Szarvasi Polgármesteri Hivatal

Informatikai Biztonsági Szabályzata

2/2015. szabályzat

2

1. Bevezetés

Az Informatikai Biztonsági Szabályzat (IBSZ) egységes szerkezetben tartalmazza Szarvasi Polgármesteri Hivatala (továbbiakban: hivatal) törvényes, szakszerű és zavartalan működésének, biztonságának, fenntartása érdekében betartandó követelmények meghatározását és az alkalmazandó eljárásokat.

A hivatal az IBSZ kiadásával biztosítani kívánja:

- A szakmai titok- és információvagyon védelemre vonatkozó előírások betartását.
- Az információs önrendelkezési jog kellő védelmét.
- Az üzemeltetett informatikai eszközök, hálózatok, stb. rendeltetésszerű használatát és megfelelő üzemvitelét.
- Az üzembiztonságot szolgáló műszaki fenntartási és karbantartási teendők hatékony elvégzését.
- A számítógépes feldolgozások és az eredményadatok további hasznosítása során a bizalmasság sérüléséből eredő károk megelőzését, illetve a kockázatok elviselhető mértékűre való csökkentését.
- Az adatállományok sértetlenségének, formai és tartalmi helyességének és épségének megőrzését.
- Az alkalmazott szoftverek integritásának, megbízható működésének biztosítását.
- Az adatállományok biztonságos mentését és megőrzését.
- A hivatal adatait kezelő, vagy feldolgozó személyek felelősségét, különösen a szervezetek vezető beosztású és az informatikai feladatokat irányító dolgozóinak a feladatait az informatikai biztonság tekintetében.
- A jogosultság és a hozzáférés rendszerének dokumentált kialakítását.

A célok elérése érdekében az egyes rendszerelemek fennállásának teljes ciklusa alatt (a tervezés, alkalmazás, üzemeltetés, felszámolás) arányos védelmet alakít ki a hivatal.

Az IBSZ az informatikai biztonsággal összefüggő normákat, eljárásokat, ezek dokumentálását és az ellenőrzésének leírását, illetve az erre való hivatkozásokat tartalmazza.

Az IBSZ rögzíti:

- az informatikai biztonság általános célkitűzéseit és tárgykörét, valamint a biztonság és a védelmi intézkedések fontosságát abban a mechanizmusban, amely az információ megosztását teszi lehetővé;
- a vezetőség elkötelezettségét, hogy miként támogatja az informatikai biztonság céljait és elveit;
- az informatikai rendszer elemeinek tervezését és új elemeinek bevezetését, üzemeltetését és használatát
- az informatikai biztonság menedzselésének (Információ Biztonsági Felelős és

informatikai üzemeltetést végzők) általános és sajátos felelősségi körei meghatározását,
- utalást mindenolyan dokumentációra, amely támogatja a szabályzatot, pl. Informatikai rendszer részletesebb biztonsági szabályzataira és eljárásaira, vagy olyan biztonsági szabályokra, amelyeket a Felhasználóknak követniük kell.

1.1. Személyi hatály:

Jelen szabályzat hatálya kiterjed a hivatal valamennyi munka- és felelősségi körében érintett dolgozójára, illetve a hivatal területén, vagy a hivatal adataival dolgozó szerződéses alvállalkozókra.

1.2. Tárgyi hatály:

Az Informatikai Biztonsági Szabályzatalkalmazása kiterjed az hivatal saját üzemeltetésű és kiszervezett informatikai rendszereiben működtetett valamennyi hardver berendezésre, szoftver elemre és ezek dokumentációira (fejlesztési, szervezési, programozási, műszaki, üzemeltetési, biztonsági) és az informatikai rendszerben feldolgozott adatállományok teljes körére.

A központi államigazgatási, közigazgatási szervek által üzemeltetett rendszerek védelmi intézkedéseit azok üzemeltetője biztosítja, illetve írja elő. Az adott rendszeren nem lehet az IBSZ-ben meghatározottaknál gyengébb védelmi intézkedések megvalósítani.

1.3. Területi hatály:

Az IBSZ hatálya kiterjed a hivatal székhelyére, minden telephelyére, továbbá mindazon objektumokra és helyiségekre, amelyekben a „Tárgyi hatály" pontban meghatározott eszközöket, szoftvereket, adatokat vagy dokumentumokat hoznak létre, tárolnak, felhasználnak, vagy továbbítanak.

1.4. Időbeli hatály:

A szabályzat a hatályba lépés napjától visszavonásig érvényes, felülvizsgálatát a szabályzatban külön meghatározottak szerint kell elvégezni.

1.5. Vonatkozó jogszabályok, külső- és belső normák

1.5.1. Alapvető jogszabályok, külső normák

- 2011. évi CXXII. törvény az információs önrendelkezési jogról és az információszabadságról
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 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
- 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről

1.5.2. Belső Normák

- Szarvasi Polgármesteri Hivatal (hatályos) szervezeti és működési szabályzata
- 9/2013. szabályzat a Szarvasi Polgármesteri Hivatal tulajdonát képező mobil és vezetékes

telefonok hivatali és önkormányzati használatához
- 1/2012. Szarvas Város Polgármesteri Hivatala szabályzata az iratkezelésről
- 9/2012. felesleges vagyontárgyak hasznosításának, selejtezésének szabályzata
- 12/2012. Szarvas Város Önkormányzatának Tűzvédelmi szabályzata
- 16/2012. Szarvas Város Polgármesteri Hivatalában az Internet- és Intranet- szolgáltatás igénybevételéről valamint a belső illetve külső E-mail szolgáltatás használatáról
- 17/2012. Szarvas Város Polgármesteri Hivatala Közszolgálat adatvédelmi szabályzat
- 14/2011. Szarvas Város Polgármesteri Hivatala Adatvédelmi és Számítástechnikai Adatbiztonsági szabályzata
- 18/ 2010. szabályzat: TakarNet hálózati igénybevétele
- 6/2008. Vagyongazdálkodási és beruházási szabályzat
- 7/2007. Szarvas város Polgármesteri Hivatal tulajdonát képező mobil munkaállomások (laptopok) személyi használatáról
- 6/2014. számú szabályzattal módosított 21/2007. .Szarvas Város Polgármesteri Hivatala Informatikai szabályzata
- 11/2006. szabályzat a szabálytalanságok kezelésének eljárásrendjéről

2. AZ INFORMATIKAI RENDSZER ÁLTALÁNOS BIZTONSÁGI ALAPELVEI

a) A hivatal az általa kezelt adatok, valamint informatikai rendszere tekintetében a felmerülő kockázatokkal arányos egyenszilárdságú védelmet alakít ki.

b) Az alkalmazott informatikai rendszerek és azok üzemeltetési rendje biztosítja a rendszer és a rendszerben feldolgozandó adatok rendelkezésre állását, hitelességét, sértetlenségét és titkosságát azok teljes feldolgozási folyamatában.

c) A hivatal az információvédelem területén biztosítja az informatikai rendszer gyártói ajánlásoknak és biztonsági követelményeknek történő megfelelését.

d) Az információ biztonsági megoldásokat úgy kell kialakítani, hogy azok a rendszerek mindennapi alkalmazásának és üzemeltetésének hatékonyságát a lehető legkisebb mértékben befolyásolják.

e) Az informatikai rendszer alkalmazására és üzemeltetésére vonatkozó szervezeti és működési rendeket, nyilvántartási és tájékoztatási szabályokat, az informatika alkalmazásából eredő biztonsági kockázatok figyelembevételével úgy kell kialakítani, hogy a felelősségi körök és az egyértelmű személyes felelősségek meghatározhatók legyenek.

f) Az információ biztonsági adminisztratív intézkedések közül kiemelt szerepet tölt be a négy szem elve. A biztonság szempontjából kritikus folyamatok esetében kötelező a négy szem elvének alkalmazása.

g) A fennmaradó kockázatok miatt bekövetkező esetleges káresemények következményeinek kezelésére megfelelő döntést kell hozni.

3. INFORMATIKAI BIZTONSÁG DOKUMENTUMAI

3.1. Informatikai Biztonsági Szabályzat

Az informatikai biztonság részletes szabályozását az Informatikai Biztonsági Szabályzatnak kell tartalmaznia. Az IBSZ-t a jegyző teszi közzé, az Informatikai Biztonsági Szabályzat szabályzatgazdája az Információ Biztonsági Felelős.
Az Információ Biztonsági Felelős valamennyi munkatárssal megismerteti a rá vonatkozó követelményeket, információ biztonsági oktatás formájában.

3.1.1. Informatikai biztonság dokumentumai

A hivatalnak rendelkeznie kell - az informatikai rendszerének biztonságos működtetésére vonatkozó - utasításokkal és előírásokkal, valamint a fejlesztésre vonatkozó tervekkel, illetve az ügymeneti tevékenységét közvetlenül vagy közvetve támogató informatikai rendszer folyamatos és biztonságos működését biztosító dokumentációval.

Az információ biztonsági szabályozások egységes felépítését a következő dokumentumok biztosítják:

a) **Informatikai Biztonsági Politika (IBP),**
b) **Informatikai Biztonsági Stratégia (IBS),**
c) **Informatikai Biztonsági Szabályzat (IBSZ),**; az felhasználók számára nélkülözhetetlen informatikai és információ biztonsági szabályozást és eljárásrendeket tartalmazza; szabályzat gazdája az Információ Biztonsági Felelős
d) **Szabályzatok:** az Informatikus és az Információ Biztonsági Felelős által előterjesztett szabályzatok, eljárásrendek, amely dokumentumokra az Informatikai Biztonsági Szabályzata megfelelő helyén hivatkozik.
e) **Nyilvántartások:** az Informatikai Biztonsági Szabályzat szerinti szabványosított jegyzőkönyvek az informatika, illetve a biztonság területén, formanyomtatványok az informatika, illetve a biztonság területén, nyilvántartások és naplók.

A szabályzatokat, utasításokat és nyilvántartásokat ezek informatika alkalmazásából eredő biztonsági kockázatok figyelembevételével úgy kell kialakítani, hogy a felelősségi körök és az egyértelmű személyes felelősségek meghatározhatók legyenek.
Minden Informatikai Biztonsági Szabályzatot érintő aktuális dokumentáció, nyilvántartás őrzéséről a szakterület szerint illetékes szervezeti egység gondoskodik, a lejárt dokumentációkat és nyilvántartásokat az utolsó használatukat követően még legalább 3 évig (a hatályos jogszabályok alapján akár ennél több évig is) meg kell őrizni.

3.1.2. Felülvizsgálat és értékelés

Az Információ Biztonsági Felelős gondoskodik az IBSZ évenkénti felülvizsgálatáról, illetve soron kívüli felülvizsgálatáról minden jelentős változást követően.

a) biztonsági esemény, vagy események természete, száma, hatása,
b) a szervezeti vagy műszaki infrastruktúra újabb sérülékenységei vagy változásai

c) a technológiai, műszaki változások hatásai.

4. AZ INFORMATIKAI BIZTONSÁG SZERVEZETE

4.1. Felelősségek, hatáskörök, elkötelezettségek

4.1.1. Általános felhasználók

A hivatal minden munkatársa, valamint minden a hivatallal szerződésben lévő informatikai alvállalkozó és természetes személy felelős:

a) az Informatikai Biztonsági Szabályzatnak a felhasználó munkaterületére vonatkozó előírásainak betartásáért és betartatásáért,

b) a felhasználó munkaterületén az adatbiztonság és a bizalmas adatok, információk megtartásáért, a nyilvánosságra hozatal megakadályozásáért.

A hivatal minden munkatársa köteles:

a) az Informatikai Biztonsági Szabályzat dokumentumában előírt ellenőrzések és az auditok sikeres megvalósítását elősegíteni és támogatni;

b) az Informatikus és az Információ Biztonsági Felelős informatikai biztonságra vonatkozó utasítások, szabályzatok betartásához kapcsolódó előzetes bejelentés nélküli és előre tervezett ellenőrzését támogatni.

4.1.2. Szervezeti egységek vezetői

a) A szervezeti egységek vezetői felelősek az IBSZ betartásának megkövetelésééért. A szervezeti egységek által kezelt adatok kezelésének szakszerűségéért.

b) A vezetőknek az adatkezeléssel kapcsolatos külső szolgáltatások igénybevétele előtt fel kell mérni azokat a kockázatokat, amelyek hatást gyakorolnak a hivatal informatikai rendszereire.

c) Meg kell határozniuk és dokumentáltan jelezniük az informatikusnak a felhasználók jogosultságait, változásait és megszűnését a szervezeti egység által használt informatikai rendszerek hozzáféréséhez.

d) Együttműködnek a szervezeti egység munkájának hatékony védelmét biztosító intézkedések kialakításában.

4.1.3. Informatikus (üzemeltetési felelős)

4.1.3.1. Feladata

a) az Informatikai rendszer Informatikai Biztonsági Szabályzatnak megfelelő működtetése;

b) az Informatikai rendszer működtetéséhez szükséges valamennyi személyi és tárgyi erőforrás a szabályzatban definiált Információ Biztonsági elvárások figyelembe vétele alapján történő biztosítása;

c) a biztonsági elvárások érvényesítése az informatikai fejlesztési és üzemeltetési feladatainak végrehajtása során;

d) az általa érzékelt vagy ismert kockázatokról az Információ Biztonsági Felelőst tájékoztatni;

4.1.3.2. Felelőssége

a) Az Informatikus felelősséggel tartozik az Informatikai rendszer(ek) működtetéséért.
b) Az Informatikus felelős a biztonság szervezési szintű megvalósításáért, valamint támogatja a védelmi intézkedések meghatározását.

4.1.3.3. Jogosultsága

Az Informatikus jogosult
a) az informatikai rendszer teljes körű ellenőrzésére;
b) az informatikai biztonságot érintő szabályzatok, utasítások és dokumentumok észrevételezésére;
c) az informatikai biztonságot érintő beruházások, beszerzések véleményezésére.

