U111

MONOR VÁROS ÖNKORMÁNYZATA

Informatikai (IT) Biztonsági Szabályzata

Érkezett: 2019 MÁJ. 3
27-526-1/2019
Melléklet:
Másolat:

Monor, 2018. december 14.

Tartalomjegyzék

I. Általános rész

1. Az IBSZ célja és hatálya

1.1. Az IBSZ célja

Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) célja, hogy a Monori Önkormányzat, intézményei és az Önkormányzat tulajdonában álló gazdasági társaságok (továbbiakban: az Önkormányzat) vezetői és munkatársai számára egyértelműen meghatározza az információbiztonsággal kapcsolatos feladatokat és kötelezettségeket.

Az Önkormányzat tevékenységének ellátásához használt informatikai rendszer biztonsága és kockázattal arányos védelme kiemelt fontossággal bír. Ezért az Önkormányzatnak ki kell alakítania a tevékenységének ellátásához használt informatikai rendszer biztonságával kapcsolatos szabályozási rendszerét és gondoskodnia kell az informatikai rendszer kockázatokkal arányos védelméről.

Az információbiztonsági szabályozás célja a következő:

a) Az Önkormányzat információs- és adatvagyonának védelme,

b) Költséghatékonysági elemzés alapján műszaki megoldások segítségével az információbiztonsági szint fejlesztése

c) Az információbiztonsági szabályok betartásának elősegítése és a tudatosság fejlesztése

1.2. Hatály

1.2.1. Szervezeti-személyi hatály

Az IBSZ szervezeti hatálya kiterjed az Önkormányzat összes szervezeti egységére valamint az önkormányzat tulajdonában álló gazdasági társaságokra, intézményeire:

Monor Város Önkormányzatára,

A Monori Polgármesteri Hivatal:

a) Polgármester

b) Alpolgármester

c) Jegyző

d) Aljegyző

e) Jegyzői Iroda

f) Építéshatósági Iroda

g) Műszaki, Városgazdálkodási és Környezetvédelmi Iroda

h) Pénzügyi Iroda, Adócsoport

valamint az Önkormányzat intézményei közül:

i) Monori Bölcsőde

j) Monori Petőfi Óvoda

k) Monori Kossuth Lajos Óvoda

l) Monori Napsugár Óvoda

m) Monori Szivárvány Óvoda

n) Monori Tesz-Vesz Óvoda

o) Dr. Borzsák István Városi Könyvtár és Helytörténeti Kiállítás

p) Monori Gondozási Központ

q) Monor Város Önkormányzata Védőnői szolgálat

továbbá:

r) Vigadó Kulturális és Civil Központ Nonprofit Kft.

s) Monori Városfejlesztő Nonprofit Kft.

t) Monori Sportcsarnok Üzemeltető Nonprofit Kft.

u) Kövál Nonprofit Zrt.

A szabályzat személyi hatálya kiterjed minden Önkormányzati munkavállalóra, köztisztviselőre, közalkalmazottra vagy szerződéses partnerre, aki az Önkormányzat informatikai rendszereit használja, vagy azokhoz hozzáfér.

1.2.2. A felelős vezető személye

Az Önkormányzat felügyelete alá tartozó intézmények, tulajdonában lévő gazdasági társaságok esetén az IBSZ szerinti felelős vezetői szerepkör az alábbiak szerint kerül kijelölésre:

Szervezet/Intézmény / Vállalat megnevezése	**Felelős vezető**
Monor Város Önkormányzata	Jegyző
Monori Polgármesteri Hivatal	Jegyző
Monori Bölcsőde	Intézményvezető
Monori Petőfi Óvoda	Intézményvezető
Monori Kossuth Lajos Óvoda	Intézményvezető
Monori Napsugár Óvoda	Intézményvezető
Monori Szivárvány Óvoda	Intézményvezető
Monori Tesz-Vesz Óvoda	Intézményvezető
Dr. Borzsák István Városi Könyvtár és Helytörténeti Kiállítás	Intézményvezető
Monori Gondozási Központ	Intézményvezető
Monor Város Önkormányzata Védőnői Szolgálat	Vezető védőnő
Vigadó Kulturális és Civil Központ Nonprofit Kft.	Ügyvezető
Monori Városfejlesztő Nonprofit Kft.	Ügyvezető
Monori Sportcsarnok Üzemeltető Nonprofit Kft.	Ügyvezető
Kövál Nonprofit Zrt.	Vezérigazgató

1.2.3. Tárgyi hatály

Az IBSZ tárgyi hatálya kiterjed az Önkormányzat adatait tároló, feldolgozó vagy az adatok továbbítását végző összes informatikai eszközre, rendszerre vagy folyamatra illetve az ezekben tárolt vagy feldolgozott adatokra.

1.2.4. Területi hatály

Az IBSZ területi hatálya kiterjed az Önkormányzat alábbi épületeire, illetve az általuk használt helyiségekre:

a) Monor Város Önkormányzata,

b) Monori Polgármesteri Hivatal

c) Monori Bölcsőde

d) Monori Petőfi Óvoda

e) Monori Kossuth Lajos Óvoda

f) Monori Napsugár Óvoda

g) Monori Szivárvány Óvoda

h) Monori Tesz-Vesz Óvoda

i) Dr. Borzsák István Városi Könyvtár és Helytörténeti Kiállítás

j) Monori Gondozási Központ

k) Monori Védőnői szolgálat

l) Vigadó Kulturális és Civil Központ Nonprofit Kft.

m) Monori Városfejlesztő Nonprofit Kft.

n) Monori Sportcsarnok Üzemeltető Nonprofit Kft.

o) Kövál Nonprofit Zrt.

1.2.5. Időbeni hatály

Jelen IBSZ a kiadás napján lép hatályba és változtatás nélkül határozatlan ideig érvényes.

2. Az IBSZ felülvizsgálata

Az IBSZ-t legalább évente egy alkalommal kötelezően felül kell vizsgálni. Az IBSZ felülvizsgálatát az Informatikai Biztonsági Felelős (továbbiakban IBF) kezdeményezi és végzi el. Az IBSZ felülvizsgálatát minden évben olyan ütemezéssel kell elkezdeni és a felülvizsgálatot valamint a frissített szabályzat kiadását elvégezni, hogy az új szabályzat NEIH felé történő frissítés és elfogadtatása a tárgyév végéig be tudjon fejeződni.

Az IBSZ soron kívüli felülvizsgálatára van szüksége:

- ha az Önkormányzat elektronikus információs rendszereiben az információbiztonsági követelményeket és szabályokat is érintő változások következnek be,
- ha az Önkormányzat elektronikus információs rendszereinek működését meghatározó jogszabályi környezetben változások következnek be.

2.1. Hatásköri és illetékességi szabályok

Az IBSZ az *1.2.1. Szervezeti-személyi hatály* fejezetben szereplő személyeken felül az Önkormányzat elektronikus információs rendszerével kapcsolatban álló (felhasználó vagy szolgáltató, Adatfeldolgozó) vállalkozások, személyek ismerhetik meg. További félnek csak az adott intézmény felelős vezetőjének engedélyével adható tovább.

3. Kapcsolódó dokumentumok

3.1. Jogszabályok

a) 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről

b) 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról

c) 2012. évi I. törvény a munka törvénykönyvéről

d) 2012. évi C. törvény a Büntető Törvénykönyvről

e) 2013. évi V. törvény a Polgári Törvénykönyvről

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

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

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

i) 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenység vizsgálat lefolytatásának szabályairól

j) 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

k) 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)

l) 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről

m) 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)

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

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

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

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

r) 1999. évi LXXVI. törvény a szerzői jogról

s) 2001. évi XXXV. törvény az elektronikus aláírásról

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

3.2. Kapcsolódó szabványok, ajánlások

a) MSZ ISO/IEC 27002:2011: Az információbiztonság irányítási gyakorlatának kézikönyve

b) MSZ ISO/IEC 27001:2006: Az információbiztonság irányítási rendszerei. Követelmények

c) NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations

d) A KIB 25. számú ajánlása: Magyar Információbiztonsági Ajánlások (MIBA) 1.0 verzió

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

f) A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár

g) Általános szerződési feltételek a PKI szolgáltatásokhoz (ÁSZF-PKI) v1.6

h) Szolgáltatási szabályzat a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz (HSZSZ-ESZIG) v1.3

i) Hitelesítési rend a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz (HR-ESZIG) v1.3

j) Időbélyegzés Szolgáltatási Rend (ISZR) v1.2

k) Szolgáltatási szabályzat a minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz (HSZSZ-M) v1.6

l) Tájékoztatás az önkormányzati ASP rendszerhez csatlakozáshoz megvalósítandó informatikai biztonsági követelményekről 1.0 (2017. október 9.)

3.3. Az IBSZ-hez kapcsolódó belső dokumentumok

a) Szervezeti és Működési Szabályzat
b) Iratkezelési Szabályzat
c) Selejtezési Szabályzat
d) Adatvédelmi szabályzat

4. Az IBSZ általános követelményei

Az IBSZ betartása minden a *2.1. Hatásköri és illetékességi szabályok* bekezdésben részletezett személy vagy szervezet számára kötelező.

A szabályok be nem tartása jogi, munkaügyi, illetve szerződésben meghatározott következményeket vonhat maga után. Az IBSZ meg nem ismerése nem mentesít a felelősség alól.

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

Az informatikai rendszerek használatának megkezdése előtt a felhasználóknak nyilatkozatot kell tenniük az IBSZ-ben foglalt szabályok betartásáról és elfogadásáról.

A felhasználói nyilatkozatot az IBSZ 6. sz. melléklete tartalmazza.

II. Az Önkormányzat információbiztonsági követelményei

Az Önkormányzatnál használt elektronikus információs rendszere biztonsági besorolását a 2. sz. melléklet tartalmazza.

Az IBSZ-ben dokumentált követelmények a 3-as biztonsági osztályt igénylő informatikai rendszerek védelmi igényinek figyelembe vételével készült.

Az IBSZ kiadását követően fel kell mérni az IBSZ-ben meghatározott védelmi intézkedések állapotát és cselekvési tervet kell készíteni a védelmi intézkedések teljesítése érdekében.

Az állapotfelmérést és a cselekvési tervet az IBSZ kiadását követő 90 napon belül el kell végezni.

III. Adminisztratív védelmi intézkedések

5. Biztonsági osztályba sorolás

Az Önkormányzatnak a

- 2013. évi L. törvény 7. § (3) bekezdése
- 2013. évi L. törvényben meghatározott technológiai biztonsági
- valamint a 41/2015. (VII. 15.) BM rendelet 1. számú melléklete alapján

biztonsági osztályba kell sorolnia az Önkormányzat szervezetét (szervezet biztonsági szint) valamint az Önkormányzat elektronikus információs rendszereit.

5.1. Biztonsági osztályba sorolás

A biztonsági osztályba sorolást a bizalmasságra, sértetlenségre és rendelkezésre állásra vonatkozóan külön-külön egy 1-től 5-ig tartó skálán kell értékelni az elektronikus információs rendszer kockázatelemzési eredményeinek figyelembe vételével.

Az elektronikus információs rendszer kockázatelemzését az alábbi szempontok alapján kell elvégezni:

a) Relatív kár

b) Kezelt/Sérült adat típusa és mennyisége

c) A kár hogyan befolyásolja a szervezet ügymenetét

d) Társadalmi / Politikai hatás

e) Anyagi kár mértéke a szervezet költségvetésének százalékában

f) Az információ rendszer sérülése veszélyeztet-e emberéletet

A kockázatelemzést a szervezetet érintő minden jelentős jogszabályi, szervezeti vagy információtechnológia változtatás esetén frissíteni kell.

Az ASP szolgáltatási platform keretében használt elektronikus információs rendszerekre vonatkozó védelmi intézkedéseket a csatlakozási szerződésben megfogalmazottak szerint kell végrehajtani.

A biztonsági osztályba sorolást háromévente felül kell vizsgálni.

