HERNÁD NAGYKÖZSÉG ÖNKORMÁNYZATA

INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Zsírosné Pallaga Mária
polgármester

Hernád, 2015. június 20.

Tartalomjegyzék

I. ÁLTALÁNOS RÉSZ

I.1. Bevezetés

Hernád Nagyközség Önkormányzata (továbbiakban: az Önkormányzat) 2015-ben Európai Uniós projekt keretében a korábban egyedileg fejlesztett és vásárolt elektronikus információs rendszereit központi, jogszabály által kijelölt ASP rendszerekre cserélte.

Ennek keretében a következő elektronikus információs rendszerek kerültek bevezetésre ASP szolgáltatás keretében:

a) ASP Gazdálkodás

b) ASP Irat

c) ASP Adó

d) ASP Ingatlanvagyon Kataszter

e) ASP Iparker

Az Ibtv. alapján a szervezeteknek a saját hatáskörükbe tartozó elektronikus információs rendszereiket kell biztonsági osztályba sorolni, illetve ezen rendszerek vonatkozásában kell megvalósítaniuk a technológiai vhr-ben előírt logikai védelmi intézkedéseket.

A fentiek alapján az ASP szolgáltatásként igénybe vett elektronikus információs rendszerek logikai védelmi intézkedéseinek megvalósításáért elsősorban az ASP rendszer működtetője felelős. Ezen rendszerek vonatkozásában az Önkormányzat csak a végfelhasználó specifikus logikai védelmi intézkedéseket köteles megvalósítani.

Az ASP R alapján csak olyan szervezet csatlakozhat az önkormányzati ASP központhoz, amely teljesíti az Ibtv.-ben foglalt információbiztonsági követelményeket.

Az ASP rendszer működtetője a későbbiekben információbiztonsági követelményeket dolgoz ki, melyeket az IBSZ felülvizsgálatakor figyelembe kell venni.

Az Önkormányzat a fentieken kívül az informatikai alapinfrastruktúráját saját maga üzemelteti, ezért erre nézve az IBSZ rendelkezései az irányadók.

I.2. Az IBSZ célja

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

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

a) A jogkövető magatartás és a jó hírnév érdekében védeni a szervezet értékeit,

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

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

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

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

I.3. Hatály

I.3.1. Szervezeti-személyi hatály

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

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

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

g) a közszolgálati jogviszony alapján foglalkoztatott munkatársak,

h) a munkaviszony alapján foglalkoztatott munkatársakra,

i) az Önkormányzattal szerződéses kapcsolatban álló természetes és jogi személyekre,

j) más szervezetek képviseletében az Önkormányzat munkahelyein tartózkodó személyekre.

I.3.2. Tárgyi hatály

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

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

Az IBSZ tárgyi hatálya nem terjed ki az ASP rendszerek rendszerelemeire, ezen rendszerelemek biztonságának megteremtése az ASP szolgáltató feladata.

I.3.3. Területi hatály

Az IBSZ területi hatálya kiterjed az Önkormányzat székhelyére.

I.3.4. Időbeni hatály

Jelen IBSZ a kiadás napján lép hatályba és visszavonásig érvényes.

I.4. Az IBSZ felülvizsgálata

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

Az IBSZ-t módosítani kell, ha változás áll be

a) az Önkormányzat szervezeti felépítésében,

b) az Önkormányzat elektronikus információs rendszereinek működésében,

c) az Önkormányzat elektronikus információs rendszereinek működését és biztonságát meghatározó jogszabályi környezetben,

d) illetve ha olyan új fenyegetettség jelenik meg, mely veszélyeztetheti az Önkormányzat elektronikus információs rendszereit vagy az azokban kezelt adatokat.

Felül kell vizsgálni továbbá az IBSZ-t, amikor az Önkormányzat vagy valamelyik elektronikus információs rendszere újabb, az Ibtv.-ben meghatározott biztonsági szintet vagy biztonsági osztályt ér el.

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

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

I.4.1. Hatásköri és illetékességi szabályok

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

I.5. Kapcsolódó dokumentumok

I.5.1. Jogszabályok

a) 2012. évi I. törvény a munka törvénykönyvéről

b) 2012. évi C. törvény a Büntető Törvénykönyvről

c) 1959. évi IV. törvény a Polgári Törvénykönyvről

d) 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről

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

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

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

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

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

j) 1999. évi LXXVI. törvény a szerzői jogról

k) 2001. évi XXXV. törvény az elektronikus aláírásról

l) 1990. évi C. törvény a helyi adókról (továbbiakban: Htv.)

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

n) 186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről

o) 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

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

q) 62/2015. (III. 24.) Korm. rendelet az önkormányzati ASP központról és a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet módosításáról (továbbiakban: ASP R)

r) 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

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

t) 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)

I.5.2. Kapcsolódó szabványok, ajánlások

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

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

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

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

I.5.3. Az IBSZ-hez kapcsolódó belső dokumentumok

a) Szervezeti és Működési Szabályzat

b) Iratkezelési Szabályzat

c) Selejtezési Szabályzat

d) Közzétételi Szabályzat

e) Cselekvési terv az Önkormányzat elvárt biztonsági szintjének eléréséhez

f) Cselekvési terv az Önkormányzat elektronikus információs rendszerei elvárt biztonsági osztályainak eléréséhez

g) Kitöltési útmutató a jogosultság igényléshez Az „Önkormányzati ASP központ felállítása" tárgyú projekthez

I.6. Az IBSZ általános követelményei

Az IBSZ és az IBSZ *{2. sz. Felhasználói Informatikai Biztonsági Házirend}* melléklete (továbbiakban: FIBH) előírásainak alkalmazása, betartása, illetve betartatása, a *{I.3.1. Szervezeti-személyi hatály}* pontban megjelöltek számára kötelező.

Az információbiztonsági előírások betartása megvédi az Önkormányzatot és a *{I.3.1. Szervezeti-személyi hatály}* pontban kifejtett személyi hatály alá eső felhasználóit, ügyfeleit, partnereit, adataik és információik jogosulatlan vagy véletlenszerű nyilvánosságra jutásától, módosításától, megrongálódásától, megsemmisülésétől.

A felhasználók részére a FIBH, az Önkormányzat vezető tisztségviselői, a rendszergazdák, az IBF, az adatgazdák részére a teljes IBSZ, a külső felekre vonatkozóan pedig az IBSZ IBF által meghatározott részei a mérvadóak.

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

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

Az Önkormányzat elektronikus információs rendszereit csak a jelen IBSZ *{6. sz. melléklet - Felhasználói Nyilatkozat}* mellékletében található nyilatkozat aláírása után lehet használatba venni.

Az Önkormányzat az IBSZ-t és a FIBH-t folyamatosan fejleszti és tökéletesíti.

I.7. Biztonsági osztályba és biztonsági szintbe sorolás

Az Önkormányzatnak az Ibtv. alapján az elektronikus információs rendszereit biztonsági osztályba kell sorolnia, illetve a szervezetét biztonsági szintbe kell sorolnia

I.7.1. Biztonsági osztályba sorolás követelménye

Az Önkormányzat elektronikus információs rendszereit a technológiai vhr által előírt módon, külön-külön a bizalmasság, a sértetlenség és a rendelkezésre állás alapfenyegetésségek vonatkozásában egy 5 fokozatú skálán biztonsági osztályba kell sorolni.

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

A biztonsági osztályba sorolást mindig kockázatelemzéssel együtt kell végezni.

A biztonsági osztályba sorolást újra el kell végezni, hogy ha

a) jelentős változás következik be Hivatal szervezeti felépítésében;

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

c) változnak a hatályos információbiztonságra vonatkozó jogszabályok.

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

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

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

I.7.2. Az Önkormányzat által használt elektronikus információs rendszerek biztonsági osztályba sorolása

Alkalmazás megnevezése	Alkalmazás leírása	Alkalmazásüzemeltető (adatfeldolgozó)	Adatgazda	Rendszerben kezelt adatok	B	S	R	Biztonsági osztály
ASP Gazdálkodás	Gazdálkodási rendszer	Magyar Államkincstár	jegyző	pénzügyi, főkönyvi adatok	2	2	2	**2**
ASP Irat	Iratkezelő rendszer	NISZ Zrt.	jegyző	iratok adatai, személyes adatok	2	2	2	**2**
ASP Adó	Önkormányzati adórendszer	Magyar Államkincstár	jegyző	helyi adók adatai	3	3	3	**3**
ASP Ingatlanvagyon Kataszter	Ingatlanvagyon-kataszter rendszer	Magyar Államkincstár	jegyző	önkormányzati ingatlanok adatai	1	2	2	**2**
ASP Iparker	A településen kereskedelmi tevékenységek végzéséről vezetett nyilvántartás	Magyar Államkincstár	jegyző	üzletek, piacok, telephelyek adatai	1	2	2	**2**

I.7.3. Az Önkormányzat biztonsági szintbe sorolásának követelményei

Az Önkormányzat a szervezetét a technológiai vhr által előírt módon 1-5-ig terjedő skálán biztonsági osztályba kell sorolnia a szervezetét a 1-5-ig terjedő skálán a technológiai vhr által előírt módon. Az Önkormányzat biztonsági szintjét az elektronikus információs rendszerek felhasználási módja határozza meg.

