölését, hogy milyen szolgáltatásokhoz történik a jogosultságigénylés;

iii. azt, hogy az érintett szolgáltatások tekintetében milyen szerepkör, vagy hozzáférési jogok (olvasás, bevitel/bővítés, törlés, módosítás, teljes) igénylése történik;

iv. annak megjelölését, hogy az érintett szolgáltatások és jogosultságok igénylése milyen adatkörre vonatkozóan történik;

v. a munkahelyi vezető aláírását.

e) A jogosultságigénylési lapot az igényelt és a beállított jogosultságok egyeztetése céljábóla Hivataltitkársága tárolja.

f) A kiosztott felhasználói jogosultságokat az IBF háromhavonta felülvizsgálja.

V.7.2. Kiemelt jogosultságok kezelése

A felhasználói jogosultságok kiadási folyamatánál szigorúbban kell kezelni a kiemelt jogokat biztosító adminisztrátori jogok megadását.

Az elektronikus információs rendszereknél a jogosultságok kiadásának engedélyezési eljárása során az alábbiakat kell figyelembe venni:

a) pontosan meg kell határozni azokat a rendszerelemeket, - pl. operációs rendszereket, adatbázis kezelő rendszert, valamint az alkalmazásokat - és az alkalmazotti kategóriát, amelyhez az adminisztrátori jogosultságokat kell hozzá rendelni;

b) az adminisztrátori jogosultságokat a „feltétlenül szükséges" és az „eseményenkénti" használat elve alapján kell kiadni;

c) az adminisztrátori jogot kizárólag ajegyző engedélyezheti írásban;

d) technikai azonosító részére adminisztrátori jogot az IBF engedélyezi írásban.

Az üzemeltetők csak az elektronikus információs rendszer, illetve alkalmazás üzemeltetéséhez szükséges információkhoz férhetnek hozzá, a részükre biztosított adminisztrátori jogosultság birtokában csak a felhasználó külön engedélyével és jelenlétében, kifejezetten a hiba elhárítása érdekében vagy a felhasználói igény kielégítése érdekében férhetnek hozzá a felhasználók által kezelt információkhoz.

A rendszergazda nem küldhet levelet más felhasználó nevében.

V.7.3. Hozzáférési jogok igénylésének eljárásrendje

Az új hozzáférési jogok igénylését, a jogosultságok módosítását és a jogosultságok visszavonását a jelen fejezetben leírtak szerint kell elvégezni.

V.7.3.1. ASP szakrendszerek hozzáférése

Az ASP szakrendszerekhez történő hozzáférés feltétele, hogy a felhasználó rendelkezzen E-személyivel, melyet az okmányirodákban és a kormányablakokban igényelhet.

ASP szakrendszerekhez történő hozzáférések esetében az új felhasználó létrehozását az önkormányzati ASP adminisztrátornak kell jelezni az igényelt szakrendszer és a szakrendszeri szerepkör megadásával, aki a szükséges hozzáférés birtokában létrehozza a felhasználót az ASP rendszerben, illetve hozzárendeli a szakrendszeri szerepkörökhöz.

Beállítandó jogosultsági elemek:

a) Szakrendszerekhez való hozzáférés:

i) Mely szakrendszerekhez vagy keretrendszeri modulokhoz férhet hozzá a felhasználó.

b) Szerepkörök szakrendszerenként:

i) Összehangolt szerepkör-megnevezések (cél a jó áttekinthetőség)

ii) Ugyanannak a felhasználónak több szerepköre is lehet (ez elsősorban a kisebb önkormányzatok esetén gyakori)

c) Iktatóhelyekhez (iktatási sávokhoz) való hozzáférés:

i) A felhasználó csak a megadott iktatóhelyek iratainak kísérőadatait tekintheti meg.

d) Szervezeti egységekre vonatkozó vezetői jogosultságok:

i) Az iratokba való betekintési jog az előadón kívül az előadó mindenkori vezetőjét is megilleti.

e) Helyettesítési jogosultságok:

i) Szabadságolások kezelése, munkahelyi vezető és titkárnő kapcsolata, közeli munkatársak feladatmegosztása

ii) A módosító műveletek automatikus naplózásakor a helyettesítő kiléte is tárolódik.

Az ASP szakrendszerek esetében az önkormányzatiASP adminisztrátor nyilvántartást vezet jogosultságokról.
A nyilvántartás a következő elemeket tartalmazza:

a) szakrendszer megnevezése;

b) felhasználó neve, beosztása;

c) szerepkör megnevezése (esetleg többlet jogosultságok);

d) jogosultság beállításának dátuma.

A kilépő felhasználókról a személyügyi ügyintézőnek értesítenie kell az önkormányzati ASP adminisztrátort, aki visszavonja a kilépő felhasználó jogosultságait.

A kiosztott jogosultságokat az önkormányzati ASP adminisztrátor évente felülvizsgálja és - az adatgazdákkal egyeztetve - a nem szükséges jogosultságokat visszavonja.

V.7.3.2. Új hozzáférési jog igénylése

Az igénylő a hozzáférési jogok igénylését a jelen IBSZ *{5. számú melléklet – Jogosultságigénylési űrlap}*mellékletében található űrlap kitöltésével kezdeményezi. Hozzáférési jogot az igényelhet, akinek a feladatellátásához az szükséges.

Az űrlapon meg kell jelölni az igényelt jogosultság szintjét, azt az időszakot, amelyre a jogosultságot biztosítani kell, illetve a jogosultságigénylés indoklását.

A kitöltött űrlapot alá kell írattatni a munkahelyi vezetővel, aki igazolja, hogy a feladatellátáshoz szükséges a jogosultság biztosítása.

Az űrlapot ezután meg kell küldeni az adatgazda részére, aki jóváhagyja a jogosultságigénylést.

A jóváhagyott jogosultságigénylési űrlapot ezután el kell küldeni rendszergazda részére, aki intézkedik a jogosultság kiadásáról.

A feldolgozás első lépése: A rendszergazda rögzíti az igényt a jelen IBSZ *{6. számú melléklet – Hozzáférések nyilvántartása űrlap}* mellékletében található űrlapon.

A feldolgozás második lépése: a rendszergazda az igényelt beállításokkal létrehozott felhasználói fiókról telefonon vagy személyesen értesíti az igénylőt, és megadja a belépéshez használatos felhasználói nevet, és az első belépést lehetővé tevő kezdeti jelszót és szükség esetén egyéb fontos adatokat.

A feldolgozás harmadik lépése: a kért feladatok elvégzésének bizonylatolása érdekében a rendszergazda aláírja a kitöltött jelen IBSZ *{5. számú melléklet – Jogosultságigénylési űrlap}*mellékletét, valamint e-mail-en tájékoztatja az igénylőt és a jóváhagyót a jogosultságok megadásáról és a felhasználói névről.

Az aláírt űrlapok ezek után a Hivatal Titkárságánkerülnek tárolásra visszakereshető formában.

Az IBFaz említett adatlapok meglétét és a tényleges jogosultság kiadását bármikor ellenőrizheti, és véleményét írásba foglalhatja, amelyet az Hivatal a jogosultsági rendjének folyamatos javítására használ fel.

V.7.3.3. Hozzáférési jog módosítása

A munkahelyi vezető a dolgozó megváltozott feladatkörének, illetve munkakörének ellátásához szükséges jogosultság módosításához kitölti a jelen IBSZ *{5. számú melléklet – Jogosultságigénylési űrlap}*mellékletében található űrlapot.

Az eljárásrend megegyezik az*{V.7.3.2Új hozzáférési jog igénylése}*fejezetben leírtakkal annyi kiegészítéssel, hogy amennyiben szervezeti egység váltás történik, akkor a rendszergazda gondoskodik a már nem szükséges jogosultságok visszavonásáról.

V.7.3.4. Hozzáférési jog visszavonása

A munkahelyi vezetőnekhaladéktalanul intézkednie kell a már nem szükséges jogosultságok visszavonása iránt. A hozzáférési jogosultság visszavonását a jelen IBSZ *{5. számú melléklet – Jogosultságigénylési űrlap}*mellékletében található űrlapon kell kezdeményezni.

Az űrlapot ezután el kell küldeni a rendszergazdarészére, aki intézkedik a jogosultság visszavonásáról.

A feldolgozás első lépése: A rendszergazda rögzíti az igényt a jelen IBSZ*{6. számú melléklet – Hozzáférések nyilvántartása űrlap}*mellékletében található űrlapon.

A feldolgozás második lépése: a rendszergazda visszavonja a jogosultságot.

A feldolgozás harmadik lépése: a rendszergazda aláírja a jelen IBSZ*{5. számú melléklet – Jogosultságigénylési űrlap}*mellékletében található, kitöltött űrlapot, valamint e-mail-en tájékoztatja a munkahelyi vezetőt a visszavonás tényéről.

V.7.3.5. A felhasználói hozzáférési jogok felülvizsgálata

Ellenőrizni kell, hogy a kiadott hozzáférési jogosultságok szintje alkalmas-e a kívánt célra (biztosítja-e az elvárt logikai védelmet). Ennek érdekében a kiosztott hozzáférési jogokat az IBF évente felülvizsgálja.

V.7.4. Hozzáférés ellenőrzés érvényre juttatása

Az elektronikus információs rendszereknek az IBSZ-szel összhangban érvényre kell juttatnia a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

V.7.5. A felelősségek szétválasztása

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

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

b) A rendszergazda nem tölthet be fejlesztő szerepet;

c) A jóváhagyó személye nem lehet azonos a végrehajtóval.

V.7.6. Legkisebb jogosultság elve

A Hivatal elektronikus információs rendszereibena jogosultságok kezelésekor a szükséges, minimum elvet kell követni, azaz mindenki csak annyi jogosultságot kapjon, ami a munkája elvégzéséhez nélkülözhetetlen.

A felhasználó a munkaállomásán nem kaphat helyi rendszergazda jogot.

V.7.7. Jogosult hozzáférés a biztonsági funkciókhoz

A Hivatal elektronikus információs rendszereiben a jelen IBSZ-ben megfogalmazott logikai védelmi intézkedések végrehajtása érdekében a következő biztonsági funkciók kerülnek megállapításra:

a) tűzfalak, behatolás-detektáló rendszerek üzemeltetése, konfigurálása;

b) kártékony kód elleni védelem üzemeltetése, konfigurálása;

c) operációs rendszerek üzemeltetése, konfigurálása;

d) EIR-ek adminisztrálása;

e) mentési rendszer üzemeltetése, konfigurálása.

V.7.8. Nem privilegizált hozzáférés a biztonsági funkciókhoz

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

V.7.9. Privilegizált fiókok

A jelen IBSZ *{V.7.7Jogosult hozzáférés a biztonsági funkciókhoz}* fejezetében meghatározott biztonsági funkciók elérésére a rendszergazda jogosult.

V.7.10. A munkaszakasz zárolása

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

V.7.11. Képernyőtakarás

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

V.7.12. A munkaszakasz lezárása

A felhasználó a munkaidő végeztével köteles a munkaállomását kikapcsolni.

V.7.13. Vezeték nélküli hozzáférés

A Hivatalban csak az IBF által jóváhagyott vezeték nélküli (továbbiakban: Wi-Fi) hozzáférési pont létesíthető. A Hivatalban ad-hocWi-Fi hálózat nem létesíthető.

Valamennyi hozzáférési pontot a Hivatal által biztosított eszközön kell létrehozni. Biztosítani kell a hozzáférési pontok felügyeletét.

Minden hozzáférési pont részére külön VLAN-t kell létrehozni, úgy hogy a hálózatok között nem lehet átjárás és az egy hálózatban lévő eszközök sem érhetik el egymást. Az internet és a belső hálózat elérése a központi tűzfalon keresztül történhet.