4.1.4. Információ Biztonsági Felelős

Az Információ Biztonsági Felelős (az elektronikus informatikai rendszerek biztonságáért felelős személy) a jegyző utasításait hajtja végre, neki alárendelten látja el a feladatait.

4.1.4.1. Feladata

Általános feladata:

a) közreműködik az informatikai rendszerben az informatikai biztonságot érintő rendszerek megvalósításában;
b) előkészíti a hivatal információ biztonsági tervezését, figyelembe véve a hivatal feladatait, stratégiai terveit;
c) elvégzi a következő évi költségvetés tervezését az új, biztonsággal összefüggő célok megvalósítására, és ennek keretében kezdeményezi új adatvédelmi eszközök vagy megoldások beszerzését;
d) véleményezi a hivatal informatikai fejlesztéseit az informatikai biztonság szempontjából;
e) biztosítja a veszélyforrások körében bekövetkező változások folyamatos követését, és ezek alapján kezdeményezi a szükséges intézkedések meghozatalát;
f) felméri az információtechnológia használatából adódó biztonsági kockázatokat a tervezés, beszerzés, üzemeltetés és az ellenőrzés területén;
g) elvégzi, felülvizsgálja és aktualizálja az információ biztonsági rendszert;
h) biztosítja az adat- és információvédelmi feladatok folyamatos belső ismertetését, a képzési terv kidolgozását és oktatását;

Ellenőrzési feladata:

a) elkészíti az Informatikai Biztonsági Szabályzat alapján az éves információ biztonsági ellenőrzési programot, majd végrehajtja az éves információ biztonsági ellenőrzési programban előírtakat.

b) ellenőrzi az információ biztonsági előírások betartatását, ami magában foglalja
   - a védelmi előírások betartásának ellenőrzését;
   - az adatvédelmi biztonsági rendszer érvényesülésének ellenőrzését;
   - az informatikai munkafolyamat bármely részének informatikai biztonság szempontú ellenőrzését;
   - az Informatikai Biztonsági Szabályzatban foglalt más területekre vonatkozó feladatok végrehajtásának ellenőrzését;
   - az Informatikussal egyeztetve biztonsági és határvédelmi ellenőrzést,
   - biztonsági és határvédelmi audit végrehajtásában/ végrehajtatásában való részvételt;

Dokumentációs feladata:

a) felülvizsgálja az Információ Biztonsági Stratégia dokumentumot és a tartalmát aktualizálja a hivatal feladatai alapján, legalább 2 évente;

b) felülvizsgálja és aktualizálja az Informatikai Biztonságpolitika, Informatikai Biztonsági Szabályzat dokumentumokat és azok kapcsolódó dokumentumait legalább 2 évente;

c) véleményezi az Informatikai Biztonsági Szabályzat tárgykörébe tartozó szabályzásokat, utasításokat;

4.1.4.2. Felelőssége

Az Információ Biztonsági Felelős, kötelezettséget vállal:

a) az Informatikai Biztonságpolitika, az Informatikai Biztonsági Szabályzat kidolgozásáért és szakmai tartalmáért;

b) az Információ Biztonsági Stratégiában foglalt célkitűzések érvényesítéséért;

c) az informatikai biztonsághoz kapcsolódó utasítások, szabályzatok és tervek kidolgozásáért, azok összhangjáért és a betartásának ellenőrzéséért

d) az informatikai biztonság tudatosításáért;

e) a biztonsági előírásokat megsértőkkel szemben szükséges intézkedések kezdeményezéséért a jegyzőnél;

f) az Informatikai rendszerben az informatikai biztonságot érintő rendszerek megvalósításáért, a megvalósítás menedzseléséért, felügyeletéért.

4.1.4.3. Jogosultságai

Az Informatikai Biztonsági Felelős jogosult:

a) az Informatikai Biztonsági Szabályzat előírásainak betartását bármely érintett szervezeti egységnél ellenőrizni;

b) az Informatikai rendszer működtetésével, fejlesztésével, valamint az adatfeldolgozásokkal kapcsolatos valamennyi dokumentumba betekinteni;

c) az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezni a Jegyzőnél.

A szabályzatok módosításának szakmai elkészítéséhez az Információ Biztonsági Felelős jogosult igénybe venni az informatikai szervezet munkatársait.

Az Információ Biztonsági Felelős a szabályzatgazdája az Informatikai Biztonságpolitikának és az Információ Biztonsági Szabályzatnak, illetve az informatikai biztonsághoz kapcsolódó egyéb utasításoknak és szabályzatoknak, valamint felel ezek összhangjáért.

Az Információ Biztonsági Felelős és az Informatikus támogatja és véleményezi a hivatal információ biztonsági tervezését, figyelembe véve a hivatal feladatait, informatikai stratégiai terveit, és ennek keretében kezdeményezi új adatvédelmi eszközök vagy megoldások beszerzését.

4.1.5. Jegyző gondoskodik

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

b) az elektronikus információs rendszer biztonságáért felelős személy megbízásáról,

c) a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonságpolitikájának kiadásáról,

d) a szervezet elektronikus információs rendszereinek információ biztonsági stratégiájának kiadásáról,

e) az Informatikai Biztonsági Szabályzat kiadásáról,

f) az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, az információbiztonsági ismeretek szinten tartásáról,

g) a biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatásáról,

h) az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,

i) a biztonsági eseményekre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,

j) az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában, javításában, az adatkezelési vagy az adatfeldolgozási tevékenységben közreműködővel szemben érvényesülő – az Ibtv-ben törvényben foglalt- szerződéses kötelmek teljesüléséről,

k) a biztonsági események és a lehetséges fenyegetések haladéktalan jelentéséről,

l) az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedések megtételéről.

4.1.6. Az informatikai biztonsággal kapcsolatos egyéb felelősségek

Az Információ Biztonsági Szabályzat általános iránymutatással szolgál a hivatalban a biztonsági szerepek és felelősségek kiosztására. Meghatározza és leírja az egyes önálló fizikai-, és információvagyon, valaminta biztonsági folyamatok helyi felelősségét.
A védelmi intézkedések betartatása az egyes területi vezetők feladata.

Az egyes vagyontárgyakért az azt használó személy, csoportos használat esetén a felhasználó terület vezetője a felelős.

4.1.7. Kapcsolat a hatóságokkal

A jogszabályoknak megfelelően a hivatal megfelelő kapcsolatot tart fenn a jogalkalmazó hatóságokkal, szabályozó és ellenőrző testületekkel.

A megfelelő kapcsolatok kiépítéséért a hivatal vezetése, illetve az általuk ezzel megbízott munkatársak felelősek.

A kapcsolatok során az információcserét a törvényi szabályozásnak, jelen szabályzatnak és az adatvédelmi törvénynek megfelelően lehet végrehajtani a védett információk jogosulatlan személyekhez kerülésének megakadályozását szem előtt tartva.

5. Harmadik fél hozzáférési biztonsága (kiszervezés)

5.1. Harmadik fél hozzáférési kockázatának azonosítása

Minden külső fél által végzett munkavégzés esetében előzetesen kockázatfelmérést kell végezni. (A munkavégzés során milyen adatokhoz, fizikai adathordozókhoz férnek hozzá fizikailag, vagy logikailag? A munkavégzés milyen veszélyekkel jár az informatikai rendszer működésére?)
Az érintett felekkel titoktartási nyilatkozatot kell aláíratni.

A kockázatfelmérést a megbízó vezető végzi, amennyiben az informatikai rendszerhez való hozzáféréshez is szükség van, akkor az Információ Biztonsági Felelős bevonásával.
A kockázatfelmérés során figyelembe kell venni az elvárt hozzáférés fajtáját, az információ értékét, a külső fél által használt óvintézkedéseket, valamint a hivatal információihoz történő hozzáférés hatását a biztonságra. A kockázatfelmérés alapján, amennyiben szükséges további külön óvintézkedéseket kell meghatározni és alkalmazni.

Az informatikai rendszert érintő óvintézkedéseket egyeztetni kell az Információ Biztonsági Felelőssel.

5.2. Harmadik fél számára adható hozzáférések

5.2.1. fizikai hozzáférés

A hivatal helyiségeihez, számítógépteremhez, tároló szekrényhez);

Azon külső felek, amelyek szerződésükben meghatározott módon, a helyszínen végeznek munkát, biztonsági kockázatot jelentenek.

a) hardvert és szoftvert karbantartó és támogató személyzet;

b) tisztító-, ellátó-személyzet, biztonsági őrség, valamint hasonló erőforrás-kihelyezést támogató szolgáltatások;
c) eseti, rövididejű alkalmazottak;
d) konzultánsok;
e) ellenőrző szervezetek munkatársai.

5.2.2. logikai hozzáférés

A hivatal adatbázisaihoz, informatikai rendszereihez.

a) a hardver és a szoftver támogatók személyzete, akiknek rendszerszintű vagy elektronikus belső adatok megismerését biztosító hozzáférésre van szükségük;
b) társszervezetek, amelyek információt cserélhetnek, amelyek hozzáférhetnek az informatikai rendszerhez vagy osztozhatnak a közös adatbázison.

5.3. A harmadik féllel kötött szerződés biztonsági követelményei

A hivatal információ-feldolgozó rendszereihez harmadik fél hozzáférési lehetőségét a féllel kötött hivatalos szerződésbe kell belefoglalni.
A szerződés tartalmazza, vagy hivatkozik minden olyan információ biztonsági követelményre, amely biztosítja a hivatal biztonsági szabályzatának és a szabványoknak való megfelelést.

Minimálisan a következő információkat tartalmazza a szerződésbe:
a) az információ biztonsági szabályzatra való hivatkozást;
b) a vagyonvédelmet, beleértve:
   - a hivatal vagyonának a védelmét, beleértve az információvagyont és a szoftvert is;
   - az óvintézkedéseket, amelyek biztosítják, hogy a szerződés lejártával vagy a szerződés érvényességi idején belül egy előre meghatározott időpontban, az átadott információkat vagy megsemmisítik, vagy pedig visszaszolgáltatják;
   - az információ másolásának és nyilvánosságra hozatalának korlátozásait;
c) valamennyi rendelkezésre bocsátandó szolgáltatás leírását;
d) a hivatal informatikai rendszeréhez történő hozzáférés esetén a megismerhető adatokat és a megengedett hozzáférés módokat;
e) a felhasználói tevékenységek ellenőrzésének a jogát.

A harmadik féllel (alvállalkozóval) a többi feltétel és körülmény mellett meg kell ismertetni az IBSZ-ben foglaltak rá vonatkozó követelményeit is. Ezért a megbízó terület vezetője felelős.

6. A VAGYON OSZTÁLYOZÁSA ÉS ELLENŐRZÉSE

6.1. Az információs vagyon nyilvántartása

6.1.1. Eszközvagyon leltár

A hivatalnak pontosan ismernie és azonosítania kell az informatikai eszközvagyonát és adatvagyonát (továbbiakban: vagyontárgy), és megállapítani ezek viszonylagos értékét és fontosságát. Erre az információra alapozva a hivatal a vagyon értékével és jelentőségével arányosan tudja megállapítani a védelmi szinteket.

Leltárt kell készíteni minden olyan jelentős vagyontárgyról, amely valamelyik informatikai rendszerrel kapcsolatos, és a leltárt karban kell tartani. Egyértelműen azonosítani kell valamennyi vagyontárgyat, meg kell állapítani és dokumentálni kell annak tulajdonjogát, felelősét és az informatikai rendszerben meglévő szerepét, valamint pillanatnyi elhelyezését.

A vagyonleltárt az Informatikus készíti el és tartja aktuális szinten, a nyilvántartás ellenőrzésért az Információ biztonsági Felelős.

Az alábbiak a vagyonleltár elemei:

a) **fizikai vagyontárgyak:** számítógépek, a távközlési berendezések, faxok, üzenetrögzítők, mágneses adathordozók (usb-kulcsok, lemezek…), egyéb műszaki berendezések (tápegységek) légkondicionáló; és az egyéb kiszolgáló helyiségek berendezései;
b) **szoftver-vagyontárgyak:** alkalmazás szoftverek, rendszerszoftverek, fejlesztési eszközök és szolgáltatások;
c) **információ-vagyontárgyak:** adatbázisok és adatállományok, rendszerdokumentáció, felhasználói/kezelői kézikönyvek, oktatási anyagok, üzemviteli, üzemeltetési és támogató eljárások, ügymenet folytonossági tervek, tartalékolási elrendezések, archivált információ;
d) **szolgáltatások:** számítástechnikai és távközlési szolgáltatások.

6.1.2. Eszközök felelősei

Az új munkavállalók belépésekor, vagy új munkaeszközök kiadásakor a szükséges eszközöket (számítógép, laptopok) eszköz átadási jegyzőkönyvben kerülnek felsorolásra és átadásra.
A munkavállaló nyilatkozik arról, hogy a működőképes állapotban átvett eszközöket az IBSZ előírásainak megfelelően használja. A mobiltelefonok átadását a gazdálkodási csoport végzi, a készülékekre vonatkoznak az IBSZ biztonsági és felelősségi szabályai.

Az egyénhez nem rendelhető informatikai vagyontárgyakat a felhasználó szervezeti egységhez, mint csoporthoz kell hozzárendelni. A felelősséget ezekben az esetekben a felhasználó szervezeti egység vezetője viseli.