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

A biztonsági osztályba sorolás eredményét az IBSZ *{2számú melléklet – Az Önkormányzat információs rendszereinek biztonsági osztályba sorolása}* melléklete tartalmazza.

6. Szervezet biztonsági szintje

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 végrehajtási rendelet alapján az Önkormányzat elvárt biztonsági szintje 4-es.

7. Kockázatelemzés és kezelés

Az információbiztonsági kockázatelemzés célja, hogy az Önkormányzat elektronikus információs rendszereinek védelmi szintjét és a kapcsolódó intézkedéseket azok relatív fontosságával arányosan legyen képes kiválasztani és bevezetni.

A kockázatelemzési és kezelési módszertan kidolgozásánál az alábbi szempontokat kell figyelembe venni:

- legyen egyszerűen megérthető és elvégezhető
- ismételhető legyen
- ellenőrizhető legyen

A kockázatelemzést évente el kell végezni figyelembe véve az utolsó kockázatelemzés eredményét és az utolsó (akár rendszeres akár soron kívüli) kockázatelemzés óta az informatikai rendszerben bekövetkezett változásokat.

Soron kívüli kockázatelemzést kell végrehajtani az alábbi esetekben:

a) jelentős változás történik az elektronikus információs rendszerben

b) megváltozik az elektronikus információs rendszer működési vagy jogszabályi környezete.

A kockázatelemzést az IBF végzi el, melynek eredményét ismerteti a felelős vezetővel.

Az Önkormányzat kockázatelemzési és kezelési eljárásrendjét a „A kockázatelemzési és kezelési módszertan eljárásrendje" tartalmazza.

8. Rendszer és szolgáltatás beszerzés – Beszerzési eljárásrend

8.1. Erőforrás igény felmérés

Az önkormányzat éves költségvetésében elkülönítetten kell szerepeltetni az információbiztonság fejlesztésére fordítandó keretösszeget. Az információbiztonsági tervet a kockázatelemzési jelentés és az ahhoz szorosan kapcsolódó kockázatkezelési cselekvési tervvel összhangban kell elkészíteni.

A tervezési dokumentumot az IBF készíti el az Önkormányzat informatikai felelősével együttműködve és a felelős vezető hagyatja jóvá.

A tervezési dokumentumot minden tárgyi hatály alá tartozó intézmény esetén külön kell elkészíteni és jóváhagyatni.

8.2. Beszerzések

8.2.1. Funkcionális biztonsági követelmények

Az új fejlesztések esetén az IBF-et a fejlesztés legkorábbi szakaszába is be kell vonni.

Az IBF meghatározza a leszállítandó rendszer biztonsági osztályát. Egy rendszer biztonsági osztálya az

- 2013. évi L. törvény 7. § (3) bekezdése
- 2013. évi L. törvényben meghatározott technológiai biztonsági
- valamint a 41/2015. (VII. 15.) BM rendelet 1. számú melléklete alapján

meghatározza az alkalmazandó információbiztonsági védelmi intézkedéseket.

Az ily módon kialakított védelmi intézkedés terv kötelező része kell legyen a szállítói szerződésben meghatározott követelményeknek.

Bármely informatikai rendszer üzembe helyezési folyamatának kötelező eleme az adott rendszer funkcionális biztonsági követelményeinek IBF általi elfogadása.

8.2.2. Garanciális biztonsági követelmények

A biztonságkritikus eszközök, alkalmazások és szolgáltatásokkal kapcsolatban a funkcionális biztonsági követelmények teljesülésére vonatkozóan megfelelő garanciális biztonsági követelményeket kell támasztani a szállítókkal szemben, úgymint:

- a funkcionális biztonsági követelmények megfelelő szintű dokumentálása, mely biztosítja és segíti az adott funkció sikeres és megfelelő használatát
- funkcionális biztonsági követelmények tesztelhetősége és tesztdokumentációja

- a funkcionális követelményekkel szemben támasztott üzemeltethetőségi környezet

8.2.3. Biztonsággal kapcsolatos dokumentációs követelmények

A szállítónak minimálisan el kell készítenie az informatikai rendszer „Adminisztrációs és üzemeltetési kézikönyvét" valamint a „Felhasználói kézikönyvet".

Mindkét dokumentumnak tartalmaznia kell a funkcionális biztonsági intézkedések biztonsági, üzemeltetői és felhasználói szintű leírását olyan mértékben mely az adott funkció megfelelő használatát lehetővé teszi.

8.2.4. A biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelmények

A biztonsággal kapcsolatos dokumentumok illetéktelenek elleni védelméről az elektronikus információs rendszer teljes életciklusa (létrehozás, módosítás, megsemmisítés) alatt.

A biztonsággal kapcsolatos dokumentumokat a következő szerepkörök ismerhetik meg:

a) fejlesztő;

b) rendszergazda;

c) IBF;

d) Felelős vezető.

8.2.5. Fejlesztési szerződések biztonsági követelményei

A fejlesztési szerződések követelményeibe be kell építeni és alkalmazni kell az IBSZ-ben dokumentált, illetve az adott elektronikus információs rendszer biztonsági osztálya által megkövetelt biztonsági védelmi követelményeket (beleértve az IBSZ-ben a dokumentálására vonatkozó követelményeket is).

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

Az Önkormányzat érvényben lévő, vonatkozó szabályzatainak tudomásul vételi és elfogadó nyilatkozatát.

8.2.6. Rendszerkövetés (támogatás)

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

a) az infokommunikációs rendszerben felmerülő hibák javítása,

b) az Önkormányzat fejlesztési igényeinek ellátása,

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

Minden egyes új verzióra kiterjedően a szoftver kód átadása az Önkormányzat részére,a kód átadásával az rendszergazda számára olyan formában, hogy a támogató cég megszűnése esetén a kód az Önkormányzat 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.

8.2.7. Az elektronikus információs rendszerre vonatkozó dokumentáció

A szállítónak következő dokumentációkat kell készítenie a fejlesztés során:

8.2.8. Adminisztrátori dokumentáció

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.

8.2.9. 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.

8.3. A védelem szempontjainak érvényesítése a beszerzés során

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

Sikeres az átadás-átvétel ha:

a) a jelen IBSZ-ben dokumentált és a hivatkozott jogszabályokban megtalálható követelményeknek az alkalmazás megfelel,

b) a kapcsolódó dokumentációkat az Önkormányzat informatikai felelőse és az IBF elfogadta,

c) a funkcionális biztonsági követelményeket az IBF külön jegyzőkönyvben elfogadta

9. Elektronikus információs rendszerek ügymenet folytonosságának tervezése

Biztosítani kell az Önkormányzat elektronikus információs rendszereinek folyamatos működését, valamint egy esetleges katasztrófa-helyzet esetére kész tervekkel kell rendelkezni a kár csökkentése és a minimálisan elvárt működési szint visszaállítására.

9.1. Ügymenet folytonosságra vonatkozó eljárásrend

Ügymenet-folytonossági tervet (továbbiakban: ÜFT) kell kidolgozni az Önkormányzat érintett részlegeinek bevonásával.

Az ÜFT-ben kell dokumentálni az Önkormányzat minimális működéséhez szükséges szolgáltatásokat és alapfunkciókat.

A minimális működéshez szükséges szolgáltatások és alapfunkciók tekintetében ki kell dolgozni a lehető legköltséghatékonyabb helyreállítási tervet.

Az ÜFT-ben pontosan meg kell határozni a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket.

Az ÜFT-t az IBF készíti el és a felelős vezető hagyja jóvá.

9.1.1. Az ÜFT felülvizsgálata

Az ÜFT-t évente kell felülvizsgálni és szükség esetén módosítani.

Az ÜFT-t

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

b) az ÜFT tesztelése során felmerülő problémák esetén

soron kívül kell felülvizsgálni és módosítani.

Az ÜFT változásairól az érintett szervezeti egységeket oktatás keretében kell tájékoztatni.

9.1.2. Az ÜFT kezelése

Az ÜFT-t úgy kell tárolni, hogy az az infrastruktúra jelentős üzemzavara esetén is nyomtatott formában elérhető legyen mind az Önkormányzat épületében mind az erre kijelölt egyéb ÜFT helyszíneken.

Az ÜFT bizalmas információkat tartalmaz az Önkormányzat informatikai infrastruktúrájáról és annak védelmi képességeiről, ezért csak az abban megjelölt személyek számára szabad hozzáférhető tenni.

9.2. Kritikus rendszerelemek meghatározása

Az ÜFT-ben kell dokumentálni az Önkormányzat minimális működéséhez szükséges szolgáltatásokat és alapfunkciókat támogató rendszerelemeket.

9.3. Folyamatos működésre felkészítő képzés

Az ÜFT-ről az érintett szervezeti egységeknek az IBF tart kötelező éves oktatást.

9.4. Az elektronikus információs rendszer mentései

Az elektronikus információs rendszereket és az azokban kezelt adatokat védeni kell a szándékos vagy véletlen károkozás és a műszaki vagy egyéb nem várt problémák által okozott adatvesztések elkerülése érdekében. Az adatok visszaállíthatóságának érdekében mentési eljárásokat 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) Kiszolgálók operációs rendszerindító partíciójának képállományba mentése

b) Virtuális kiszolgálók virtuális lemezeinek mentése

c) Felhasználói adatok (ügyviteli adatok) mentőszoftveren keresztüli napi mentése

d) rendszerszintű információk

e) Adatbázismentések

f) naplóinformációk mentése az üzemeltetett rendszertől független naplószerverre

g) a rendszerrel kapcsolatos dokumentációk.

Az adatok elvesztésének valószínűségét a mentési adathordozók másodlagos telephelyre szállításával és tárolásával kell minimalizálni. A szállítás és tárolás során az elsődleges szerverhelyiség által nyújtott fizikai védelmi kontrollok egyenértékű védelmi intézkedések alkalmazásával kell védeni a mentési adathordozókat.

9.5. Infokommunikációs szolgáltatások

Az ASP rendszer folyamatos elérésének biztosítása érdekében az Önkormányzatnak rendelkeznie kell másodlagos internet szolgáltatással.

9.6. Szolgáltatás-prioritási rendelkezések

Az internet szolgáltatókkal kötött szerződéseknek tartalmazniuk kell az elvárt

a) szolgáltatási időszakot,

b) szolgáltatási szintet,

c) helyreállítási időket.

9.7. Az elektronikus információs rendszer helyreállítása és újraindítása

Az ÜFT kötelező eleme a rendszerek helyreállítási terve, melynek az alábbiakat kell tartalmaznia:

a) 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) az elektronikus információs rendszerek vészleállításának és újraindításának folyamatát leíró dokumentumot;

i) a helyreállítási terv tesztelése, karbantartása.

A helyreállítási terveket a rendszergazda készíti, teszteli és gondoskodik folyamatos frissítésükről. A helyreállítási terveket az IBF-nek információbiztonsági szempontból rendszeresen ellenőriznie és véleményeznie kell.

10. Emberi tényezőket figyelembe vevő – személy – biztonság

10.1. Az információbiztonsági felelősségi rend meghatározása

Az elektronikus információs rendszerekkel kapcsolatos tervezési, fejlesztési, üzemeltetési és ellenőrzési feladatokat szervezeti szinten szét kell választani.

Az információbiztonsági feladatok ellátása érdekében az alábbi szerepkörök kerültek kialakításra:

a) a felelős vezető,

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.