Valamennyi hozzáférési pont esetében szabványos, ismert sérülékenységektől mentes kriptográfiai megoldással támogatott azonosítást és hitelesítést kell alkalmazni.

A Hivatal hálózatában csak olyan Wi-Fi hozzáférési pont létesíthető, amely minimum WPA2 titkosítást alkalmaz. Kockázat elemzéssel kell meghatározni a szükséges védelmet és a megfelelő hitelesítési módszert.

A kiosztott kulcsok létrehozására vonatkozóan a következőket kell követni:

a) A kulcs hossza minimum 12 karakter.

b) A kulcs tartalmazzon kisbetűt, nagybetűt, számot vagy speciális karaktert.

A kulcsot háromhavonta meg kell változtatni.

A Hivatal belső hálózatából a munkaállomásokról és laptopokról tilos mobil internet megosztással internetelérést kezdeményezni.

V.7.14. Mobil eszközök hozzáférése

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

V.7.15. Titkosítás

A Hivatal által biztosított mobil eszközökön be kell kapcsolni a teljes eszköz vagy tároló titkosítást. A titkosításhoz szabványos, sérülékenységektől mentes kriptográfiai algoritmusokat kell alkalmazni.

V.7.16. Külső elektronikus információs rendszerek használata

A Hivatal belső elektronikus információs rendszereinek külső hozzáférése során ismert sérülékenységektől mentes titkosítású VPN kapcsolatot kell alkalmazni, melynek során egyedileg kell azonosítani a felhasználót. A munka befejeztével bontani kell a VPN kapcsolatot.

A Hivatal belső elektronikus információs rendszereinek külső hozzáféréséhez csak olyan biztonságos infokommunikációs eszköz használható, amely megfelel a következő követelményeknek:

a) Az eszközökön a felhasználóknak rendszergazdai jog nem adható.

b) Az eszközökön naprakész kártékony kód elleni védelmet kell megvalósítani.

c) Az eszközökön az operációs rendszer és a felhasználói programok naprakészségét biztosítani kell.

d) Az eszközökön bekapcsolt tűzfalat kell alkalmazni.

A felhasználók képzésénél kiemelt figyelmet kell fordítani ezen eszközök biztonságos kezelésére.

A felhasználókat egyedileg kell azonosítani és a hálózati kapcsolatot szabványos kriptográfiai módszerrel titkosítani kell.

V.7.17. Korlátozott használat

Külső elektronikus információs rendszert abban az esetben lehet a Hivatal elektronikus információs rendszereihez történő hozzáférés céljából felhasználni, hogy ha jelen IBSZ *{V.7.16.Külső elektronikus információs rendszerek használata}*pontjában foglalt követelményeket

a) egyedi felhasználás során a külső elektronikus információs rendszerbenaz IBF előzetesen ellenőrizte, vagy

b) cégszerű felhasználás során szerződésben rögzítették.

V.7.18. Hordozható adattároló eszközök

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

V.7.19. Információ megosztás

A Hivatal elektronikus információs rendszereiben kezelt adatok külső fél részére történő továbbítása előtt az érintett felhasználónak meg kell vizsgálnia, hogy a vonatkozó szerződés vagy jogszabály alapján az adat átadható-e. Különös figyelmet kell fordítani a jogszabály által védett adatok továbbítására.

Az információ megosztással kapcsolatos követelményeket az adott terület vezetőjének ismertetnie kell a felhasználókkal.

V.7.20. Nyilvánosan elérhető tartalom

Az információk közzétételével kapcsolatban a Hivatal a jogszabályokat, a vonatkozó belső szabályzatát és az erkölcsi normákat követi.

A nyilvános tartalmak kezelésével kapcsolatban a következők szerint kell eljárni:

a) Ki kell jelölni azokat a személyeket, akik jogosultak a Hivatal honlapján a Hivatal és a Hivatal működésével kapcsolatos bármely információ közzétételére;

b) A kijelölt személyeket képzésben kell részesíteni annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános (pl.: személyes adatokat, üzleti titkokat) információkat;

c) gondoskodni kell arról, hogy közzététel előtt átvizsgálásra kerüljenek a publikálandó tartalmak;

d) Időszakosan át kell vizsgálni a Hivatal honlapját a nem nyilvános információk tekintetében, és gondoskodni kell azok eltávolításáról.

V.8. Rendszer és információ sértetlenségre vonatkozó eljárásrend

Az elektronikus információs rendszerek, illetve az adatok sértetlenségére vonatkozóan a következő eljárásrendet kell alkalmazni.

V.8.1. Hibajavítás

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

A rendszergazdának biztosítania kell, hogy a rendszerszoftver naprakész állapotban legyen, és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek az üzemeltetők számára.

Az alapszoftver módosítással egy időben a változásokat a dokumentációban is át kell vezetni.

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

Új hardverek üzembe állításakor a fentieket kell értelemszerűen alkalmazni.

Gondoskodni kell arról, hogy a munkaállomásokon telepített operációs rendszerek és egyéb segédprogramok naprakészek legyenek.

V.8.1.1. Microsoft termékek biztonsági frissítéseinek telepítése

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

V.8.1.2. Nem Microsoft termékek biztonsági frissítéseinek telepítése

A nem Microsoft termékek frissítését a gyártói ajánlások figyelembe vételével kell elvégezni. A biztonsági frissítések telepítése a rendszergazda feladata.

V.8.2. Kártékony kódok elleni védelem

A Hivatalnak meg kell őriznie az elektronikus információs rendszerek és az információ bizalmasságát, sértetlenségét és rendelkezésre állását a kártékony kódok és a kéretlen üzenetek támadásaival szemben.

A kártékony kódok elleni védekezés során a következőkről kell gondoskodni:

a) Munkaállomások és kiszolgálók esetében memóriában rezidens kártékony kód elleni megoldásokat kell alkalmazni.

b) Hetente egyszer egy teljes körű, ütemezett átvizsgálást kell elvégezni.

c) Kártékony kód elleni megoldás nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem üzemeltethető.

d) Egyéb infokommunikációs eszközök tekintetében a gyártói ajánlások és a lehetőségek figyelembe vételével törekedni kell a kártékony kódok elleni védekezésre.

e) A kártékony kód elleni alkalmazások adatbázisát automatikusan frissíteni kell.

f) A kártékony kód elleni alkalmazásnak az email-ek csatolmányát ellenőriznie kell, a futtatható állományok szűrését be kell kapcsolni.

g) A hordozható számítógépek esetében az üzemeltetőnek gondoskodnia kell a kártékony kód elleni alkalmazás adatbázisának automatikus frissítéséről, közvetlenül a hordozható számítógép bekapcsolása után.

h) A külső forrásból származó a cserélhető adathordozókat használatba vétel előtt automatikus kártékony kód ellenőrzés alá kell vetni.

i) A felhasználókat meg kell ismertetni a kártékony kód felmerülésének esetében követendő előírásokkal.

j) A kártékony kód felfedezésekor teendő intézkedéseket és a jelentési rendszert szabályozni kell. A rendszergazdának értesítenie kell az IBF-et. A további teendőket az IBF határozza meg.

k) Kártékony kód általi fertőzéskor a munkaállomást haladéktalanul le kell választani a hivatali hálózatról és így kell megtenni a szükséges vírusirtást vagy a rendszer újratelepítését.

l) A vírusfertőzésekkel és elhárításukkal kapcsolatban tett intézkedéseket dokumentálni kell.

V.8.2.1. Vírusriadó

A vírusriadót az IBF javaslatára a Jegyző rendelheti el.

Abban az esetben, ha egyértelműen megállapítható, hogy a tapasztalt jelenségeket vírusfertőzés okozza, és a vírus egy-két gépet fertőzött csak meg, akkor vírusriadót nem szükséges elrendelni. A fertőzött gépeket azonnal le kell kapcsolni a hálózatról, meg kell kísérelni a vírusok kiirtását. Ha ez nem sikerül, akkor vírusriadót kell elrendelni.

Feltétlenül vírusriadót kell elrendelni a következő esetek bármelyikénél:

a) ha a szokásosnál sokkal több vírusincidens történt;

b) a vírusfertőzést magas kockázatúnak értékeli a vírusvédelmi szoftver gyártója;

c) ugyanaz a vírus fordul elő egyszerre kettőnél több gépen, különböző állományokban;

d) valamely számítógépen aktivizálódika vírus romboló rutinja, vagy a vírus valamilyen effektust (videó, hang stb.) produkál annak ellenére, hogy a vírusadatbázis frissített, a víruskereső motor működött;

e) adatátvitel során, egy számítógépen jelentkező szokványostól eltérő működés, átkerül más számítógépekre is;

f) szerver oldali vírusfertőzés esetén.

A vírusriadó idején a vírusmentesítés szakmai felügyeletét az IBF és a rendszergazdaközösen látják el.

V.8.2.2. Teendők vírusfertőzés, vírusriadó esetén

Az IBF feladata a vírus fertőzés kivizsgálásának irányítása, a felelősség megállapítása.

A rendszergazda a feladatai:

a) a vírusvédelmi rendszer támogatójának értesítése;

b) a vírus fertőzés következtében szükséges intézkedések koordinálása;

c) a fertőzés tényének és a foganatosított intézkedéseknek a rögzítése;

d) a vírusos számítógép leválasztása a hálózatról;

e) a felhasználók értesítése a vírusról;

f) az e-mail rendszer leállítása, ha mail-ben terjedő vírusról van szó;

g) a hálózaton terjedő vírus esetén a külső kapcsolat megszakítása;

h) a vírus adatait tartalmazó vírus tudásbázis letöltése és teljes vírusellenőrzés végrehajtása;

i) a fertőzöttség lehetőségeinek feltérképezése, gondolva a hálózaton, cserélhető adathordozók által, vagy e-mail-en történő fertőzésekre;

j) a kliensek frissítése;

k) manuális vírus ellenőrzés végrehajtása azokon a munkaállomásokon, amelyek megfertőződhettek;

l) amennyiben az a hivatalon kívülre is terjedhetett, értesíteni kell az érintett szervezeteket;

m) a vírus fertőzés okának kivizsgálása a vírusvédelmi szoftver támogatójával közösen.

V.8.3. Az elektronikus információs rendszer felügyelete

Az elektronikus információs rendszerek napi üzemeltetéséhez tartozik a működés felügyelete, a mentések elvégzése, illetve hiba esetén az eszközök javítását végzők bevonása.

Az elektronikus információs rendszerek felügyelete az alkalmazások, az adatbázisok, a kiszolgálók és az alapszoftverek, az informatikai hálózat és a munkaállomások működésének folyamatos figyelemmel kísérését kívánja meg.

Automatikus eszközökkel monitorozni kell a tűzfalak, a kiszolgálók, a hálózati aktív eszközök erőforrásait és az azokon futó kritikus szolgáltatásokat.

A fenti feladatok végrehajtása a rendszergazda feladata.

A rendszergazdának ismernie kell a Hivatal rendszereszközeinek, elektronikus információs rendszereinek működését és azok figyelmeztető és hibaüzeneteit. A szükséges reagálásokat tartalmazó leírást tudniuk kell alkalmazni.

A rendszergazdának rendszeresen el kell végeznie azokat a tevékenységeket, amelyek alapján meggyőződhet arról, hogy az elektronikus információs rendszer üzemszerűen működik, így különösen rendszeresen ellenőriznie kell

a) az EIR-ek működőképességét;

b) a vírusdefiníciós állományok naprakészségét;

c) a kártékony kód elleni védelem naplóállományait;

d) az EIR-ek mentésének sikeres lefutását;

e) a monitorozó eszközök riasztásait;

f) a központi tűzfal működőképességét és naplóállományait.