A biztonsági szintbe sorolást újra el kell végezni, hogy ha

a) jelentős változás következik be Hivatal szervezeti felépítésében;

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

c) változnak a hatályos információbiztonságra vonatkozó jogszabályok.

Ha nem történik lényegi változás, a biztonsági szintbe sorolást háromévente felül kell vizsgálni.

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

I.7.4. Az Önkormányzat biztonsági szintjének megállapítása

Az Önkormányzat biztonsági szintje 3-as, mivel az Önkormányzat

a) nem üzemeltet és nem fejleszt elektronikus információs rendszert, és saját hatáskörben erre más szervezetet, vagy szolgáltatót (ide nem értve a telekommunikációs szolgáltatót) sem vesz igénybe,

b) jogszabály alapján kijelölt szolgáltatót vesz igénybe[1],

c) szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt,

d) helyi adók formájában kritikus adatot[2] kezel.

Az Önkormányzat nem rendelkezik elektronikus információs rendszer

a) fejlesztését végző,

b) üzemeltetését végző,

c) üzemeltetéséért felelős vagy

d) információbiztonságáért felelős

szervezeti egységekkel.

I.8. Cselekvési tervek

Az Önkormányzatnak a biztonsági osztályba és biztonsági szintbe sorolást követő 90 napon belül cselekvési tervet kell készítenie az Önkormányzat elvárt biztonsági szintjére, illetve az Önkormányzat által használt elektronikus információs rendszereinek elvárt biztonsági osztályaira vonatkozó követelmények teljesítése érdekében.

A cselekvési terveket az IBF készíti elö és a jegyző hagyja jóvá.

A cselekvési terveket az Önkormányzat biztonsági szintjének és az Önkormányzat elektronikus információs rendszereinek biztonsági osztályba sorolásának felülvizsgálatával párhuzamosan felül kell vizsgálni.

A tényleges és az elvárt biztonsági szint és a biztonsági osztályok különbségeire nézve irányadó, hogy a cselekvési tervekben foglalt feladatok végrehajtásáig is törekedni kell az IBSZ-ben foglalt követelmények lehető legnagyobb mértékben történő teljesítésére.

I.9. Az Önkormányzat és az elektronikus információs rendszereinek információbiztonsági követelményei

Jelen IBSZ - az Ibtv.-ben meghatározott felkészülési időkre tekintettel – a 2-es biztonsági szintet és a 2-es biztonsági osztály követelményeit veszi figyelembe.

---

[1] Htv. 44. §-a alapján az önkormányzati adóhatóság hatáskörébe tartozó adókat és adók módjára behajtandó köztartozásokat kizárólag a kincstár által rendelkezésre bocsátott számítógépes programrendszerrel lehet nyilvántartani.

[2] Ibtv. 1. § (1) bekezdése 32a. alapján kritikus adat: az Infotv. szerinti **személyes adat**, különleges adat vagy valamely **jogszabállyal védett adat**.

II. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

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

II.1. Szervezeti biztonság

II.1.1. Információbiztonsági tevékenységek

Az Önkormányzatban a következő információbiztonsági tevékenységeket kell ellátni:

e) biztonsági osztályba és biztonsági szintbe sorolás,

f) cselekvési tervek készítése az elvárt biztonsági osztályok és az elvárt biztonsági szint eléréshez,

g) információbiztonsági szabályozó rendszer kialakítása,

h) információbiztonsági képzés, tudatosítás,

i) informatikai kockázatelemzés és kezelés,

j) elektronikus információs rendszerek biztonsági felügyelete,

k) információbiztonsági incidensek kezelése,

l) új elektronikus információs rendszerek információbiztonsági véleményezése és elfogadása,

m) szervezetek közötti információbiztonsági együttműködés,

n) az információbiztonság független felülvizsgálata.

II.1.2. Az információbiztonsági felelősségi rend meghatározása

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

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

Az Önkormányzat információbiztonsági feladatainak ellátása során a következő szerepkörök érintettek:

a) a jegyző,

b) az információbiztonsági felelős,

c) a rendszergazda,

d) ASP rendszerek működtetéséért felelős szervezetek

e) az adatgazdák,

f) a szervezeti egység vezetője,

g) a felhasználók.

II.1.3. A jegyző

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

II.1.3.1. A jegyző feladatai

A jegyző

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

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

c) elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,

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

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

f) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy az Önkormányzat elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,

g) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,

h) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,

i) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,

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

k) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,

l) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

A jegyző köteles együttműködni a jogszabályban meghatározott hatóságokkal. Ennek során

a) az IBF személyéről tájékoztatást nyújt,

b) az Önkormányzat információbiztonsági szabályzatát tájékoztatás céljából megküldi,

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

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

II.1.3.2. A jegyző felelőssége

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

II.1.4. Az IBF

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

II.1.4.1. Az IBF feladatai

Az IBF az Önkormányzat információbiztonsági irányítási rendszerének működtetése és ellenőrzésével kapcsolatos feladatai a következők:

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

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

c) előkészíti az Önkormányzat elektronikus információs rendszereire vonatkozó információbiztonsági politikát, információbiztonsági stratégiát és az információbiztonsági szabályzatot,

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

e) előkészíti az Önkormányzat elektronikus információs rendszereinek biztonsági osztályba sorolását és az Önkormányzat biztonsági szintbe történő besorolását,

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

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

Az IBF biztosítja a jogszabályokban meghatározott követelmények teljesülését

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

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

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

II.1.4.2. Az IBF jogai

Az IBF az Önkormányzat információbiztonságának fenntartása érdekében, illetve információbiztonsági incidens esetében jogosult:

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

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

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

II.1.4.3. Az IBF felelőssége

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

II.1.5. A rendszergazda

A rendszergazda információbiztonsággal kapcsolatos feladata és kötelessége a következő:

II.1.5.1. A rendszergazda feladata

A rendszergazda feladata, hogy

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

b) kidolgozza a hatáskörébe tartozó üzemeltetési eljárásokat,

c) biztosítja a rendszerfelügyeletet;

d) üzemelteti az Önkormányzat informatikai alapinfrastruktúráját;

e) vezeti az IBSZ-ben előírt nyilvántartásokat.

II.1.5.2. A rendszergazda felelőssége

A rendszergazda felelőssége az Önkormányzat informatikai alapinfrastruktúrájának jelen IBSZ-ben foglaltak szerinti biztonságos üzemeltetése.

II.1.6. ASP rendszerek működtetéséért felelős szervezetek

Az Önkormányzat által használt elektronikus információs rendszereket jogszabály által kijelölt szervezetek (továbbiakban: ASP működtetők) működtetik.

Az ASP működtetők feladatait jogszabály, valamint az Önkormányzat és a működtető között létrejött szolgáltatási szerződések tartalmazzák.

II.1.7. Az adatgazda

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

Az adatgazdák a jelen IBSZ *II.7.2 Az Önkormányzat által használt elektronikus információs rendszerek biztonsági osztályba sorolása!* mellékletében kerültek kijelölésre.

II.1.7.1. Az adatgazda feladatai

Az adatgazda információbiztonsággal kapcsolatos feladatai a következők:

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

II.1.7.2. Az adatgazda felelőssége

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

II.1.8. A szervezeti egység vezetője

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

II.1.9. A felhasználó

Az Önkormányzat felhasználóinak az elektronikus információs rendszerek biztonságával kapcsolatban a következők a jogai, a kötelességei és a felelőssége:

II.1.9.1. A felhasználó jogai

A felhasználó jogosult:

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

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

c) információbiztonsági képzésre,

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

e) meghibásodás, üzemzavar esetén az elhárítás igénylésére.

II.1.9.2. A felhasználó kötelessége

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

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

a) az informatikához kapcsolódó tevékenység fennakadása, megszakadása,

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

c) információbiztonsági esemény.

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

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

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

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

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

II.1.9.3. A felhasználó felelőssége

A felhasználó felelősséggel tartozik:

a) a szabályok betartásáért,

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

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

d) az elektronikus információs rendszerben végzett műveletekért,

e) az Önkormányzat elektronikus információs rendszereinek szakszerű kezeléséért és

f) a személyi használatra átvett eszközök megfelelő fizikai védelméért.

II.2. Személyi biztonság

II.2.1. A munkaköri felelősség és az alkalmazás feltételei

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

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

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

Az Önkormányzat elektronikus információs rendszereit csak a jelen IBSZ *[6. sz. melléklet - Felhasználói Nyilatkozat]* mellékletében található nyilatkozat aláírása után lehet használatba venni.

II.2.2. Az információbiztonság oktatása és képzése

Az Önkormányzat elektronikus információs rendszereit csak olyan személyek használhatják, akik megfelelő számítástechnikai, informatikai ismeretekkel rendelkeznek.

Rendszeres belső oktatásokkal gondoskodni kell arról, hogy a felhasználókban tudatosodjanak az alapvető információbiztonsági fogalmak, illetve ismerjék meg a munkájuk során felmerülő

információbiztonsági fenyegetettségeket. Gondoskodni kell arról is, hogy a napi feladatok végzése során a felhasználók kellőképpen felkészültek legyenek a jelen IBSZ-ben foglaltak betartására.