6.1.3. Az eszközök megfelelő használata

Az informatikai eszközök használatának során a következő biztonsági szempontokat kell betartani:

a) A felhasználó köteles az eszközöket és a szoftvereket rendeltetésüknek megfelelően használni.
b) A felhasználó köteles a tőle elvárható gondossággal eljárni az eszközök használata során. Az eszközöket védeni köteles rongálás vagy szándékos károkozás ellen.
c) A felhasználó a rábízott eszközöket nem adhatja kölcsön harmadik személynek kockáztatva így az eszköz épségét, és az esetlegesen rajta lévő adatok biztonságát és sértetlenségét.

d) A felhasználó bármilyen hibát vagy sérülést észlel, azonnal jelentenie kell az informatikusnak.
e) A felhasználó a használatába adott eszközökön csak a munkavégzéséhez szükséges feladatokat végezheti, magán célokra nem használhatja azt.
f) Az eszközök rendszerbeállításait nem változtathatja meg, szoftvereket és alkalmazásokat nem telepíthet.
g) Személyes adatokat csak indokolt esetben és a hivatali adatoktól elkülönítetten tárolhat az eszközökön.
h) Tilos az eszközök személyes haszonszerzés, illetve nem a hivatal érdekében történő használata.
i) Tilos a politikai (a hivatali feladatokon kívüli) vagy erkölcsi, vagy más törvénybe, vagy jó erkölcsbe ütköző anyagok készítése, tárolása, közlése, megjelenítése a hivatal eszközein.
j) A hivatal információ feldolgozó eszközeit a hivatal helyiségeiből csak külön engedéllyel szabad kivinni.
k) A hivatal információ feldolgozó rendszeréhez személyes információ feldolgozó eszközt csatlakoztatni csak külön engedéllyel szabad.

6.2. Az információ (adat) osztályozása

6.2.1. Osztályozási irányelvek

Az ügymenetek során az informatikai rendszerben az adatok kezelése a mindenkor hatályos jogszabályokkal összhangban történik.

A 2013. évi L. törvény és végrehajtási rendelete alapján az informatikai rendszereket biztonsági osztályokba kell besorolni, mely figyelembe veszi a rendszerek, illetve az általuk kezelt és tárolt adatok bizalmasságát, sértetlenségét és rendelkezésre állását.

A rendszerek biztonsági osztályba sorolásának és az ezzel kapcsolatos óvintézkedéseknek a Vhr. szerinti követelményeket figyelembe vételével történik.

Az informatikai rendszerek biztonsági osztályba és a védelmi intézkedések szintjének besorolását az Információ Biztonsági Felelős végzi el, melyben közreműködik az informatikus.

A besorolást a szabályzat mellékletében kell nyilvántartani.

6.2.2. Az adatok kezelése

Az informatikai rendszerben megvalósított adat- és információvédelmet az Informatikai Biztonsági Szabályzattal összhangban kell meghatározni.

A hivatal az informatikai rendszereiben kezelt adatok védelme érdekében elvárás:

a) az informatikai rendszer eszközeinek a biztonsági osztályba sorolásuknak megfelelő védelme,
b) erős felhasználó azonosítás és hitelesítés,
c) a felhasználók felelősségének megállapítását biztosító biztonsági beállítások,
d) audit és esemény naplók működtetése.

7. A SZEMÉLYI BIZTONSÁG

7.1. Az alkalmazás alatt

7.1.1. Vezetői felelősségek

A hivatal vezetőinek feladata, hogy biztosítsák az alkalmazottak, illetve szerződő felek, vagy a hivatalnál egyéb jogviszony alapján munkát végzők:

a) megfelelő tájékoztatását az információbiztonsági feladataikról és felelősségükről mielőtt az érzékeny információkhoz vagy információs rendszerekhez hozzáférést biztosítanak számukra;
b) a biztonsági irányelvekhez (szabályzatokhoz) való hozzáférését;
c) a biztonsági szabályzat betartásának fontosságával tisztában legyenek;
d) megfelelő tudatossági szintet érjenek el a biztonságra vonatkozóan;
e) a munkavégzéshez szükséges megfelelő jártasságuk és minősítésük legyen.

7.1.2. Információ biztonsági tudatosság, oktatás és képzés

A felhasználók, valamint a kijelölt (közvetlen felügyelet nélküli munkát végzők) külsős munkatársak számára az informatikai rendszer biztonságos használatával kapcsolatos rendszeres oktatás rendjét az Információ Biztonsági Felelős alakítja ki, és tartja karban.

A felhasználók biztonság tudatossági oktatását legalább évente meg kell tartani, melyet az Információ Biztonsági Felelős szervez.

Az oktatással célja, hogy a felhasználók felismerjék azokat a veszélyhelyzeteket, amelyek az intézménynek károkat okozhatnak (pl. vírusok terjesztése, adatvesztés, adatlopások, szoftverek jogosulatlan használata vagy másolása stb.),
A személyes adatkezelést végző területek felhasználói számára az adatvédelmi ismeretek oktatásával egészíthető ki a képzés.

A külső munkatársak információ biztonsági oktatását a munkavégzés megkezdése előtt kell elvégezni, melyet az Információ Biztonsági Felelős szervez meg.

7.1.3. Fegyelmi eljárások

Az IBSZ megsértését ki kell vizsgálni. A kivizsgálást az Információ Biztonsági Felelős végzi, az informatika munkatársainak illetve a szakterület vezetője által kijelölt belső szakértő munkatárs bevonásával.

A vizsgálat eredményéről, a megtett és javasolt intézkedésekről az Információ Biztonsági Felelősnek feljegyzést kell készíteni, a Jegyző számára.

Bármilyen, az informatikai rendszerben, vagy informatikai rendszerrel végzett tevékenységgel összefüggésben a hivatalnak történő károkozás esetén, a munkatárs helytállási kötelezettségét az érintett munkajogviszonyára vonatkozó rendelkezések alapján állapítja meg a munkáltató. Bűncselekmény elkövetése esetén büntetőjogi felelősségre vonatkozó szabályokat kell alkalmazni.

7.2. Az alkalmazás megszűnése vagy megváltozása esetén

7.2.1. A felelősségek megszűnése

Az alkalmazás befejezése után továbbra is érvényben maradó felelősségeket (pl. titoktartás) és kötelezettségeket (pl. eszközök átadása) az alkalmazott, szerződő fél vagy harmadik fél felhasználó szerződésében, vagy egyéb dokumentumban kell szerepeltetni. Ezért a

munkavégző szakterületének vezetője a felelős.

7.2.2. Az eszközök visszaszolgáltatása

Minden, használatra kiadott informatikai eszközt a jogviszony megszűnésének napjáig az Informatikusnál le kell adni. Az eszközök visszavételét az Informatikus az eszköz átadás-átvételi jegyzőkönyvön igazolja. Az igazolás nélkül a dolgozó jogviszonyát nem lehet megszűntetni.

Szerződő fél végső teljesítés igazolása, amennyiben informatikai és/vagy kommunikációs eszközöket vett át a munka elvégzéséhez, csak a visszaszolgáltatási igazolás megléte esetén igazolható.

7.2.3. Hozzáférési jogok eltávolítása

Legkésőbb, az informatikai rendszerekhez hozzáférést biztosító jogviszony megszűnésének utolsó napján az összes hozzáférési jogosultságot deaktiválni kell. A deaktiválás időpontját az adott szervezeti egység vezetője közli az informatikussal, aki végrehajtja a módosítást.

Gondoskodni kell a felhasználó által készített, illetve használt hivatalos elektronikus dokumentumok archiválásáról és az illetékes szervezeti egység vezetőjének való átadásról. Az archivált dokumentumok őrzésének idejét, vagy törlésének végrehajtását a szervezeti egység vezetője jelöli ki.

Szerződéses munkavégző esetén a hozzáférési jogosultságokat csak a munkavégzés idejére szabad kiadni. A jogosultságok visszavonásának megtörténtét írásban, vagy e-mailben dokumentálni kell.

A hozzáférésre nem jogosult felhasználó azonosítóját inaktívvá kell tenni, és az azonosítót egy éven belül újra kiadni tilos.

A felhasználó távozása miatt az email hozzáférés jogosultságát is meg kell szüntetni. Ezeket az inaktív email címeket 1 évig kell fenntartani és biztosítani, hogy a címre emailt küldők automatikus válaszban kapjanak tájékoztatást a cím használaton kívüliségéről és az új ügyintéző elektronikus elérhetőségéről. Az inaktív email cím levelezését 1 évig kell archíválni a szervezeti egység vezetője által elérhető tárhelyen.

Az informatikai jogosultság nyilvántartást az informatikusnak folyamatosan aktualizálni kell.

8. FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG

8.1. Biztonsági zónák

A biztonsági zóna lehet a lezárt iroda vagy néhány helyiség a fizikai biztonsági védősávon belül, amelyek vagy maguk zárhatók, vagy amelyekben zárható szekrények és páncélszekrények vannak.

A biztonsági körlet kiválasztása és megtervezése során figyelembe kell venni mindazokat a lehetséges károkat, amelyek tűzből, vízből, robbanásból, vagy bármely más formájú természeti vagy ember okozta katasztrófából eredhetnek.

8.1.1. Biztonsági védelem

A biztonsági felület- és térvédelmet olyan körletek esetében kell használni, amelyekben információ-feldolgozó eszközök vannak elhelyezve.

Fizikai biztonsági védelem bármi, ami akadályt képez, pl. fal, kártyavezérelt beléptető kapu vagy személyzettel ellátott beléptető porta. A fizikai biztonsági védőeszközök elhelyezésére vonatkozó terveket az Információ Biztonsági Felelős és az Informatikus véleményezi.

8.1.2. Fizikai beléptetési óvintézkedések

A biztonsági zónába (szerverszobába) belépőknek a helyiségben elhelyezett benntartózkodási naplóba kötelesek magukat bejegyezni.

A szerverszobában egyéb munkát végezni alapvetően csak az informatikusok jelenlétében lehet. A felügyelet nélkül végezhető munkákat a szervezeti egység vezetője engedélyezi a munkát végző személyek, a cégnév és munkavégzés leírása és az időtartamának a megjelölésével.

A benntartózkodási naplóban a bejegyzést a dátum, cégnév, munkavégző személy, munkavégzés leírása, érkezés és távozás időpontja, aláírás rovatok kitöltésével kell megtenni.

A benntartózkodási napló tartalmát 1 évig kell megőrizni, amely az Informatikus feladata.

8.1.3. Az irodák, a helyiségek és az eszközök biztonságba helyezése

A hivatal irodákkal, és az eszközök biztonságba helyezésével kapcsolatos szabályok betartása kiemelten fontos feladat.

Az alábbi védelmi intézkedéseket kell megvalósítani:

a) a kulcsfontosságú eszközöket úgy kell elhelyezni, hogy a jogosulatlan személyek hozzáférését elkerüljük;
b) irodai berendezéseket és eszközöket, mint a fénymásolókat, faxokat, lehetőleg úgy kell elhelyezni, hogy a nyilvánosság hozzáférését elkerüljük;
c) az ajtókat és ablakokat, ha nincs a közelben felügyelő személyzet, zárva kell tartani. Az ablakok külső védelméről is gondoskodni kell, különösen a földszinten;
d) veszélyes vagy gyúlékony anyagokat a biztonsági körlettől, informatikai eszközöktől biztos távolságban kell tárolni;
e) a tartalék berendezéseket és a mentett adatokat tartalmazó adathordozókat olyan biztonságos távolságban kell elhelyezni, amellyel elkerülhető, hogy a központi telephely katasztrófája esetén kárt szenvedjenek.

A szabályok betartását az Információ Biztonsági Felelős ellenőrzi.

8.1.4. Külső és környezeti fenyegetések elleni védelem

a) Kockázatokkal arányos fizikai védelmet kell kialakítani a tűz, árvíz, földrengés, robbanás, polgári zavargás és más természeti vagy emberi jellegű károsodás ellen.
b) megfelelő tűzoltó-berendezéseket és ezek megfelelő elhelyezését kell biztosítani.

8.1.5. Biztonsági zónában való munkavégzés

Biztonsági zónaként kell kijelölni az informatikai rendszerek működése szempontjából létfontosságú eszközök, tevékenységek helyszínét.

A biztonsági zónában el kell kerülni a felügyelet nélküli munkát egyrészt a biztonság érdekében, másrészt a rosszindulatú tevékenység lehetőségének megelőzésére.

A felügyelet nélkül hagyott biztonsági körleteket fizikailag le kell zárni és időről időre ellenőrizni.

A biztonsági helyiségekhez és az érzékeny információt feldolgozó eszközökhöz csak korlátozott hozzáférést szabad adni és azt is csak a szükséges esetben a harmadik félként munkát végző cég munkavállalóinak. Ezt a fajta hozzáférést korlátozott időpontra kell megadni és ellenőrizni.

Ezeken a területeken fénykép-, video-, audio- vagy más felvétel a Jegyző külön engedélyével készíthető.

8.1.6. A berendezések biztonsága

A hivatal működése szempontjából kritikus rendszerek csak és kizárólag a szerverszobába, illetve azzal megegyező biztonsági szinte biztosító védelmi intézkedések megvalósításával telepíthetők.

Az informatikai rendszer adat- és üzembiztonságának megfelelő szinten tartása érdekében a legmagasabb biztonsági osztályba sorolt rendszerek esetében lehetőleg redundáns megoldásokat kell alkalmazni.

Fentiek betartatását az Informatikus, ellenőrzését az Információ Biztonsági Felelős valósítja meg.

8.1.7. A berendezések elhelyezése és védelme

A berendezéseket elhelyezésénél és védelménél a környezeti fenyegetések és veszélyek kockázatának, valamint a jogosulatlan hozzáférés lehetőségének a csökkentése a cél.

A hivatal óvintézkedésekkel csökkenti a lopás, a tűz, a robbanóanyagok, a füst, a víz (vagy a vízellátás meghibásodása), a köd, a rázkódás, vegyi behatások, a villamos energiaellátás zavarai, elektromágneses sugárzás. fenyegetésekből fakadó kockázatokat.

A szerverszobába csak és kizárólag az üzemeltetéséhez feltétlenül szükséges közműhálózat csatlakozhat.