Az üzembiztonság érdekében a kiszolgálók operációs rendszereinek telepítőkészleteit tartalék adathordozón is tárolni kell, valamint az operációs rendszer beállításait rendszeresen menteni kell.

Az üzemeltetési eljárások megfelelőségét az információbiztonsági felülvizsgálatok alkalmával az IBF felülvizsgálja, a szükséges módosításokat átvezetik, a jegyző pedig jóváhagyja.

Az internet irányába kipublikált szolgáltatásokat behatolás detektáló/megelőző rendszerrel kell védeni.

V.8.3.1. ASP hálózati eszközök felügyelete

Az ASP rendszer eléréséhez szükséges eszközöket (ASP router, switch, szünetmentes tápegység) zárt rack szekrényben kell működtetni.

A rack szekrények kulcsait a rendszergazda őrzi.

A menedzselhető hálózati eszközök (switchek) konfigurálásánál a következőket kell elvégezni:

a) az eszközök hálózatba illesztéséről készüljön dokumentáció;

b) az eszköz gyári, alapértelmezett bejelentkezési azonosítói (név, password) kerüljenek megváltoztatásra;

c) a hozzáférési azonosítókat zárt borítékban, és biztonságosan zárható helyen kell tárolni;

d) a hálózati eszközöket csak a rendszergazda, valamint szerződésben a hálózati eszközök karbantartására kijelölt fél kezelheti;

e) az eszközök firmware frissítése a legutolsó stabil változatnak megfelelően történjen meg;

f) a menedzselhető eszközök legfrissebb konfigurációja legyen elmentve és zárható helyen tárolva;

g) az ASP rendszerhez csatlakozó munkaállomásokat menedzselhető hálózati eszközökre kell kötni;

h) ezeken az eszközökön - az idegen eszközök hálózatba történő csatlakozása elleni védelem megvalósítása érdekében - be kell kapcsolni a port security megoldást.

V.8.4. Biztonsági riasztások és tájékoztatások

A Hivatalnak az IBF útján folyamatosan figyelemmel kell kísérnie a Kormányzati Eseménykezelő Központ által kiadottriasztásokat, valamint a Nemzeti Elektronikus Információbiztonsági Hatóság által közzétett értesítéseket.

Az IBF-nek meg kell vizsgálnia, hogy az adott riasztás vagy értesítés érinti-e a Hivatalt, illetve annak elektronikus információs rendszereit és szükség esetén belső riasztást kell kiadnia az érintett szerepkörök részére.

V.8.5. Bemeneti információ ellenőrzés

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

V.8.6. A kimeneti információ kezelése és megőrzése

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

i) gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről,

j) gondoskodni kell arról, hogy a kimeneti információhoz történő fizikai és logikai hozzáférés csak az arra jogosított személyekre korlátozódik,

k) gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat,

l) biztosítani kell, hogy a megsemmisítési eljárások során az kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.

V.9. Naplózási eljárásrend

Az elektronikus információs rendszereknél a következő naplózási eljárásrendet kell kialakítani.

V.9.1. Naplózható események

Biztosítani kell, hogy az alkalmazott elektronikus információs rendszerek a következő eseményeket naplózni tudják:

a) a felhasználók adminisztrációs tevékenysége:

- bejelentkezés;
- kijelentkezés;
- jelszómódosítás.

b) az adatállományok (adatbázisok) módosítása az alkalmazási rendszerekben;

c) a rendszergazdák a rendszer bármely rétegébe történő be-és kijelentkezése;

d) a rendszergazdák tevékenysége a rendszer bármely rétegében;

e) a felhasználói jogosultságok módosítása;

f) rendszer események, esetleges hibák;

g) konfigurációs beállítások módosítása.

h) Az esemény típusának megfelelően az általános feldolgozási eseményt az eseménynaplóban, a biztonsággal összefüggő eseményeket pedig a biztonsági naplóba kell rögzíteni.

Az elektronikus információs rendszerek naplózása kialakításakor be kell vonni a rendszer adatgazdáját is, annak érdekében, hogy adatgazdai oldalról meghatározásra kerüljenek azok a többletinformációk, amelyeket az adatgazdák igényelnek.

V.9.2. Naplóbejegyzések tartalma

A naplóbejegyzéseknek a következőket kell tartalmaznia:

a) a rendszerelem azonosítóját,

b) az adatazonosítót (fájl / rekord / mező),

c) az esemény ismertetését / a funkcióazonosítót,

d) a felhasználó azonosítóját,

e) az esemény időpontját,

f) az esemény elemzéséhez szükséges adattartalmakat vagy az arra vonatkozó hivatkozásokat, illetve annak végrehajtási státuszát.

V.9.3. Időbélyegek

Az elektronikus információs rendszereknek a naplóbejegyzésekhez készített időbélyegeket a rendszer belső órái alapján kell elkészítenie.

A Hivatalnak szinkronizálnia kell az EIR-ek belső rendszer óráit a belső hálózatban kijelölt eszközhöz, a kijelölt eszköznek pedig külső, megbízható időszolgáltatóhoz kell szinkronizálnia.

V.9.4. A napló információk védelme

Az elektronikus információs rendszereknek a jelen IBSZ-ben foglaltaknak megfelelően meg kell védenie a napló információkat és a napló eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

V.9.5. A naplóbejegyzések megőrzése

A biztonsági események utólagos kivizsgálása érdekében a naplóbejegyzéseket 1 évig meg kell őrizni.

V.9.6. Naplógenerálás

Olyan elektronikus információs rendszereket kell alkalmazni, melyek

a) biztosítják a naplóbejegyzések előállítási lehetőségét a *{V.9.1.Naplózható események}* pontban meghatározott naplózható eseményekre;

b) lehetővé teszik meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az információs rendszer egyes elemeire;

c) naplóbejegyzéseket állít elő a *{V.9.2.Naplóbejegyzések tartalma}*pontban meghatározottak szerinti eseményekre az *{V.9.1.Naplózható események}*pontban meghatározott tartalommal.

V.10. Rendszer és kommunikáció védelmi eljárásrend

Az elektronikus információs rendszerek és a kommunikáció védelmére vonatkozóan a következő eljárásrendet kell alkalmazni.

V.10.1. A határok védelme

Mind a belső, mind a külső hálózati szolgáltatókhoz történő hozzáférést a következő módon kell ellenőrizni:

a) **Minden tilos, ami kifejezetten nincs megengedve!** Ez azt jelenti, hogy alaphelyzetben mindenforgalmat tiltani kell, majd csak azt megengedni, amelyre valóban szükség van.

b) A belső hálózat irányából az internet irányába kapcsolatot csak azokra a protokollokra/szolgáltatásokra engedélyezünk, amelyre szükség van.

c) Kifejezetten tiltani kell a belső hálózat irányából az internet irányába a levelezési (SMTP) kapcsolatokat. Levelet továbbítani csak a levelező szerveren keresztül szabad.

d) Megfelelő interfészt kell alkalmazni a Hivatal és más szervezet tulajdonában lévő, vagy nyilvános hálózat között;

e) Ellenőrizni kell a felhasználók információszolgáltatáshoz való hozzáférését.

f) A Hivatal belső hálózatáról Internet kapcsolat kizárólag jóváhagyott tűzfalakon keresztül létesíthető.

g) Biztosítani kell, hogy a Hivatal elektronikus információs rendszerei alapértelmezés szerint ne legyenek elérhetők az Internet felől. Amelyeknél az Internet felöli hozzáférés szükséges igény, ott kizárólag biztonságos és ellenőrzött kapcsolaton keresztül történhet hozzáférés.

h) Minden Internet elérést naplózni kell, annak érdekében, hogy kellő mennyiségű információt lehessen összegyűjteni a szabálytalan internetes tevékenységek detektálása és kiderítése érdekében.

i) Figyelni kell és 1 héten belül telepíteni kell a tűzfal operációs rendszere/firmware-e biztonsági frissítéseit.

j) Kiemelt figyelmet kell fordítani a tűzfal operációs rendszere biztonsági frissítéseinek figyelésére és telepítésére.

k) A tűzfalat úgy kell konfigurálni, hogy az utasítsa el a port letapogatási próbálkozásokat.

A felhasználóknak tilos az Internet felhasználási szabályait és biztonsági beállításait megváltoztatni, illetve megkerülni.

A felhasználók kizárólag jóváhagyott szoftvereket használhatnak az Internet elérésére.

Az IBF köteles ellenőrizni, hogy a felhasználók számára biztosított az Internet elérést lehetővé tevő szoftverek mentesek a komolyabb biztonsági hibáktól.

A Hivatal központi tűzfalát csak a belső hálózatból vagy a konzolról lehet adminisztrálni. A külső hozzáférés nem engedélyezett.

A fentiek végrehajtása érdekében tűzfal biztonsági politikát kell készíteni, mely tartalmazza a

a) tűzfal kialakítására vonatkozó követelményeket,

b) a tűzfalon engedélyezett portokat, protokollokat és szolgáltatásokat,

c) a tűzfal adminisztrálásával kapcsolatos feladatokat és felelősségi köröket

d) a tűzfal biztonsági politikában foglaltak ellenőrzését.

V.10.1.1. A hálózati szolgáltatások belső használatának szabályozása

A Hivatal elektronikus információs rendszerében a felhasználók csak azokhoz a hálózati szolgáltatásokhoz férhetnek hozzá, amelyek használata a munkavégzésükhöz feltétlenül szükségesek.

A hálózatokkal és a hálózati szolgáltatásokkal kapcsolatosan az alábbiakat kell figyelembe venni:

a) a felhasználókkal meg kell ismertetni azoknak a hálózatoknak és hálózati szolgáltatásoknak a felsorolását, amelyeket igénybe vehetnek;

b) a hálózati kapcsolatokhoz és szolgáltatásokhoz való hozzáférés védelmére szolgáló óvintézkedések és eljárások tartalmazzanak bejelentkezési védelmet vagy más, az alkalmazások jogosításának ellenőrzésére szolgáló védelmet;

A hálózati szolgáltatások használatával kapcsolatos szabályozást összhangban kell tartani a hozzáféréseket meghatározó követelményekkel.

A Hivatal elektronikus információs rendszerében TILOS modemet csatlakoztatni.

V.10.1.2. Hálózat szegmentálás

A Hivatal hálózatában az infokommunikációs szolgáltatásokat, felhasználókat és elektronikus információs rendszereket szegmentálni kell. A külső felhasználók Internet irányából csak a szükséges elektronikus információs rendszereket érhetik el. A belső hálózatot tűzfal válassza el a többi zónától.

Az Internet és a Hivatal elektronikus információs rendszere közötti hálózati forgalom szűrésére, a lehetőségek korlátozására tűzfalak, tartalomszűrők, illetve meghatározott címekkel a kapcsolat tiltását biztosító megoldások szolgáljanak.

V.10.1.3. A hálózati összeköttetések ellenőrzése

A hálózatok hozzáférését szabályozni, a felhasználók felkapcsolódási lehetőségeit korlátozni kell.

Az Internet és a Hivatal elektronikus információs rendszere közötti hálózati forgalom ellenőrzésére a tűzfalak naplói szolgáljanak.

V.10.1.4. A hálózati üzenettovábbítás ellenőrzése

A hálózati üzenettovábbítás ellenőrzését a tűzfalaknak, illetve kapcsolódó tartalomszűrő és címfordító megoldásoknak, valamint azok naplóinak kell biztosítaniuk.

V.10.1.5. Nyilvános elektronikus információs rendszerek védelme

A Hivatal honlapját web hosting szolgáltató működteti, ezért a vele kötött szerződésben elő kell írnia nyilvánosan elérhetőtartalmakkal és rendszerekkel kapcsolatos információbiztonsági követelményeket.