Új dolgozó munkába lépésekor a dolgozóval a munkába állás előtt az információbiztonsági előírásokat meg kell ismertetni. Bonyolultabb alkalmazói rendszerek felhasználói vizsgára is kötelezhetők. Ennek végrehajtására évente frissítő oktatást kell szervezni.

A kiemelt jogosultságokkal rendelkező munkatársak részére külön oktatást kell tartani.

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

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

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

II.2.3. Jelentés a biztonsági eseményekről

Dokumentált eljárást kell kialakítani a biztonsági eseményekről szóló jelentések elkészítésére, a visszajelzések kezelésére.

A biztonságot érintő eseményekről, a felfedezésük után, haladéktalanul tájékoztatni kell a felfedező közvetlen munkahelyi vezetőjét és az IBF-et.

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

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

II.2.4. Jelentés a biztonság gyenge oldalairól

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

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

II.2.5. 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 {II.2.3 Jelentés a biztonsági eseményekről}* pontjának megfelelően kivizsgálja az eseményt.

II.2.6. Okulás a biztonsági eseményekből

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

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

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

II.2.7. Eljárás jogviszony megszűnésekor

A jogviszony megszüntetésekor a következő feladatok végrehajtása szükséges:

a) Jogosultságok megszüntetése, úgy hogy a régi állapot mentésre vagy dokumentálásra kerül.

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

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

A fenti feladatok végrehajtásáért a rendszergazda a felelős.

II.2.7.1. Vagyontárgyak visszaszolgáltatása

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

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

II.2.7.2. Hozzáférési jogok megszüntetése

Valamennyi alkalmazottnak, a szerződőknek és a felhasználó harmadik feleknek információkhoz és információ-feldolgozó eszközökhöz való hozzáférési jogosultságát legkésőbb a munkaviszony megszűnésének napján meg kell szüntetni. Harmadik fél vagy szerződéses partner esetében, amikor alkalmazásuk megszünik, szerződésük, illetve megállapodásuk lejár.

A feladatok végrehajtásáért a rendszergazda a felelős.

II.2.7.3. Információbiztonsági kötelmek a jogviszony megszűnése után

A személyügyi referensnek figyelmeztetnie kell a dolgozót kell arról, hogy a jelen IBSZ-ben foglalt kötelezettségei a jogviszony megszűnése után is fennállnak, az abban foglaltak megsértése jogi következményeket von maga után.

II.2.8. Fegyelmi intézkedések

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

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

II.2.9. Harmadik felekkel kapcsolatos előírások

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

Az Önkormányzat és szerződéses partnerei megfelelő biztonsági intézkedéseket kötelesek foganatosítani annak érdekében, hogy a kicserélt (átadott/átvett) adatok és dokumentumok véletlen vagy szándékos kompromittálódását megakadályozzák.

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

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

Harmadik fél hozzáférése az Önkormányzat adataihoz és információihoz, a munkájához elengedhetetlenül szükséges minimum szintre kell korlátozni. A hozzáférések feltételeit szerződésben kell részletezni. A szerződés csak az Önkormányzat jelen IBSZ-ével összhangban lévő követelményeket tartalmazhat.

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

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

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

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

Harmadik fél az Önkormányzat adatait és az elektronikus információs rendszereit a hozzáférést rögzítő szerződés vagy titoktartási nyilatkozat aláírása előtt nem ismerheti meg.

II.2.9.1. 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.

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

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

II.2.9.2. A harmadik féllel kötött szerződés biztonsági követelményei

A szerződésekben, szükség esetén az alábbiakat kell figyelembe venni:

a) az informatikai biztonság fő szabályait;

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

c) az információk másolásának és nyilvánosságra hozatalának feltételeit;

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

e) a felek felelősségének meghatározását;

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

g) a teljesítések ellenőrizhetőségét, monitorozását és jelentések készítését;

h) a felmerülő problémák kezelését;

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

j) világos és egyértelmű jelentéskészítési struktúrát és rendszert;

k) a változáskezelések egyértelmű és meghatározott folyamatát;

l) óvintézkedések meghatározását a kártékony kódok ellen;

m) biztonsági események kivizsgálására és jelentésére vonatkozó intézkedések meghatározását;

n) az alvállalkozók bevonására vonatkozó szabályokat.

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

II.3. Az elektronikus információs rendszerek nyilvántartása

Nyilvántartást kell vezetni az Önkormányzat valamennyi elektronikus információs rendszeréről. A nyilvántartásnak minden elektronikus információs rendszerre nézve minimálisan a következőket kell tartalmaznia:

a) annak 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.

II.4. Az információbiztonsággal kapcsolatos engedélyezési eljárás

Az Önkormányzatnak a jelen IBSZ-ben foglaltak szerint kell az információbiztonsággal kapcsolatos engedélyezési eljárásokat lefolytatni. Az engedélyezési eljárásoknak ki kell terjedniük valamennyi

a) emberi, fizikai és logikai erőforrásra;

b) eljárási és védelmi szintre és folyamatra.

II.5. Kockázatelemzés és kezelés

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

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

Az Önkormányzat kockázatelemzési és kezelési eljárásrendjét az *[4. sz. melléklet – Kockázatelemzési és kezelési módszertan]* tartalmazza.

II.5.1. Kockázatelemzés

A kockázatarányos védelem kialakításához rendszeres és tervszerű informatikai kockázatelemzésre van szükség. A kockázatelemzést a jelen IBSZ *[4. sz. melléklet – Kockázatelemzési és kezelési módszertan]* mellékletében leírt módszertan alapján az IBF végzi el.

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

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

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

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

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

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

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

II.6. Elektronikus információs rendszerek ügymenet folytonosságának tervezése

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

A jelen fejezetet az Önkormányzat informatikai alapinfrastruktúrájára nézve kell alkalmazni.

II.6.1. Ügymenet folytonosságra vonatkozó eljárásrend

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

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

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

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

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

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

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

II.6.1.1. Az ÜFT felülvizsgálata

Az Ügymenet-folytonossági tervet évente felül kell vizsgálni.

Az Ügymenet-folytonossági tervet soron kívül felül kell vizsgálni

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

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

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

II.6.1.2. Az ÜFT kezelése

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

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

II.6.2. Az elektronikus információs rendszer mentései

Az elektronikus információs rendszerek és az azokban kezelt adatok az adatgazdák és a jogszabályok által elvárt, megfelelő rendelkezésre állásának biztosítása érdekében mentési eljárásrendet 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 adatfajták mentését kell biztosítani:

a) felhasználói szintű adatok (ügyviteli adatok)

b) rendszerszintű információk

c) a rendszerrel kapcsolatos dokumentációk.

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

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

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

II.6.3. Az elektronikus információs rendszer helyreállítása és újraindítása

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

a) katasztrófát követő helyreállítandó célállapot;

b) a katasztrófa események definíciója;

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

d) a helyreállítási terv hatóköre;

e) a megelőzés érdekében végzett tevékenységeket;

f) felkészülés a katasztrófa elhárítására;

g) katasztrófa esetén végrehajtandó tevékenységek;

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

i) a helyreállítási terv tesztelése, karbantartása.

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

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

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

II.7. Tervezés

II.7.1. Rendszerbiztonsági terv

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

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

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

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

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

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

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

Az elektronikus információs rendszerek rendszerbiztonsági tervét kétévente felül kell vizsgálni.

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

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

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

II.7.2. Az internet használat és az elektronikus levelezés szabályai

Az Önkormányzat által nyújtott internetkapcsolat és elektronikus levelezési szolgáltatás igénybevételének a következők a szabályai.

II.7.2.1. A web böngészés szabályai

Az Internethez való kapcsolódás csak és kizárólag a munkavégzést szolgálja!

Az Internet és az elektronikus levelezés használatának főbb szabályai:

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

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

Tilos internetes vagy más jellegű szolgáltatást nyújtó külső féllel hálózati kapcsolat kialakítása.

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

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

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

II.7.2.2. E-mail használat

Az Önkormányzat által biztosított elektronikus levél cím és az elektronikus levelezési szolgáltatás kizárólag társasági munkavégzés céljára biztosított, ezért a felhasználóknak tilos az önkormányzati e-mail címüket nem társasági minőségben használni (pl.: regisztráció letöltési weboldalakra, on-line játék oldalakra, közösségi oldalakra stb.)!

Az Önkormányzat által nem támogatott levelezőrendszer (pl.: Gmail, Freemail) használata munkavégzésre nem engedélyezett.

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

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

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

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

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

Ismeretlen helyről származó e-mail-t megnyitni nem szabad, mert maga a levél vagy annak csatolmánya vírus lehet, ezért ezeket olvasatlanul törölni kell.

II.8. Rendszer és szolgáltatás beszerzés

Az Önkormányzat saját hatókörében informatikai szolgáltatást, vagy eszközöket nem szerez be, és nem végez, vagy végeztet rendszerfejlesztési tevékenységet.[3]

III. FIZIKAI VÉDELMI INTÉZKEDÉSEK

III.1. Alapelvek

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

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

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

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

III.2. A területek fizikai biztonsági követelményei

III.2.1. Fizikai biztonság védősávja

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

A jelen IBSZ *(I.3.2 Tárgyi hatály)* pontja alá eső területeket az alábbi kategóriák egyikébe kell besorolni:

a) belső terület;

b) védett terület.