10.2. A felelős vezető feladatai

a) biztosítja az elektronikus információs rendszer biztonsági osztályában meghatározott követelmények teljesülését,

b) biztosítja a szervezetbiztonsági szintre meghatározott követelmények teljesülését,

c) kinevezi vagy megbízza az elektronikus információs rendszer biztonságáért felelős személyt,

d) jóváhagyja és kiadja végrehajtásra az IBF által készített információbiztonsági szabályzatot,

e) gondoskodik a védelmi feladatok és felelősségi körök rendszeres oktatásáról,

f) elrendeli a rendszeres biztonsági kockázatelemzéseket, ellenőrzéseket és auditokat

g) felelős az Önkormányzat elektronikus információs rendszereinek jogszabályi megfelelőség szerinti biztonságáért

h) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,

i) biztosítja a biztonsági események elhárításához és kezeléséhez szükséges emberi, eszköz és pénzügyi feltételeket,

j) az elektronikus információs rendszerrel kapcsolatba kerülő harmadik felekkel csak a megfelelő biztonsági záradékot tartalmazó szerződéseket hagy jóvá és ír alá,

k) a szervezet elektronikus információs rendszerével adatkezelési vagy az adatfeldolgozási tevékenység kapcsán közreműködő felekkel csak az IBSZ betartását szerződéses kötelezettségként biztosító biztonsági záradékot tartalmazó szerződést hagy jóvá,

l) haladéktalanul tájékoztatja az érintetteket a biztonsági eseményekről és a lehetséges fenyegetésekről,

m) elrendeli az elektronikus információs rendszer védelme érdekében szükséges intézkedéseket.

A felelős vezető köteles együttműködni a jogszabályban meghatározott hatóságokkal. Ennek során

a) tájékoztatja a hatóságot az IBF személyéről,

b) megküldi az Önkormányzat információbiztonsági szabályzatát,

c) megküldi az Önkormányzat elvárt szervezeti 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.

10.3. A felelős vezető felelőssége

A felelős vezető felelős az előírt biztonsági szintnek és biztonsági osztályok megvalósulásáért, valamint az ezek végrehajtásához szükséges erőforrások biztosításáért.

10.4. Az IBF feladatai

a) az elektronikus információs rendszerek biztonságával kapcsolatos tevékenységek megszervezése,

b) elvégzi az információ biztonsági tervezési, szervezési, koordinálási és ellenőrzési feladatokat

c) az információbiztonsági politika, stratégia és szabályzat előkészítése,

d) elkészíti, karbantartja és felülvizsgálja az információbiztonsági cselekvési tervet,

e) előkészíti az Önkormányzat elektronikus információs rendszereinek biztonsági osztályba sorolását

f) előkészíti az Önkormányzat biztonsági szintbe történő besorolását,

g) véleményezi az elektronikus információs rendszerek biztonsága érintő szabályzatokat és szerződéseket,

h) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal

i) részt vesz az Önkormányzat valamennyi olyan elektronikus információs rendszerének biztonsági tervezésében, fejlesztésének felügyeletében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében ahol az Önkormányzat adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe

10.5. Az IBF jogai

Az IBF rendszeres bejárás keretében az információbiztonság fenntartásának érdekében, illetve információbiztonsági incidens bekövetkezése esetében jogosult:

a) külön engedély nélkül bármely olyan helyiségbe belépni ahol az információbiztonságot érintő munkavégzés folyik,

b) a jogszabályok betartásával adott üggyel kapcsolatos folyó információbiztonsági vizsgálat szempontjából érintett bármely számítógép, adathordozó vagy számítógépes lista tartalmát megtekinteni, és

c) minden információbiztonsági vonatkozású értekezleten részt venni és azon észrevételt és javaslatot tenni.

10.6. Az IBF felelőssége

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

10.7. A rendszergazda feladata

a) megtervezi információbiztonsági követelmények megvalósításához szükséges infrastruktúrát;

b) üzemeltetési eljárásokat dolgoz ki,

c) felügyeli és üzemelteti az elektronikus információs rendszerek;

d) eleget tesz az IBSZ-ben előírt feladatainak.

e) folyamatosan frissíti az elektronikus információs rendszerek nyilvántartását.

10.8. A rendszergazda felelőssége

A rendszergazda felelőssége az elektronikus információs rendszerek jelen IBSZ-ben foglaltak szerinti biztonságos üzemeltetése.

10.9. Az adatgazda feladatai

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

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

Az adatgazda információbiztonsággal kapcsolatos feladatai a következők:

a) jóváhagyja a szükséges-elégséges hozzáférési elv alapján a hozzáférők körét;

b) jóváhagyja az egyedi hozzáféréseket

c) Elvégzi a hozzáférések rendszeres felülvizsgálatát.

10.10. Az adatgazda felelőssége

Az adatgazda felelős a hozzáférések „szükséges, minimális jogosultságok" elve alapján történő engedélyezéséért.

10.11. A szervezeti egység vezetője

A szervezeti egység vezetőjének felelőssége az információbiztonsági előírások betartatása közvetlen beosztottjaival.

10.12. Önkormányzati ASP adminisztrátor

Az Önkormányzat jogszabály alapján ASP használatra kötelezett szervei és szervezeti egységei esetében az önkormányzati ASP adminisztrátor kezeli az önkormányzati szintű felhasználókat, azaz

a) a regisztrálja és szakrendszeri szerepkör(ök)höz rendeli a felhasználókat;

b) az Önkormányzati felhasználók tanúsítványainak kezelése

10.13. Önkormányzat szakrendszeri adminisztrátor

Feladat a szakrendszeri jogosultságok beállítása, adminisztrációja és karbantartása.

10.14. A felhasználó jogai

A felhasználó jogosult:

a) az informatikai rendszerek rendeltetésszerű használatára,

b) a munkájához szükséges adatállományok elérésére,

c) információbiztonsági képzésre,

d) a működtetéshez szükséges támogatás igénylésére,

10.15. A felhasználó kötelessége

A felhasználó kötelessége felettesét vagy a rendszergazdát haladéktalanul értesíteni az alábbi eseményekről:

a) az elektronikus információs rendszer szokatlan, rendellenes működéséről,

b) olyan adathoz fér hozzá, melynek kezelésében nem illetékes

c) információbiztonsági esemény.

A felhasználó köteles bizalmasan kell kezelnie a rábízott felhasználói azonosítókat, jelszavakat, eToken-t, kulcsokat vagy egyéb, az Önkormányzat erőforrásaihoz hozzáférést biztosító eszközt.

A felhasználó köteles együttműködni az információbiztonsági incidensek kivizsgálásában.

Tilos más felhasználó azonosító adatait felhasználni.

Tilos a hálózat monitorozása, felderítése és a jelszavak próbálgatása vagy ezek kísérlete is.

10.16. A felhasználó felelőssége

a) Az ASP rendszer által közzétett felhasználói biztonsági követelmények betartásáért,
b) A megismert információk bizalmasságának megőrzése.
c) a védett területre belépést biztosító kártyájának/kártyáinak védelme,
d) az azonosítójával az elektronikus információs rendszerben végzett műveletekért,
e) a rábízott elektronikus információs rendszerek rendeltetésszerű, szakszerű kezeléséért és
e) a személyi használatra átvett eszközök megfelelő fizikai védelméért.

10.17. A munkaköri felelősség és az alkalmazás feltételei

A munkaköri leírásoknak tartalmazni kell az általános és az adott munkakörhöz tartozó információbiztonsági feladatokat és felelősségeket.

A dolgozókat tájékoztatni kell információbiztonsági előírásokkal kapcsolatos jogi felelősségükről és kötelezettségeikről.

A dolgozók információbiztonsági felelőssége a nem az Önkormányzatban töltött munkaidőn kívüli időszakra is vonatkozik.

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

Az Önkormányzat elektronikus információs rendszereit csak a jelen IBSZ *{6. számú melléklet – Felhasználói Nyilatkozat}* mellékletében található nyilatkozat és az ASP titoktartási nyilatkozat aláírása után lehet használatba venni.

10.18. Munkakörök, feladatok biztonsági szempontú besorolása

Az Önkormányzati információbiztonsághoz kapcsolódó munkakörök és betöltésükhöz szükséges feltételek:

Munkakör	Munkakör betöltéshez szükséges feltételek
Rendszergazda	Erkölcsi bizonyítvány, szakirányú végzettség, 2 év szakmai tapasztalat, alapfokú angol nyelvtudás
Információbiztonsági felelős	Erkölcsi bizonyítvány, szakirányú végzettség, 5 év szakmai tapasztalat, alapfokú angol nyelvtudás
Adatgazda	Erkölcsi bizonyítvány, szakirányú végzettség, informatikai alapismeretek,

Munkakör	Munkakör betöltéshez szükséges feltételek
	önkormányzati szakrendszerek használatában szerzett jártasság
Önkormányzati ASP adminisztrátor	Erkölcsi bizonyítvány, szakirányú végzettség, informatikai alapismeretek, önkormányzati szakrendszerek használatában szerzett jártasság
Önkormányzati szakrendszeri adminisztrátor	Erkölcsi bizonyítvány, szakirányú végzettség, informatikai alapismeretek, önkormányzati szakrendszerek használatában szerzett jártasság
Felhasználó	Erkölcsi bizonyítvány, szakirányú végzettség, informatikai alapismeretek, önkormányzati szakrendszerek használatában szerzett jártasság

Az információbiztonsági munkakörök betöltéséhez szükséges feltételeket évente ellenőrizni kell.

10.19. A személyek ellenőrzése

Az elektronikus információs rendszerhez a hozzáférést csak akkor szabad engedélyezni, ha a munkavállaló a 10.18–as fejezet feltételeinek megfelel. A feltételek teljesülését az Önkormányzat felelős vezető által kijelölt ügyintézőjének kell ellenőrizni az alábbiak szerint:

a) az életrajz ellenőrzése a teljességre és pontosságra vonatkozóan,

b) referenciák ellenőrzése,

c) a legmagasabb iskolai végzettség igazoló bizonyítványok (szakképzettség) ellenőrzése,

d) nyelvtudást igazoló okiratok ellenőrzése,

e) személyazonosságot azonosító iratok ellenőrzése,

f) erkölcsi bizonyítvány ellenőrzése.

Külső szerződő felek esetében az IBF feladata az előzetes ellenőrzés elvégzése.

10.20. Biztonsági események kezelése

10.20.1. Jelentés a biztonsági eseményekről

A biztonsági események jelentésének és a visszajelzések kezelésének folyamatát dokumentálni kell. Minden a biztonságot csökkentő eseményt biztonsági eseménynek nevezünk.

A biztonsági eseménykezelést az alábbi lépésekben kell végezni:

1. A biztonsági eseményeket észlelésüket követően haladéktalanul jelenteni kell a felelős vezetőnek és a rendszergazdának. A biztonsági eseményekről szóló jelentések elkészítésére az IBSZ *{3számú melléklet – Biztonsági események* jelentése*}* mellékletében található űrlapot kell használni.
2. Ha a rendszergazda a bejelentett eseményt biztonsági eseményként értékeli, akkor jelenti azt az IBF-nek. Biztonsági esemény esetén az IBF látja el a biztonságieseménykezelési megbízott feladatait.
3. Az IBF a saját Ügyfélkapuján keresztül haladéktalanul jelentenie kell a biztonsági eseményt a Kormányzati Eseménykezelő Központ (továbbiakban GovCert) részére.
4. Az önkormányzati ASP rendszer érintettsége esetén, a biztonsági eseményt az önkormányzati ASP rendszer működtetőjének is jelenteni kell.
5. Az IBF-nek csatolnia kell a bejelentéshez a biztonsági eseményhez kapcsolódó valamennyi bizonyítékot.
6. Az IBF-nek és az Önkormányzatnak együtt kell működnie a GovCert-tel a biztonsági esemény kezelésében és a GovCert által javasolt intézkedéseket végre kell hajtania.
7. Az IBF-nek kivizsgálást kell kezdeményeznie a beérkezett jelentés alapján és javaslatot kell tennie a felelős vezető részére az esemény előfordulási esélyének csökkentése, illetve az okozott kár mérséklése érdekében.
8. Amennyiben a biztonsági esemény igazoltan a szabályok megsértéséből adódik, úgy az IBF-nek javaslatot kell tennie a felelős vezető részére a fegyelmi eljárások lefolytatása érdekében.

10.20.2. Jelentés a biztonság gyenge oldalairól

Az elektronikus információs rendszerben felfedezett gyenge pontokat, biztonsági veszélyeket minden felhasználó köteles az IBF-nek jelenteni.

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

10.20.3. 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 {10.20.1 Jelentés a biztonsági eseményekről}* pontjának megfelelően kivizsgálja az eseményt.