V.10.2. Kriptográfiai kulcs előállítása és kezelése

A kriptográfiai kulcsok védelmének módját a kriptográfiai eszközök biztonságos használatát garantáló szabályozásban kell kidolgozni, az adott elektronikus információs rendszer használatba vételét megelőzően.

A vonatkozó szabványoknak vagy szabványként elfogadott előírásoknak megfelelő kulcsgondozó rendszerek használhatók. A belső előírásokat kriptográfiai utasításban, illetve a megfelelő alkalmazás leírásaiban kell meghatározni.

V.10.3. Kriptográfiai védelem

A Hivatalnak az elektronikus információs rendszereiben az adatok sértetlenségének és bizalmasságának védelmére a vonatkozó mértékadó dokumentumokban biztonságosnak minősített kriptográfiai műveleteket kell alkalmaznia.

A Hivatalban a következő kriptográfiai megoldások engedélyezettek:

a) Szimmetrikus kulcsú titkosítás esetén: AES 126, 192, 256,

b) Aszimmetrikus kulcsú titkosítás: RSA 2048 bit,

c) elektronikus aláírás: RSA: 2048 bit vagy ECDSA (pLEN 256 bit),

d) Kulcscsere: Diffie-Helmann 2048 bit,

e) Lenyomatolás: SHA1, SHA 2, SHA3 (minimum 256 bit)

f) Jelszótárolás: PBKDF2,scrypt, bcrypt.

V.10.3.1. A kriptográfiai óvintézkedések használatának szabályzata

A Hivatalelektronikus információs rendszereiben a kriptográfiai eszközök bevezetése esetén ki kell dolgozni az eszközök biztonságos használatát garantáló szabályozást, melynek a következőket kell tartalmaznia:

a) az eszközök védelmét biztosító előírások;

b) az eszközök felhasználására vonatkozó követelmények;

c) a kulcsok generálására, elosztására, tárolására és megsemmisítésére vonatkozó szabályok;

d) a rejtjelzett adatok visszaállításának szabályai és eljárásai azokra az esetekre, amikor a kulcs megsérült vagy elveszett.

V.10.3.2. Kriptográfiai megoldások alkalmazásának feltételei

A Hivatal elektronikus információs rendszereiben csak olyan kriptográfiai megoldások alkalmazhatók, amelyek:

a) a vonatkozó szabványoknak vagy szabványként elfogadott előírásoknak megfelelő kriptográfiai algoritmusokat és protokollokat használnak;

b) az implementációt külső független szakértő auditálta;

c) alkalmazását az IBF jóváhagyta.

V.10.4. Együttműködésen alapuló számítástechnikai eszközök

A Hivatal elektronikus információs rendszereiben együttműködésen alapuló számítástechnikai eszközt (pl.: kamera, mikrofon) csak akkor lehet aktiválni/használni, ha azt a felhasználó előzőleg jóváhagyta.

V.10.5. A folyamatok elkülönítése

A Hivatal elektronikus információs rendszereiben csak olyan modern, gyártó által támogatott operációs rendszerek használhatóak, amelyek biztosítják az elkülönített végrehajtási tartomány fenntartását minden végrehajtó folyamat számára.

VI. Mellékletek

1.számú melléklet – Értelmező Rendelkezések

2.számú melléklet – A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása

3. számú melléklet –Biztonsági események jelentése

4. számú melléklet – Kockázatelemzési és kezelési módszertan

5. számú melléklet – Jogosultságigénylési űrlap

6. számú melléklet – Hozzáférések nyilvántartása űrlap

7. számú melléklet – Felhasználói Informatikai Biztonsági Házirend

8. számú melléklet – Felhasználói Nyilatkozat

9. számú melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén

10. számú melléklet – Titoktartási Nyilatkozat

1. számú melléklet – Értelmező Rendelkezések

Az IBSZ-ben használt, és a gyakorlatban alkalmazott, az információbiztonság tárgykörébe tartozó kifejezések, meghatározások megfelelnek az Ibtv., a Közigazgatási Informatikai Bizottság 25. számú ajánlása Magyar Információbiztonsági Ajánlások és az MSZ ISO/IEC 27001:2006 szabvány és jelen IBSZ 4.1 fejezetében meghatározott jogszabályok által használt kifejezéseknek, és értelmezésük is azonos ezekkel.

(1) Adat: Az információ megjelenési formája, azaz a tények, elképzelések nem értelmezett, de értelmezhető közlési formája.

(2) Adatállomány: Valamely elektronikus információs rendszerben lévő adatok logikai összefogása, amelyet egy névvel jelölnek. Ezen a néven keresztül férhetünk hozzá a tartalmazott adatokhoz.

(3) Adatbiztonság: Az adatok jogosulatlan megismerése és kezelése (másolás, módosítás, törlés stb.) elleni szervezési és adminisztratív intézkedések, fizikai védelmi eszközök, műszaki és logikai megoldások összehangolt rendszere.

(4) Adatgazda: Felelős azért, hogy az adott adat teljes életciklusa folyamán az adat megvédéséhez a megfelelő biztonság teljesüljön. Az adatgazda joga és kötelessége, hogy a dolgozók részére meghatározza a munkájuk elvégzéséhez minimálisan szükséges hozzáférés szintjét az adatokhoz.

(5) Alapszintű védelem: Egy elektronikus információs rendszer vagy szervezet számára létrehozott minimális védelem.

(6) Auditálás: Az elektronikus információs rendszer biztonsági mechanizmusainak, a számítógépes tevékenységeknek független szakértők által történő átvizsgálása IT biztonsági szempontból, továbbá a rendszer-ellenőrzések megfelelősségének vizsgálata, a kialakított biztonsági stratégia és a működtetési eljárások megfelelősségének megállapítása céljából.

(7) Azonosítás és hitelesítés: Az adott elektronikus információs rendszer biztonsági mechanizmusok segítségével azonosítja és hitelesíti a hozzá fordulókat, mielőtt valamelyik szolgáltatást biztosítaná. Azonosításra és hitelesítésre három dolog alkalmas: amit az egyed ismer (pl. jelszó, PIN-kód), amit az egyed birtokol (pl. intelligens kártya) és ami az egyed sajátossága (pl. biometrikus jellemzők).

(8) Bizalmasság: az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról.

(9) Biztonsági audit napló: A biztonsági auditáláshoz gyűjtött, és esetleg fel is használt adatok.

(10) Biztonsági kockázat: A fenyegetettség mértéke, amely megmutatja, hogy valamely fenyegetés milyen mértékű kárt okozhat, ha kihasználja az elektronikus információs rendszer sebezhetőségét.

(11) Biztonsági mechanizmus: Eljárási módszer, eszköz vagy megoldási elv, ami azt a célt szolgálja, hogy egy vagy több biztonsági követelmény teljesüljön.

(12) 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

(13) Elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt ada-

tok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

(14) Elégséges-védelem: A védelem akkor kielégítő erősségű (mértékű), ha a védelemre akkora összeget és olyan módon fordítanak, hogy ezzel egyidejűleg a releváns fenyegetésekből eredő kockázat a szervezet számára még elviselhető szintű vagy annál alacsonyabb.

(15) E-személyi: Olyan hatósági igazolvány, amely a polgár személyazonosságát és a vonatkozó jogszabályban meghatározott adatait közhitelesen igazolja, illetve a polgár törvényben meghatározott esetekben gyakorolhatja vele a külföldre utazás jogát. Az állandó személyazonosító igazolvány emellett – új elemként – alkalmas a polgár elektronikus úton történő közhiteles azonosítására, valamint a vonatkozó jogszabályokban meghatározott kivételekkel – a polgár kérelmére – elektronikus aláírás létrehozására.

(16) Felelősségre vonhatóság: Az elektronikus információs rendszer biztonsági mechanizmusai biztosítják, hogy az elektronikus információs rendszerrel kapcsolatba kerülő emberek (felhasználók, operátorok, üzemeltetők, külső munkatársak stb.) a biztonsággal kapcsolatos tevékenységükért utólag felelősségre vonhatók.

(17) Felhő-alapú tárhely-szolgáltatás: A szolgáltatásokat nem egy dedikált hardvereszközön üzemeltetik, hanem a szolgáltató eszközein elosztva, a szolgáltatás üzemeltetési részleteit a felhasználótól elrejtve. Ezeket a szolgáltatásokat a felhasználók hálózaton keresztül érhetik el, publikus felhő esetében az interneten keresztül, privát felhő esetében a helyi hálózaton vagy az interneten.

(18) Fenyegetés: Egy fenyegető tényező lehetősége arra, hogy véletlenül vagy szándékosan kiváltson, kihasználjon egy adott sebezhetőséget. Ez gyakorlatilag egy elektronikus információs rendszeren, vagy tevékenységen belüli bármilyen szoftver, információ, hardver, adminisztratív, fizikai, kommunikációs, vagy személyzeti erőforrás megsértésének vagy elvesztésének a lehetőségét jelenti.

(19) Fenyegetettség elemzés: Az a folyamat, amely felsorolja, jellemzi a vizsgált folyamatok és erőforrások fenyegetettségét (azaz a releváns fenyegetéseket, megvalósíthatóságuk nehézségét)

(20) Fenyegető tényező: Olyan körülmény vagy esemény, amely az adat, illetve információ valamely elektronikus információs rendszerben történő feldolgozásának rendelkezésre állását, sértetlenségét, bizalmasságát vagy hitelességét illetve az elektronikus információs rendszernek és az elektronikus információs rendszer elemeinek működőképességét fenyegetheti. A fenyegető tényezők közé soroljuk nemcsak a személyektől eredő támadásokat, amelyek valamely elektronikus információs rendszer ellen irányulnak, hanem valamennyi szélesebb értelemben vett fenyegetést, mint például véletlen eseményeket, külső tényezők általi behatásokat és olyan körülményeket, amelyek általában magának az informatikának a sajátosságaiból adódnak (pl. tűz, áramkimaradás, adatbeviteli hibák, hibás kezelés, hardver tönkremenetele, kártékony kódok, alkalmazáshibák).

(21) Folytonos védelem: Folytonos a védelem, ha az az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul.

(22) Helyreállítás: Egy szolgáltatás akkor tekinthető helyreállítottnak, ha a felhasználó újra képes az adott szolgáltatást igénybe venni, azaz az elektronikus információs rendszer és a rendelkezésre álló adatok visszaállítása megtörtént, a szükséges teszteket elvégezték, a felhasználót minderről tájékoztatták.

(23) Hitelesség: A hitelesség az adat olyan biztonsági jellemzője, amely arra vonatkozik, hogy az adat (bizonyíthatóan) egy elvárt forrásból származik. Ehhez szükséges, hogy az informatikai kapcsolatban lévő partnerek kölcsönösen (és egyértelműen) felismerjék egymást, és ez az állapot a kapcsolat teljes ideje alatt fennálljon.

(24) Információs vagyonelemek: Az információs vagyonelemek közé az elektronikus információs rendszer különböző jellegű összetevői tartoznak, például: fizikai infrastruktúra, számítástechnikai eszközök, alkalmazások, adatbázisok és adatállományok, archivált adatok, rendszerdokumentáció, használói és kezelői kézikönyvek, oktatási anyagok, üzemviteli, üzemeltetési és támogató eljárások, tartalékolási elrendezések stb.

(25) Információbiztonság: az elektronikus információs rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelynek védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

(26) Kockázat áthárítása: A kockázat kezelés olyan módja, amelynél a kockázatokat (káros hatásokat) megosztjuk egy másik (külső) szervezettel.[3]

(27) Kockázat becslés: Olyan folyamat, amely a releváns fenyegetések szintjét és hatását értékkel jellemzi és megállapítja a fenyegetések szintje, hatásuk, illetve a védelmi igények[4] alapján a kockázatok szintjét.