További védett terület kategóriákat az IBF határozhat meg.

Az Önkormányzat területére és létesítményeibe történő belépés és benntartózkodás szabályait az Önkormányzat erre vonatkozó, belső rendelkezései tartalmazzák.

[3] Ide nem értve a jellemzően kis értékű, kereskedelmi forgalomban kapható általában irodai alkalmazásokat, szoftvereket, vagy azokat a hardver beszerzéseket, amelyek jellemzően a tönkrement eszközök pótlása, vagy az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából történnek, valamint a javítás, karbantartás céljára történő beszerzéseket. Jelen fejezet alkalmazása szempontjából nem minősül fejlesztésnek a kereskedelmi forgalomban kapható szoftverek beszerzése és frissítése. (Lásd technológiai vhr 4. sz. melléklet 3.1.4.1. pontja

III.2.2. Belső terület

Belső területnek tekintendők az Önkormányzat bejárata utáni közös használatú helyiségei és folyosói.

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

III.2.3. Védett terület

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.

III.2.4. Az irodák, a helyiségek és az eszközök védelme

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

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

b) a védett és érzékeny helyiségek átlagos kinézetűek legyenek, ne hívják fel magukra a figyelmet, ne legyen rajtuk 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) azokban az időszakokban, amikor a helyiségek felügyelet nélkül maradnak, az ajtókat és ablakokat zárva kell tartani.

III.3. Az infokommunikációs eszközök biztonsága

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

III.3.1. Az infokommunikációs eszközök elhelyezése és védelme

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

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

a) be kell tartani a tűzvédelmi előírásokat;

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

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

III.3.2. Tápáramellátás

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

III.3.3. A kábelezés biztonsága

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

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

III.3.4. „Üres asztal - üres képernyő" szabály

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

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

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

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

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

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

f) ügyfelet tilos egyedül hagyni olyan helyiségben, ahol számítástechnikai tevékenységet végeznek.

III.3.5. Felügyelet alól kikerülő eszközök

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

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

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

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

A ki- és beszállítások ellenőrzése 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.

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

III.3.6. Munkavégzés biztonságos környezetben

Az érzékeny területeken dolgozó és az ideiglenes jellegű munkát végző harmadik félre vonatkozóan elő kell írni, hogy számukra a hozzáféréseket csak korlátozott mértékben és ellenőrzés mellett szabad biztosítani. A hozzáférések szabályait előzőleg az IBF-nek jóvá kell hagynia.

III.4. Fizikai belépési engedélyek

Az Önkormányzatnak össze kell állítania azon személyek listáját, akik jogosultak a védett területekre történő belépésre.

A listát a jegyző hagyja jóvá.

Az IBF háromhavonta felülvizsgálja a belépésre jogosult személyek listáját és eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése már nem indokolt.

IV. LOGIKAI VÉDELMI INTÉZKEDÉSEK

A logikai védelmi intézkedések a technológiai vhr alapján kerültek kialakításra. A jelen fejezetben előírt követelmények a 2-es biztonsági osztályra vonatkoznak.

IV.1. Konfigurációkezelési eljárásrend

A jelen fejezetet az Önkormányzat informatikai alapinfrastruktúrájára nézve kell alkalmazni.

IV.1.1. Alap konfiguráció

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

A dokumentációnak minimálisan a következő elemeket kell magában foglalnia:

a) Hardver elemek;

b) Szoftverek;

c) Telepítőkészletek;

d) Egyes szoftverkomponensek alapkonfigurációi.

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

IV.1.2. Elektronikus információs rendszerelem leltár

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

IV.1.3. A szoftver használat korlátozásai

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

Az alkalmazott szoftverekről leltárt kell vezetni.

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

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

A szerzői jogokkal védett szellemi termékek felhasználását nyomon kell követni.

IV.1.4. A felhasználó által telepített szoftverek

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

A felhasználók munkaállomásain telepített alkalmazások megfelelőségét az IBF szúrópróbaszerűen ellenőrzi.

IV.1.5. Rendszer karbantartási eljárásrend

Az elektronikus információs rendszerek karbantartására vonatkozóan a jelen fejezetben leírtak az irányadók. A jelen fejezetet az Önkormányzat informatikai alapinfrastruktúrájára nézve kell alkalmazni.

IV.1.5.1. Rendszeres karbantartás

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

IV.1.5.2. A karbantartások engedélyezése

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

IV.1.5.3. A karbantartások dokumentálása, nyilvántartása

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

a) az elvégzett karbantartás megnevezése,

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

c) a karbantartás engedélyezője,

d) a karbantartás elvégzője,

e) a karbantartás dátuma,

f) leállási idő (ha volt ilyen).

A jegyzőkönyveket csatolni kell a karbantartási nyilvántartáshoz.

IV.1.5.4. A karbantartások ütemezése

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

IV.1.5.5. Kiszállítás

Amennyiben az adatot tartalmazó adathordozó kiszállítása válik szükségessé, akkor az *[IV.2.2 Az infokommunikációs eszközök biztonságos újrahasznosítása vagy mások rendelkezésére bocsátása]* fejezetben leírtak szerint kell eljárni. A kiszállítást a rendszergazda engedélyezi.

IV.1.5.6. 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.

IV.1.5.7. Karbantartók

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

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

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

a) szervezet megnevezése,

b) szerződésszám,

c) szerződés időtartama,

d) szerződéses kapcsolattartó neve, elérhetősége,

e) karbantartás végzők neve, elérhetősége,

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

Külsős szerződő fél munkavégzése esetén a rendszergazdának ki kell jelölnie azokat a személyeket, akiknek folyamatos felügyeletet kell biztosítani a karbantartás során.

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

IV.2. Adathordozók védelmére vonatkozó eljárásrend

Az adathordozók védelmére a következő előírások vonatkoznak. A jelen fejezetet az Önkormányzat informatikai alapinfrastruktúrájára nézve kell alkalmazni.

IV.2.1. Hozzáférés az adathordozókhoz, adathordozók használata

Az Önkormányzatban 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.

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

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

IV.2.2. Az infokommunikációs eszközök biztonságos újrahasznosítása vagy mások rendelkezésére bocsátása

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

a) a rajtuk tárolt adatokat 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.

IV.2.3. Az infokommunikációs eszközök Hivatalon kívüli biztonsága

Az Önkormányzat területén kívüli infokommunikációs eszközök használatát a legszükségesebb mértékűre kell korlátozni. Kizárólag az Önkormányzat tulajdonát képező hordozható infokommunikációs eszköz használata engedélyezhető.

IV.2.4. 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 a jegyző részére át kell adni.

IV.2.5. 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 tartalmaz-e bárminemű érzékeny információt. (Előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban is megerősítve.)

IV.3. Azonosítási és hitelesítési eljárásrend

A jelen fejezet előírásait az Önkormányzat informatikai alapinfrastruktúrájára és az ASP rendszerekre nézve is alkalmazni kell.

IV.3.1. Azonosítás és hitelesítés

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.

IV.3.2. Azonosító kezelés

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

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

A fentiek havi rendszerességgel történő végrehajtása az rendszergazdák feladata

IV.3.3. A hitelesítésre szolgáló eszközök kezelése

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

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 90 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.

IV.3.4. 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;

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

g) könnyen megjegyezhető, és nehezen kitalálható legyen;

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

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

j) ne legyen sorozat.

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

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

IV.3.5. 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.

IV.3.6. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

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

IV.3.7. Hitelesítés szolgáltatók tanúsítványának elfogadása

Az Internet irányába létesített hálózati kapcsolatokat az átmenő adatok bizalmasságának és sértetlenségének megőrzése céljából szabványos kriptográfiai eszközökkel titkosítani kell. A hálózati kapcsolatok titkosításához csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat lehet felhasználni.

IV.4. Hozzáférés ellenőrzési eljárásrend

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

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

b) A felhasználók a munkaállomásukon nem rendelkezhetnek rendszergazda jogokkal.

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

IV.4.1. Felhasználói fiókok kezelése

A felhasználók csak jóváhagyott hozzáférés-védelmi megoldásokat alkalmazhatnak.

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

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

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

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

d) Az összeférhetetlenségi szabályokat figyelembe kell venni.

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

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

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

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

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

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

b) A csoportos felhasználó azonosítók használatát tiltani kell.

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

i. a felhasználó munkakörét és az azzal kapcsolatos feladatait;

ii. a munkaköri feladatok végrehajtásához minimálisan szükséges jogosultságok elvét;

iii. a felhasználó jogviszonyát;

iv. a felhasználó munkahelyét.

IV.4.2. Kiemelt jogosultságok kezelése

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

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

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

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

c) az adminisztrátori jogot kizárólag a jegyző engedélyezheti írásban.

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

A rendszergazda nem küldhet levelet más felhasználó nevében.

IV.4.3. Hozzáférési jogok igénylésének folyamata

Az ASP rendszerekhez történő hozzáférések igénylését az ASP rendszer működtetője által biztosított, a jelen IBSZ *(5. sz. melléklet – Jogosultságigénylési űrlap)* mellékletében található űrlapon kell igényelni.