10.20.4. Okulás a biztonsági eseményekből

Az IBF a bejelentett biztonsági eseményekről és működési zavarokról háromhavonta jelentést készít a felelős vezető számára.

Az IBF a biztonsági események kezeléséből levont tapasztalatok felhasználásával a meglévő biztonsági rendszert felülvizsgálja és módosítja.

A különleges eseményeket (nagy kár, gyakori előfordulás) soron kívül jelenteni kell a felelős vezetőnek.

10.21. Eljárás jogviszony megszűnésekor

A felhasználó jogviszonya keletkezhet:

a) rendes alkalmazásból, munkavállalói szerződésből,

b) harmadik féllel kapcsolatos szerződésből,

c) illetve egyedi megállapodásból.

A jogviszony megszüntetésekor a következő feladatok végrehajtása szükséges:

d) Jogosultságok visszavonása

e) A felhasználói adatokat (e-mail-ek, dokumentumok), archiválni kell

f) Az archivált adatokat a törvényi előírásoknak megfelelően tárolni kell, illetve ha szükséges a megadott idő után törölni a rendszerből.

A fenti feladatok végrehajtását a rendszergazda végzi.

10.21.1. Vagyontárgyak visszaszolgáltatása

Valamennyi felhasználó köteles a használatra átvett vagyontárgyakat visszaszolgáltatni jogviszonyuk megszűnésekor.

Az eszközök hiánytalan és pontos leadását a rendszergazda ellenőrzi.

10.21.2. Hozzáférési jogok megszüntetése

A felhasználó alkalmazási jogviszonyának megszűnéskor a hozzáférési jogosultságait meg kell szűntetni.

A fentiektől eltérni a felelős vezető írásos engedélyével lehetséges.

A feladatok végrehajtásáért a rendszergazda a felelős.

10.21.3. Információbiztonsági kötelmek a jogviszony megszűnése után

A jogviszony megszűnéskor a felhasználót tájékoztatni kell, hogy az IBSZ-ben foglalt kötelezettségei a jogviszony megszűnése után is fennállnak és azok megsértése jogi következményeket von maga után.

A felhasználót az IBSZ *{7. számú melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén}* mellékletében foglaltak szerint kell tájékozatni.

10.22. Áthelyezések, átirányítások és kirendelések kezelése

Az érintett munkatárs ellenőrzését az IBSZ *{III.10.19 A személyek ellenőrzése}* pontjában foglaltak alapján áthelyezés esetén is el kell végezni.

Az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését át kell vezetni az informatikai rendszerekre is.

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

10.23. Fegyelmi intézkedések

Az IBSZ szabályainak megszegéséről az IBF-et az észtlelést követően azonnal tájékoztatni kell.

Az IBF a tudomására jutott események súlyosságának mérlegelése után szükség esetén jelentést tesz a felelős vezetőnek.

Az IBSZ szabályainak megszegőjével szemben fegyelmi eljárás kezdeményezhető, mely az alkalmazói jogviszony megszűnését eredményezheti.

Az eljárást az IBSZ kezdeményezi és a felelős vezető az Önkormányzat belső szabályozása alapján folytatja le.

10.24. Belső egyeztetés

Az Önkormányzat az információbiztonsággal kapcsolatos folyamatok és cselekvési tervek zökkenőmentes végrehajtásának érdekében rendszeres egyeztetések tart az érintett szervezeti egységekkel.

10.25. Viselkedési szabályok az interneten

10.25.1. A web böngészés szabályai

Az Internethez való kapcsolódás csak és kizárólag a munkavégzést szolgálja!

A nem munkavégzést szolgáló tartalmak Önkormányzati szerveren tárolása és letöltése tilos.

Az internetről csak a munkavégzéssel kapcsolatos célból engedélyezett fájlokat letölteni!

Tilos fájlletöltő szolgáltatások használata.

Különösen tilos jogvédett, illetve illegális tartalmak, fájlok letöltése, tárolása!

Tilos az elektronikus információs rendszerek biztonságát szolgáló rendszerprogramok beállításainak megváltoztatása.

Önkormányzati adatok tárolása a nem az Önkormányzat vagy az ASP szolgáltató által üzemeltetett felhőszolgáltatáson vagy az Interneten keresztül elérhető rendszeren még átmeneti jelleggel is tilos.

Tilos az elektronikus információs rendszerek használata az alábbi tartalmak letöltésére, megtekintésére: 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 az interneten nem nyilvános Önkormányzati információt közzétenni!

Az internetes oldalak elérése megfigyelésre és naplózásra kerül.

A munkavégzéssel összefüggésbe nem hozható oldalak elérhetőségét az informatikai üzemeltetés jogosult korlátozni.

10.25.2. E-mail használat

Az elektronikus levelezési szolgáltatás kizárólag Önkormányzati munkavégzés céljára biztosított.

A felhasználóknak tilos az Önkormányzati e-mail címüket nem Önkormányzati minőségben használni.

Elektronikus levél önmagában nem használható kötelezettség vállalására, illetve annak visszaigazolására.

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

Minden elektronikus levelezést használónak gondoskodnia kell arról, hogy az információk elektronikus levél általi elosztása szabályozott körülmények között, az adott információra vonatkozó védelmi igények betartásával történjen.

Az elektronikus levelezés használata során tilos az üzenetek hamisítása vagy a küldő azonosítójának álcázása.

Az Önkormányzati elektronikus levelezőrendszer felhasználóinak tilos automatikus továbbító funkciót használniuk belső levelek külső elektronikus levelezőrendszerbe továbbítására (pl. Hotmail-be, Gmail-be, Citromail-be). Kivétel a szabály alól az "Out of office" jelentések használata.

Publikus elektronikus levelező rendszerek használata Önkormányzati kommunikáció céljára tilos.

Távoli elektronikus levelezés elérés csak az Önkormányzat által elfogadott távoli hozzáférési módszerekkel engedélyezett.

A kimenő elektronikus levelekhez adatvédelmi közleményt kell csatolni.

Az Önkormányzati elektronikus levelező rendszerek használatát naplózni kell. A naplózásnak elegendő információt kell szolgáltatnia az esetleges vizsgálatok (bűnügyi, adatvédelmi, munkaügyi, stb.) lefolytatásához és az elektronikus levelezés használata során elkövetett visszaélések felderítéséhez.

Az Internet felé nyitott elektronikus levelezési átjárókat úgy kell konfigurálni, hogy ellenőrizzék a bejövő levelek forráscímét így biztosítva, hogy a monor.hu címekről érkező levelek kizárólag elfogadott levelező rendszerekből származnak.

Minden elektronikus levelezési átjárót úgy kell konfigurálni, hogy megakadályozzák a spamek és a kártékony programok (vírusok, férgek, kémprogramok, stb.) továbbjutását.

A levelek végén lévő felhasználói aláírásnak követnie kell az Önkormányzatnál elfogadott formátumot.

10.26. Harmadik felekkel kapcsolatos előírások

Harmadik fél csak szerződéses jogviszony keretében meghatározott időre és meghatározott feladat ellátásához látható el jogosultsággal.

A hozzáférést az elektronikus információs rendszer adatgazdájának és az IBF-nek kell engedélyezni.

Harmadik fél hozzáférése során gondoskodni kell az IBSZ-ben dokumentált védelmi intézkedések betartásáról az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása érdekében.

Ha a szerződés keretében az információ feldolgozása vagy kezelése kiszervezett tevékenységnek minősül, a szerződésnek tartalmaznia kell a betartandó biztonsági követelményeket is.

A szerződésnek tartalmaznia kell továbbá a szellemi tulajdonjogokra, a szerzői jogok átruházásra vonatkozó garanciákat is

Harmadik fél hozzáférését az Önkormányzat elektronikus információs rendszereihez csak a szerződés és az IBSZ *{8. számú melléklet – Titoktartási Nyilatkozat}* mellékletében található titoktartási nyilatkozat aláírása után szabad engedélyezni és beállítani.

10.26.1. A harmadik fél hozzáférési kockázatának azonosítása

Az Önkormányzatnak fel kell mérnie, és meg kell határoznia, hogy mekkora a kockázata annak, ha a harmadik félnek hozzáférési joga van az Önkormányzat információs vagyonához.

Harmadik fél alkalmazása esetén az le kell folytatni a kockázatelemzési eljárást.

A kockázatelemzési eljárást az érintett szervezeti egység vezetője kezdeményezi. A szerződés megkötése előtt az informatikai biztonsági felelőst be kell vonni a szerződéskészítés folyamatába.

10.26.2. A harmadik féllel kötött szerződés biztonsági követelményei

A szerződésekben, szükség szerint az alábbiakat kell előírni:

a) az információbiztonságot érintő felelősségi köröket;

b) személybiztonsági követelmények betartása;

c) meg kell követelni, hogy a szerződő fél dokumentálja a személybiztonsági követelményeket;

d) hozzáférés kezelési folyamatok működése az Önkormányzat és a harmadik fél között;

e) az elvárt szolgáltatási szintek és szolgáltatási időszakok;

f) a felek felelősségének meghatározását;

g) a szellemi tulajdon védelmére és másolására vonatkozó szabályok;

h) a teljesítések ellenőrizhetőségét, monitorozását és jelentések készítését;

i) problémakezelés folyamatát;

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

k) jelentéskészítések rendjét;

l) a változáskezelés rendjét;

m) az alvállalkozók bevonására vonatkozó szabályokat.

11. Biztonság tudatosság képzés

Az információbiztonsági tudatosság növelésével és ezáltal a biztonsági követelmények minél magasabb fokú betartásával kell csökkenteni az elektronikus információs rendszereket érő, a felhasználók viselkedéséből és szabálykövetési hajlandóságából fakadó veszélyeket.

11.1. Alapképzés

A minden felhasználóra kiterjedő kötelező alapképzést kell tartani.

Az információbiztonsági szabályokat új munkavállaló esetén minden esetben az elektronikus információs rendszer használatának megkezdése és a jogosultságok kiadása előtt kell ismertetni.

A felhasználók tudatosságának fenntartása érdekében évente frissítő oktatást kell szervezni.

Az információbiztonsági oktatás megtartása és a képzések kidolgozása az IBF feladata.

Az oktatáson minden felhasználó számára kötelező a részvétel.

Az oktatás elvégzését oktatási naplóban kell dokumentálni.

11.2. Belső fenyegetés

A biztonságtudatossági oktatást úgy kell kialakítani, hogy a felhasználók képesek legyenek felismerni az információbiztonsági veszélyhelyzeteket.

11.3. Szerepkör vagy feladat alapú biztonsági képzés

A felelős vezetőnek, a rendszergazdának és az IBF-nek a Nemzeti Közszolgálati Egyetem által szervezett, külön jogszabályban előírt, a következő továbbképzésen és éves továbbképzésen kell részt venniük:

Szerepkör megnevezése	Képzés megnevezése
Jegyző	elektronikus információs rendszerek védelméért felelős vezető
Intézményvezető	elektronikus információs rendszerek védelméért felelős vezető
Ügyvezető	elektronikus információs rendszerek védelméért felelős vezető
Rendszergazda	elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy
IBF	elektronikus információbiztonsági vezető

12. Az elektronikus információs rendszerek nyilvántartása

Az Önkormányzatnak teljes körű és naprakész informatikai nyilvántartást kell létrehoznia. A nyilvántartásnak tartalmaznia kell az összes informatikai rendszert azok teljes életciklusát lefedve a beszerzéstől a selejtezésig. Minden új informatikai eszközt hozzá kell adni ehhez a leltárhoz legfeljebb 30 napon belül.

Az informatikai eszközök leltárát az IBF évente egy alkalommal ellenőrzi

A nyilvántartás minimálisan az alábbiakat tartalmazza:

a) a rendszer alapfeladatait;

b) a rendszerek által biztosítandó szolgáltatásokat;

c) az érintett rendszerekhez tartozó licenc számot;

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

e) 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 vezetnie és naprakészen tartania.