A szerverszobában csak és kizárólag olyan kellékanyagokat szabad tárolni, amelyek az üzemeltetés kockázatait nem növelik.

Az informatikai rendszer biztonságos működése számára a szerverszobában szünetmentes tápellátást, tűzjelző- és oltóberendezést kell biztosítani.

A berendezésekre vonatkozó előírásokat az Informatikus az Információ Biztonsági Felelőssel közösen határozza meg.

A berendezéseket meg kell védeni a tápáramellátás, illetve más közmű szolgáltatások meghibásodásától és más villamos rendellenességektől. Olyan villamos tápáramellátást kell alkalmazni, amelyik megfelel a berendezésgyártó specifikációjának,

A tápáramellátás folyamatosságát az alábbi megoldásokkal, illetve azok kombinációjával kell biztosítani:

a) központi megszakításmentes tápegység alkalmazása (UPS);
b) tartalék áramforrás alkalmazása;
c) a rendelkezésre állásra érzékeny eszközöknek helyi tartalék tápegység

Fentiek betartatását az Informatikus, ellenőrzését az Információ Biztonsági Felelős valósítja meg.

8.1.8. A kábelezés biztonsága

A tápáramellátás kábelezését, valamint az adattovábbító és az informatikai szolgáltatások ellátásában használt távközlő kábeleket meg kell védeni a zavaroktól és a sérülésektől.

Az információ-feldolgozó rendszerekhez csatlakozó energetikai és távközlési kábeleket, ahol lehetséges, a föld alatt kell vezetni, vagy megfelelő alternatív védelemmel kell ellátni.

A hálózati kábelezést meg kell védeni a jogosulatlan lehallgatástól vagy károsodástól, külön védőcsövek alkalmazásával, illetve a nyilvános hozzáférésű területek elkerülésével.

Fentiek betartásáért az Informatikus, az ellenőrzésért az Információ Biztonsági Felelős felel.

8.1.9. A berendezések karbantartása

A berendezéseket kezelése és karbantartása során a gyári dokumentációjukban leírtaknak megfelelően kell eljárni, biztosítva az eszközök kellő hosszúságú életciklusát és folyamatos rendelkezésre állását.

A berendezéseket a gyártó által ajánlott szervizidőszakok és specifikációk szerint kell karbantartani.

A berendezéseken a javításokat és a szerviz-tevékenységeket kizárólag az arra feljogosított, megfelelő szakértelemmel rendelkező személyzet végezheti.

Valamennyi megelőző és javító karbantartásról feljegyzést kell készíteni.(„hajónapló")

Megfelelő védelmi intézkedéseket kell életbe léptetni akkor, amikor berendezések karbantartásra házon kívülre kerülnek.

8.1.10. A berendezés házon kívüli biztonsága

A hordozható számítógépeket kézipoggyászban, és ahol lehet, utazás közben elrejtett módon kell szállítani.

A gyártók berendezés-védelmi utasításait mindenkor be kell tartani.

A mobil berendezések védelméről a vonatkozó szakaszban foglaltak szerint kell eljárni.

Minden munkatársnak az elvárható gondossággal kell eljárnia az eszközök házon kívüli szállítása és használata esetén.

8.1.11. A berendezés biztonságos újrahasznosítása vagy az azzal való biztonságos rendelkezés

Berendezések gondatlan átengedése, vagy tévedés miatt az adathordozók ismételt használatba vétele az adatok biztonságának veszélyeztetéséhez vezethet.

A védett adatokat tartalmazó tárolóeszközöket, vagy fizikailag meg kell semmisíteni, vagy biztonságosan, helyreállíthatatlanul felül kell írni (pl. többszörös felülírásos törlés) az egyszerű, szokásos törlési művelet alkalmazása helyett.

A berendezések adatot tartalmazó valamennyi részegységét (pl. a lemezegységeket) ellenőrizni kell, hogy a védett adatokat és a vásárolt szoftvereket arról eltávolították és felülírták, mielőtt mások rendelkezésére bocsátották volna.

A védett adatokat tartalmazó, de sérült tárolóeszközök tartalmának kritikussága alapján kell meghatározni, hogy az adott eszköz megsemmisítésre, vagy javításra kerüljön.

Az eljárások megvalósítása az Informatikus, ellenőrzése az IBF feladata.

8.1.12. A hivatali tulajdon szállítása

A Hivatal tulajdonát képező informatikai berendezést, adatot vagy szoftvert házon kívülre kivinni a Jegyző írásos engedélye alapján lehet (állandó vagy eseti).

Helyszíni ellenőrzéseket kell végezni annak érdekében, hogy a vagyontárgyak illetéktelen eltávolítását észre lehessen venni. A helyszíni ellenőrzések lehetőségéről mindenkit tájékoztatni kell.

Az ellenőrzést az Információ Biztonsági Felelős és az Informatikus végzi.

9. A KOMMUNIKÁCIÓ ÉS AZ ÜZEMELTETÉS MENEDZSELÉSE

9.1. Az üzemeltetési tevékenységek és felelősségek

9.1.1. Dokumentált tevékenységek

Az informatikai rendszer eszközei üzemeltetésének és rendelkezésre állásának biztosítása az Informatikus feladata.

Az informatikai rendszer váratlan események, meghibásodások, illetve a katasztrófahelyzetek elhárítását a szakszerűen és haladéktalanul meg kell kezdeni.

Az informatikai rendszer vagy valamely eleme leállásairól, meghibásodásairól feljegyzést kell készíteni.

Az informatikai rendszer biztonságos üzemeltetését, a feldolgozások biztonságát veszélyeztető eseményekről az Információ Biztonsági Felelőst haladéktalanul tájékoztatni kell.

9.1.2. Változáskezelés

Az informatikai rendszerben bármely változás csak ellenőrzött módon vezethető be.

A változtatások bevezetésének szakszerű végrehajtása az Informatikus feladata.

A változások bevezetését a Jegyző engedélyezi az IBF és az Informatikus javaslata alapján.

A változásokat az informatikai rendszerek eseményei (informatikai „hajónapló") nyilvántartásban rögzíti az informatikus és az Információ Biztonsági Felelős köteles ellenőrizni.

9.1.3. Fejlesztési, teszt és üzemeltetési eszközök szétválasztása

A fejlesztői és tesztelési tevékenységeket, amennyire csak lehetséges, szét kell választani.

9.2. Harmadik fél által nyújtott szolgáltatás menedzselése

9.2.1. Szolgáltatás nyújtása

Az információ-feldolgozó eszközök menedzselésére alkalmazott külső szerződő fél fokozott biztonsági veszélyt jelent.

A szerződéskötés előtt fel kell mérni az ebből eredő kockázatokat, és megfelelő óvintézkedéseket kell bevezetni, melyekről a szerződő felet is tájékoztatni kell. A szükséges elemeket a szerződésbe is bele kell foglalni.

A szerződést kötő munkatársnak informatikai szolgáltatásokra kötött szerződést egyeztetni kell az Információ Biztonsági Felelőssel és az Informatikussal.

9.2.2. Harmadik fél által nyújtott szolgáltatás monitorozása és felülvizsgálata

A harmadik féllel javasolt SLA szerződéseket kötni. A szolgáltatások színvonalát, jelentéseket és feljegyzéseket rendszeresen ellenőrizni, felügyelni, és évente felül kell vizsgálni. A felülvizsgálatokat a szerződés „gazdája" kezdeményezi és az Információ Biztonsági Felelőssel folytatják le.

A szolgáltatás monitorozása és felülvizsgálata legalább az alábbiakat kell, hogy tartalmazza:

a) a szolgáltatás-teljesítési színvonalának figyelemmel kísérése, a megállapodások betartásának ellenőrzése;
b) információ szolgáltatása az információbiztonsági incidensekről és szükség esetén a harmadik fél és a szervezet közötti megállapodások felülvizsgálata;
c) a szolgáltatásnyújtással kapcsolatos hibák és megszakadások nyomon követése;
d) minden azonosított probléma kezelése a megoldásig.(„hajónapló")

9.2.3. Harmadik fél által nyújtott szolgáltatás változáskezelése

A harmadik fél által végzett változásokat (pl. új alkalmazás, rendszerfejlesztés) az előre meghatározott és elfogadott követelményeknek megfelelően kell végrehajtani.

A szolgáltatás nyújtásában bekövetkező változtatásokat, illetve a szolgáltatással kapcsolatosan végbemenő változásokat kezelni kell. Szükség szerint változtatásokat kell végrehajtani, a szolgáltatással érintett rendszerek és kapcsolódó folyamatok kockázataival arányosan. A biztonsági szabályok betartásáért és betartatásáért a kapcsolattartó szervezeti egység vezetője a felelős.

9.3. A rendszer tervezése és átvétele

9.3.1. Kapacitásmenedzsment

Az Informatikus figyelemmel kíséri a változó kapacitásigényt és elkészíti a jövőre vonatkozó kapacitás bővítések terveit annak érdekében, hogy megfelelő mértékben álljon rendelkezésre feldolgozási teljesítmény és tároló hely.

Az informatikai rendszer elemeinek beszerzésekor, az Informatikusnak és az Információ Biztonsági Felelősnek előzetesen meg kell határozni a beszerezni kívánt termékre vonatkozó biztonsági követelményeket, és a beszerzésre vonatkozó döntés előtt vizsgálni kell a követelmények teljesülését.

9.3.2. A rendszer átvétele

Az új rendszerek átvételi követelményeit és kritériumait előzetesen és egyértelműen kell meghatározni, lehetőleg szerződésben rögzíteni.

Az informatikai rendszer új elemeinek, a korszerűsítések és a verziók átvétele előtt az Informatikusnak és az Információ Biztonsági Felelősnek dokumentáltan el kell végezni az előzetesen meghatározott átvételi követelményeinek teljesülésének ellenőrzését.(„hajónapló")

9.4. Védelem rosszindulatú szoftver ellen

9.4.1. A rosszindulatú kódok elleni óvintézkedések

Az informatikai rendszerben a vírus és egyéb programozott támadások megelőzése, kivédése

érdekében, a vonatkozó kockázatokkal arányos, rendszeresen frissített vírusvédelmi rendszert kell üzemeltetni.

Az Informatikus feladata szükséges frissítéseket rendszeres időközönként történő elvégzése, melyet az Információ Biztonsági Felelősnek szúrópróbaszerűen ellenőrizni kell.

A külső forrásból érkező adathordozókat, elektronikus leveleket felhasználásuk előtt vírusvédelmi szempontból ellenőrizni kell.

A fizikai adathordozó eszközök csatlakoztatását vírusvédelmi ellenőrzési eljárással kell összekötni. a kapcsolódás fizikai szintjén.

Az elektronikus levelezés rosszindulatú kódok elleni szűrését központilag végzi a hivatal.

A vírusvédelemnek - többszintű vírusvédelmi rendszer működtetetése útján - az informatikai rendszer egész területén érvényesülnie kell.

Az informatikai rendszer vírusvédelmét szervereken és munkaállomásokon működtetett vírusvédelmi rendszerek üzemeltetését az Informatikus végzi.

Az Informatikai rendszerben az adatbázisok rendszeres frissítését automatikus letöltésekkel kell biztosítani.

A vírusellenőrzést folyamatos módon szükséges megszervezni.

Az informatikai rendszer berendezésein a vírusellenőrző program felhasználó általi kikapcsolása, kikerülése tilos.

Ha a kikapcsolás rendkívüli esetben szükségessé válik, akkor ezt kizárólag az Informatikus hajthatja végre.

A vírusvédelmet a lehető legrövidebb időn belül vissza kell kapcsolni. A vírusellenőrző program ki- és visszakapcsolását dokumentálni kell.(„hajónapló")

Az informatikai rendszerben a közvetlen kárt okozó vírusfertőzés biztonsági eseménynek számít, ezért azt haladéktalanul az Információ Biztonsági Felelős felé jelenteni, majd kivizsgálni szükséges.

9.4.2. A mobil kódok elleni óvintézkedések

Mobil kódok (Java, Flash Player, makrók) az általában az internetről letölthető, és a helyi munkaállomáson - általában kifejezett telepítés nélkül - végrehajtódó állományok.

A hivatalban mobil kódok használata, futtatása csak külön engedéllyel lehetséges, melyet az Informatikus állít be. A mobil kódot futtató eszközökön biztosítani kell, hogy a biztonsági beállítások megelőzzék a rosszindulatú mobil kódok futását. Biztosítani kell azt is, hogy nem engedélyezett mobil kódot ne lehessen futtatni.

9.5. Biztonsági mentés

Az Informatikusnak a hivatal működésének biztosításához alkalmazott rendszereiről, valamint az ügyvitel szempontjából kritikus informatikai eszközökön elhelyezett adatokról rendszeres mentést kell készíteni, a naplóadatokat archiválni szükséges.

A hivatal tevékenysége ellátásához rendelkeznie kell olyan eszközzel, amely lehetővé teszi a rendszerek és adatok olyan mentési rend végrehajtásával végzett biztonsági mentését (mentések típusa, módja, visszatöltési és helyreállítási tesztek, eljárási rend), amely az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszi.

Az Informatikus a kialakított gyakorlat szerint végzi a rendszerek mentendő és archiválandó adatainak meghatározott körében a mentéseket és archiválásokat.

Az Információ Biztonsági Felelős rendszeresen (minimum évente) ellenőrzi a mentések elkészültét, valamint a visszaállítási tesztek megtörténtét.

A Hivatal eszközein tárolt személyes adatok tekintetében a munkáltató nem végez adatkezelést. Kérdéses esetben - a hivatal eszközén található adatok közül - az érintett hozzájárulásával, személyes, vagy jogi képviselő közreműködésével a Hivatal kijelölt szakértőjével közösen leválogathatja a hivatali adatokat. Együttműködés hiányában a hivatali anyagokat kigyűjtését a Hivatal kijelölt szakértőjével végezteti el.