Az űrlap kitöltési útmutatóját a *{Kitöltési útmutató a jogosultság igényléshez Az „Önkormányzati ASP központ felállítása" tárgyú projekthez}* dokumentum tartalmazza.

IV.4.4. 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 hathavonta felülvizsgálja.

IV.4.5. Hozzáférés ellenőrzés érvényre juttatása

Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényre kell juttatnia a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

IV.4.6. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

Az Önkormányzatban nincsenek azonosítás és hitelesítés nélkül engedélyezett tevékenységek.

IV.4.7. Külső elektronikus információs rendszerek használata

Az Önkormányzat belső elektronikus információs rendszereinek 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.

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

IV.4.8. Nyilvánosan elérhető tartalom

Az információk közzétételével kapcsolatban az Önkormányzat a jogszabályokat, a Közzétételi Szabályzatot és az erkölcsi normákat követi.

IV.5. Naplózási eljárásrend

Az Önkormányzat informatikai alapinfrastruktúrájában a következő naplózási eljárásrendet kell kialakítani.

IV.5.1. Naplózható események

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

a) a felhasználók adminisztrációs tevékenysége:

- bejelentkezés;
- kijelentkezés;
- jelszómódosítás.

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

c) a rendszergazdák tevékenysége a rendszer bármely rétegében;

d) a felhasználói jogosultságok módosítása;

e) rendszer események, esetleges hibák;

f) konfigurációs beállítások módosítása.

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

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

IV.5.2. 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.

IV.5.3. 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.

IV.5.4. A napló információk védelme

Az elektronikus információs rendszereknek meg kell védenie a napló információkat és a napló eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

IV.5.5. A naplóbejegyzések megőrzése

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

IV.5.6. Naplógenerálás

Olyan elektronikus információs rendszereket kell alkalmazni, melyek

a) biztosítják a naplóbejegyzések előállítási lehetőségét a *{IV.5.1 Naplózható események}* pontban meghatározott naplózható eseményekre;

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

c) naplóbejegyzéseket állít elő a *{IV.5.1 Naplózható események}* pontban meghatározottak szerinti eseményekre az *{IV.5.2 Naplóbejegyzések tartalma}* pontban meghatározott tartalommal.

IV.6. Rendszer és információ sértetlenségre vonatkozó eljárásrend

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

IV.6.1. Hibajavítás

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

A rendszergazdának biztosítania kell, hogy az elektronikus információs rendszerek rendszerszoftverei naprakész állapotban legyen.

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

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

Új hardverek üzembe állításakor a fentieket kell értelemszerűen alkalmazni.

IV.6.2. 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 központilag felügyelt kártékony kód elleni megoldásokat kell alkalmazni.

b) Kártékony kód elleni megoldás 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 rendszeresen, a szállító által meghatározott ütemezéssel, vagy automatikusan frissíteni kell.

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

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

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

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

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

IV.6.3. 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.

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 jegyző pedig jóváhagyja.

IV.6.4. A kimeneti információ kezelése és megőrzése

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

a) gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről,

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

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

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

IV.7. Rendszer és kommunikáció védelmi eljárásrend

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

IV.7.1. A határok védelme

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

a) megfelelő interfészt kell alkalmazni az Önkormányzat és más szervezet tulajdonában lévő, vagy nyilvános hálózat között;

b) a felhasználókat jelszóval megfelelően hitelesíteni kell;

c) ellenőrizni kell a felhasználók információszolgáltatáshoz való hozzáférését.

Az Önkormányzat belső hálózatáról Internet kapcsolat kizárólag jóváhagyott tűzfalakon keresztül létesíthető.

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

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

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 hivatali email címmel hozzászólni,

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

d) hivatali 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.

IV.7.2. 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 hálózatoknak és hálózati szolgáltatásoknak a felsorolását, amelyeket igénybe vehetnek;

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

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

Az Önkormányzat elektronikus információs rendszerében TILOS modemet csatlakoztatni. Az Önkormányzat hálózatában csak olyan Wi-Fi eszköz csatlakoztatható, amely minimum WPA2 (technikai korlátok esetén WPA) titkosítást alkalmaz.

Kockázat elemzéssel kell meghatározni a szükséges védelmet és a megfelelő hitelesítési módszert.

IV.7.3. A felhasználó hitelesítése külső összeköttetésekhez

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

IV.7.4. 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. 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.

IV.7.5. A hálózati összeköttetések ellenőrzése

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

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

IV.7.6. A hálózati üzenettovábbítás ellenőrzése

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

IV.7.7. Nyilvános elektronikus információs rendszerek védelme

Az Önkormányzat honlapját web hosting szolgáltató működteti, ezért a vele kötött szerződésben elő kell írni a nyilvánosan elérhető tartalmakkal és rendszerekkel kapcsolatos információbiztonsági követelményeket.

IV.7.8. Kriptográfiai védelem

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

IV.7.9. 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.

IV.7.10. Kriptográfiai kulcs előállítása és kezelése

Az ASP szolgáltatók az általuk biztosított elektronikus információs rendszerek eléréséhez és bizonyos müveletek végrehajtásához elektronikus aláíró eszközt biztosít.

Ezen eszközök vonatkozásában a kriptográfiai kulcs előállítására és kezelésére vonatkozóan az ASP szolgáltatók előírásai a mérvadóak.

IV.1. Együttműködésen alapuló számítástechnikai eszközök

Az Önkormányzat nem müködtet együttmüködésen alapuló számítástechnikai eszközöket.

IV.2. A folyamatok elkülönítése

Operációs rendszer szintjén biztosítani kell, hogy minden folyamat részére külön végrehajtási terület kerüljön lefoglalásra a memóriában, és ne legyen mód és lehetőség arra, hogy az egyik folyamat elérje a másik folyamat részére biztosított memóriaterületet.

V. MELLÉKLETEK

1. sz. melléklet - Értelmező Rendelkezések

2. sz. Felhasználói Informatikai Biztonsági Házirend

3. sz. melléklet - Biztonsági események jelentése

4. sz. melléklet – Kockázatelemzési és kezelési módszertan

5. sz. melléklet – Jogosultságigénylési űrlap

6. sz. melléklet - Felhasználói Nyilatkozat

1. sz. 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) 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).

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

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

(6) 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

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

(8) 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.

(9) 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.

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

(11) 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).

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

(13) 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 mindenről tájékoztatták.

(14) 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.

(15) 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.

(16) Kritikus adat: az Infotv. szerinti személyes adat, különleges adat vagy valamely jogszabállyal védett adat.

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

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

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

(20) 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.

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

(22) Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

(23) Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát)

is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

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

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

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

Felhasználói Informatikai Biztonsági Házirend

1. Általános rész

1.1. A Felhasználói Informatikai Biztonsági Házirend célja

A Felhasználói Informatikai Biztonsági Házirend (a továbbiakban: FIBH) célja, hogy az Önkormányzat elektronikus információs rendszereinek felhasználói részére előírja az információbiztonsági előírások rájuk vonatkozó részét.

Az Önkormányzat elektronikus információs rendszereinek védelme érdekében az Önkormányzat kidolgozta az Informatikai Biztonsági Politikáját, Informatikai Biztonsági Stratégiáját és az Informatikai Biztonsági Szabályzatát.

Az Informatikai Biztonsági Szabályzat (továbbiakban: az IBSZ) tartalmazza valamennyi információbiztonsággal kapcsolatos szabályt, melynek betartásával az érintettek által elvárt szinten tartható az Önkormányzat elektronikus információs rendszereinek és az azokban kezelt adatok biztonsága.

Az IBSZ számos olyan védelmi intézkedést tartalmaz, amely közvetlenül nem kapcsolódik az Önkormányzat felhasználóihoz, ezért a jelen FIBH-nak az is célja, hogy egy kivonatot adjon az IBSZ felhasználókra vonatkozó előírásairól, illetve néhány helyen kiegészítse és tovább részletezze az IBSZ-ben foglalt magasabb szinten meghatározott követelményeket.

1.2. A FIBH általános követelményei

A FIBH előírásainak alkalmazása, betartása, illetve betartatása, a jelen IBSZ *{I.3.1. Szervezeti-személyi hatály}* **pontban megjelöltek számára kötelező. A szabályok be nem tartása jogi, munkaügyi, illetve szerződésben meghatározott következményeket vonhat maga után. A FIBH el nem olvasása nem mentesít a felelősség alól.**

Az információbiztonsági előírások betartása megvédi az Önkormányzatot és a jelen IBSZ *{I.3.1. Szervezeti-személyi hatály}* pontban kifejtett személyi hatály alá eső felhasználóit, ügyfeleit, partnereit, adataik és információik jogosulatlan vagy véletlenszerű nyilvánosságra jutásától, módosításától, megrongálódásától, megsemmisülésétől.

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

Az Önkormányzat elektronikus információs rendszereit csak a jelen IBSZ *{6. sz. melléklet - Felhasználói Nyilatkozat}* mellékletében található nyilatkozat aláírása után lehet használatba venni.

Az Önkormányzat a FIBH-t az IBSZ-szel együtt folyamatosan fejleszti és tökéletesíti.