(28) Kockázat elkerülése: A kockázat kezelés olyan módja, amelynél a felelős vezető úgy dönt, hogy a kockázatos helyzetet eredményező tevékenységet a szervezet nem folytatja tovább.

(29) Kockázat ellenőrzés: Kockázat menedzsment során hozott döntéseket megvalósító tevékenységek tartoznak a kockázat ellenőrzés körébe. Ilyen lehet a kockázatok felülvizsgálata, rendszeres ellenőrzése, illetve a kockázat menedzsment elvárásoknak való megfelelés fenntartása.

(30) Kockázat felmérés: A kockázat elemzést és kockázat kiértékelést átfogó folyamat.

(31) Kockázat felmérési beszámoló: A kockázat felmérés eredmény termékének (dokumentumának) neve, amely a kockázatok ismertetésére szolgál.

(32) Kockázat ismertetés: A döntéshozók és az érintett felek közötti, kockázatokról szóló információ csere vagy tájékoztatás.

(33) Kockázat kezelési terv: A kockázat kezelés eredmény termékének (dokumentumának) neve, amely a kockázat kezelést biztosító intézkedéseket ismerteti[5].

(34) Kockázat kiértékelés: Folyamat, amely során a megbecsült kockázatok összevetésre kerülhetnek a tolerálható szinttel.[6]

---

[3] Törvényi előírások és jogszabályok megtilthatják a kockázat áthárítását. A kockázat áthárítására jó példa a biztosításkötés. Fenyegetett adatok, folyamatok átadása nem kockázat áthárítás (hanem elkerülés).

[4] Olyan súlyozó szempont, amely az érintett felek szemszögéből az érintett adatok és folyamatok érzékenységét, sérülésének közvetlen vagy közvetett kárát fejezi ki.

[5] Tartalmazhatja a kockázat kezelés módját és kiválasztásának indoklását; tevékenységek prioritási rendjét; erőforrás és költségbecslést; mérföldkövek és ütemezés kijelölését; a megvalósítás és ellenőrzés felelőseinek, illetve időpontjainak kijelölését stb..

[6] A kockázatok elviselhetőségének mérlegelését jelenti, melyben segítséget nyújt a jelen dokumentum kockázat kiértékelési fejezetében ismertetett un. tolerancia mátrix.

(35) Kockázat megtartás: A kockázat kezelés olyan módja, amelynél a lehetséges káros hatásokat (tehát a kockázatokat) a szervezet elfogadja bekövetkezésük esetén.[7]

(36) Kockázat optimalizálása: A kockázat kezelés olyan módja, amelynél a kockázatokat csökkentjük a fenyegetések szintjének és / vagy lehetséges hatásuk csökkentésével, amíg az elfogadható szintre nem csökken.

(37) Kockázatcsökkentés: intézkedések, amelyeket egy kockázattal kapcsolatos valószínűség vagy a negatív következmények (vagy mindkettő) enyhítésére hoztak

(38) Kockázatkezelés: Azoknak a biztonsági kockázatoknak az elfogadható költségen történő minimalizálása vagy megszüntetése, amelyek hatással lehetnek elektronikus információs rendszerekre.

(39) Kockázattal arányos védelem: A kockázatokkal arányos a védelem, ha egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel.

(40) Kriptográfia: az információ titkos, az illetéktelen hozzáféréssel szemben biztonságos feldolgozásának és továbbításának elmélete és gyakorlata.

(41) Letagadhatatlanság: Az elektronikus információs rendszer biztonsági mechanizmusai biztosítják, hogy az elektronikus információs rendszerrel kapcsolatos tevékenységek letagadhatatlanok. Ezt a funkciót titkosítási (rejtjelezési) és digitális aláírási technikákra alapozzák.

(42) Maradványkockázat: Az a kockázat, ami a kockázatcsökkentés után megmarad.

(43) Megkerülhetetlenség: Az elektronikus információs rendszer biztonsági mechanizmusai biztosítják, hogy a védelmet nem lehet kijátszani, azaz az elektronikus információs rendszer egyetlen eleme sem hagyható ki vagy nem kerülhető meg az elektronikus információs rendszer.

(44) Rendelkezésre állás: Az elektronikus információs rendszerelem – ide értve az adatot is – tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszerelem a szükséges időben és időtartamra használható.

(45) Sértetlenség fenntartása: Biztosítják, hogy az adatot, információt vagy alkalmazás csak az arra jogosultak változtathatják meg, azok észrevétlenül nem módosulhatnak, illetve nem semmisíthetők meg.

(46) Sértetlenség:Az adat tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes, és bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.

(47) Sérülékenység, sebezhetőség: Egy információs vagyon, vagy vagyon csoport gyengesége, hibája vagy hiányossága, amellyel egy fenyegetés vissza tud élni.

(48) Szoftver-vagyontárgyak: A szoftver-vagyontárgyak közé tartoznak: alkalmazási szoftverek, rendszerszoftverek, fejlesztési segédprogramok stb.

(49) Teljes körű védelem: Teljes körű a védelem, ha az az elektronikus információs rendszer összes elemére kiterjed.

(50) Tenant: Az önkormányzati ASP rendszerhez történő csatlakozással bevezetett fogalom: Felhasználók csoportja, akik hozzáférnek a részükre biztosított jogosultságoknak megfelelően az ASP rendszer által nyújtott szolgáltatásokhoz.

[7] A kockázatok kiértékelése során felhasznált szempont rendszer ebben segítséget nyújthat.

(51) Változás-felügyelet: Eljárások, amelyek biztosítják, hogy minden változtatás ellenőrzött legyen, beleértve annak kérelmezését, rögzítését, elemzését, a vonatkozó döntés meghozását, jóváhagyását, kivitelezését és a változtatás megvalósítás utáni áttekintését is.

(52) Zárt felhasználói kör: Az elektronikus információs rendszer biztonsági mechanizmusai mindenkit kizárnak az elektronikus információs rendszer adott szolgáltatásából, kivéve azokat, akik számára az kifejezetten engedélyezett.

(53) Zárt szolgáltatási kör: Az elektronikus információs rendszer biztonsági mechanizmusai biztosítják, hogy minden informatikai szolgáltatás tilos az adott elektronikus információs rendszerben, kivéve az, ami kifejezetten engedélyezett.

(54) Zárt védelem: Zárt a védelem, ha az az összes releváns fenyegetést figyelembe veszi.

2. számú melléklet – A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása

A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása

EIR megnevezése	EIR leírása	EIR adatgazdája	EIR-ben kezelt adatok	EIR biztonsági osztályba sorolása		
				Bizalmasság	Sértetlenség	Rendelkezésre állás
ÖNKADÓ (archív)	helyi adó nyilvántartás	Jegyző	adóügyek	**2**	**2**	**2**
KATWAWIN (archív)	vagyonkataszter	Jegyző	tárgyi eszközök, ingatlanok, földterületek	**2**	**2**	**2**
WINSZOC	szociális ügyek nyilvántartása	Jegyző	személyi adatok, szociális ügyek előzményei, állapota	**2**	**2**	**2**
Govsys iratkezelő (archív)	iktatórendszer	Jegyző	érkeztetés, iktatás, iratkezelés	**2**	**2**	**2**
Gordius pénzügyi rendszer (archív)	pénzügyi-számviteli rendszer	Jegyző	pénzügyi-számviteli adatok	**2**	**2**	**2**
ASP – KERET (tervezett)	Önkormányzati ASP – keretrendszer	Jegyző	Hivatali felhasználók adatai, A Hivatal szervezeti adatai, Üzleti naplók, Rendszerhasználati statisztikák, Migrációs adatok, E-learning tananyagok	**4(2)**[8]	**4(2)**	**4(2)**
ASP – ADÓ (tervezett)	Önkormányzati ASP – önkormányzati adórendszer	Jegyző	személyes adatok, adóbevételek, adókönyvelés	**4(2)**	**4(2)**	**4(2)**

[8] Az önkormányzati ASP rendszer esetében a Magyar Államkincstár elvégezte a szakrendszerek biztonsági osztályba sorolását. A zárójelben található biztonsági osztályok a Hivatal saját adataira vonatkozik.

EIR megnevezése	EIR leírása	EIR adatgazdája	EIR-ben kezelt adatok	EIR biztonsági osztályba sorolása		
				Bizalmasság	Sértetlenség	Rendelkezésre állás
ASP – BUGNET (tervezett)	Önkormányzati ASP – támogató rendszer (hibajegykezelő)	Jegyző	személyes adatok, bejelentett hibák	**2(2)**	**2(2)**	**2(2)**
ASP – GAZDÁLKODÁS (tervezett)	Önkormányzati ASP – gazdálkodási rendszer	Jegyző	pénzügyi-számviteli adatok, személyes adatok	**3(2)**	**3(2)**	**3(2)**
ASP – HAGYATÉK (tervezett)	Önkormányzati ASP – hagyaték leltár rendszer	Jegyző	személyes adatok, vagyoni adatok	**3(2)**	**3(2)**	**3(2)**
ASP – INGATLANVAGYONKATASZTER (tervezett)	Önkormányzati ASP – ingatlan vagyon-kataszter rendszer	Jegyző	ingatlan adatok	**3(2)**	**3(2)**	**3(2)**
ASP – IPAR ÉS KERESKEDELEM (tervezett)	Önkormányzati ASP – ipar és kereskedelmi rendszer	Jegyző	üzletek, rendezvények, telephelyek ügyintézéséhez szükséges adatok	**3(2)**	**3(2)**	**3(2)**
ASP – IRATKEZELŐ (tervezett)	Önkormányzati ASP – iratkezelő rendszer	Jegyző	ügyiratok	**3(2)**	**3(2)**	**3(2)**
ASP – PORTÁL (tervezett)	Önkormányzati ASP – települési portál rendszer, elektronikus ügyintézési rendszer, elektronikus űrlapszolgáltatás	Jegyző	elektronikus ügyintézéssel kapcsolatos adatok	**3(2)**	**3(2)**	**2(2)**
ASZA	Anyakönyvi rendszer	Jegyző	személyes adatok	**2**	**2**	**2**
NVR	Nemzeti Választási Rendszer	Jegyző	személyes adatok	**2**	**2**	**2**

3. számú melléklet –Biztonsági események jelentése

A biztonsági esemény megnevezése:

A tapasztalás helye és idő pontja:

Az érintett személyek megnevezése:

Az esemény pontos leírása:

Az észlelő neve:

Dátum:_____év___hó___nap ....

Észlelő aláírása IBF aláírása

Az esemény kivizsgálásának leírása:

Tett intézkedés leírása:

Az intézkedés életbelépésének időpontja:

Végleges-e az intézkedés:

☐	*Igen*
☐	*Nem*

Igényel-e kockázatelemzést az esemény:

☐	*Igen*
☐	*Nem*

Dátum:_____év___hó___nap ....

Információbiztonsági felelős aláírása jegyző aláírása

4. számú melléklet – Kockázatelemzési és kezelési módszertan

Kockázatelemzési és kezelési módszertan

A jelen dokumentum célja, hogy a jelen IBSZ*{III.1.4. Kockázatelemzés}* fejezetében foglalt követelmények végrehajtásának módját leírja.

Vagyonleltár

Az elektronikus információs rendszerekre ható fenyegetettségek különbözőek, attól függően, hogy az elektronikus információs rendszer melyik összetevőjét fenyegetik.

A fenyegetettségek megfelelő azonosítása érdekében a létre kell hozni és értelemszerűen fel kell tölteni a következő vagyonelem csoportokat a Hivatal vagyonelemeivel:

a) Környezeti infrastruktúra
b) Hardver
c) Szoftver
d) Adatok
e) Dokumentumok
f) Humán erőforrások

Helyzetfelmérés

Az információbiztonsági kockázatelemzés elvégzéséhez fel kell mérni, meg kell ismerni az elektronikus információs rendszereket és azok környezetét, valamint azok jelenlegi információbiztonsági szintjét.