9.6. Hálózatmenedzselés

9.6.1. A hálózati óvintézkedések

A hivatal fizikailag független, illetve virtuális hálózataiban egységes biztonsági szabályrendszert kell alkalmazni.

A LAN, WLAN, WAN hálózati forgalomban - továbbiakban: hálózati forgalom - a hálózaton továbbított adatok felfedésének kockázatával, azok minősítésének megfelelő arányos biztonsági megoldásokat kell alkalmazni.

A kommunikációs rendszereket úgy kell kialakítani, hogy biztosítsák az adatátvitel bizalmasságát, rendelkezésre állását, hitelességét és sértetlenségét.
A külvilág felől jelentkező fenyegetettség elfogadható szintre történő csökkentése érdekében a hálózati forgalom folyamatos szűrésére preventív biztonsági megoldásokat kell alkalmazni.

A hálózat elemeit, a hálózati forgalmat rendszeresen ellenőrizni kell annak érdekében, hogy a hálózati forgalom illetéktelen monitorozása felfedésre kerüljön.

Minden informatikai rendszerhez csatlakoztatott vagy attól függetlenül használt hivatali munkaállomásról pontos és aktualizált nyilvántartást kell vezetni.

Az informatikai rendszerben a felhasználók számára az informatikai erőforrások használatát hozzáférés-menedzsment útján kell szabályozni. Minden Felhasználó csak a munkaköri feladatai ellátásához szükséges erőforrásokhoz férhet hozzá.

Az Informatikus által generált és nyilvántartott hálózati felhasználói azonosító és jelszó segítségével lép be minden felhasználó a kliens oldalon. Kliensek statikus felhasználói fiókjaiba beléptetést a hálózati jelszóval kell biztosítani.

Az előzetesen engedélyezett alapfelhasználói hozzáférési jogosultságok a bejelentkezést követően válnak aktívvá.

A helyi hálózat számítógépközponton kívüli diszkrét és aktív elemeit lehetőség szerint zárható, biztonsági szempontból feltörésvédett szekrényben kell elhelyezni.

9.6.2. A hálózati szolgáltatások biztonsága

Az informatikai rendszer a külvilág felé szigorúan szabályozott módon, a kezelt adatok minősítésének megfelelő, hitelesítési és forgalom ellenőrzési eljárások betartásával, tűzfalon keresztül kapcsolódhat.

A nyilvános és a magánhálózatokon elérhető szolgáltatásokat igénybe vevő szervezeti egységeknek gondoskodniuk kell arról, hogy el legyenek látva valamennyi igénybevett szolgáltatás biztonsági jellemzőinek egyértelmű leírásával. (Célszerű a szerződésben rögzíteni.)

A szükséges biztonsági beállításokhoz az informatikus munkatársak nyújtanak segítséget.

9.7. Az adathordozók kezelése és biztonsága

9.7.1. A hordozható számítógépes adathordozók menedzselése

Az olyan eltávolítható számítógépi adathordozók védelmére, mint a CD-k, DVD-k, lemezek, usb-kulcsok, memóriakártyák, stb. megfelelő eljárásokat alakít ki a hivatal.(törlés, titkosítás)

Bármely újrahasználható adathordozó tartalmát visszaállíthatatlan módon kell törölni az informatikusnak, amennyiben arra már nincs szükség és az adathordozót a szervezeti egységtől elviszik (pl. szervízelés).

A hivatali adathordozót azonosítóval kell ellátni és ezt lehetőség szerint láthatóan, illetve digitálisan fel kell tüntetni.

Minden adathordozót biztonságosan kell tárolni az adathordozón levő adatok besorolása, valamint a gyártói előírások szerint.

Adathordozónak számítanak a következő eszközök:

a) USB kulcs
b) CD lemez
c) DVD lemez
d) Mágneses adathordozók
e) Mikrofilm
f) Notebook, laptop, (okostelefon a beállításától függően)
g) Hordozható merevlemez
h) Asztali számítógép
i) Szerver

Biztosítani kell, hogy az adathordozók kezelése a vonatkozó iratkezelési szabályok szellemében, a tartalmazott adatok szempontjából egyenértékű papír dokumentumokkal azonos módon történjék. Az adathordozók kezelése során az adathordozó által tartalmazott adatok védelmi szintjének megfelelően kell eljárni.

A hivatalban csak rendszeresített, nyilvántartott és védelemmel ellátott a pendrive-ok használhatók.

Az adathordózok szabályszerű kezelése az adathordozó felhasználója és az Informatikus feladata, amit az IBF ellenőriz.

9.7.2. Rendelkezés az adathordozók felett

Az adathordozókat, amennyiben már nincsenek rendszeres használatban, biztonságos és védett módon kell elhelyezni. Az adathordozók nem megfelelő elhelyezése védelem alatt álló adatok jogosulatlan személyekhez hozzáféréséhez vezethet.

A védett adatokat tartalmazó adathordozókat biztonságos és védett módon kell tárolni, felülírni vagy megsemmisíteni.

Amennyiben külső szervezetet végzi a papíralapú dokumentumok, valamint az informatikai berendezések és adathordozók megsemmisítését, akkor olyan szerződő felet lehet igénybe venni, aki a kellő védelmi intézkedéssel és gyakorlattal, illetve hatósági engedélyekkel is rendelkezik.

9.7.3. A szállítás alatt álló adathordozók biztonsága

Az adatok kifejezetten sérülékenyek szállítás alatt a jogtalan hozzáféréssel, a visszaéléssel, vagy a rongálódással szemben.

A számítógépes adathordozók szállítása közben az alábbi óvintézkedéseket kell szükség szerint alkalmazni:

Belső alkalmazottat, vagy megbízható szállító és futárszolgálatot kell használni.

a) A csomagolás a gyártó specifikációs előírásai szerinti kell, hogy legyen, és elegendő ahhoz, hogy megvédje a tartalmat a szállítás alatt bekövetkező bármilyen sérüléstől.
b) Szükség esetén külön óvintézkedéseket kell tenni ahhoz, hogy a védett adatokat a jogosulatlan közzétételtől és módosítástól megóvjuk az alábbi intézkedések valamelyikével, vagy kombinációjával:
    - kézi kézbesítés;
    - megbontásra érzékeny csomagolásmód (amely segítségével kimutatható minden hozzáférési kísérletet);
    - digitális aláírás és titkosító kódolás használata.

9.7.4. A rendszerdokumentáció biztonsága

A rendszerdokumentáció különböző érzékenységű információt tartalmazhat.

Annak érdekében megóvjuk a jogosulatlan hozzáféréstől:

a) a rendszerdokumentációt biztonságosan kell tárolni;
b) a rendszerdokumentációhoz minél kevesebb személy rendelkezzen hozzáféréssel.

A fenti szempontok megvalósításáért az Informatikus a felelős.

9.8. Információtovábbítás

9.8.1. Információtovábbításra vonatkozó szabályzat és eljárások

Az információ védelmének érdekében a következő irányelveket kell követni:

a) Bizalmas megbeszélések nem történhetnek nyilvános helyen, nyitott irodákban vagy vékonyfalú helyiségekben.
b) Védett adatok telefonon való közlését kerülni kell.
c) Telefonbeszélgetés során szem előtt kell tartani a lehallgatás lehetőségét.
d) Üzenetrögzítőn nem hagyhatóak védett adatot tartalmazó üzenetek.
e) Fax küldése előtt ellenőrizni kell a címzett faxszámát, valamint, ha lehetséges a készülék kijelzőjén a tárcsázni kívánt számot.
f) Fax küldését követően, amennyiben az érzékeny információt tartalmaz lehetőség szerint meg kell győződni, hogy azt tényleg a címzett kapta meg.

9.8.2. Az elektronikus üzenetek biztonsága

A hivatal fontosnak tartja munkatársai hatékony belső és külső kommunikációját, ezért munkatársai számára elektronikus levelezési lehetőséget biztosít.

Az informatikai rendszer levelezőrendszerében az üzenetek és a levelek a személyes elektronikus postaládákon keresztül érhetők el a felhasználók számára.

A hivatal az elektronikus levelek tartalmát vírusellenőrzésnek veti alá és szűri a kéretlen leveleket (SPAM).

Az Informatikusoknak címzett elektronikus levélben lehet kérni azoknak a leveleknek a beengedését, amelyeket a spamszűrő nem enged át, de a felhasználó feladatellátásához szükségesek.

Jogszabályi megalapozottság esetén a hivatal jogosult az elektronikus levelezőrendszerében továbbított üzenet, levél vagy fax tartalmát, az üzenet, levél vagy fax feladójának, vagy címzettjének kiszolgáltatása nélkül, a jogkörrel rendelkező hatóság számára - kérésre - átadni. A hivatal a hatóság kérését minden esetben bizalmasan kezeli.

Különleges és indokolt esetben a jegyző által meghatalmazott személy - az ide vonatkozó törvényi szabályozás keretein belül - jogosult az érintettel közreműködve az elektronikus levelek és faxok biztonsági szempontú ellenőrzésére azzal a céllal, hogy az elektronikus levelezés használata megfelel-e a hatályos előírásoknak.

Rendellenes események felderítése esetén köteles az eseményről a jegyző felé feljegyzést készíteni és abban intézkedési javaslatot tenni. Az elektronikus levelek és faxok ellenőrzése minden más személy számára tilos.

9.8.3. Az elektronikus irodai rendszerek biztonsága

A hivatal irodáiban elhelyezett fénymásolók és hálózati nyomtatók csak a jogosult munkavállalók számára hozzáférhetők, használhatók.

A munkavállalók felelőssége ügyelni az eszközökben másolt, továbbított, nyomtatott papír alapú dokumentumok kezelésére. Használat után minden esetben ellenőrizni kell, hogy nem maradtak-e dokumentumok az eszközökben, kiadó tálcáin, illetve környezetében.

Az őrizetlenül hagyott dokumentumokat lehetőség szerint el kell juttatni azok tulajdonosának.

A hálózati nyomatók egyedi azonosítóval biztosítják a jogosultság-alapú nyomtatást.

Az elektronikus irodai rendszerek használata, során biztonsági szempontból figyelembe kell venni az alábbiakat:

a) az irodai rendszerekben az információ sérülékenységét, például a telefonhívások és a konferenciabeszélgetés rögzítését, a hívások titkosságát, a faxüzenetek tárolását, levelek felbontását és a levelek szétosztását;
b) az érzékeny információ egyes kategóriái továbbításának kizárását, ha a rendszer nem nyújt elegendő védelmet;
c) az eszköz által tárolt információ érzékenységét.

9.9. A hivatal honlap kezelése, rendszerhasználat menedzselése

9.9.1. A hivatali honlap kezelése

A hivatal nyilvánosan hozzáférhető adatfelülete a hivatal weboldala (városi honlap is egyben), mely egyirányú információáramlást tesz lehetővé a hivatal irányából az ügyfelek/állampolgárok felé. A városi honlap kezelését a 16/2012. szabályzat alapján kell folytatni.

9.9.2. Nyilvánosan hozzáférhető tartalmak

Az 16/2012. szabályzat alapján az internet szolgáltatásokat kizárólag a munkaköri feladatok ellátásához lehet igénybe venni. Az igénybevételt a szervezeti egység vezetője ellenőrzi.

9.10. Monitorozás

A hivatal folyamatosan felügyeli a rendszereket annak érdekében, hogy az előírtak, illetve a normál működéshez képest minden eltérést észlelni és rögzíteni lehessen, hogy bizonyítékkal szolgálhassanak az esemény kivizsgálása, illetve az esetleges további eljárás során.

A rendszerfelügyelet lehetővé teszi az alkalmazott védelmi intézkedések hatékonyságának ellenőrzését is.

9.10.1. A rendszerhasználat figyelése

Az információ-feldolgozó eszközök használatát, monitorozni kell. Az egyes eszközök esetében a megkívánt ellenőrzési szintet a kockázatok elemzésével kell meghatározni.
A naplóellenőrzést indokolt esetben a konkrét cél érdekében folytatott elemzéssel kell végrehajtani.
Szükség esetén segédprogramokat vagy átvilágítási eszközöket lehet alkalmazni annak érdekében, hogy a biztonsági megfigyelés számára lényeges eseményeket azonosítani lehessen.

9.10.2. Naplóbejegyzések védelme

A biztonsághoz köthető naplóinformációkat rögzíteni kell. (Rendszernapló.)

A keletkező adatokat védeni kell az illetéktelen hozzáféréstől, hogy megelőzzük az információk utólagos módosítását, törlését. A naplóinformációk biztonsági esemény esetén később bizonyítékul szolgálhatnak, így védelmük fontos. A naplóinformációkat az információ feldolgozó eszközökön a jogosultságok megfelelő beállításával, illetve szükség esetén további titkosítási eljárásokkal kell védeni.
A naplóbejegyzéseket lehetőség szerint központilag kell gyűjteni, az elemzések megkönnyítése érdekében. A naplóbejegyzések integritását meg kell őrizni azáltal, hogy a naplófájlban szereplő adatok személy, vagy program által a későbbiekben ne legyenek módosíthatók. A rendszerek lokális óráit szinkronizálni kell, a kézzel történő átállítást meg kell akadályozni.
A naplót a létrehozásától kezdve folyamatosan karban kell tartani, valamint védeni kell az illetéktelen módosítástól és törléstől, ezért ember számára olvasható formában is kell tárolni.

A rendszernapló adatait rendszeresen archiválni kell és szükség szerint ellenőrizni.

A megfelelő óvintézkedések kialakításáért az Információ Biztonsági Felelős, a végrehajtásáért az Informatikus felel.