2. Bevezetés

Az Önkormányzat által kezelt információk érzékenysége miatt azok védelme, azaz bizalmas kezelése, sértetlensége, valamint megfelelő szintű rendelkezésre állása kritikus tényező.

Az Önkormányzat 2015-ben Európai Uniós projekt keretében a korábban egyedileg fejlesztett és vásárolt elektronikus információs rendszereit központi, jogszabály által kijelölt ASP rendszerekre cserélte.

Ennek keretében a következő elektronikus információs rendszerek kerültek bevezetésre ASP szolgáltatás keretében:

k) ASP Gazdálkodás

l) ASP Irat

m) ASP Adó

n) ASP Ingatlanvagyon Kataszter

o) ASP Iparker

Az önkormányzati ügyviteli folyamatok működése nagymértékben az elektronikus információs rendszereire épül, így ezek kiesése, vagy megsemmisülése esetén az Önkormányzat egyes funkciói működésképtelenné válhatnak, valamint az Önkormányzat által kezelt érzékeny információk illetéktelen kezekbe kerülhetnek.

Az Önkormányzat elektronikus információs rendszereinek minden felhasználója személyes felelősséggel tartozik a munkájával kapcsolatban a birtokában lévő, illetve a tudomására jutott információk megfelelő kezeléséért, a biztonsági szabályok betartásáért.

3. A felhasználó jogai, kötelességei és felelőssége

A felhasználóknak az elektronikus információs rendszerek használata során a következők a kötelességeik, jogaik és felelősségeik.

3.1. A felhasználó jogai

A felhasználó jogosult:

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

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

c) információbiztonsági képzésre,

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

e) meghibásodás, üzemzavar esetén az elhárítás igénylésére.

3.2. A felhasználó kötelessége

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

Amennyiben a felhasználó olyan adatokhoz fér hozzá, amelyek kezelésében nem illetékes, a hibát jeleznie kell munkahelyi vezetőjének.

Valamennyi alkalmazott köteles azonnal értesíteni a rendszergazdát minden olyan körülményről, ami az informatikához kapcsolódó tevékenység fennakadásához, megszakadásához vezethet. A rendszergazda szükség esetén értesíti az információbiztonsági felelőst, aki megteszi a további, szükséges intézkedéseket.

Valamennyi információbiztonsággal kapcsolatos észrevételt vagy szabályszegésre vonatkozó feltételezést haladéktalanul jelenteni kell az információbiztonsági felelősnek.

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

A személyi azonosító kódokat, jelszavakat szigorúan titokban kell tartani. Még a közeli munkakapcsolatban álló, egymást jól ismerő kollégák sem közölhetik ezeket egymással. A hozzáférési kódok a rendszergazdáknak sem adhatók ki és a rendszergazdáknak nincs is joga ezeket elkérni.

Az információbiztonsági hiányosságok megelőzése céljából a felhasználók kötelesek rámutatni az információbiztonsági szint romlására, illetve annak lehetőségére, és a tapasztalatokat a további problémák elkerülésében felhasználni.

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

Az Önkormányzat infokommunikációs eszközei és elektronikus információs rendszerei kizárólag hivatali munkavégzés céljából használható, azok magáncélú használata tilos!

Az Önkormányzat a vonatkozó adatvédelmi jogszabályok figyelembevételével jogosult a felhasználó hivatalos elektronikus levelezését és internetforgalmát vizsgálni.

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

Az Önkormányzatban az alkalmazottak csak az Önkormányzat tulajdonát képező informatikai eszközöket és engedélyezett szoftvereket használhatják. Ettől eltérni csak a jegyző engedélyével lehet.

A rendszergazdát kivéve, tilos az Önkormányzat számítógépeire szoftvereket telepíteni, és azokat futtatni.

Kizárólag a munkavégzéshez szükséges adathordozók használata engedélyezett.

A nyomtatásra, lapolvasásra, fénymásolásra, faxolásra alkalmas készülékek, multifunkcionális eszközök használatánál ügyelni kell arra, hogy:

a) az érzékeny információt tartalmazó nyomtatványok ne maradjanak a készülékben;

b) illetéktelenek ne férhessenek hozzá, mert belső tárolóikban tárolódott üzenetek visszahívhatók, így illetéktelenek kezébe kerülhetnek;

c) véletlen vagy szándékos átprogramozás során az üzenetek egy nem megfelelő számra kerülhetnek;

d) félretárcsázás vagy hibásan tárolt szám miatt az üzenetek illetéktelen személyhez kerülnek.

3.3. A felhasználó felelőssége

A felhasználó felelősséggel tartozik:

a) a szabályok betartásáért;

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

c) a személyére szóló és védett területre belépést biztosító kártyájának/kártyáinak védelméért és át nem ruházásáért;

d) az elektronikus információs rendszerben végzett műveletekért;

e) az Önkormányzat infokommunikációs eszközeinek (számítógép, nyomtató, scanner, stb.) szakszerű kezeléséért;

f) a személyi használatra átvett eszközök megfelelő fizikai védelméért.

3.4. A felhasználó jogai

A felhasználó jogosult:

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

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

c) információbiztonsági képzésre;

d) a működtetéshez szükséges támogatás igénylésére, a munkavégzéshez szükséges általa nem ismert szoftver eszközökhöz támogatást, képzést kérni;

e) meghibásodás, üzemzavar esetén a lehető legrövidebb időn belüli elhárítás igénylésére.

4. Az információ kezelésének szabályai

4.1. Munkaállomások hozzáférés védelme

A felhasználó munkaállomást csak saját nevével és jelszavával belépve használhat. Harmadik fél csak a munkaállomás nevesített felhasználója vezetőjének előzetes írásbeli engedélyével használhat munkaállomást, ebben az esetben is a személyesen hozzárendelt azonosító használatával. Hibaelhárítás vagy támogatás esetén a rendszergazda saját azonosítójával a felhasználó engedélyével a felhasználó munkaállomására beléphet.

A felhasználónak rendszergazdai jog nem adható!

4.2. A hozzáférés kiosztás folyamata

Az informatikai rendszerekbe belépést lehetővé tevő azonosítót a vezető igényli a felhasználóknak, az IBSZ *{IV.4.3 Hozzáférési jogok igénylésének folyamata}* fejezetében leírt folyamat szerint.

A munkaállomás operációs rendszerébe belépést lehetővé tevő azonosítót és a kezdeti jelszót a rendszergazda személyesen adja át az új felhasználónak. Az átadás során a rendszergazda az azonosító használatáról, a kezdeti jelszó megváltoztatásáról és az egyéb testre szabási lépésekről oktatásban részesíti a felhasználót.

4.3. Hálózati hozzáférés, hozzáférés az egyes alkalmazói programokhoz

Az Önkormányzat vezetése felügyeli az elektronikus információs rendszerek használatát a visszaélések megakadályozására és jogosult az elektronikus információs rendszer használatát ellenőrizni.

Az Önkormányzat infokommunikációs eszközein működtetett szoftvereket és alkalmazói rendszereket a felhasználó a számára beállított jogosultságnak megfelelően használhatja az alábbiak szerint:

a) A felhasználó a számítógépbe/hálózati szolgáltatások eléréséhez személyre szóló azonosítót és jelszót kap, mely a belépéshez szükséges bizalmas információkat tartalmaz.

b) Az azonosító és a megfelelő erősségű és titokban tartott jelszó használatával a belépő védelemmel rendelkezik a nevében történő visszaélések ellen, ezért a személyre szóló azonosítót és jelszavát szigorúan védeni kell, és a kezdeti jelszót első bejelentkezéskor meg kell változtatni.

A felhasználói jelszavak képzéséhez az alábbi szabályokat kell betartani:

a) A jelszó legalább nyolc karakter hosszú legyen, és tartalmaznia kell kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;

b) a jelszavakat 90 naponta meg kell változtatni,

c) az előző jelszavak újra használatát kerülni kell.

A felhasználói jelszavak alkalmazásakor az alábbi szabályokat kell betartani:

a) a felhasználó a jelszavát köteles titokban tartani,

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

c) a felhasználói jelszót TILOS leírni,

d) ha bármilyen jel mutat arra, hogy a jelszó kompromittálódhatott, azonnal meg kell változtatni és értesíteni kell az információbiztonsági felelőst,

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

f) a jelszó minél komplexebb, annál kisebb a valószínűsége, hogy nevünkben visszaélést követnek el.

A felhasználói jelszavak képzésénél az alábbi szempontokat kell betartani:

a) könnyen megjegyezhető, és nehezen kitalálható legyen;

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

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

d) ne legyen sorozat.

4.4. Hozzáférés védelem mobil infokommunikációs eszköz esetén

A mobilitás miatt sokkal nagyobb veszélynek kitett mobil infokommunikációs eszközök esetében is jelszót kell használni a rendszerbe történő belépéshez. Bár ez a védelem megnehezíti a hozzáférést, a merevlemezt (winchestert) eltávolítva az ott nyíltan tárolt adatok így is megszerezhetők.

A fentiek miatt fokozottan kell törekedni ezen eszközök fizikai védelmére is az elvesztés, illetve ellopás ellen.