A következő területeket kell a dokumentációk bekérésével, illetve szakmai interjúk lefolytatásával megismerni:

a) Adminisztratív védelmi intézkedések
    i. A Hivatalra vonatkozó jogszabályok, szabályzatok
    ii. Az elektronikus információs rendszerre vonatkozó szabályzatok
    iii. Szerződések, külső felek kezelése
    iv. Alkalmazásfejlesztés, változáskezelés
    v. Jogosultságigénylés
    vi. Biztonsági események kezelése
    vii. Üzemeltetési eljárások
    viii. Szervizelés, eszközcsere, selejtezés
b) Logikai védelmi intézkedések
    i. Mentési megoldások
    ii. Kártékony kód elleni védekezés
    iii. Biztonsági frissítések telepítése
    iv. Hálózat felépítése
    v. Biztonsági rendszerek
    vi. Kriptográfiai megoldások
c) Fizikai biztonság
    i. Beléptetés
    ii. Számítógépterem kialakítása
    iii. Épületben történő közlekedés
    iv. Irodák kialakítása, tiszta asztal, üres képernyő politika.

Gyenge pontok meghatározása

A helyzetfelmérés alapján megszerzett információk birtokában meg kell határozni az egyes vagyonelemek gyenge pontjait.

Fenyegetettségek elemzése

Az egyes vagyonelemek gyenge pontjaira bizonyos fenyegetettségek hatnak.

Az informatikai erőforrásokra ható fenyegetettségek vagy fenyegető tényezők (például: üzleti hírszerzés, rosszindulatú hackerek, természeti katasztrófák) mindig a sérülékeny pontokon keresztül fejtik ki hatásukat, így az ellenük való védekezés legfőbb eleme a sérülékenységek azonosítása és megszüntetése.

Az egyes vagyonelemek gyenge pontjait és fenyegetettségeit *{KIB 25. számú ajánlása: 25/1-3. kötet: Az Információbiztonság Irányításának Vizsgálata (IBIV) 1.0 verzió a „gyenge pontok" és a „fenyegetettségek"}*segédletei alapján érdemes azonosítani.

Sérülékenységek elemzése

A sérülékenység egy bizonyos gyenge pont kihasználása a rá ható fenyegetettség által. Meg kell vizsgálni, hogy a beazonosított gyenge pontokon keresztül mely fenyegetettségek tudják kifejteni a káros hatásukat.

Kárérték szintek kialakítása, károk rávetítése a vagyonelemekre

A következő kárérték szintek kerültek meghatározásra:

Kárérték szint	Kár leírása
1	1-es biztonsági osztályba sorolt EIR sérülhet vagy egyéb jelentéktelen kár
2	Egy adott 2-es biztonsági osztályba sorolt EIR sérül
3	Több 2-es biztonsági osztályba sorolt EIR sérül
4	A Hivatal valamennyi 2-es biztonsági osztályba sorolt EIR-re sérül
5	Önkormányzati ASP, ASZA vagy Választási rendszer sérül

A kockázatok megállapításához az elektronikus információs rendszerek vagyonelemeire rá kell vetíteni a kárérték szinteket.

A bekövetkezési valószínűségek meghatározása

Következő lépésként meg kell becsülni a sérülékenységek bekövetkezési valószínűségét.
A bekövetkezési valószínűséghez a következő értékeket kell használni:

- „5" - bármikor bekövetkezhet
- „4" - gyakori
- „3" – közepes
- „2" - ritka
- „1" –nagyon ritka

Kockázatok meghatározása

Az információbiztonsági kockázatokat a sérülékenység bekövetkezésének a valószínűsége és az okozott kár szorzata fogja megadni.

A kockázatok minősítéséhez a következő kockázati mátrixot kell definiálni:

		Bekövetkezési valószínűségek				
		1	2	3	4	5
Kárértékek	5	A	K	M	NM	NM
	4	A	K	M	NM	NM
	3	NA	A	K	M	M
	2	NA	A	A	K	K
	1	NA	NA	NA	A	A

A kockázatok jelölése a következő:

- NA - Nagyon alacsony
- A – Alacsony
- K – Közepes
- M – Magas
- Nagyon magas

Elviselhető kockázatok meghatározása

A Hivatal azt a döntést hozta, hogy minden közepes, illetve közepesnél nagyobb kockázatot kezelni kíván.

Ennek megfelelően a toleranciamátrix a következő:

		Bekövetkezési valószínűségek				
		1	2	3	4	5
Kárértékek	5	T	NT	NT	NT	NT
	4	T	NT	NT	NT	NT
	3	T	T	NT	NT	NT
	2	T	T	T	NT	NT
	1	T	T	T	T	T

A táblázatban alkalmazott jelölések értelmezése a következő:

- T – Tolerálható
- NT – Nem tolerálható

Kockázatok kezelése

A nem tolerálható kockázatokat kezelni kell. A Hivatal a kockázatokat a következőképpen kezeli:

a) Megfelelő intézkedésekkel csökkenti a fenyegetés bekövetkezési gyakoriságát vagy hatását (Kockázat csökkentés);
b) Tudatosan, a következményeket felmérve elfogadja a kockázatot (Kockázat elfogadás);
c) Elkerüli a kockázatot azáltal, hogy az érintett tevékenységet felfüggeszti (Kockázat elkerülés);

d) Áthárítja a kockázatot például biztosítással, vagy megfelelő beszállítói szerződésekkel. (Kockázat áthárítás).

Kockázatcsökkentő intézkedések

A PreDeCo elv alapján a kockázatcsökkentés három szemszögből közelíthető meg:

a) Megelőző jellegű (preventív kontrollok)

A hibák, gyengeségek, sérülékenységek, illetve ezek kihasználására való lehetőségek kiküszöbölése.

b) Korlátozó vagy javító (korrektív kontrollok)

Egy veszély hatását csökkentő, enyhítő óvintézkedések, további tevékenységek szükségessége nélkül.

c) Észlelő és reagáló (detektív kontrollok)

A sebezhetőségek támadásának észlelése, ártalmas kihatások enyhítésére, illetve válaszreakciók kidolgozása.

Intézkedési terv

Az el nem viselhető kockázatok kezelésére a Hivatalnak intézkedési tervet kell készítenie az egyes feladatok mellé rendelt felelős, határidő és esetleg költség feltüntetésével.

Az intézkedései tervet az IBF készíti elő a rendszergazda bevonásával és a jegyző hagyja jóvá.

5. számú melléklet – Jogosultságigénylési űrlap

Hozzáférési jogok igénylése űrlap

Iktatószám:

JOGOSULTSÁGIGÉNYLŐ ADATAI

Igénylő neve: .....

Szervezeti egység: .....

Telefon: .....

Email: .....

Igényelt művelet

Elektronikus információs rendszer megnevezése:.....

Jogosultság kezdete: ..... Jogosultság vége: .....

Új jogosultság
Jogosultság törlése
Jogosultság módosítása

Egyéb:.....
.....
.....

INDOKLÁS

A jogosultságigényléshez kapcsolódó feladatellátás megnevezése:
.....
.....

Kelt: ....
igénylő aláírása

Munkahelyi vezetői jóváhagyás

Vezető: .....
Beosztása: ....
Kelt: ..... vezető aláírása

Adatgazdai jóváhagyás

Adatgazda: ....
Kelt ..... adatgazda aláírása

A jogosultságot beállító aláírása

Rendszergazda: ....
Kelt ..... rendszergazda aláírása

6. számú melléklet – Hozzáférések nyilvántartása űrlap

Sorszám	Iktatószám	Felhasználó neve	Igényelt jogo-sultság	Igénylés dátuma	Munkahelyi vezető

Felhasználói Informatikai Biztonsági Házirend

1. ÁLTALÁNOS RÉSZ

1.1. A Felhasználói Informatikai Biztonsági Házirend célja

A Felhasználói Informatikai Biztonsági Házirend (a továbbiakban: FIBH) célja, hogy aSárbogárdi Polgármesteri Hivatal(továbbiakban: a Hivatal) elektronikus információs rendszereinek felhasználói részére előírja az információbiztonsági előírások rájuk vonatkozó részét.

A Hivatal elektronikus információs rendszereinek védelme érdekében a Hivatal kidolgozta az Informatikai Biztonsági Szabályzatát.

Az Informatikai Biztonsági Szabályzat (továbbiakban: az IBSZ) tartalmazza valamennyi információbiztonsággal kapcsolatos szabályt, melynek betartásával az érintettek által elvárt szinten tartható a Hivatal elektronikus információs rendszereinek és az azokban kezelt adatok biztonsága.

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

1.2. A FIBH általános követelményei

A FIBH előírásainak alkalmazása, betartása, illetve betartatása, a jelen IBSZ*{I.2.1. Szervezeti-személyi hatály}* **pontban megjelöltek számára kötelező. A szabályok be nem tartása jogi, munkaügyi, illetve szerződésben meghatározott következményeket vonhat maga után. A FIBH el nem olvasása vagy nem ismeretenem mentesít a felelősség alól.**

Az információbiztonsági előírások betartása megvédi a Hivatalt és a jelen IBSZ*{I.2.1. Szervezeti-személyi hatály}* pontban kifejtett személyi hatály alá eső felhasználóit, ügyfeleit, partnereit, adataik ésinformációik jogosulatlan vagy véletlenszerű nyilvánosságra jutásától, módosításától, megrongálódásától, megsemmisülésétől.

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

A Hivatal elektronikus információs rendszereit csak a jelen IBSZ *{8. számú melléklet – Felhasználói Nyilatkozat}*mellékletében található nyilatkozat aláírása után lehet használatba venni.

A Hivatal a FIBH-t az IBSZ-szel együtt folyamatosan fejleszti és tökéletesíti.

2. BEVEZETÉS

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

A Hivatal elvégezte a jogszabályok által előírt módon az elektronikus információs rendszereinek biztonsági osztályba sorolását, melynek során valamennyi elektronikus információs rendszert besorolta egy 1-5-ig terjedő skálán. Az elektronikus információs rendszer biztonsági osztálya adja meg a védelem elvárt szintjét.

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

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

3. A FELHASZNÁLÓ JOGAI, KÖTELESSÉGEI ÉS FELELŐSSÉGE

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

3.1. A felhasználó jogai

A felhasználó jogosult:

a) a számára biztosított infokommunikációs eszközök, szoftverek üzemszerű használatára,

b) a beállított jogosultságának megfelelően, a munkájához szükséges adatállományok elérésére,

c) információbiztonsági képzésre,

d) a működtetéshez szükséges támogatás igénylésére, a munkavégzéshez szükséges általa nem ismert szoftverek használatához támogatást kérni,

e) meghibásodás, üzemzavar esetén az elhárítás igénylésére.

3.2. A felhasználó kötelessége

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

Amennyiben a felhasználó olyan adatokhoz fér hozzá, amelyek kezelésében nem illetékes, a hibát jeleznie kell munkahelyi vezetőjének.

Valamennyi alkalmazott köteles azonnal értesíteni a rendszergazdátminden olyan körülményről, ami az informatikához kapcsolódó tevékenység fennakadásához, megszakadásához vezethet. A rendszergazda szükség esetén értesíti az információbiztonsági felelőst, aki megteszi a további, szükséges intézkedéseket.

Valamennyi információbiztonsággal kapcsolatos észrevételt vagy szabályszegésre vonatkozó feltételezést haladéktalanul jelenteni kell az információbiztonsági felelősnek.