IV. Fizikai védelmi intézkedések

13. Alapelvek

Az fizikai védelmi intézkedések kialakítása során az alábbi követelményeket kell betartani:

a) az elektronikus információs rendszereket fizikailag védett, biztonságos helyre kell telepíteni

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

c) a környezeti feltételeket fenntartó berendezések tartalékolásáról és működésük monitorozásáról gondoskodni kell

14. A területek fizikai biztonsági követelményei

14.1. Fizikai biztonság védősávja

Az Önkormányzat területeit biztonsági zónákba kell besorolni. Az IBSZ *{1.2.3 Tárgyi hatály}* pontja alá eső területeket az alábbi kategóriák egyikébe kell besorolni:

a) **Belső terület:** a bejárata utáni közös használatú helyiségei és folyosói. A belső terekben infokommunikációs eszközök nem telepíthetők, a kivételek jóváhagyása az IBF feladata.

b) **Védett terület**: valamennyi iroda és tárgyaló helyiség. A védett területeket zárva kell tartani. A védett területek bejárati ajtajában a kulcsokat nem szabad a zárban hagyni, illetve ha az ajtó nyitva van, a helyiséget nem szabad őrizetlenül hagyni.

c) **Érzékeny terület**: az Önkormányzat szerverszobái és a strukturált kábelezés rendező központjai.

14.2. Az irodák, a helyiségek és az eszközök védelme

Az irodák, a szobák és a számítógépterem védelmét az alábbiak szerint kell szabályozni:

a) a kulcsokat elzárva, idegenek számára nehezen hozzáférhető helyen kell tárolni;

b) a védett és érzékeny helyiségeken ne legyen olyan jelzés, amelyből kiderül a funkciójuk;

c) a fénymásoló és nyomtató berendezéseket, a fax készülékeket védett területen belül kell elhelyezni

d) a dokumentumok tárolása védett területen történjen;

e) a felügyelet nélkül hagyott helységek ajtóit és ablakait zárva kell tartani.

15. Az infokommunikációs eszközök biztonsága

15.1. Az infokommunikációs eszközök elhelyezése és védelme

Az infokommunikációs eszközöket úgy kell telepíteni, hogy az illetéktelen hozzáférések lehetősége a minimálisra csökkenjen.

Minimalizálni kell a környezeti hatások okozta meghibásodásokat a megfelelő védelmi intézkedések biztosításával, ezért:

a) meg kell követelni a tűzvédelmi előírásokat betartását;

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

c) a monitorokat úgy kell elhelyezni, hogy illetéktelenek ne tudják elolvasni a képernyőtartalmat;

d) Az ASP rendszer használatára jogszabály alapján kötelezett szerv, illetve szervezeti egység esetén különös figyelmet kell fordítani az önkormányzati ASP rendszert elérő munkaállomások elhelyezésére, gondoskodni kell az illetéktelen hozzáférések megakadályozásáról.

15.2. Tápáramellátás

A szerverhelyiségnek az ott üzemeltetett szerverek és azok működését támogató eszközök (pl. légkondicionáló, tűzjelző, beléptető rendszer) elektromos igényeit folyamatosan el kell tudnia látni. Az energiaellátást a mindenkori terheléshez kell méretezni figyelembe véve az elektromos biztonsági tartalékot. Lehetőség szerint redundáns betáplálást kell alkalmazni.

A szervereket és az azokat közvetlenül kiszolgáló aktív eszközöket megfelelő kapacitású szünetmentes tápegységgel kell ellátni. A szünetmentes tápegységeket az ÜFT előírásoknak megfelelően kell méretezni. Gondoskodni kell a szünetmentes üzemről történő, megfelelő sorrendű, automatikus vészleállítási megoldásról, valamint a szünetmentes üzem távjelzési megoldásáról, annak érdekében, hogy az esetlegesen távol lévő rendszergazdák minden fontos automatikus eseményről és státuszról értesüljenek.

A szerverhelyiségeket befogadó épületeknek rendelkezniük kell villámvédelemmel, amelynek meg kell felelnie a vonatkozó előírásoknak

15.3. A kábelezés biztonsága

Biztosítani kell az elektromos és adatvezetékek megszakadás, rongálás és rágcsálók 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.

15.4. „Tiszta asztal – Tiszta képernyő" szabály

Az illetéktelen hozzáférések megakadályozása érdekében az alábbi szabályokat minden felhasználónak be kell tartani:

a) A monitorokat úgy kell elhelyezni, hogy ki lehessen zárni illetéktelen leolvasást. A monitorokat úgy kell elhelyezni, 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 köteles zárolni az őrizetlenül hagyott munkaállomását (a Ctrl +Alt +Del billentyűk, majd Zárolás vagy a WINDOWS+L gombok egyidejű leütése),

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

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

e) a felhasználóknak a védett helyiséget be kell zárniuk, ha a helyiségben senki nem tartózkodik;

f) ügyfelet irodában felügyelet nélkül hagyni tilos.

15.5. Felügyelet alól kikerülő eszközök

A felügyelet alól kikerülő eszközök esetében a rendszergazdának gondoskodnia kell az adatokat tartalmazó adathordozók törléséről vagy szervizbe szállítás esetén az adathordozó eltávolításáról.

Eszközt kiszállítani csak a rendszergazda írásos engedélyével lehet.

A ki- és beszállítások ellenőrzése a rendszergazda 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.

.

16. Fizikai belépési engedélyek a fizikai belépés ellenőrzése

Naprakész nyilvántartást kell vezetni az Önkormányzat védett és érzékeny területeire belépésre jogosultak listájáról.

E belépésre jogosultak listáját a felelős vezető által kijelölt helyen kell tárolni.

A belépésre jogosultak nyilvántartását a felelős vezető által kijelölt ügyintéző félévente dokumentáltan felülvizsgálja.

Az alkalmazás jogviszonyának megszűnése esetén a fizikai belépési jogosultságot meg kell szüntetni.

A belépésre jogosultak listáját a felelős vezető hagyja jóvá.

16.1. Fizikai belépések

A fizikai belépések alatt azokat az eseteket értjük, amikor az információs rendszer olyan elemeihez lehetséges a közvetlen hozzáférés, amelyek magas kockázattal járó információs adatvagyont tárolnak, feldolgoznak, továbbítanak vagy biztosítják ezen berendezések működésikörnyezetei feltételeit. Ilyen helyiségek jellemzően a szerverszoba, hálózati rendezőhelyiség vagy szekrény, adatátviteli csomópont, energiaellátási helyiség vagy szekrény, külső adattárolókat tartalmazó helyiség vagy szekrény. Érzékeny vagy védett terület alatt azokat a helyiségeket értjük, ahol információ feldolgozó végponti eszközök (munkaállomás, nyomtató, scenner), valamint papír alapú adathordozó található.

16.2. Fizikai belépések naplózása

E magas kockázatú helyiségekbe történő fizikai belépések esetén rögzíteni kell a be- és kilépés pontos idejét, és a be- és kilépést végző személy azonosító adatait, valamint az ott tartózkodás célját.

16.3. Vendégek kísérete

Az érzékeny területre belépő vendégek, ügyfelek kíséretét és azonosítását biztosítani kell. Az azonosítási folyamatnak biztosítani kell a vendég személyes adatait, a látogatás célját, valamint a ki-és belépés időtartamát. A kíséretet annak a munkatársnak kell biztosítani, akihez a vendég érkezik.

16.4. Kulcsok megóvása

A védett területeken található helyiségek ajtajait kulcsra kell zárni, amennyiben nem tartozik Önkormányzati dolgozó a területen. A kulcsok kezelésére és megőrzéséről gondoskodni kell.

Egy kulcs elvesztése esetén az adott ajtó zárját ki kell cserélni.

A kulcs cseréjét a felelős vezetőnek haladéktalanul jelenteni kell, aki gondoskodik a zárcseréről.

16.5. Belépések ellenőrzése, felügyelete

Az Önkormányzat érzékeny területeire történő be-és kilépések felügyeletét biztosítani kell. A felügyeletet a felelős vezető által kijelölt ügyintéző végzi, aki megteszi a szükséges intézkedéseket a felelős vezető felé, amennyiben a szabályoktól eltérést észlel.

16.6. Rendellenességek jelentése

A fizikai belépéssekkel és a kulcskezeléssel kapcsolatos bármilyen rendellenes viselkedést jelenteni kell a felelős vezetőnek.

16.7. Hozzáférés az adatátviteli berendezésekhez és csatornákhoz

Látogatók belépése az érzékeny területre csak hivatalos célból, ellenőrzötten és kísérővel történhet. A látogatók 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 felelős vezető által kijelölt helyen kell tárolni.

Az érzékeny területek elérésére a felelős vezető, a rendszergazda és az IBF jogosultak. Minden más személy részére csak a felelős vezető 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.

16.8. Tűzvédelem

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

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

A szerverszoba elhelyezésével, lehetőség szerint gondoskodni kell arról, hogy a helységet a vizet szállító csővezetékek hibájából fakadóan ne érhesse kár. A víz vagy egyéb anyagot szállító csővezeték hibájának esetére az elzáró szelepeket a felelős vezető által kijelölt személyek számára hozzáférhetővé kell tenni.

V. Logikai védelmi intézkedések

17. Általános védelmi intézkedések

17.1. Engedélyezés

A védelmi intézkedéseket úgy kell kialakítani, hogy biztosított legyen

Biztosítani kell az elektronikus információs rendszer:

a) a biztonsági állapotának felügyeletét,

b) fenntartásához szükséges szerepköröket és felelősségi köröket,

c) kijelölésre kerüljenek az ezeket betöltő személyek,

d) az információbiztonsági engedélyezési folyamatok és az Önkormányzati szintű kockázatkezelési eljárásokat integrálni kell.

e) az információbiztonsággal kapcsolatos engedélyezés terjedjen ki minden, az Önkormányzat hatókörébe tartozó:

f) emberi, fizikai és logikai erőforrásra;

g) eljárási és védelmi szintre és folyamatra.

17.2. Elektronikus Információs rendszer kapcsolódásai

Az elektronikus információs rendszer engedély nélküli összekapcsolása más szervezetek informatikai rendszerével nem engedélyezett.

Az összekapcsolást a felelős vezetőnek, a rendszergazdának, és az IBF-nek is jóvá kell hagynia.

Más szervezetekhez kapcsolódás esetén dokumentálni kell:

- az interfészek paramétereit,
- a biztonsági követelményeket,
- kapcsolaton keresztül átvitt elektronikus információk típusát.

A kapcsolódó szervnek szerződésben kell vállalni, hogy biztosítja a saját elektronikus információs rendszerében legalább 3-as biztonsági osztályra előírt követelmények teljesülését.

Információbiztonsági incidens esetén az Önkormányzat jogosult a kapcsolatot felfüggeszteni.

Az átvitt adatok bizalmasságának és sértetlenségének titkosítással kell biztosítani.

Az alkalmazott műszaki megoldásnak biztosítani kell a kapcsolódás hálózati cím (IP cím) szintű korlátozását.

A kapcsolódási pontokat és azok dokumentációját évente egyszer ellenőrizni kell.

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

17.3. Belső rendszerkapcsolatok

Az Önkormányzat belső elektronikus információs rendszerének kapcsolódási pontjait is dokumentálni és engedélyeztetni kell. Az belső kapcsolódási pontokat IBF engedélyezi.

17.4. Külső kapcsolódásokra vonatkozó korlátozások

Az Önkormányzat határvédelmi védelmi intézkedései során minden kapcsolatot explicit engedélyeztetni kell. Alapesetben minden kapcsolatot tiltani kell. A működéshez szükséges portok, protokollok és a hozzátartozó szolgáltatásokról nyilvántartást kell vezetni, melyet nyilvántartást a rendszergazda tart naprakészen. A nyilvántartásban jóváhagyott kapcsolatokat és a határvédelmi eszközökben beállított tényleges kapcsolódási paramétereket az IBF évente egyszer ellenőrzi.

A kapcsolatokat az IBF előzetes jóváhagyásával lehet beállítani.