Külső munkahelyen történő feladat elvégzése után a keletkezett adatokat a hálózati meghajtóra kell menteni.

A mobil infokommunikációs eszközökről a feleslegessé vált adatokat le kell törölni.

Nyilvános helyeken történő használatnál ügyelni kell arra, hogy illetéktelenek ne olvashassák el a képernyő tartalmát, az eszközhöz illetéktelenek ne férhessenek hozzá.

Mobil infokommunikációs eszközök esetén rendszergazda jog felhasználónak nem adható.

4.5. Adatmentések, az adathordozók nyilvántartása és tárolása

Az adatokat nem a helyi munkaállomáson, hanem a „központi fájlszerver" megfelelő könyvtáraiban kell tárolni, ahol biztosított azok rendszeres mentése és biztonságos tárolása. Minden felhasználó számára rendelkezésre áll a „Saját" könyvtár a saját adatok tárolására, illetve minden iroda rendelkezik külön könyvtárral a szervezeti egységen belül keletkező és közösen kezelendő adatok tárolására. A nem megfelelő könyvtárba mentés a felhasználó felelőssége.

A rendszergazda nem vállal felelősséget a helyi gépen tárolt adatokért.

A rendszergazda a „központi fájlszerver"-en tárolt ügyviteli adatokról meghatározott módon és gyakorisággal mentést készítenek. Ebből adódóan lehetőség van az állományok, adattáblák statikus visszaállítására a mentés időpontjának megfelelő tartalommal. Folyamatok előre-, illetve visszagörgetésére a rendszer nincs felkészítve. Speciális mentési igényekről a rendszergazdát írásban értesíteni kell, és egyeztetni kell a kivitelezés lehetőségéről.

Az adat visszaállítást az adatgazda írásbeli (e-mail) igénye alapján a rendszergazda végzi el.

A feljegyzésnek tartalmaznia kell a visszaállítani kívánt adat:

a) utoljára ismert pontos helyét;

b) megnevezését, és a

c) visszaállítandó időpontot.

A felhasználónak a jogviszonyának megszűnésekor a munkaállomásán és a központi tárhelyen tárolt adatok törlése tilos!

5. Felhasználók számítógépes környezete

5.1. Számítógépek és a hálózat kezelési előírásai

A felhasználó felelős az infokommunikációs eszközön általa végzett, nyilvánvalóan szakszerűtlen beavatkozásának következményeiért.

A felhasználó semmilyen infokommunikációs eszközt nem telepíthet az Önkormányzat elektronikus információs rendszerébe, azok elhelyezését, telepítési módját nem változtathatja meg. Semmilyen szoftvert nem telepíthet, nem törölhet, és nem módosíthat.

A felhasználónak infokommunikációs eszköz, illetve szoftver telepítési igényével a rendszergazdát kell megkeresnie. Az igénylést a munkahelyi vezetővel egyeztetve a jegyző hagyja jóvá.

A rendszergazda bizonyos szoftver elemek telepítését központi szétosztással, automatikusan végzi. Az ilyen távolról történő frissítéskor meg kell várni a frissítés befejeződését, a folyamatot leállítani tilos. El kell fogadni, hogy ez alatt az idő alatt a számítógép valamivel lassabban működik.

Az Önkormányzat belső hálózatához idegen infokommunikációs eszköz nem csatlakoztatható.

5.2. Internethasználat, web böngészés

Az Internethez való kapcsolódás csak és kizárólag a munkavégzést szolgálja!

Az Internet és az elektronikus levelezés használatának főbb szabályai:

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

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

Tilos Internetes vagy más jellegű szolgáltatást nyújtó külső féllel hálózati kapcsolat kialakítása.

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

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

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

Az internet kapcsolatot a használat végeztével a felhasználó bontani köteles!

5.3. E-mail használat

Az Önkormányzat által biztosított elektronikus levél cím és az elektronikus levelezési szolgáltatás kizárólag hivatali munkavégzés céljára biztosított, ezért a felhasználóknak tilos az önkormányzati e-mail címüket nem hivatalos minőségben használni (pl.: regisztráció letöltési weboldalakra, on-line játék oldalakra, közösségi oldalakra stb.)!

Az Önkormányzat által nem támogatott levelezőrendszer (pl.: Gmail, Freemail) használata önkormányzati munkavégzésre nem engedélyezett.

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

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

Elektronikus levél önmagában nem használható kötelezettség vállalására, illetve annak visszaigazolására. Egyéb, pl. telefon megerősítést kell alkalmazni.

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

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

Ismeretlen helyről származó e-mail-t megnyitni nem szabad, mert maga a levél vagy annak csatolmánya vírus lehet, ezért ezeket olvasatlanul törölni kell.

6. Vírusvédelem

6.1. A vírusvédelem alkalmazásának előírásai

A rendszergazda a számítógépek vírusok elleni védelmére rendszeresen frissített vírusvédelmi rendszert, és anti-spyware programot üzemeltet. Ez a védelem kiterjed a kiszolgálók, munkaállomások valamint a teljes Internet és elektronikus levélforgalom folyamatos ellenőrzésére. Új vírus megjelenése esetén még így is előfordulhat fertőzés, valamint csatolmányok, CD és DVD lemezek, cserélhető adathordozók, illetve internetről letöltött fájlok használata esetében.

Vírusvédelem nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem használható.

Dokumentumok esetében lehetőség szerint kerülni kell a makrók megnyitását, külső forrásból érkező dokumentumok esetében pedig nem szabad engedélyezni.

Ha a vírus helye nem lokalizálható, a rendszergazda jogosult a hálózat egyes funkcióit, vagy a teljes hálózat felhasználói szolgáltatásait a vírusveszély elhárításáig felfüggeszteni.

6.2. Teendők vírusgyanú esetén

Vírusgyanú esetén a felhasználó köteles azonnal felhívni a rendszergazdát, aki ellátja utasítással, vagy intézkednek a jelzés továbbításáról az információbiztonsági felelős felé.

7. Az informatikai eszközök fizikai védelme

7.1. Számítógép használatának előírásai

A munkaállomást és a perifériákat a napi munkavégzés befejezésekor ki kell kapcsolni. Ez alól kivételek azok az eszközök, amelyek automatikusan kikapcsolnak (hálózati nyomtatók vagy a modern monitorok többsége stb.). Az infokommunikációs eszközöket üzem közben letakarni, a szellőző nyílásokat eltakarni tilos!

7.2. „Üres asztal - tiszta képernyő" politika

Az „üres asztal - tiszta képernyő" politika megvalósítása az alábbiakat jelenti:

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

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

c) A munkavégzés befejeztével a munkaállomásból ki kell jelentkezni, illetve ki kell azt kapcsolni;

d) Elfelejtés esetére jelszóvédett, automatikus zárolás kerül beállításra, úgy, hogy az maximum 10 perc várakozást követően zárolja a számítógépet;

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

f) A kinyomtatott, faxolt vagy másolt iratokat nem szabad őrizetlenül a nyomtatókban, multifunkcionális eszközökben, fax-okban hagyni.

g) Ügyfelet nem szabad felügyelet nélkül az irodában hagyni.

7.3. Mobil infokommunikációs eszközök védelme

A munkaállomásokra vonatkozó előírásokon kívül az alábbi védelmi szabályokat kell betartani:

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

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

c) a mobilitás és a kis méret miatt a mobil infokommunikációs eszközök fokozottan vannak kitéve lopásveszélynek. Gondoljunk erre, és ne hagyjuk őrizetlenül autóban, szállodai szobában stb. (zárjuk el fizikailag, használjuk, ha lehet az értékmegőrzőt, ha nincsenek érzékeny adatok a gépen);

A mobil infokommunikációs eszközök ellopása esetén:

a) az ellopás tényét a lehető leggyorsabban jelenteni kell az információbiztonsági felelősnek és a munkahelyi vezetőnek;

b) értesíteni kell a rendőrséget;

c) értesíteni kell a szálloda vezetését, ha a számítógépet a szállodai szobából vagy a szálloda területén álló kocsiból lopták el;

d) valamennyi rendőrségi jelentést meg kell őrizni és az Önkormányzat részére át kell adni.

Infokommunikációs eszköz elvesztése

Bármely infokommunikációs eszköz eltűnését a lehető leggyorsabban jelenteni kell a munkahelyi vezetőnek és az információbiztonsági felelősnek és tájékoztatni kell őket arról, hogy a berendezés tartalmaz-e bárminemű érzékeny információt. (Előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban is megerősítve.)

8. Információbiztonsági események kezelése

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

a) a szolgáltatás, a berendezés vagy az eszközök elvesztése;

b) a rendszer hibás működése vagy túlterhelések (Dos-támadás);

c) emberi hibák;

d) a szabályzatoknak vagy irányelveknek való nem megfelelés;

e) a fizikai biztonsági rendelkezések megsértése;

f) nem ellenőrzött rendszerbeli változások;

g) a szoftver vagy hardver hibás működése;

h) hozzáférési előírások megsértése;

i) kártékony kód általi fertőzés;

j) a nem teljes vagy nem pontos működési adatokból eredő hibák;

k) a bizalmasság és sértetlenség megsértése;

l) az elektronikus információs rendszerrel való visszaélés.