9.10.3. Rendszergazda és operátor naplók

Az informatikai rendszerben végrehajtott műveleteket, objektumokhoz történő hozzáférést a kockázatokkal arányosan kell naplózni mind alkalmazás, mind operációs rendszer, mind adatbázis rendszer szinten. Az alkalmazott naplózásnak és a kapcsolódó kiegészítő adminisztrációnak olyan részletesnek kell lennie, hogy abból az esemény érdemi értékelése elvégezhető, az egyértelmű személyes felelősség megállapítható legyen.

Az informatikai rendszer naplózási rendszerében biztosítani kell az informatikai rendszer legfontosabb elemeinek (eszközök, folyamatok, személyek) egyértelmű és visszakereshető azonosítását.

Gondoskodni kell olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza.

Minden naplózást lehetőség szerint úgy kell beállítani, hogy a felhasználó éles adathoz naplózási lehetőségek megkerülésével ne férhessen hozzá.

9.10.4. Hiba naplózás

Az informatikai rendszer biztonsági és egyéb meghibásodását, vagy rendellenes működését szóban vagy e-mail-en keresztül kell bejelenteni az üzemeltetőnek. Felelős: a meghibásodást vagy rendellenes működést észlelő személy.

A bejelentett hibákat a hibát fogadó személy a biztonsági naplóba köteles rögzíteni. („hajónapló")

Minden bejelentett biztonsági eseményt jelenteni kell az Informatikai Biztonsági Felelősnek.
A hiba kijavítását követően a hiba elhárításáról a hibát bejelentő személyt értesíteni kell. Felelős: az elhárítást végző, illetve külső támogató cég közreműködése esetén az azt felügyelő üzemeltető munkatárs.

9.10.5. Időszinkronizálás

Az Informatikus biztosítja a központi szerverek órajelének automatikus pontos beállítását, hogy szavatolni lehessen az esemény- és biztonsági naplók pontosságát vizsgálatkor, illetve későbbiekben bizonyítékként szolgálhatnak.

10. HOZZÁFÉRÉS-ELLENŐRZÉS

10.1. A hozzáférés-ellenőrzés követelményei

A felhasználó részére az informatikai rendszerbe belépést engedélyezni csak és kizárólag abban az esetben szabad, ha a felhasználó valamilyen módon azonosítja magát.

Az informatikai rendszer erőforrásait és felhasználóinak hozzáférési jogait egységes elvek alapján határozza meg és osztja ki a hivatal.

Az informatikai rendszer felhasználóinak hozzáférési jogait a hivatal központilag nyilvántartja.

A központi jogosultság-nyilvántartási rendszer tartalmazza a jogosultság kezeléshez kapcsolódó mindazon adatokat, amelyekből egyértelműen megállapítható, hogy kinek, milyen rendszerhez, milyen jogosultságai vannak.

A nem egyértelműen egy természetes vagy jogi személyhez kötött felhasználói azonosítók (technikai, vagy service accountok) esetén a jelszavakra a négy szem elv alkalmazását kell előírni.

Az informatikai rendszerben haladéktalanul meg kell szüntetni/fel kell függeszteni azon személyek hozzáférési jogait, akiknek jogviszonya a hivatallal megszűnt. A jogviszony megszűnését a szervezeti egység vezetője írásban jelzi az informatikusnak a jogosultság kizárása időpontjának pontos megjelölésével.

10.2. A hozzáférések felhasználói azonosítói

A felhasználó-azonosítók kiosztásakor alkalmazandó névkonvenciót, az azonosítók kiosztásának és karbantartásának a rendjét az Informatikus határozza meg.

Az informatikai rendszerben használt minden nem nevesített belső rendszerazonosítót, szerviz-azonosítót, és szállítói vagy támogatói azonosítót nyilván kell tartani az Informatikusnak. A nyilvántartások vezetéséért az Informatikus, az ellenőrzéséért az

Informatikai Biztonsági Felelős felel.

10.3. A felhasználói hozzáférés kezelése

Az informatikai rendszerben minden felhasználó csak és kizárólag munkakörének maradéktalan elvégzéséhez szükséges hozzáférési jogosultságokkal rendelkezhet, figyelembe véve az összeférhetetlenségeket.
Kivételt képezhet, ha az informatikai rendszer működtetése ezt nem teszi lehetővé, ebben az esetben a kockázatnövekedést egyéb ellenőrző intézkedésekkel kell ellensúlyozni.
Az éles rendszerben hibajavítás, fejlesztés, technológiai vagy egyéb változások miatt szükséges átmeneti jogosultságokat csak a szükséges időtartamra szabad kiadni.

A munkavégzésre irányuló jogviszony időleges vagy végleges megszűnése esetében a munkavállaló jogosultságainak visszavonását az írásban megadott megszűnési dátum figyelembevételével, az Informatikus a megszűnés napján (időpontban) hajtja végre.

10.3.1. A felhasználó nyilvántartásba vétele

Minden több felhasználós informatikai rendszerhez és szolgáltatáshoz a hozzáférési jog megadásakor a felhasználó jogosultságait nyilvántartásba kell venni.

A helyettesítést lehetőség szerint úgy kell megoldani, hogy olyan személy vegye át a feladatokat, akinek a helyettesítettel megegyező (vagy hasonló, de a munka végzéséhez elegendő) jogosultsága van az adott rendszerhez és így a saját jogán végzi a feladatokat.

A más felhasználó nevével (felhasználói fiókjával) történő munkavégzés nem megengedett.

10.3.2. Kivételek menedzselése

A kivételek, kiemelt jogosultságok kiosztását és használatát korlátozni és ellenőrizni kell. A kiváltságok kiosztását ellenőrzötten kell elvégezni.

10.3.3. A felhasználói jelszó gondozása

A jelszó a felhasználó azonosságát igazolja, hogy hozzáférhessen az informatikai rendszerhez vagy egy szolgáltatáshoz. A jelszavakat szabályos jelszógondozási folyamattal kell kísérni:

a) gondoskodni kell arról, hogy azoknál a rendszereknél, ahol a felhasználóktól megkívánják saját jelszavaik karbantartását, cseréjét, ott első alkalommal egy biztonságos ideiglenes jelszóval legyenek ellátva, de azt kényszerüljenek azonnal lecserélni. Ideiglenes jelszavakkal a jelszavukat elfelejtő felhasználókat csak akkor szabad ellátni, ha már a felhasználó azonosítása megtörtént;
b) a felhasználók, nyilatkozzanak, hogy titokban tartják személyes jelszavaikat és a csoportjelszavakat kizárólag a csoporttagokra korlátozzák;
c) a felhasználóknak az ideiglenes jelszavakat csak biztonságos környezetben szabad átadni. Az ideiglenes jelszavak használatát a szükséges minimumra kell csökkenteni. Ideiglenes jelszavakat harmadik személy bevonásával vagy elektronikus levélüzenetben továbbítani tilos. A felhasználók nyugtázzák a jelszavak átvételét. A jelszavakat nem szabad jelszót számítógépen védetlen formában tárolni.

10.3.4. A felhasználói hozzáférési jogok felülvizsgálata

Az adatokhoz és az informatikai rendszerekhez való hozzáférés hatékony ellenőrzését azzal kell fenntartani, hogy a felhasználók hozzáférési jogait az Információ Biztonsági Felelős visszatérően rendszeresen felülvizsgálja:

a) a felhasználók hozzáférési jogait rendszeresen felül kell vizsgálni általánosan - legalább évente, vagy az informatikai alkalmazásokban bekövetkező jelentős változást követően;

b) a külön kiváltsággal rendelkező hozzáférési jogokra szóló felhatalmazásokat félévente kell felülvizsgálni.

10.4. A felhasználó felelősségi köre

10.4.1. Jelszóhasználat

A jelszó eszközt jelent a felhasználó azonosságának igazolására és arra, hogy az informatikai rendszer elemeihez, illetve szolgáltatásaihoz hozzáférési jogai érvényesüljenek.

A felhasználóknak a jelszavak kiválasztásában és használatában az alábbiakban felsorolt biztonsági gyakorlatot kell követniük:

a) a jelszavakat titokban kell tartani;

b) kerülni kell a jelszavak papírra rögzítését;

c) a Hivatal saját rendszereihez tartozó jelszavakat legalább évente cserélni kell;

d) jelszót kell cserélni, ha bármi jel arra mutat, hogy a rendszer vagy a jelszó veszélyeztetve van, illetve a rendszer a cserét megköveteli;

e) olyan jelszót kell használni, amely legalább 6 karaktert hosszú és lehetőség szerint tartalmaz nagy- és kisbetűt, számot és különleges karaktert,

f) nem lehet beírni a jelszavakat automatikus bejelentkezési folyamatokba, amelyet a számítógép, makrók vagy funkcionális billentyűk tárolnak.

10.4.2. Felügyelet nélkül hagyott felhasználói berendezés

A felhasználóknak és az Informatikusnak gondoskodniuk kell arról, hogy a felügyelet nélkül hagyott berendezések kellő védelemmel rendelkezzenek. Az irodákban telepített berendezések, mint a munkaállomások, külön védelmet igényeinek a jogosulatlan hozzáféréssel szemben, amennyiben hosszabb időre felügyelet nélkül maradnak. Amennyiben ez megoldható, a védelemnek automatikusnak kell lennie. A szabályok alkalmazását az Információ Biztonsági Felelős ellenőrzi.

A felhasználók a feladata, hogy

a) az aktív folyamatokat zárják le, ha a munka befejeződött és jelentkezzenek ki, vagy zárolják a munkaállomást, mely zárolást csak jelszóval lehet feloldani;

b) amikor a munkafolyamatokat befejezték, jelentkezzenek ki (nem elegendő ilyenkor a PC vagy munkaállomás egyszerű kikapcsolása);

c) a PC-t, vagy a munkaállomást, ha nincsen használatban, a jogosulatlan használattal szemben tegyék biztonságossá úgy, hogy vagy kijelentkeznek és kikapcsolják, vagy zárolják, mely zárolást csak jelszóval lehet feloldani.

10.4.3. „Üres asztal - tiszta képernyő" szabály

A hivatal munkatársainak be kell tartaniuk az „üres asztal" szabályt, mind a papíralapú anyagokra, mind a hordozható adattárolókra, valamint a „tiszta képernyő" szabályt az információ-feldolgozó eszközökre vonatkozóan, hogy ezáltal lecsökkenjen a jogosulatlan hozzáférés, az információvesztés és információrongálás kockázata, mind a rendes munkaidőben, mind azon kívül. Ennek felügyeletéért és ellenőrzéséért a szervezeti egység vezetők a felelősek.

A munkatársak gondoskodni kötelesek arról, hogy a munkaasztalukon csak azokat a dokumentumokat és adathordozókat tartsák, amelyek az aktuális munkavégzéshez szükségesek.

A papíranyagokat és a számítógépek adathordozóit megfelelő, lehetőség szerint zárható szekrényben vagy más, hasonlóan biztonságos helyen kell tárolni, amikor éppen nincsenek használatban, különösen a munkaidőn kívüli időszakokban.

Személyi számítógépeket, munkaállomásokat nem szabad bejelentkezve hagyni, felügyelet nélkül. A képernyőkímélő alkalmazásakor a visszalépéshez jelszót kell használni.

Az informatikai rendszerben előállított vagy tárolt védett adatok nyomtatása csak személyesen felügyelt nyomtatóra történhet, és gondoskodni kell arról, hogy nyomtatás eredménye illetéktelen kezébe ne kerülhessen.

10.4.4. A hálózati szolgáltatások használatának szabályozása

Az Informatikus az informatikai rendszerben jogosultságrendszer működtetése útján gondoskodik arról, hogy az informatikai rendszerben tárolt programokhoz, adatállományokhoz, adatokhoz kizárólag ellenőrzött és dokumentált módon lehessen csak hozzáférni, és az illetéktelen hozzáférés, az adatolvasás, az adatmegsemmisítés, az adathamisítás megakadályozható legyen.

A megvalósulását az Információ Biztonsági Felelős az ellenőrzi.

Egy hálózati szolgáltatáshoz hozzáférési jogot az a munkatárs kaphat:

a) akinek munkavégzéséhez az adott szolgáltatás használata szükséges;
b) aki rendelkezik az adott szolgáltatás biztonságos használatához szükséges szakmai, és információbiztonsági ismeretekkel;
c) és biztonsági vagy egyéb okból (pl. összeférhetetlenség} nem esik korlátozás alá.

Az informatikai rendszer távolról történő eléréséhez indokolt esetben kizárólag a Jegyző adhat jogot az Információ Biztonsági Felelős és az Informatikus véleményezésével.

10.4.5. A felhasználó hitelesítése külső hozzáférés esetén

A hivatal informatikai rendszerének távolról történő elérése kizárólag VPN kapcsolattal engedélyezhető.

10.4.6. Távdiagnosztikát végző csatlakozópont védelme

Amennyiben az eszközöket, alkalmazásokat távolról menedzselhető jogosultságokat, a távdiagnosztikát végző hálózati csatlakozópontok (portok) gyári alapbeállításait tartalmazó hozzáférésekkel rendelkezik, akkor ellenőrizni kell és át kell állítani, illetve szavatolni kell az ellenőrzött hozzáférést.

10.4.7. Biztonságos bejelentkezési eljárások

Biztonságos bejelentkezési folyamattal kell lehetővé tenni a hozzáférést az informatikai szolgáltatásokhoz. Valamely számítógép-rendszerhez a belépési eljárást úgy kellkialakítani, hogy a jogosulatlan hozzáférés esélyét a minimálisra csökkentsük.
A beléptető eljárásnak a rendszerről csak a lehető legkevesebb információt szabad közreadnia, hogy elkerülhessük, hogy a jogosulatlan felhasználót segítse.