Minden felhasználónak bizalmasan kell kezelnie valamennyi felhasználói azonosítót, jelszót, eToken-t, kulcsot, vagy bárminemű egyéb, a Hivatal erőforrásaihoz hozzáférést biztosító eszközt.

A személyi azonosító kódokat, jelszavakat szigorúan titokban kell tartani. Még a közeli munkakapcsolatban álló, egymást jól ismerő kollégák sem közölhetik ezeket egymással. A hozzáférési kódok a rendszergazdáknak sem adhatók ki és a rendszergazdáknak nincs is joga ezeket elkérni.

Az önkormányzati ASP központtól kapott szoftveres tanúsítvány nem adható át az önkormányzati ASP központ által fel nem jogosított személynek. A tanúsítványhoz tartozó jelszót tilos másnak elárulni.

Az információbiztonsági hiányosságok megelőzése céljából a felhasználók kötelesek rámutatni az információbiztonsági szint romlására, illetve annak lehetőségére, és a tapasztalatokat a további problémák elkerülésében felhasználni.

Az információbiztonságot veszélyeztető események kivizsgálására irányuló felülvizsgálatokban a felhasználó köteles együttműködni a kivizsgálókkal.

A Hivatal infokommunikációs eszközei és elektronikus információs rendszerei kizárólag hivatali munkavégzés céljából használható, azok magáncélú használata tilos!

A Hivatal a vonatkozó adatvédelmi jogszabályok figyelembevételével jogosult a felhasználó hivatalos elektronikus levelezését és internetforgalmát vizsgálni.

A felhasználó számára büntetőjogi, illetve munkajogi felelősségre vonás terhe mellett tilos illetéktelenül más felhasználó jogosultságainak használata, a hálózat monitorozása, felderítése, jelszavak kipróbálása, illetve ezek kísérlete is.

A Hivatalban az alkalmazottak csak a Hivatal tulajdonát képező informatikai eszközöket és engedélyezett szoftvereket használhatják. Ettől eltérni csak a jegyző engedélyével lehet.

A rendszergazdát kivéve, tilos a Hivatal számítógépeire szoftvereket telepíteni, és azokat futtatni.

Kizárólag a munkavégzéshez szükséges adathordozók használata engedélyezett.

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

a) az érzékeny információt tartalmazó nyomtatványok ne maradjanak a készülékben;

b) illetéktelenek ne férhessenek hozzá, mert belső tárolóikban tárolódott üzenetek visszahívhatók, így illetéktelenek kezébe kerülhetnek;

c) véletlen vagy szándékos átprogramozás során az üzenetek egy nem megfelelő számra kerülhetnek;

d) félretárcsázás vagy hibásan tárolt szám miatt az üzenetek illetéktelen személyhez kerülnek.

3.3. A felhasználó felelőssége

A felhasználó felelősséggel tartozik:

a) a szabályok betartásáért;

b) a birtokában lévő, vagy tudomására jutott információk bizalmasságának megfelelő kezeléséért;

c) a személyére szóló és védett területre belépést biztosító kártyájának/kártyáinak védelméért és át nem ruházásáért;

d) az elektronikus információs rendszerben végzett műveletekért;

e) a Hivatal infokommunikációs eszközeinek (számítógép, nyomtató, scanner, stb.) szakszerű kezeléséért;

f) a személyi használatra átvett eszközök megfelelő fizikai védelméért.

3.4. A felhasználó jogai

A felhasználó jogosult:

a) a számára biztosított infokommunikációs eszközök, szoftverek üzemszerű használatára;

b) a beállított jogosultságának megfelelően, a munkájához szükséges adatállományok elérésére;

c) információbiztonsági képzésre;

d) a működtetéshez szükséges támogatás igénylésére, a munkavégzéshez szükséges általa nem ismert szoftver eszközökhöz támogatást, képzést kérni;

e) meghibásodás, üzemzavar esetén a lehető legrövidebb időn belüli elhárítás igénylésére.

4. AZ INFORMÁCIÓ KEZELÉSÉNEK SZABÁLYAI

4.1. Munkaállomások hozzáférés védelme

A felhasználó munkaállomást csak saját nevével és jelszavával belépve használhat. Harmadik fél csak a munkaállomás nevesített felhasználója vezetőjének előzetes írásbeli engedélyével használhat munkaállomást, ebben az esetben is a személyesen hozzárendelt azonosító használatával. Hibaelhárítás vagy támogatás esetén a rendszergazda saját azonosítójával a felhasználó engedélyével a felhasználó munkaállomására beléphet.

A felhasználónak rendszergazdai jog nem adható!

4.2. A hozzáférés kiosztás folyamata

Az informatikai rendszerekbe belépést lehetővé tevő azonosítót a vezető igényli a felhasználóknak, az IBSZ *{V.7.3Hozzáférési jogok igénylésének eljárásrendje}*fejezetében leírt folyamat szerint.

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

Az önkormányzati ASP szakrendszereihez történő csatlakozás többtényezős hitelesítéssel történik. A felhasználónak rendelkeznie kell E-személyi-vel, valamint kártyaolvasóval.

Az E-személyihez csak a hozzá tartozó PIN kód megadásával lehet hozzáférni. A sikeres azonosítást és hitelesítést követően az ASP rendszer az egyes szakrendszerekhez történő hozzáférés során további azonosító adatokat (felhasználói név, jelszó) kérhet.

4.3. Hálózati hozzáférés, hozzáférés az egyes alkalmazói programokhoz

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

A Hivatal infokommunikációs eszközein működtetett szoftvereket és alkalmazói rendszereket a felhasználó a számára beállított jogosultságnak megfelelően használhatja az alábbiak szerint:

a) A felhasználó a számítógépbe/hálózati szolgáltatások eléréséhez személyre szóló azonosítót és jelszót kap, mely a belépéshez szükséges bizalmas információkat tartalmaz.

b) Az azonosító és a megfelelő erősségű és titokban tartott jelszó használatával a belépő védelemmel rendelkezik a nevében történő visszaélések ellen, ezért a személyre szóló azonosítót és jelszavát szigorúan védeni kell, és a kezdeti jelszót első bejelentkezéskor meg kell változtatni.

A felhasználói jelszavak képzéséhez az alábbi szabályokat kell betartani:

a) A jelszó legalább nyolc karakter hosszú legyen, és tartalmaznia kell kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;

b) a jelszavakat 90 naponta meg kell változtatni,

c) az előző jelszavak újra használatát kerülni kell.

A felhasználói jelszavak alkalmazásakor az alábbi szabályokat kell betartani:

a) a felhasználó a jelszavát köteles titokban tartani,

b) a jelszószabályok betartása minden felhasználónak jól felfogott érdeke. A felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el az informatikai rendszerben,

c) a felhasználói jelszót TILOS leírni,

d) ha bármilyen jel mutat arra, hogy a jelszó kompromittálódhatott, azonnal meg kell változtatni és értesíteni kell az információbiztonsági felelőst,

e) nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé, pl. makróra, vagy funkció billentyűre;

f) a jelszó minél komplexebb, annál kisebb a valószínűsége, hogy nevünkben visszaélést követnek el.

A felhasználói jelszavak képzésénél az alábbi szempontokat kell betartani:

a) könnyen megjegyezhető, és nehezen kitalálható legyen;

b) semmi olyasmin ne alapuljon, aminek alapján valaki kitalálhatja, ilyenek a nevek, telefonszámok, születési dátumok, stb.;

c) ne legyen a gépnévre vagy a felhasználói névre utaló;

d) ne legyen sorozat.

4.4. Hozzáférés védelem mobil infokommunikációs eszköz esetén

A mobilitás miatt sokkal nagyobb veszélynek kitett mobil infokommunikációs eszközök esetében is jelszót kell használni a rendszerbe történő belépéshez. Bár ez a védelem megnehezíti a hozzáférést, a merevlemezt (winchestert) eltávolítva az ott nyíltan tárolt adatok így is megszerezhetők.

A fentiek miatt fokozottan kell törekedni ezen eszközök fizikai védelmére is az elvesztés, illetve ellopás ellen.

Külső munkahelyen történő feladat elvégzése után a keletkezett adatokat a hálózati meghajtóra kell menteni.

A mobil infokommunikációs eszközökről a feleslegessé vált adatokat le kell törölni.

Nyilvános helyeken történő használatnál ügyelni kell arra, hogy illetéktelenek ne olvashassák el a képernyő tartalmát, az eszközhöz illetéktelenek ne férhessenek hozzá.

Mobil infokommunikációs eszközök esetén rendszergazda jog felhasználónak nem adható.

4.5. Adatmentések, az adathordozók nyilvántartása és tárolása

Az adatokat nem a helyi munkaállomáson, hanem a „központi fájlszerver" megfelelő könyvtáraiban kell tárolni, ahol biztosított azok rendszeres mentése és biztonságos tárolása. Minden felhasználó számára rendelkezésre áll a „Saját" könyvtár a saját adatok tárolására, illetve minden iroda rendelkezik külön könyvtárral a szervezeti egységen belül keletkező és közösen kezelendő adatok tárolására. A nem megfelelő könyvtárba mentés a felhasználó felelőssége.

A rendszergazda nem vállal felelősséget a helyi gépen tárolt adatokért.

A rendszergazda a „központi fájlszerver"-en tárolt ügyviteli adatokról meghatározott módon és gyakorisággal mentést készítenek. Ebből adódóan lehetőség van az állományok, adattáblák statikus visszaállítására a mentés időpontjának megfelelő tartalommal. Folyamatok előre-, illetve visszagörgetésére a rendszer nincs felkészítve. Speciális mentési igényekről a rendszergazdát írásban értesíteni kell, és egyeztetni kell a kivitelezés lehetőségéről.

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

A feljegyzésnek tartalmaznia kell a visszaállítani kívánt adat:

a) utoljára ismert pontos helyét;

b) megnevezését, és a

c) visszaállítandó időpontot.

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

4.6. Adathordozók kezelése

Az eszközhasználatot, a Hivatal elektronikus információs rendszereihez történő csatlakoztatása után, a Hivatal minden előzetes értesítés nélkül figyelheti, monitorozhatja.

A Hivatal informatikai infrastruktúrájából kivitt adatok biztonságát ebben az esetben is biztosítani kell a következő védelmi intézkedésekkel:

a) Otthoni számítógép esetén gondoskodni kell az operációs rendszer és az egyéb irodai alkalmazások naprakészségéről;

b) Az operációs rendszerbe épített helyi tűzfalat be kell kapcsolni;

c) Kémprogram elleni védekezéssel ellátott, naprakész vírusvédelemmel kell rendelkezni.

d) A napi munkavégzéshez használt felhasználói azonosítónak rendszergazda jog nem adható.

A Hivatal az informatikai rendszerében használt adathordozókat információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozhatja.

5. FELHASZNÁLÓK SZÁMÍTÓGÉPES KÖRNYEZETE

5.1. Számítógépek és a hálózat kezelési előírásai

A felhasználó felelős az infokommunikációs eszközön általa végzett, nyilvánvalóan szakszerűtlen beavatkozásának következményeiért.

A felhasználó semmilyen infokommunikációs eszközt nem telepíthet a Hivatal elektronikus információs rendszerébe.

A Hivatal által biztosított infokommunikációs eszközök elhelyezését, telepítési módját nem változtathatja meg, azok borítását nem bonthatja meg, a konfigurációját nem módosíthatja. A Hivatal által biztosított infokommunikációs eszközökre szoftvert (ideértve a csak másolással telepíthető szoftvereket is) nem telepíthet, nem törölhet, és nem módosíthat.

A felhasználónak infokommunikációs eszköz, illetve szoftver telepítési igényével a rendszergazdát kell megkeresnie. Az igénylést a munkahelyi vezetővel egyeztetve a jegyző hagyja jóvá.