Jelentés a biztonsági eseményekről

A biztonságot érintő eseményekről a felfedezésük után, haladéktalanul tájékoztatni kell a felfedező közvetlen munkahelyi vezetőjét és a rendszergazdát. A rendszergazda értesíti az információbiztonsági felelőst, aki jogosult az esemény kivizsgálására.

A biztonságot érintő eseményekről szóló jelentések elkészítésére az IBSZ *(3. sz. melléklet - Biztonsági események jelentése)* mellékletét kell használni.

8.1. Jelentés a szoftverzavarokról

Az elektronikus információs rendszerekben tapasztalt szoftverzavarokat jelenteni kell a rendszergazdának. Szoftverzavarra utaló jelek lehetnek, amikor az alkalmazás nem a várt eredményt adja vagy nem a megszokott képernyőképek jelennek meg.

A jelentéshez az IBSZ *(3. sz. melléklet - Biztonsági események jelentése)* mellékletét kell használni. Szoftverzavarok esetén legalább a következő feladatokat végre kell hajtani:

a) fel kell jegyezni a zavaró jelenséget és a képernyön megjelenő minden üzenetet és

b) be kell szüntetni az adott számítógép használatát.

A felhasználóknak tilos a hibásnak feltételezett szoftvert eltávolítaniuk az elektronikus információs rendszerből, illetve kísérletet tenni a hiba elhárítására.

A hibaelhárítást és helyreállítást a rendszergazda hajthatja végre.

Abban az esetben, ha feltételezhető az információbiztonság sérülése, akkor az eseményt a rendszergazdának jelentenie kell az információbiztonsági felelősnek, aki kivizsgálja az eseményt.

3. sz. melléklet - Biztonsági események jelentése

A biztonsági esemény megnevezése:

A tapasztalás helye és idő pontja:

Az érintett személyek megnevezése:

Az esemény pontos leírása:

Az észlelő neve:

Dátum:_____év__hó__nap ....

Észlelő aláírása IBF aláírása

Az esemény kivizsgálásának leírása:

Tett intézkedés leírása:

Az intézkedés életbelépésének időpontja:

Végleges-e az intézkedés:

☐	*Igen*
☐	*Nem*

Igényel-e kockázatelemzést az esemény:

☐	*Igen*
☐	*Nem*

Dátum:_____év__hó__nap ....

Információbiztonsági felelős aláírása jegyző aláírása

Kockázatelemzési és kezelési módszertan

Az egyes vagyonelemekre a biztonsági osztályba sorolás során megállapított biztonsági szinteket (kárértékeket) rá kell vetíteni. Ezután vagyonelem csoportonként meg kell vizsgálni, hogy azokat milyen fenyegetettségek érhetik.

Gyenge pontok

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

Fenyegetettségek elemzése

Az egyes vagyonelemek gyenge pontjaira bizonyos fenyegetettségek hatnak.

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

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

Sérülékenységek

A sérülékenység egy bizonyos gyenge pont kihasználása a rá ható fenyegetettség által.

A bekövetkezési valószínűségek

Következő lépésként meg kell becsülni a sérülékenységek bekövetkezési valószínűségét.

A bekövetkezési valószínűséghez a következő értékeket kell használni.

"3" - gyakori,

"2" - közepes,

"1" - ritka,

Kockázatok

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

A kockázatok minősítéséhez a következő kockázati mátrixot kell definiálni:

		Bekövetkezés valószínűsége		
		1	**2**	**3**
Védelmi igény (kárérték szint)	**1**	A	A	K
	2	A	K	K
	3	A	K	M

A kockázatok jelölése a következő:

A – Alacsony

K – Közepes

M – Magas

Elviselhető kockázatok meghatározása

Az Önkormányzat azt a döntést hozta, hogy minden közepes, illetve közepesnél nagyobb kockázatot kezelni kíván.

Ennek megfelelően a toleranciamátrix a következő:

		Bekövetkezés valószínűsége		
		1	2	3
Védelmi igény (kárérték szint)	1	T	T	T
	2	T	NT	NT
	3	T	NT	NT

A táblázatban alkalmazott jelölések értelmezése a következő:

T – Tolerálható

NT – Nem tolerálható

Kockázatok kezelése

Az Önkormányzat a kockázatokat a következőképpen kezeli:

a) Megfelelő intézkedésekkel csökkenti a fenyegetés bekövetkezési gyakoriságát vagy hatását (Kockázat csökkentés)

b) Tudatosan, a következményeket felmérve elfogadja a kockázatot (Kockázat elfogadás)

c) Elkerüli a kockázatot azáltal, hogy az érintett tevékenységet felfüggeszti (Kockázat elkerülés)

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

Kockázatcsökkentő intézkedések

A PreDeCo elv alapján a kockázatcsökkentés három szemszögből közelíthető meg:

a) Megelőző jellegű (preventív kontrollok)

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

b) Korlátozó vagy javító (korrektív kontrollok)

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

c) Észlelő és reagáló (detektív kontrollok)

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

Az el nem viselhető kockázatok kezelésére az Önkormányzat intézkedési tervet készít az egyes feladatok mellé rendelt felelős, határidő és esetleg költség feltüntetésével.

5. sz. melléklet – Jogosultságigénylési ürlap

Jogosultság igénylő lap

A) Iktatási adatok

Beérkezési dátum:	Igénylő beadásának helye:	Iktatószám:

B) Igénylés típusa

Új jogosultság	☐
Meglévő jogosultság módosítása	☐
Meglévő jogosultság törlése	☐
Jogosultság felfüggesztése	☐
Jogosultság újraaktiválása	☐

Meglévő felhasználónév/Azonosító:

C) Személyes adatok

Név:	Leánykori név:	Beosztás:
Születési hely, dátum:	Cím:	Dolgozói azonosító:
Telefon:	E-mail cím:	Felettes:
		Csoport:

Munkavállalói adatok

D) Jogosultságok

Önkormányzat	Szakrendszer	Szerepkör	Jogosultság időtartama	Jogosultság leírása
	GAZD			
	ADO			
	IRAT			
	ING			

	IPAR			
	PORT			
	GAZD/Vezető			
	GAZD/PU			

Megjegyzés/indoklás:

E) Tájékoztató

kérjük, hogy az esetleges adatokkal való visszaélések elkerülése érdekében, csak és kizárólag az Ön munkavégzéséhez szükséges jogosultságokat igényelje meg. Amennyiben Ön határozott ideig veszi igénybe valamely jogosultságot, kérjük, hogy kizárólag arra az időszakra igényelje meg. Amennyiben nincs pontos információja arról, hogy az adott jogosultság milyen alrendszerekhez, adatokhoz való hozzáférést engedélyez, akkor ebben az esetben a jogosultság leírása mező segít Önnek a kitöltésben. A szakrendszerekhez, alrendszerekhez tartozó kódokat a kitöltési útmutatóban találja. Amennyiben az általános gyakorlattól eltérően speciális jogosultságokra is szüksége van, kérjük, hogy ezt indokolja is az erre szolgáló mezőben.

F) Elbírálás (befogadó szervezet tölti ki)

Jóváhagyás: ☐ Kerelem elbírálást végezte:

Elutasítás: ☐ Aláírás:

G) Nyilatkozat

Alulírott Felhasználó, az ASP rendszer központi nyilvántartása számára rendelkezésre bocsátom az alábbi személyes adataimat. Tudomásul veszem, hogy a központi jogosultság kezelők a személyes adataimat az informatikai rendszerekhez való hozzáférés érdekében, az önkéntes beleegyezésem alapján tárolja és kezeli. Aláírásommal igazolom az adatok valódiságát.

Jelen jogosultság igénylő lap aláírásával tudomásul veszem és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 5. § (1) bekezdés a) pontjára figyelemmel elfogadott hozzájárulásomat adom, hogy az Önkormányzat jelen jogosultság igénylő lapon megadott személyes adatainak az informatikai rendszerekhez történő hozzáférés biztosítása céljából tárolja, feldolgozza és kezelje hozzájárulásom visszavonásáig vagy a jogosultság megszűnését követő 5 évig.

Kelt: _____ . _____ Aláírás: _____

6. sz. melléklet - Felhasználói Nyilatkozat

Nyilatkozat

Alulírott

Név: _____

Beosztás: _____

Szervezeti egység: _____

Sz. ig. szám: _____

kijelentem, hogy a Hernádi Polgármesteri Hivatal Informatikai Biztonsági Szabályzatának és/vagy[4] Felhasználói Informatikai Biztonsági Házirendjének tartalmát megismertem és elfogadom, hogy azt munkám során betartom, illetve betartatom (vezetők esetén).

Nyilatkozom továbbá, hogy az önkormányzati munkavégzésem során tudomásomra az önkormányzati adatokat bizalmasan kezelem, harmadik félnek nem tovább nem adom.

Tudomásul veszem, hogy a jelen nyilatkozatomban vállalt kötelezettségeim a jogviszonyom megszűnése után is fenn álnak.

Tudomásul veszem továbbá, hogy a jelen nyilatkozatban foglaltak megsértése büntetőjogi és polgári jogi következményeket von maga után.

Hernád, 201. .....

.....
Aláírás

[4] A megfelelő rész aláhúzandó.