Az informatikusnak, ahol a rendszer lehetővé teszi, be kell állítania, hogy

a) a rendszer a belépés előtt a lehető legkevesebb információt szolgáltassa a technológiáról;
b) sikertelen belépés esetén a rendszer nem jelölheti meg, hogy a megadott adatok mely része hibás;

10.4.8. A felhasználó azonosítása és hitelesítése

Minden felhasználót - a műszaki személyzetet is beleértve - kizárólagos személyi használatra egyedi azonosítóval (felhasználói ID-vel) kell ellátni, hogy azt követően bármely tevékenység nyomon követhető legyen, egészen az azért felelős személyig bezárólag.
A felhasználói ID-k nem mutathatják semmi jelét a felhasználó kiváltságainak.

Az informatikai rendszerekhez való hozzáférés csak a felhasználói azonosító megadásával legyen lehetséges.

A felhasználó hitelesítésére az azonosító mellett jelszavakat kell használni. Ahol a kezelt adatok érzékenysége megkívánja, a rendszert úgy kell kialakítani, hogy az alkalmazáshoz való hozzáféréshez is a felhasználónak felhasználói névvel és jelszóval azonosítania kell magát.

A felhasználói azonosítókat az Informatikus állítja be és az azonosítókra vonatkozó biztonsági szempontok megvalósulását az Informatikai Biztonsági Felelős ellenőrzi.

10.4.9. Az alkalmazás- és információ-hozzáférés ellenőrzése

Biztonságtechnikai eszközöket úgy kell alkalmazni, hogy az alkalmazásokon belüli hozzáféréseket korlátozzák. A logikai hozzáférést a szoftverhez és az információhoz a jogosult felhasználókra kell korlátozni.

Az alkalmazások

a) ellenőrizzék a felhasználói hozzáférést az információhoz és az alkalmazás funkcióihoz;
b) nyújtsanak védelmet a jogosulatlan hozzáférés ellen valamennyi olyan operációs rendszerbeli és segédszoftver számára, amelyek képesek a rendszer vagy az alkalmazási vezérlések hatástalanítására;
c) kerüljék el más, olyan rendszerek biztonsági veszélyeztetését, amelyekkel az adott rendszer osztozik valamely informatikai erőforrás használatában;
d) legyenek képesek arra, hogy csak az arra megnevezett, felhatalmazott személyeknek vagy felhasználói csoportoknak vagy a tulajdonosnak tegyék lehetővé a hozzáférést az információhoz.

10.4.10. Az információhoz való hozzáférés korlátozása

Az alkalmazások felhasználóit, a műszaki támogató személyzetet is beleértve, a munkaköréhez tartozó jogosultságoknak megfelelően kell ellátni hozzáféréssel az informatikai infrastruktúra és az alkalmazások funkcióihoz.

Védelmi intézkedéseket kell alkalmazni a hozzáférés-korlátozás megvalósítására a felhasználók hozzáférési jogainak szabályozását, írás, olvasás, törlés tekintetében.

10.5. A mobil számítástechnika és a távmunka

10.5.1. Mobil számítástechnika és telekommunikáció

Mobil számítástechnikai eszközök (notebook, laptop,) használata esetén is gondoskodni kell az adatok biztonságáról. Tablet és mobil telefon használata során ki kell alakítani a hivatali adatok tárolásának specifikus védelmét.

Jelenleg a mobileszközöket a hivatali irodahelyiségekben használják a felhasználók. A hivatalon kívüli használat engedélyezése esetén ki kell alakítani a külső használatnak megfelelő védelmet (merevlemez-titkosítás, vírusvédelem önálló frissítése)

Mobil számítástechnikai eszközök közterületeken, konferenciatermekben és más védetlen körzetben, a hivatal saját telephelyén kívüli használatakor fokozottan figyelni kell a biztonságra, arra, hogy az adatokhoz, információkhoz más jogosulatlan személyek (a közelben levő személyek) ne férjenek hozzá.

Intézkedni kell a rajtuk tárolt adatok bizalmasságának biztosítására, az eszközök hivatali hálózathoz csatlakozásakor, különösen az védelem alatt álló adatok távoli hozzáféréssel történő elérésekor. A hálózati hozzáférés csak sikeres azonosítás és a feljogosítás után történhet meg.
A mobil számítástechnikai eszközt fizikailag is védeni kell a lopás ellen, különösen akkor, ha például gépkocsiban vagy más szállítóeszközön, hotelszobában, konferencia teremben és tanácskozó helyen hagyjuk. Berendezés, amely fontos, érzékeny és/vagy kritikus információt hordoz nem hagyható felügyelet nélkül, és ahol lehetséges azt fizikailag is el kell zárni, vagy azon a berendezés biztonsága érdekében különleges zárat kell alkalmazni.

11. INFORMÁCIÓ BIZTONSÁGI INCIDENS KEZELÉS

11.1. Az információ biztonsági események dokumentálása

Az informatikai rendszer felhasználóinak feladatuk jelezni a rendszerekben, vagy a szolgáltatásokban minden felismert, vagy feltételezett biztonsági eseményt, a rendellenestől eltérő működést, illetve sérülékenységet. Ezeket haladéktalanul jelezni kell saját vezetőiknek, az Informatikusnak, vagy az Információ Biztonsági Felelősnek.

A biztonsági eseményeket, a NEIH, CERT-Hungary riasztásait, tájékoztatásait, illetve az azokra tett intézkedéseket, a hiba eseményeket a biztonsági naplóban („hajónapló") kell rögzíteni.

A naplót havonta ellenőrzi az IBF, illetve az adott időszakra vonatkozó bejegyzéseket az Informatikus kinyomtatja.

A biztonsági esemény kivizsgálása az Információ Biztonsági Felelős feladata. A kivizsgálásba szükség esetén bevonhatja az Informatikust, illetve külső szakértőt.

Az informatikai rendszer lényeges üzemzavarát, fontos elemeinek meghibásodását rögzíteni kell.

A bejelentést fogadónak legalább a következőket kell feljegyeznie a bejelentett eseményekről: a bejelentés ideje, a bejelentő neve, az esemény rövid leírása, feltételezett oka, az elhárítás

résztvevője, az elhárítás kezdete, az elhárításához megtett intézkedés, az elhárítás vége.

11.2. A biztonsági eseményekre és incidensekre adott válasz és fejlesztés

11.2.1. Felelősségek és eljárások

A biztonsági események kezelésének felelősségeit és eljárásait úgy kell megállapítani, hogy a biztonsági eseményekre gyorsan, hatékonyan és rendben meg lehessen tenni a válaszlépéseket.

Biztonsági incidensek bekövetkezésekor a napló állományokat és hasonló bizonyítékokat össze kell gyűjteni és azokat biztonságosan meg kell őrizni.

Az ismétlődő és jelentős hatású biztonsági eseményeket elemezni, értékelni kell és ezek alapján kiegészítő és továbbfejlesztett védelmi intézkedéseket kell bevezetni, vagy a biztonsági szabályzat felülvizsgálati folyamatában, illetve a képzési tervben figyelembe venni a későbbi előfordulások gyakorisága, kára és költségei korlátozására.

Az információ biztonsági óvintézkedések kialakításakor törekedni kell arra, hogy az informatikai biztonság esetleges sérülése esetén a hivatal kellő bizonyítékkal rendelkezzen ahhoz, hogy indokolt esetben a bizonyíték támogasson egy intézkedést egy személy vagy más szervezet ellen.

Számítógép-adathordozón rögzített bizonyíték esetében a hordozható adathordozók, valamint a háttértárolón és a központi tárolón talált információ másolatait meg kell őrizni és rendelkezésre állásáról gondoskodni kell.

A másolási folyamat során valamennyi tevékenységről naplófeljegyzést kell elkészíteni és tanú jelenléte szükséges. A napló és az adathordozó egy-egy példányát biztonságosan meg kell őrizni (1 évig).

12. AZ ÜGYMENET-FOLYTONOSSÁG MENEDZSELÉSE

Az ügymenet folytonosságának menedzselése magában foglalja a kockázatokat azonosító és csökkentő, a károkozó véletlen események következményeit korlátozó, valamint a fontos működés időben történő újrafelvételét szavatoló védelmi intézkedéseket és követelményeket.

A hivatal ügymenetének, működésének folyamatos és biztonságos biztosítása érdekében megelőző intézkedéseket alkalmaz. A végrehajtásához szükséges személyi, tárgyi, anyagi erőforrások biztosítása a Jegyző feladata.

A tervek kialakítása során a hatályos információ biztonsági alapelveket és követelményeket is figyelembe kell venni, a terveket rendszeresen tesztelni kell és az esetlegesen változó követelmények tükrében felül kell vizsgálni.

13. MEGFELELŐSÉG

13.1. Megfelelés a jogi követelményeknek

13.1.1. A hatályos jog megállapítása

A hivatalra vonatkozó törvényes, szabályozói, vagy szerződéses követelményt folyamatosan figyelemmel kel kísérni és vizsgálni azok hatását az információs rendszerekre. A hatályos jog érvényesülésének követése valamennyi felhasználó feladata.

13.1.2. Adatvédelem és a személyes információ védelme

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben meghatározott védelemnek és az adatbiztonság követelményeinek érvényesülését hivatal Adatvédelmi és Adatbiztonsági Szabályzat biztosítja.

A hivatal informatikai biztonságának kialakításánál összhangot kell teremteni az adatvédelem részletes szabályait tartalmazó Adatvédelmi és Adatbiztonsági Szabályzattal.

13.2. A biztonsági szabályzat és a műszaki megfelelőség felülvizsgálata

13.2.1. Megfelelés a biztonsági szabályzatnak

A vezetők biztosítják, hogy a felelősségi körükbe tartozó valamennyi biztonsági eljárás helyes végrehajtását. A hivatalon belül Információ Biztonsági Felelősnek valamennyi területet időről időre felül kell vizsgálni annak érdekében, hogy működésük megfeleljen az Informatikai Biztonsági Szabályzatnak, valamint a többi szabályzat informatikai biztonsággal kapcsolatos részeinek.

13.2.2. A műszaki megfelelőség ellenőrzése

Az informatikai rendszert visszatérő jelleggel ellenőrizni kell a biztonság megvalósítását előíró szabványoknak való megfelelőség tekintetében. (Sérülékenység vizsgálat.)

Az Informatikus feladata az ismert sérülékenységek és az arra megjelent megoldások megvalósításának rendszeresen végrehajtása.

A felülvizsgálatnak ki kell terjednie a hivatal folyamatainak ellátásához szükséges számítógépekre, informatikai eszközökre, szoftverekre, valamint tartalék berendezésekre, és az adatátviteli hálózatra.

Bármely műszaki megfelelősség-ellenőrzést csak az illetékes, erre felhatalmazott személyek végezhetik, illetve legalább felügyelniük kell azt.

13.3. A Rendszer megfelelőségének folyamatos karbantartása

A rendszer és elemei biztonságának napi szintű fenntartása érdekében figyelemmel kell kísérni és haladéktalanul végre kell hajtani a hardverek és szoftverek a kiadott frissítéseinek adaptálását, valamint a NEIH és a CERT-Hungary riasztásainak megfelelő kezelését

13.4. Rendszer megfelelőség vizsgálata

Az ellenőrzéseket, az ellenőrzések eljárásrendjét olyan módon kell kialakítani, hogy azok biztosítsák, hogy az ellenőrzés tárgyának összes hiányosságát fel lehessen tárni, amellett, hogy a vizsgálat során a legkisebb behatás érje a vizsgálandó rendszert, így minimális esélye legyen egy véletlenszerű károkozásnak.
Az ellenőrzések fajtái:

a) Nyilvántartások pontosságának és teljességének ellenőrzése;
b) A licencnyilvántartás adatainak ellenőrzése útján;
c) Felhasználói jogosultságok ellenőrzése;
d) Naplózási rendszerrel kapcsolatos ellenőrzések;
e) Vírusvédelmi rendszer ellenőrzése;
f) Változások nyilvántartásának ellenőrzése;
g) Kézi naplók (hibanapló, eseménynapló, benntartózkodási napló) ellenőrzése;
h) A hagyományos jelszavak cseréjének ellenőrzése;
i) Beszállítók és alvállalkozók ellenőrzése.

A rendszerek vizsgálatát - biztonsági osztályba sorolását - a 2013. L. törvény alapján kell elvégezni, valamint minden jelentős, az informatikai rendszert érintő változás esetén felül kell vizsgálni.

13.5. Rendszer-vizsgálati óvintézkedések

Az éles üzemi rendszer vizsgálatának követelményeit, valamint az ellenőrzést is magában foglaló tevékenységeket meg kell tervezni és egyeztetni, hogy ezzel minimalizálni lehessen a folyamatok megszakadásának, akadályozásának kockázatát.

14. Záró rendelkezések

Jelen szabályzat 2015. május 15. napján lép hatályba. Ezzel egyidejűleg a 2007. 08.01. napján hatályba lépett Informatikai Szabályzata hatályát veszti.

Szarvas, 2015. április 30.

Készítette:

Dr. Farkas Tamás
Informatikai biztonsági felelős

Kiadja:

dr. Melis János
jegyző

3 Mellékletek

1. sz. melléklet: Információs rendszerek besorolása

s. sz.	Informatikai rendszer neve	Biztonsági Osztály	Biztonsági szint
1.	Központi informatikai rendszer	3	0
2.	TITAN gazdálkodási rendszer	3	3

3. sz. melléklet: **FELHASZNÁLÓ REGISZTRÁCIÓS LAP**

(A felhasználó szervezeti vezetője tölti ki)

Belépő felhasználó neve	
Beosztása	
Felettes	
Szervezeti egység neve	
Irodai telefonszám	
Hivatali mobilszám	

Felhasználó hozzáférés kérése (szervezeti egység vezetője tölti ki):

	Hozzáférés	(X)
1	operációs rendszer szintű azonosító kérése	
2	alkalmazás szintű azonosító kérése	
3	felhasználói csoporttagság	
4	hálózati meghajtó hozzáférés	
5	postafiók létrehozása	

.....