18. Tervezés - Biztonságtervezési eljárásrend

18.1. Rendszerbiztonsági terv

El kell készíteni az elektronikus információs rendszerek rendszerbiztonsági tervét, amelynek tartalmaznia kell a rendszer feladatait, a kezelt adatok biztonsági osztálybesorolását, kapcsolódásait más rendszerhez, a biztonsági követelményeket, a vonatkozó védelmi intézkedéseket.

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

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

Az elektronikus információs rendszer változása esetén a rendszerbiztonsági tervet soron kívül frissíteni kell.

Az ellenőrzések által feltárt hiányosságok megszűntetésére cselekvési tervet kell kidolgozni.

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

18.2. Cselekvési terv

A cselekvési tervre vonatkozó követelményeket a jelen IBSZ {*II Az Önkormányzat információbiztonsági követelményei*} fejezete tartalmazza.

18.3. Személybiztonság

A személybiztonságra vonatkozó követelményeket a jelen IBSZ {*I.4 Az IBSZ általános követelményei*} pontja tartalmazza.

19. Konfigurációkezelési eljárásrend

19.1. Alap konfiguráció

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

A dokumentációnak minimálisan tartalmaznia kell a hardver elemek, szoftverek, telepítőkészletek és egyéb komponensek alapkonfigurációját.

Az alapkonfigurációt a rendszergazda hathavonta felülvizsgálja, és a módosításokat átvezeti.

19.2. Elektronikus információs rendszerelem leltár

A rendszergazdának nyilvántartást kell vezetni a kiszolgálók és munkaállomások pontos és naprakész hardver konfigurációjáról, az elhelyezkedésükről, a működő alkalmazások egyedi beállításairól és az értük felelős személy nevéről.

19.3. Legszűkebb funkcionalitás

Az elektronikus információs rendszerekben mind jogosultági szintek, mind az engedélyezett kommunikációs csatornák tekintetében a legszűkebb funkcionalitás elvét kell alkalmazni, így:

- a szoftvereket a lehető legkisebb jogosultsági szinttel kell futtatni
- csak a szükséges portokat, protokollokat és szolgáltatásokat szabad engedélyezni

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.

19.4. Duplikálás elleni védelem

Az Önkormányzatnak ellenőriznie kell, hogy az elektronikus információs rendszer elemei nincsenek-e többszörösen felvéve a saját nyilvántartásában, illetve a saját eszközei nem szerepelnek-e más elektronikus nyilvántartásban.

19.5. A szoftver használat korlátozásai

Az Önkormányzatban kizárólag jogtiszta, a megfelelő licence-el rendelkező, vagy nyílt forráskódú szoftverek használata engedélyezett. Mind a kereskedelmi forgalomban kapható licence köteles, mind a szabad vagy nyílt forráskódú szoftverek használatát a felelős vezető engedélyezi.

Az alkalmazott szoftverekről leltárt kell vezetni és a telepítőkészletek egy mesterpéldányát valamint a licence-ket elzárva, megfelelően biztonságos helyen kell tárolni.

A szerzői jogokkal védett szellemi termékek felhasználását nyomon kell követni.

19.6. A felhasználó által telepített szoftverek

A felhasználóknak tilos a munkaállomás szoftveres konfigurációját megváltoztatni, így:

- szoftvert telepíteni
- az rendszerszoftver alapkonfigurációját megváltoztatni

Fenti tevékenységeket csak a rendszergazda végezheti.

A munkaállomások rendszerszoftverének és a telepített alkalmazásainak megfelelőségét az IBF félévente ellenőrzi.

20. Rendszer karbantartási eljárásrend

20.1. Rendszeres karbantartás

20.2. A karbantartások engedélyezése

A felhasználókat a karbantartás megkezdése előtt legalább 1 héttel értesíteni szükséges, ha a karbantartás az elektronikus információs rendszer leállításával vagy az ügymenetet befolyásoló időpontban történik.
A tervezett karbantartásokat dokumentált formában az felelős vezető engedélyezi

20.3. A karbantartások dokumentálása, nyilvántartása

Az elvégzett munkákat a karbantartási nyilvántartásban kell dokumentálni. 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).

20.4. A karbantartások ütemezése

A rendszergazda éves karbantartási tervet készít, melyet az felelős vezető hagy jóvá.

20.5. Kiszállítás

Amennyiben az adatot tartalmazó adathordozó szállítása válik szükségessé, akkor a jelen IBSZ *{V.22.3 Adathordozók szállítása}* fejezetben leírtak szerint kell eljárni. Az elszállítást a rendszergazda engedélyezi.

20.6. 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.

20.7. Karbantartók

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

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

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

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

b) szerződéses kapcsolattartó neve, elérhetősége,

c) a szerződő szervezet, kapcsolattartó megnevezése,

d) karbantartás végzők neve, elérhetősége,

e) szerződés azonosítója,

f) szerződés időtartama,

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

A külső féllel kötött szerződésbe bele 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.

20.8. Adathordozók ellenőrzése

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

20.9. Távoli karbantartás

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

A távoli hozzáférések során VPN kapcsolatot kell alkalmazni, mely megfelelő erősségű titkosítással, ismert sérülékenységet nem tartalmazó kriptográfiai algoritmussal épül fel.

A VPN kapcsolódáskor a kapcsolódó felet egyedileg kell azonosítani és hitelesíteni. A távoli karbantartás elvégzése után a távoli félnek bontania kell a VPN kapcsolatot.

A távoli karbantartásokról a rendszergazdának nyilvántartást kell vezetni (naplózni).

Távoli hozzáféréseket csak olyan eszközről lehet kezdeményezni, melyen

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

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

c) a helyi tűzfal bekapcsolásra került.

21. A változások kezelésének eljárásrendje

Az Önkormányzat elektronikus információs rendszereinek megbízható és biztonságos működésének fenntartása érdekében új hardver vagy szoftver elemmel kerül kiegészítésre a meglévő elektronikus információs rendszer, vagy egy régi hardver vagy szoftver kerül megváltoztatásra, esetleg megszüntetésre, akkor az alábbi előírásokat kell teljesíteni.

Az elektronikus információs rendszer fejlesztéseknél a fejlesztések szállítóinak felelőssége minden, az új rendszer implementálásához szükséges dokumentum szolgáltatása. Ezen dokumentumok:

d) funkcionalitások ismertetése;

e) felhasználói kézikönyv;

f) installációs terv/forgatókönyv;

g) rendszer kapacitási követelményei;

h) rendszer kapcsolatainak ismertetése.

i) fejlesztői funkcionális teszt;

j) kapcsolatokat ellenőrző teszt;

k) terheltség teszt;

l) biztonsági teszt;

m) migrációs teszt.

Az új hardver vagy szoftver elemeknek az Önkormányzat elektronikus információs rendszerébe való illesztéséhez a fent említett dokumentumokra és tesztekre azért van szükség, hogy ezek alapján az felelős vezető és szükség esetén az informatikai biztonsági felelős döntést tudjanak hozni a bevezetés engedélyezéséről.

22. Adathordozók védelmére vonatkozó eljárásrend

22.1. Hozzáférés az adathordozókhoz, adathordozók használata

Az Önkormányzatnál csak az Önkormányzat tulajdonában lévő, regisztrált adathordozót lehet használni. Adathordozó igénylését a rendszergazdához kell benyújtania a szervezeti egység vezetőjének.

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

Nem publikus adatot adathordozón, elektronikus levélben vagy egyéb más módon (Pl.: felhőszolgáltatás) az Önkormányzat informatikai rendszeréből kijuttatni csak az Adatgazda írásos engedélyével szabad. Az adatok kivitelét az Adatgazdának vagy a szervezeti egység vezetőjének kell engedélyeznie, minden esetben írásos formában.

Az Önkormányzat az adathordozók használatát információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozhatja.

22.2. Adathordozók tárolása

Az Önkormányzat elektronikus információs rendszereinek kiszolgáló oldali adathordozóit a szerverhelyiségben kell tárolni. A szerverhelyiség fizikai védelmét a jelen IBSZ {*IV.16.7 Hozzáférés az adatátviteli berendezésekhez és csatornákhoz*} fejezetében foglaltaknak megfelelően kell kialakítani.

A felhasználók részére kiosztott mobil adathordozókat használaton kívül elzártan kell tárolni.

22.3. Adathordozók szállítása

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

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

22.4. 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.

22.5. Ismeretlen tulajdonos

Az Önkormányzat elektronikus információs rendszereiben tilos az Önkormányzat tulajdonát nem képező adathordozót csatlakoztatni.

22.6. 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 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.

22.6.1. 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;

d) a mobil infokommunikációs eszközök 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 az felelős vezető részére át kell adni.

22.6.2. 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.)

23. Azonosítási és hitelesítési eljárásrend

23.1. Azonosítás és hitelesítés (szervezeten belüli felhasználók)

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

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

23.2. 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 havi rendszerességgel történő végrehajtása az rendszergazdák feladata.

23.3. A hitelesítésre szolgáló eszközök kezelése

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

Az Önkormányzat 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 180 naponta meg kell változtatni;

c) a jelszavakat két napon belül nem szabad megváltoztatni;

d) az előző jelszavak újra használatát kerülni kell;

e) zárolás esetén előre beállított időtartam eltelte után engedélyezze vissza a felhasználói fiókot.

23.4. Jelszó (tudás) alapú hitelesítés

Az Önkormányzatnál csak olyan azonosítási rendszert lehet alkalmazni, mely nem tárolja a jelszót nyílt formában. A megfelelő, ismert sérülékenységektől mentes kriptográfiai algoritmus kiválasztásába be kell vonni az IBF-et.

23.5. Birtoklás alapú hitelesítés

Az ASP rendszer használatára jogszabály alapján kötelezett szervezetnél, illetve szervezeti egységnél 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.

23.6. A felhasználó felelősségi köre a jelszó használat során

Az Önkormányzat elektronikus 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;

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

a) könnyen megjegyezhető, és nehezen kitalálható legyen;

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

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

d) ne legyen sorozat.

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

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

23.7. 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.

23.8. A hitelesítésre szolgáló eszköz visszacsatolása

Az illetéktelen hozzáférések elkerülése érdekében olyan hitelesítési módszereket kell alkalmazni, amely a sikertelen bejelentkezési kísérletekről nem ad vissza semmilyen olyan érdemi információt, amelyet egy támadó ki tud használni és illetéktelenül hozzá tud férni az Önkormányzat elektronikus információs rendszereihez.

23.9. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

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

23.10. Hitelesítés szolgáltatók tanúsítványának elfogadása

Az Önkormányzat elektronikus információs rendszereihez az Internet irányából csak szabványos, kriptográfiai módszerrel azonosított és hitelesített felhasználó, titkosított hálózati kapcsolaton keresztül lehet hozzáférni.

A hálózati kapcsolatok titkosításához csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat lehet felhasználni.

24. 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 napi munkavégzéshez (nem kiemelt jogosultsággal kezelhető esetekben) a normál felhasználói jogú azonosítót (nem admin) kell használnia.

d) A rendszergazda rendszergazdai feladatok ellátását nevesített admin felhasználóval végezheti.

24.1. Felhasználói fiókok kezelése

A jogosultságok és a hozzáférések kezelésekor az alábbi alapelveket kell figyelembe venni:

a) Olyan minimális jogosultságok alkalmazásával kell a felhasználóknak rendelkezniük, melyekkel minimális szintre csökkenthető a rosszindulatú vagy egyéb jogosulatlan hozzáférés kockázata.

b) A felhasználóknak a munkájuk ellátásához szükséges minimális jogosultságokat kell biztosítani, a munkavégzésük időtartamára.

c) Az azonos tevékenységet ellátó felhasználók jogosultságai szerepkörökbe legyenek sorolva, és a felhasználók a szerepkörökbe kerüljenek besorolásra.

d) Az összeférhetetlenségi szabályokat figyelembe kell venni.

e) Az elektronikus információs rendszerben alkalmazott hozzáférési jogosultságok tényét és jóváhagyási folyamatát dokumentálni kell.