A rendszergazda bizonyos szoftver elemek telepítését központi szétosztással, automatikusan végzi. Az ilyen távolról történő frissítéskor meg kell várni a frissítés befejeződését, a folyamatot leállítani tilos. El kell fogadni, hogy ez alatt az idő alatt a számítógép valamivel lassabban működik.

A Hivatal belső hálózatához idegen infokommunikációs eszköz nem csatlakoztatható.

5.2. Internethasználat, web böngészés

Az Internet és a web böngészés használatának főbb szabályai:

Az Internethez való kapcsolódás csak és kizárólag a munkavégzést szolgálja!

A felhasználók kizárólag jóváhagyott szoftvereket használhatnak az Internet elérésére.

A nem munkavégzést szolgáló hálózati sávszélesség foglalása (pl. nagyméretű állományok letöltése), és adatok kiszolgálón történő tárolása esetén a felhasználó figyelmeztetésben részesül. Ismételt előfordulás esetén az rendszergazda jelentést tesz az IBF-nek, aki eljár az ügyben a jegyző felé.

Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, kiiktatása. Ebbe a körbe tartoznak a vírusellenőrző és Internet böngésző kontrollok is.

Tilos az IBF engedélye nélkül külső féllel nem web alapú hálózati kapcsolat kialakítása (pl.: FTP).

Tilos az elektronikus információs rendszerek használata a hivatali értékekkel összhangban nem álló célokra, vagyis pl. szexuális jellegű fájlok fogadására, küldésére, fenyegetésre vagy megfélemlítésre, megkülönböztetésre, gyűlölködésre, fegyverekkel és illegális drogokkal való kereskedésre, erőszakra, internetes- illetve szerencsejátékokra, bármilyen kereskedelmi illetve jogellenes tevékenységre.

Tilos nem a munkavégzést szolgáló közösségi oldalak látogatása.

Tilos a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele.

Főszabály szerint tilos hivatali adatok tárolására külföldi felhő-alapú tárhely-szolgáltatást igénybe venni. Amennyiben külföldi felhő-alapú tárhely-szolgáltatás igénybe vételére van szükség, úgy előzetesen engedélyeztetni kell a Nemzeti Elektronikus Információbiztonsági Hatósággal, de ebben az esetben is csak EGT tagállamon belüli adatkezelés, illetve adatfeldolgozás lehetséges.

Az internetről csak hivatali célból lehet fájlokat letölteni! Tilos fájlletöltő szolgáltatások használata. Különösen tilos jogvédett, illetve illegális tartalmak, fájlok letöltése, tárolása!

Az internetes oldalak elérése monitorozásra és naplózásra kerülhet, a munkával összefüggésbe nem hozható oldalak elérhetőségét az informatikai üzemeltetés jogosult korlátozni.

5.3. E-mail használat

A Hivatal által biztosított elektronikus levél cím és az elektronikus levelezési szolgáltatás kizárólag hivatali munkavégzés céljára biztosított, ezért a felhasználóknak tilos a hivatali e-mail címüket nem hivatali minőségben használni (pl.: regisztráció letöltési weboldalakra, on-line játék oldalakra, közösségi oldalakra, az Interneten elérhető nyilvános chat-és fórum oldalakon hivatali email címmel hozzászólni stb.)!

A Hivatal által nem támogatott levelezőrendszer (pl.: Gmail, Freemail) használata munkavégzésre nem engedélyezett.

Az e-mail a munkavégzéssel kapcsolatos levelezést szolgálja, ahol az egy felhasználóra eső tárterület korlátozott, és ennek túllépése esetén a rendszer figyelmeztetést küld, további figyelmeztetési határok átlépése esetén pedig megszűnhet a további levelezési lehetőség.

Az elektronikus levelek és csatolmányok védelmi előírásai megegyeznek az egyéb dokumentumok védelmének előírásaival.

A Hivatal elektronikus levelező rendszeréből elküldött elektronikus levél önmagában nem használható kötelezettség vállalására, illetve annak visszaigazolására.

A Hivatal elektronikus levelező rendszeréből csak akkor lehet bizalmas, jogszabály által védett adatot, titkot (személyes adatok, különleges adatok, adótitok stb.) elküldeni, hogy ha szabványos, sérülékenységektől mentes kriptográfiai algoritmussal az adat titkosításra került.

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

A felhasználónak tilos a postafiókjában kezelt elektronikus levelek automatikus vagy manuális továbbítása más, külső elektronikus levelező rendszerbe (pl.: a saját magán email címére).

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

Ismeretlen helyről származó e-mail-ek esetében fokozott óvatossággal kell eljárni, mert maga a levél vagy annak csatolmánya kártékony lehet.

6. VÍRUSVÉDELEM

6.1. A vírusvédelem alkalmazásának előírásai

A rendszergazda a számítógépek vírusok elleni védelmére rendszeresen frissített vírusvédelmi rendszert, és anti-spyware programot üzemeltet. Ez a védelem kiterjed a kiszolgálók, munkaállomások valamint a teljes Internet és elektronikus levélforgalom folyamatos ellenőrzésére.

Új vírus megjelenése esetén még így is előfordulhat fertőzés, valamint csatolmányok, CD és DVD lemezek, cserélhető adathordozók, illetve internetről letöltött fájlok használata esetében.

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

Dokumentumok esetében lehetőség szerint kerülni kell a makrók megnyitását, külső forrásból érkező dokumentumok esetében pedig nem szabad engedélyezni.

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

6.2. Teendők vírusgyanú esetén

Vírusgyanú esetén a felhasználó köteles azonnal felhívni a rendszergazdát, aki ellátja utasítással, vagy intézkednek a jelzés továbbításáról az információbiztonsági felelős felé.

7. AZ INFORMATIKAI ESZKÖZÖK FIZIKAI VÉDELME

7.1. Számítógép használatának előírásai

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

7.2. „Üres asztal - tiszta képernyő" politika

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

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

b) A felhasználó a munkaállomását zárolni köteles (a Ctrl +Alt +Del billentyűk, majd Zárolás), ha azt őrizetlenül hagyja;

c) A munkavégzés befejeztével a munkaállomásból ki kell jelentkezni, illetve ki kell azt kapcsolni;

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

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

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

g) Ügyfelet és más külső felet nem szabad felügyelet nélkül az irodában hagyni.

7.3. Mobil infokommunikációs eszközök védelme

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

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

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

c) a mobilitás és a kis méret miatt a mobil infokommunikációs eszközök fokozottan vannak kitéve lopásveszélynek. Gondoljunk erre, és ne hagyjuk őrizetlenül autóban, szállodai szobában stb. (zárjuk el fizikailag, használjuk, ha lehet az értékmegőrzőt, ha nincsenek érzékeny adatok a gépen).

7.3.1. Mobil infokommunikációs eszközök ellopása

A mobil infokommunikációs eszközök ellopása esetén:

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

b) értesíteni kell a rendőrséget;

c) értesíteni kell a szálloda vezetését, ha a számítógépet a szállodai szobából vagy a szálloda területén álló kocsiból lopták el;

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

7.3.2. Infokommunikációs eszköz elvesztése

Bármely infokommunikációs eszköz eltűnését a lehető leggyorsabban jelenteni kell a munkahelyi vezetőnek és az információbiztonsági felelősnek és tájékoztatni kell őket arról, hogy a berendezés tartalmaz-e bárminemű érzékeny információt. (Előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban is megerősítve.)

8. INFORMÁCIÓBIZTONSÁGI ESEMÉNYEK KEZELÉSE

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

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

b) a rendszer hibás működése vagy túlterhelések (Dos-támadás);

c) emberi hibák;

d) a szabályzatoknak vagy irányelveknek való nem megfelelés;

e) a fizikai biztonsági rendelkezések megsértése;

f) nem ellenőrzött rendszerbeli változások;

g) a szoftver vagy hardver hibás működése;

h) hozzáférési előírások megsértése;

i) kártékony kód általi fertőzés;

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

k) a bizalmasság és sértetlenség megsértése;

l) az elektronikus információs rendszerrel való visszaélés.

8.1. Jelentés a biztonsági eseményekről

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

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

A biztonságot érintő eseményekről szóló jelentések elkészítésére az IBSZ*{3. számú melléklet – Biztonsági események jelentése}* mellékletét kell használni.

8.2. Jelentés a szoftverzavarokról

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

A jelentéshez az IBSZ *{3. számú melléklet –Biztonsági események jelentése}* mellékletét kell használni. Szoftverzavarok esetén legalább a következő feladatokat végre kell hajtani:

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

b) be kell szüntetni az adott számítógép használatát.

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

A hibaelhárítást és helyreállítást a rendszergazda hajthatja végre.

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

8. számú melléklet – Felhasználói Nyilatkozat

Nyilatkozat

Alulírott (név: ,.....beosztás:..... ..... szervezeti egység: .....), kijelentem, hogy Sárbogárdi Polgármesteri HivatalInformatikai Biztonsági Szabályzatának és/vagy Felhasználói Informatikai Biztonsági Házirendjének tartalmát megismertem és elfogadom, hogy azt munkám során betartom, illetve betartatom (vezetők esetén).

....., 2018. .....

.....
Aláírás

9. számú melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén

Információbiztonsági tájékoztatás

1. Tájékoztatom, hogy aSárbogárdi Polgármesteri Hivatallal (továbbiakban: a Hivatal) fennálló köztisztviselői jogviszonya megszűnésének napjától, 201... . .....-től a Hivatal elektronikus információs rendszereihez való hozzáférési jogosultsága megszűnik. Legkésőbb ezen a napon köteles a használatában lévő, a Hivatal elektronikus információs rendszerével kapcsolatos valamennyi eszközt hiánytalanul, sértetlenül munkáltatója részére visszaszolgáltatni.

2. A Hivatalban működő elektronikus információs rendszereket a Hivatal kizárólag hivatali munkavégzés céljából biztosítja a munkatársak részére, az elektronikus információs rendszerekben keletkező és ott tárolt, kezelt adatok, információk vonatkozásában a Hivatal fenntartja magának a tulajdonjogot.

3. A Hivatalnak továbbra is hozzáférési lehetősége van az Ön által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz.

4. Közszolgálati jogviszonyának megszűnését követően nem jogosult a Hivatal elektronikus információs rendszereiben tárolt, közszolgálati jogviszonya folytán készített, illetve megismert adatokat felhasználni, azokat további személyek tudomására hozni, valamint a megismert és használt elektronikus információs rendszerek összetételéről, felépítéséről, működéséről további személyek számára bárminemű információt közölni.

5. A 4-es pontban megfogalmazott jogellenes magatartásnak polgári- és büntetőjogi következményei lehetnek.

6. Jelen tájékoztatás célja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 41/2013. (VII.15.) BM rendelet 3. § (1) bekezdésében foglaltak szerint, az e rendelet 3. számú mellékletében meghatározott követelményeknek a 4. számú melléklet 3.1.6.4.1.3.pontjában meghatározott módon való megvalósítása.

Sárbogárd, 201 ... .

.....
jegyző

A fenti tájékoztatást tudomásul vettem:

Sárbogárd, 201.....

.....
köztisztviselő neve

.....
aláírása

10. számú melléklet – Titoktartási Nyilatkozat

TITOKTARTÁSI NYILATKOZAT

Alulírott

Név: .....

Anyja neve: .....

Lakcím: .....

Sz. ig. szám: .....

a ..... munkatársa kijelentem, hogy

a**Sárbogárdi Polgármesteri Hivatal,** mint **Megrendelő,**

valamint.....

mint**Vállalkozó**

között

.....tárgyú,

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

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

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

Sárbogárd, 201 .....

.....

Nyilatkozó

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