.....

.....

.....

.....

A belépő felhasználó szervezeti vezetőjének soron kívüli kérései:

.....

.....

.....

.....

.....

(Az informatika tölti ki)

A felhasználó operációs rendszer szintű azonosítójának aktiválása

Felhasználó-azonosító (Tartomány\felhasználó)	Aktiválás időpontja	Aktiválást végző személy olvasható aláírása

A felhasználó alkalmazás szintű azonosítójának/kulcsának aktiválása:

Felhasználói azonosító	Alkalmazás adatai Abszolút elérési út, programnév	Aktiválás időpontja	Aktiválást végző személy olvasható aláírása

Felhasználói csoporttagság, hálózati hozzáférés regisztráció

Csoport azonosító	Hálózati meghajtó elérési út, könyvtár vagy fájl név	Hozzáférési jog (Olvasás, Létrehozás, Módosítás, Törlés) vagy Módosítás)	Jogok igénylése az alkönyvtárakban is (igen/nem)	Engedélyező szervezeti vezető olvasható aláírása	Aktiválás dátum	Aktiváló aláírás

A felhasználó postafiókjának létrehozása

Postafiók	Aktiválás időpontja	Aktiválást végző személy olvasható aláírása

Az informatika egyéb észrevételei a beléptetési folyamattal kapcsolatban:

.....

.....

.....

.....

.....

.....

.....

A felhasználó tudomásul veszi, hogy:

- a rábízott adatokért és jogosultságokért, különösen azok titokbantartásáért, valamint az Informatikai Biztonsági Szabályzat betartásáért személyes felelősséget vállal,
- felhasználói-azonosítóját és jelszavát nem szolgáltathatja ki más személynek,
- A Hivatalban alkalmazott informatikai rendszerek fixen telepített, vagy mobil (okostelefon, laptop) informatikai eszközökkel történő használatakor az IBSZ szabályait kell betartania, melynek megsértéséért felelősséggel tartozik
- a felhasználó helytállási kötelezettséggel tartozik a gondatlan, vagy szándékos magatartásával okozott károkért
- a saját számítógépén és a hozzákapcsolódó rendszerekben létrehozott és kezelt állományok (beleértve az elektronikus levelezést is), a Hivatal tulajdonát képezik, ezért a Hivatal szabályzatokban és utasításokban feljogosított ellenőrző szerveinek ezekhez az állományokhoz, a vizsgálathoz szükséges mértékig betekintési joga van.

	Dátum	Aláírás
felhasználó		
szervezeti egység vezetője		
informatikus		

4. sz. melléklet: **Digitális kulcsok kezelése**

(A felhasználó szervezeti vezetője tölti ki)

Belépő felhasználó neve	
Beosztása	
Felettes	
Szervezeti egység neve	
Irodai telefonszám	
Hivatali mobilszám	

Felhasználó kulcs kezelése (szervezeti egység vezetője tölti ki):

	Hozzáférés
1	kulcs használata a(z) ..... alkalmazáshoz
2	kulcs használata a(z) ..... alkalmazáshoz
3	kulcs használata a(z) ..... alkalmazáshoz
4	kulcs használata a(z) ..... alkalmazáshoz
5	kulcs használata a(z) ..... alkalmazáshoz

Kulcskezelési adatok

Azonosító	Felhasználói kulcs	Aktiválás időpontja	Aktiválást végző aláírása	Biztonsági mentésének helye	Mentés időpontja	Mentést végző aláírása

5. sz. melléklet: **Távoli hozzáférés, VPN használata**

(A felhasználó szervezeti vezetője tölti ki)

Belépő felhasználó neve	
Beosztása	
Felettes	
Szervezeti egység neve	
Irodai telefonszám	
Hivatali mobilszám	

1.

Távoli hozzáférés VPN engedélyezése

Azonosító	Aktiválás időpontja	Aktiválást végző aláírása	Engedélyező vezető aláírása

6. sz. melléklet: Felhasználói hozzáférések megszüntetése

(A felhasználó szervezeti vezetője tölti ki)

A kilépő felhasználó neve	
Felhasználó-azonosító (username)	
Beosztása	
Szervezeti egység neve	
Szervezeti egység vezetője	
Irodai telefonszám	
Hivatali mobil telefonszám	

Felhasználó hozzáférés módosítás/megszüntetés kérése (szervezeti egység vezetője tölti ki):

	Hozzáférés	Megszüntetés(X)	Módosítás(X)
1	operációs rendszer szintű azonosító		
2	alkalmazás szintű azonosító/kulcs		
3	felhasználói csoporttagság		
4	hálózati meghajtó hozzáférés		
5	postafiók létrehozása		

A felhasználó operációs rendszer szintű azonosítójának letiltása

Felhasználó-azonosító	Letiltás időpontja	Letiltásért végző személy olvasható aláírása

A felhasználó alkalmazás szintű azonosítójának letiltása

Felhasználó-azonosító	Letiltás időpontja	Letiltásért végző személy olvasható aláírása

Távoli hozzáférés letiltása

Azonosító	Deaktiválás időpontja	Deaktiválást végző személy olvasható aláírása

Kulcskezelési adatok:

Felhasználó-azonosító kulcsok	Visszavonás időpontja:	Letiltást végző személy olvasható aláírása

Munkaállomás Adatainak mentése (amennyiben szükséges)

Munkaállomás azonosító	Mentési útvonal vagy média azonosító	Mentés időpontja	Mentés lejáratának időpontja	Mentést végző személy olvasható aláírása

A szerveren lévő felhasználói könyvtár archiválása

Felhasználói könyvtár	Mentési útvonal vagy média azonosító	Mentés időpontja	Mentés lejáratának időpontja	Mentést végző személy olvasható aláírása

A felhasználó postafiókjának mentése

Postafiók :	Mentési útvonal vagy média azonosító	Mentés időpontja	Mentés lejáratának időpontja	Mentést végző személy olvasható aláírása

Az informatikus egyéb észrevételei a kiléptetési folyamattal kapcsolatban:

.....
.....
.....
.....
.....

Dátum	
Informatikus	

7. sz. melléklet: Hálózati hozzáférési engedély (külső személy részére)

(A felhasználó szervezeti vezetője tölti ki)

A felhasználó neve	
Lakcíme	
Vállalkozás neve, címe	
Felhasználó-azonosító (username)	
Engedélyt kérő szervezeti egység	

Hálózati hozzáférés kérésének indoklása:

.....
.....
.....
.....
.....

A harmadik személyt alkalmazó vezető soron kívüli kérései az engedélyezéssel kapcsolatban:

.....
.....
.....
.....
.....

.....
Hozzáférést kérő szervezeti vezető neve

.....
Aláírása

Engedélyező rendelkezése a hozzáféréssel kapcsolatban:
Titoktartási nyilatkozat: nem szükséges szükséges, mellékelve
(A kívánt rész aláhúzandó!)
(Az informatikus tölti ki:)

A felhasználó rendszer szintű azonosítójának aktiválása

Felhasználó-azonosító (Tartomány\felhasználó)	Aktiválás időpontja	Aktiválást végző személy olvasható aláírása

A felhasználó alkalmazás szintű azonosítójának aktiválása:

Felhasználói azonosító	Alkalmazás adatai elérési út, programnév	Aktiválás időpontja	Aktiválást végző személy olvasható aláírása

Távoli hozzáférés engedélyezése

Azonosító	Aktiválás időpontja	Visszahívás száma	Engedélyező vezető aláírása	Beállítást végző személy olvasható

Felhasználói csoporttagság regisztráció

Csoport azonosító	Engedélyező szervezeti vezető olvasható aláírása

Hálózati meghajtó hozzáférés regisztráció

Hálózati meghajtó elérési út, könyvtár vagy fájl név	Hozzáférési jog (Olvasás, Létrehozás, Módosítás, Törlés)	Jogok igénylése az alkönyvtárakban is (igen/nem)

Kulcskezelési adatok

Felhasználó-azonosító kulcsok	Aktiválás időpontja	Aktiválást végző személy olvasható aláírása

Azonosító	Kulcsok biztonsági mentésének	Mentés időpontja	Mentés lejáratának időpontja	Mentését végző személy olvasható aláírása

A szerveren lévő felhasználói könyvtár adatai

Felhasználói könyvtár elérési útja	Könyvtár jogosultsági beállításai	Aktiválásért Felelős személy neve, aláírása

A felhasználó postafiókjának létrehozása

Postafiók	Aktiválás időpontja	Aktiválást végző személy olvasható aláírása

Telefon hozzáférés

Felhasználó telefonszáma/azonosítója	Aktiválásért felelős személy olvasható aláírása

Az informatikus egyéb észrevételei a visszavonási folyamattal kapcsolatban:

.....

.....

.....

.....

Dátum	
Informatikus	

8. sz. melléklet: **TITOKTARTÁSI NYILATKOZAT**

Alulírott ..... (..... alatti lakos,
sz.ig.sz.:.....),
mint a Szarvasi Polgármesteri Hivatallal üzleti kapcsolatban (szerződéses jogviszonyban) álló partner kijelentem, hogy a Szarvasi Polgármesteri Hivatal biztonsági szabályait megismerem, a Szarvasi Polgármesteri Hivatal üzleti információvédelmi követelményeit magamra nézve kötelező jelleggel elfogadom, azt betartom.

A szerződéses jogviszonyom során tudomásomra jutott információkat és adatokat üzleti titokként kezelem. Kijelentem továbbá, hogy tisztában vagyok az üzleti titok megsértésének büntetőjogi következményeivel, a tudomásomra jutott titkokat az érdekkörön kívüli személlyel nem közlöm, a titkok megőrzéséért teljes büntetőjogi felelősséggel tartozom. Ezen felelősségem fennáll azt követően is, ha szerződéses jogviszonyom bármely okból megszűnik.

Kötelezettséget vállalok arra, hogy szerződéses jogviszonyom ideje alatt, továbbá annak megszűnése után a üzleti titkait, továbbá a munkavégzés során tudomásomra jutott információt, adatot, dokumentumot nem közlöm harmadik féllel, nem hozom nyilvánosságra, nem reprodukálom, kivéve, ha a közléshez a Szarvasi Polgármesteri Hivatal, illetve az adat tulajdonosa előzetesen írásban hozzájárult.

Az adatok védelmére vonatkozó kötelezettségem megszegése esetén vállalom a büntetőjogi és polgári jogi felelősséget.

Kelt: Szarvas, 20.....

.....
nyilatkozattevő

8. sz. melléklet: **Engedély informatikai eszköz(ök) szállítására/tárolására**

…….. (felhasználó) részére engedélyezem a lentebb felsorolt és a Hivatal tulajdonát képző eszközök Szarvasi Polgármesteri Hivatal területén kívül történő szállítását/tárolását a megjelölt időpontig.

s.sz.	Az eszköz típusa	Az eszköz gyári száma	Az eszköz leltári száma	Szállítás, tárolás célja/helye	Az engedély érvényessége (visszavonásig, meghatározott időtartamig)

Szarvas, 20… év …… hó ……. nap

……
Jegyző

9. sz. melléklet: **A rendszernapló alkalmazása**

A Hivatal informatikai rendszereinek biztonságos működése érdekében elektronikus rendszernaplózást alakít ki. Az elektronikus rendszernaplózás külön Syslog szerver kialakításával valósul meg.

A Syslog szerver a következő eseményeket naplózza.

I. A helyi hálózat esetében:

1. Novell log bejegyzések;

II. A vírusvédelem esetében:

1. A vírusvédelmi szoftver által generál valamennyi log bejegyzés.

III. A határvédelmet ellátó routerek esetében:

1. WAN,
2. CALL,
3. USER,
4. VPN,
5. FIREWALL

kategóriákban generált log bejegyzéseket.

A biztonsági események dokumentálhatósága érdekében a rendszernapló rendszeresen mentésre, archiválásra kerül.

10.sz. melléklet: **Szarvasi Polgármesteri Hivatal Wifi használata**

A Hivatal biztonsági okokból korlátozza a hivatali Wifi hálózat használóinak körét.
A Wifi hálózat rejtett és a belső hálózattól elszigetelt módon kerül kialakításra és csak internet érhető el rajta.
A hozzáférés a Hivatal vezetőinek, az általuk kijelölt személyeknek (pl. vendégek) és a képviselők részére biztosított.
Minden jogosult igénylő a szervezeti egység vezetőjétől kaphatja meg a hozzáférési kódot.
A Wifit használók figyelmét fel kell hívni az internet jogkövető használatára.

A jelszavakat az Informatikus havonta változtatja és küldi meg a szervezeti egységek vezetőinek.

3.1 11. sz. melléklet: **..... helyiségben tartózkodási napló**

s.sz.	Belépő neve	szervezeti egység/ cégnév	A tartózkodás célja	Felügyelő személy	engedélyező	Belépés időpontja	Kilépés időpontja	Aláírás

12.sz. melléklet: **Informatikai eszköz(ök) átadása**

A mai napon ..... felhasználó részére az alábbi informatikai eszközök kerültek átadásra visszavételezésre.

s.sz.	Eszköz típusa	Az eszköz gyári száma	Az eszköz leltári száma	Átadás időpontja

Megjegyzés:

.....
.....
.....
.....
.....
.....
.....
.....

Kelt: Szarvas, 20.... év ..... hó ..... nap

....

átadó átvevő

13.sz. melléklet: **Informatikai eszköz(ök) visszavétele**

A mai napon .....
felhasználótól az alábbi informatikai eszközök kerültek visszavételezésre.

s.sz.	Eszköz típusa	Az eszköz gyári száma	Az eszköz leltári száma	Átadás időpontja

Megjegyzés:
.....
.....
.....
.....
.....
.....
.....
.....

Kelt: Szarvas, 20.... év ..... hó ..... nap

....
átadó átvevő