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

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

h) Az éles környezetekben a fejlesztők nem rendelkezhetnek hozzáférési jogosultságokkal.

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 szervezeti egység vezető aláírását.

e) A jogosultságigénylési folyamat által előállt dokumentumot (elsősorban elektronikus, vagy papír alapú) ellenőrzés céljából visszakereshető módon tárolni kell.

f) A kiosztott felhasználói jogosultságokat az Adatgazdáknak félévente felül kell vizsgálni.

24.2. Kiemelt jogosultságok kezelése

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

A kiemelt jogosultságok kiadásának engedélyezési eljárása során az alábbiakat kell figyelembe venni:

a) pontosan meg kell határozni azokat a rendszerelemeket (szerver, hálózati eszköz, appliance, operációs rendszerek, adatbázis kezelők, alkalmazások), amelyhez az adminisztrátori jogosultságokat kell hozzá rendelni;

b) az adminisztrátori jogosultságokat a szükséges minimum használat elve alapján kell kiadni;

c) az adminisztrátori jogot kizárólag az felelős vezető engedélyezheti írásban.

Az üzemeltetők csak az elektronikus információs rendszer, illetve alkalmazás üzemeltetéséhez szükséges információkhoz férhetnek hozzá. A részükre biztosított adminisztrátori jogosultság birtokában 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.

24.3. Hozzáférési jogok igénylésének eljárásrendje

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

24.3.1. ASP szakrendszerek hozzáférése

Az ASP rendszer használatára jogszabály alapján kötelezett szerve, vagy szervezeti egységek vonatkozásában 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 önkormányzati ASP 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.

24.3.2. Új hozzáférési jog igénylése

Az igénylő a hozzáférési jogok igénylését a jelen IBSZ *{4. 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 jóvá kell hagyatni (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:

- rögzíti az igényt a jogosultság kezelő rendszerben, vagy a jelen IBSZ *{5. számú melléklet – Hozzáférések nyilvántartása űrlap}* mellékletében található űrlapon.
- 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 kért feladatok elvégzésének bizonylatolása érdekében a rendszergazda rögzíti a beállítás tényét a jogosultság kezelő rendszerben, vagy aláírja a Jogosultságigénylési űrlapot, valamint e-mail-en tájékoztatja az igénylőt és a jóváhagyót a jogosultságok megadásáról.

Az aláírt űrlapok ezek után a felelős vezető által kijelölt helyen kerülnek tárolásra visszakereshető formában.

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

24.3.3. Hozzáférési jog módosítása

A felelős vezető a dolgozó megváltozott feladatkörének, illetve munkakörének ellátásához szükséges jogosultság módosításához kitölti a jelen IBSZ *{4. számú melléklet – Jogosultságigénylési űrlap}* mellékletében található űrlapot.

Az eljárásrend megegyezik az *{24.3.2 Új hozzáférési jog igénylése}* fejezetben leírtakkal annyi kiegészítéssel, hogy amennyiben szervezeti egység váltás történik, akkor a rendszergazda gondoskodik a már nem szükséges jogosultságok visszavonásáról.

24.3.4. Hozzáférési jog visszavonása

A felelős vezetőnek haladéktalanul intézkednie kell a már nem szükséges jogosultságok visszavonása iránt. A hozzáférési jogosultság visszavonását a jogosultság kezelő rendszerben vagy a jelen IBSZ *{4. számú melléklet – Jogosultságigénylési űrlap}* mellékletében található űrlapon kell kezdeményezni.

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

- rögzíti az igényt a jogosultság kezelő rendszerben, vagy a jelen IBSZ *{5számú melléklet – Hozzáférések nyilvántartása űrlap}* mellékletében található űrlapon.
- visszavonja a jogosultságot.
- rögzíti a beállítás tényét a jogosultság kezelő rendszerben, vagy aláírja a jelen IBSZ *{4. számú melléklet – Jogosultságigénylési űrlap}* mellékletében található, kitöltött űrlapot, valamint e-mail-en tájékoztatja a munkahelyi vezetőt a visszavonásról.

24.3.5. 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 háromhavonta felülvizsgálja.

24.4. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

Az Önkormányzatnál nincsenek azonosítás és hitelesítés nélkül engedélyezett tevékenységek.

24.5. A felelősségek szétválasztása

Az Önkormányzat 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.

24.6. Legkisebb jogosultság elve

Az Önkormányzat elektronikus információs rendszereiben a jogosultságok kezelésekor a szükséges, minimum elvet kell követni, azaz mindenki csak annyi jogosultságot kapjon, ami a munkája elvégzéséhez nélkülözhetetlen.

A felhasználó a munkaállomásán nem kaphat helyi rendszergazda jogot.

24.7. Jogosult hozzáférés a biztonsági funkciókhoz

Az Önkormányzat 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

24.8. 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.

24.9. Privilegizált fiókok

A jelen IBSZ {*24.7 Jogosult hozzáférés a biztonsági funkciókhoz*} fejezetében meghatározott biztonsági funkciók elérésére a rendszergazda jogosult.

24.10. A munkaszakasz zárolása

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

24.11. Képernyőtakarás

A munkaszakasz zárolását oly módon kell megvalósítani, hogy a zárolási képernyőn ne látszódjanak adatokat tartalmazó alkalmazások ablakai.

24.12. A munkaszakasz lezárása

A felhasználó a munkaidő végeztével köteles a munkaállomását kikapcsolni.

24.13. Vezeték nélküli hozzáférés

Az Önkormányzatnál csak az IBF által jóváhagyott vezeték nélküli (továbbiakban: WIFI) hozzáférési pont létesíthető.

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

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

24.14. Mobil eszközök hozzáférése

Mobil eszközzel csak az Önkormányzat által biztosított elektronikus levelezéshez lehet hozzáférni. Ebben az esetben csak az Önkormányzat által biztosított mobil eszköz vagy védelmi rendszerrel is ellátott mobil eszköz használható.

24.15. Titkosítás

Az Önkormányzat által biztosított mobil eszközökön, vagy a védelmi rendszerrel is ellátott mobil eszközön be kell kapcsolni a teljes eszköz vagy tároló titkosítást.

24.16. Külső elektronikus információs rendszerek használata

Az Önkormányzat 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.

Az Önkormányzat 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.

24.17. Korlátozott használat

Külső elektronikus információs rendszert abban az esetben lehet az Önkormányzat elektronikus információs rendszereihez történő hozzáférés céljából felhasználni, hogy ha jelen IBSZ *{V.24.16 Külső elektronikus információs rendszerek használata}* pontjában foglalt követelményeket

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

b) cégszerű felhasználás során szerződésben rögzítették.

24.18. 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.

24.19. Információ megosztás

Az Önkormányzat 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, különös tekintettel a személyes adatokra.

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

24.20. Nyilvánosan elérhető tartalom

A nyilvános tartalmak kezelésével kapcsolatban a következők szerint kell eljárni:

a) Ki kell jelölni azokat a személyeket, akik jogosultak az Önkormányzat honlapján az Önkormányzat és az Önkormányzat 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 az Önkormányzat honlapját a nem nyilvános információk tekintetében, és gondoskodni kell azok eltávolításáról.

25. Rendszer és információ sértetlenségre vonatkozó eljárásrend

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

25.1. Hibajavítás

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

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

A módosításokkal egy időben a változásokat a dokumentációkban 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.

Gondoskodni kell arról, hogy a munkaállomásokon telepített operációs rendszerek és egyéb segédprogramok naprakészek legyenek, tartalmazzanak minden stabilnak számító frissítést.

25.1.1. 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.

25.1.2. 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.

25.2. Kártékony kódok elleni védelem

Az Önkormányzatnak 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) Kártékony kód elleni védelmi mechanizmus nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem üzemeltethető.

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

d) A kártékony kód elleni alkalmazások adatbázisát automatikusan, lehetőség szerint naponta többször frissíteni kell.

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

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

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

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

i) A kártékony kód felfedezésekor értesítenie kell az IBF-et, az intézkedési lépéseket szabályozni kell.

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

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

25.2.1. Vírusriadó

A vírusriadót az IBF javaslatára az felelős vezető 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 aktivizálódik a 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 vírus mentesítés szakmai felügyeletét az IBF és a rendszergazda közösen látják el.

25.2.2. Teendők vírusfertőzés, vírusriadó esetén

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

A rendszergazda a feladatai:

a) a vírusos számítógép leválasztása a hálózatról;

b) a vírusvédelmi rendszer támogatójának értesítése;

c) a vírus fertőzés következtében szükséges intézkedések koordinálása;

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

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 az Önkormányzaton kívülre is terjedhetett, értesíteni kell az érintett szervezeteket;

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

25.3. 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.

A fenti feladatok végrehajtása a rendszergazda feladata.

A rendszergazdának ismernie kell az Önkormányzat 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.

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 felelős vezető pedig jóváhagyja.

25.3.1. 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.

25.4. Biztonsági riasztások és tájékoztatások

Az Önkormányzatnak az IBF útján folyamatosan figyelemmel kell kísérnie a Kormányzati Eseménykezelő Központ által kiadott riasztásokat, valamint a Nemzeti Elektronikus Információbiztonsági Hatóság által közzétett értesítéseket.

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

25.5. Bemeneti információ ellenőrzés

Az ASP rendszer használatára jogszabály erejénél fogva kötelezett szervezet, illetve szervezeti egység vonatkozásában az önkormányzati ASP rendszer esetében meg kell határoznia a felelős vezetőnek, hogy mely Önkormányzati munkaállomásról jogosult a felhasználó elérni az önkormányzati ASP rendszert. A működtető által kiadott kliens oldali tanúsítvány telepítésével biztosítható a bemeneti információ belépési pontok érvényessége.

25.6. A kimeneti információ kezelése és megőrzése

A kimeneti információk (pl.: nyomtatás) kezelésével és szétosztásával kapcsolatban az Önkormányzat 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.

26. Naplózási eljárásrend

Az elektronikus információs rendszereknél a következő naplózási eljárásrendet kell kialakítani.

26.1. Naplózható események

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

a) a felhasználók adminisztrációs tevékenysége:

- sikeres/sikertelen bejelentkezés;
- sikeres 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.

i) naplózások be és kikapcsolása

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.

26.2. 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.

26.3. Időbélyegek

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

Az Önkormányzatnak szinkronizálnia kell a rendszer belső rendszer órákat a belső, illetve a külső időszolgáltatóval.

26.4. 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.

26.5. A naplóbejegyzések megőrzése

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

26.6. Naplógenerálás

Olyan elektronikus információs rendszereket kell alkalmazni, melyek

a) biztosítják a naplóbejegyzések előállítási lehetőségét;

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

27. Rendszer és kommunikáció védelmi eljárásrend

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

27.1. Határvédelem

Mind a belső, mind a külső hálózati szolgáltatókhoz történő hozzáférés esetében az alábbi biztonsági követelményeket kell megvalósítani:

a) Alaphelyzetben minden forgalmat tiltani kell, és csak azt szabad engedélyezni, amelyre az IT szolgáltatások működéséhez szükség van.

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

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

d) Teljes körűen definiált, minimális protokollt felhasználó interfészt kell alkalmazni az Önkormányzat és más szervezet tulajdonában lévő hálózat között.

e) A felhasználókat jelszóval vagy indokolt esetben tanúsítvány használattal kell hitelesíteni.

f) Az Önkormányzat belső hálózatáról Internet kapcsolat kizárólag tűzfallal védett útvonalon keresztül létesíthető.

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

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

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

j) 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 felhasználónak az Internet használata során tilos:

a) az Önkormányzattal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele,

b) az Interneten elérhető nyilvános chat-és fórum oldalakon Önkormányzati email címmel hozzászólni,

c) fájlcserélő alkalmazásokat futtatni, illetve nem Önkormányzati munkavégzéshez szükséges letöltéseket végezni,

d) Önkormányzati email címmel nyilvános levelezőlistákra, hírlevelekre feliratkozni.

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.

Az Önkormányzat 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.

27.1.1. A hálózati szolgáltatások belső használatának szabályozása

Az Önkormányzat 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 hálózatokat és hálózati szolgáltatásokat, 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;

Az Önkormányzat elektronikus információs rendszerében TILOS modemet csatlakoztatni.

27.1.2. A felhasználó hitelesítése külső összeköttetésekhez

A felhasználókat jelszóval hitelesíteni kell és ellenőrizni kell a felhasználók információszolgáltatáshoz való hozzáférését.

27.1.3. Hálózat szegmentálás

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

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

27.1.4. A hálózati összeköttetések ellenőrzése

A publikus Internet szolgáltatások, valamint más Hivatalok (Kincstár, Takarnet, stb.) és az Önkormányzat elektronikus információs rendszere közötti hálózati forgalom ellenőrzésére a tűzfalak naplói szolgáljanak.

27.1.5. A hálózati üzenettovábbítás ellenőrzése

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

27.1.6. Nyilvános elektronikus információs rendszerek védelme

Amennyiben az Önkormányzat valamely szervezeti egységének honlapját web hosting szolgáltató működteti, akkor a vele kötött szerződésben elő kell írni a nyilvánosan elérhető tartalmakkal és rendszerekkel kapcsolatos információbiztonsági követelményeket.

27.2. Kriptográfiai védelem

Az Önkormányzatnak az elektronikus információs rendszereiben az adatok sértetlenségének és bizalmasságának védelmére szabványos, a vonatkozó jogszabályokban biztonságosnak minősített kriptográfiai műveleteket kell alkalmaznia.

27.2.1. A kriptográfiai óvintézkedések használatának szabályzata

Az Önkormányzat elektronikus 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 rejtjelezett adatok visszaállításának szabályai és eljárásai azokra az esetekre, amikor a kulcs megsérült vagy elveszett.

27.2.2. Kriptográfiai megoldások alkalmazásának feltételei

Az Önkormányzat 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.

27.3. 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.

Az önkormányzati ASP rendszerhez történő csatlakozás során használandó E-személyi kezelését a következő szolgáltatói dokumentumok szabályozzák:

a) Általános szerződési feltételek a PKI szolgáltatásokhoz (ÁSZF-PKI) v1.6

b) Szolgáltatási szabályzat a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz (HSZSZ-ESZIG) v1.3

c) Hitelesítési rend a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz (HR-ESZIG) v1.3

d) Időbélyegzés Szolgáltatási Rend (ISZR) v1.2

e) Szolgáltatási szabályzat a minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz (HSZSZ-M) v1.6

27.4. Mobilkód korlátozása

Az ASP rendszer használatára jogszabály erejénél fogva kötelezett szervezet, vagy szerezeti egység vonatkozásában az önkormányzati ASP szakrendszerhez kapcsolódó munkaállomások web böngészőiben tiltani kell a következő mobil kódok futtatását:

a) Java Applet

b) JavaScript

c) VB Script

d) CGI

e) ActiveX

f) Shockwave

g) Flash

Az alapértelmezett beállításokhoz képest a további szigorításokat kell a web böngészőkben beállítani:

a) Előreugró ablakok - blokkolás

b) Mikrofonok, kamerák hozzáférése - tiltás

c) Automatikus letöltés - rákérdezés

A web böngészők fentieknek megfelelő biztonsági beállításáért a rendszergazda a felelős.

A web böngészők helyes beállításait az IBF-nek ellenőriznie kell.

28. A biztonság ellenőrzésének eljárásrendje

Az Önkormányzat információbiztonsági szintjét rendszeres belső értékelésnek veti alá az alábbiakban meghatározottak szerint.

28.1. Biztonsági értékelések

A rendszeres biztonsági értékelést a felelős vezető rendeli el az IBF által készített és előterjesztett ellenőrzési terv alapján. Az értékelések során ellenőrizni kell:

- az elektronikus információs rendszer védelmi intézkedéseinek hatékonyságát
- felülvizsgálni a bevezetett intézkedések hatékonyságát és működőképességét

Az IBF az értékelések eredményéről jelentést készít és ismerteti annak tartalmát a szervezet minden információbiztonsági szerepkört betöltő szereplőjével.

A biztonsági értékeléseket minden évben legalább egyszer el kell végezni.

VI. HATÁLYBA LÉPTETŐ RENDELKEZÉSEK

Jelen Informatikai (IT) Biztonsági Szabályzat 2018. december 15. napján lép hatályba, rendelkezéseit e naptól kell alkalmazni.

Monor, 2018. december 14.

VII. EGYETÉRTÉSI, MEGISMERÉSI ÉS KIADMÁNYOZÁSI ZÁRADÉK

Egyetértési nyilatkozat

A 2018. december 15-től hatályos Informatikai (IT) Biztonsági Szabályzatban foglaltakkal egyetértek:

Név	Feladat, hatáskör	Dátum	Aláírás
dr. Zsombok László	polgármester	2018.12.14	

Megismerési, elfogadási és kiadási nyilatkozat

Az Informatikai (IT) Biztonsági Szabályzatban foglaltakat megismertem, az általam vezetett intézményre és gazdasági társaságok vonatkozóan elfogadom és kiadom.

Tudomásul veszem, hogy az abban foglaltakat a munkám során köteles vagyok betartani, egyben az intézmény, illetve a gazdasági társaság érintett foglalkoztatottjaira és alkalmazottaira, valamint a szerződésben álló, vagy egyéb módon közreműködő érintett külső félre vonatkozóan betartatni:

Név	Feladat, hatáskör	Dátum	Aláírás
Monori Polgármesteri Hivatal dr. Urbán Hajnalka	jegyző	2018.12.14.	
Monori Kossuth Lajos Óvoda Trincsiné Márton Zsuzsanna	intézményvezető	2018.12.14.	
Monori Petőfi Óvoda Zsember Ágnes	intézményvezető	2018.12.14.	
Monori Tesz - Vesz Óvoda Seres Istvánné	intézményvezető	2018.12.14.	
Monori Szivárvány Óvoda Bánné Keller Márta	intézményvezető	2018.12.14.	
Monori Napsugár Óvoda Técsiné Vas Ildikó	intézményvezető	2018.12.14.	
Monori Bölcsőde Fazekas Józsefné	intézményvezető	2018.12.14.	
Monori Gondozási Központ Iványi Margit	intézményvezető	2018.12.14.	
Dr. Borzsák István Városi Könyvtár és Helytörténeti Kiállítás Szántóné Horváth Éva	igazgató-helyettes	2018.12.14.	
Monor Város Önkormányzata Védőnői Szolgálat Molnárné Virág Erika	vezető védőnő	2018.12.14.	

Vigadó Kulturális és Civil Központ Nonprofit Kft. Hanzelik Andrea	ügyvezető	2018.12.14.	
Monori Városfejlesztő Nonprofit Kft. Rajki László	ügyvezető	2018.12.14.	
Monori Sportcsarnok Üzemeltető Nonprofit Kft. Rajki László	ügyvezető	2018.12.14.	
Kövál Nonprofit Zrt. Takár Gábor	vezérigazgató	2018.12.14.	

1. Mellékletek

1. számú melléklet – Értelmező Rendelkezések

2. számú melléklet – Az Önkormányzat információs rendszereinek biztonsági osztályba sorolása

3. számú melléklet – Biztonsági események jelentése

4. számú melléklet – Jogosultságigénylési űrlap

5. számú melléklet – Hozzáférések nyilvántartása űrlap

6. számú melléklet – Felhasználói Nyilatkozat

7. számú melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén

8. 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.[1]

(27) Kockázat becslés: Olyan folyamat, amely a releváns fenyegetések szintjét és hatását értékkel jellemzi és megállapítja a fenyegetések szintje, hatásuk, illetve a védelmi igények[2] 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[3].

(34) Kockázat kiértékelés: Folyamat, amely során a megbecsült kockázatok összevetésre kerülhetnek a tolerálható szinttel.[4]

---

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

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

[3] 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..

[4] 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.[5]

(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.

[5] 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 – Az Önkormányzat információs rendszereinek biztonsági osztályba sorolása

Az Önkormányzat által üzemeltetett, a Önkormányzatban, valamint az önkormányzati intézményekben működtetettinformációs rendszereinek biztonsági osztályba sorolása

Informatikai Rendszer(IR) megnevezése	IR leírása	Adatgazda	A rendszerben kezelt adatok	Bizalmasság	Sértetlenség	Rendelkezésre állás	A rendszer biztonság i osztálya
Kimera	Dokumentumok iktatása	Jegyző	személyes adatok, beszámoló, költségvetés, szerződések, kötelezettségvállalás	3	3	2	3
Winszoc	Szociális segélyezési rendszer	Jegyző	személyes adatok	3	3	2	3
Szoszo	Gondozói program	Jegyző	szociális gondozi nyilvántartása	1	1	1	1
Corzó	Pénzügyi	Jegyző	pénzügyi adatok	2	3	2	3
Önkadó	Helyi adók nyilvántartása	Jegyző	helyi adók, személyes adatok	2	3	2	3
Vagyonkataszter	Ingatlan vagyon-kataszter rends	Jegyző	önkormányztai ingatlanok adatai	1	2	1	2
Cégnyilvántartás	Ipar és kereskedelmi rendszer	Jegyző	Cégek és telephelyengedélywk adatai	3	3	2	3

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 felelős vezető aláírása

4. 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

Felelős vezetői jóváhagyás

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

Adatgazdai jóváhagyás

Adatgazda: ....
Kelt ..... adatgazda aláírása

A jogosultságot beállító aláírása

Rendszergazda: ....
Kelt ..... rendszergazda aláírása

5. számú melléklet – Hozzáférések nyilvántartása űrlap

Sorszám	Iktatószám	Felhasználó neve	Igényelt jogo-sultság	Igénylés dátuma	Felelős vezető

6. számú melléklet – Felhasználói Nyilatkozat

Nyilatkozat

Alulírott

név: .....

beosztás: .....

szervezeti egység: .....

kijelentem, hogy az Önkormányzat Informatikai Biztonsági Szabályzatának tartalmát megismertem és elfogadom, hogy azt munkám során betartom, illetve betartatom (vezetők esetén).

....., 2018. .....

.....
Aláírás

7. számú melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén

Információbiztonsági tájékoztatás

1. Tájékoztatom, hogy az Önkormányzattal (továbbiakban: az Önkormányzat) fennálló köztisztviselői, közalkalmazotti, munka, egyéb foglalkoztatási jogviszonya megszűnésének napjától, 201... . .....-től az Önkormányzat elektronikus információs rendszereihez való hozzáférési jogosultsága megszűnik. Legkésőbb ezen a napon köteles a használatában lévő, az Önkormányzat elektronikus információs rendszerével kapcsolatos valamennyi eszközt hiánytalanul, sértetlenül munkáltatója részére visszaszolgáltatni.

2. Az Önkormányzatnál működő elektronikus információs rendszereket az Önkormányzat kizárólag Önkormányzati munkavégzés céljából biztosítja a munkatársak részére, az elektronikus információs rendszerekben keletkező és ott tárolt, kezelt adatok, információk vonatkozásában az Önkormányzat fenntartja magának a tulajdonjogot.

3. Az Önkormányzatnak továbbra is hozzáférési lehetősége van az Ön által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz.

4. Közszolgálati, munka, illetve egyéb foglalkoztatotti jogviszonyának megszűnését követően nem jogosult az Önkormányzat elektronikus információs rendszereiben tárolt, 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.

Monor, 201 ... .

.....
felelős vezető

A fenti tájékoztatást tudomásul vettem:

Monor, 201.....

.....
köztisztviselő/közalkalmazott/munkavállaló egyéb foglalkoztatott neve

.....
aláírása

8. számú melléklet – Titoktartási Nyilatkozat

TITOKTARTÁSI NYILATKOZAT

Alulírott

Név: _____

Anyja neve: _____

Lakcím: _____

Sz. ig. szám: _____

a ..... munkatársa kijelentem, hogy

az **Önkormányzat,** 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.

Monor, 201 .....

.....

Nyilatkozó

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