a Fejér Megyei Jegyző

2/2015. (V.1.) számú utasítása

a Fejér Megyei Önkormányzati Hivatal

Informatikai Biztonsági Szabályzatának módosításáról

(egységes szerkezetben a 2/2014. (VII.1.) számú utasítással)

Tartalom

1 Bevezető

A Hivatal különös jelentőséget tulajdonít a működését, ügymenetét közvetlenül vagy közvetve érintő adatok, információk rendelkezésre állása, hitelessége, bizalmassága és sértetlensége védelmének, az adatkezelése jogszerűségének és minőségének biztosításának, különös tekintettel, a számítástechnikai eszközökkel támogatott informatikai rendszerben keletkező, tárolt, feldolgozott, illetve a rendszerek segítségével továbbított adatokra.

1.1 Az Informatikai Biztonsági Szabályzat célja

Jelen Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) célja, hogy rögzítse az adat- és információbiztonság feltételeit, környezetét, előírja kapcsolódó más belső szabályzatok, utasítások elkészítését.

További cél, hogy a megvalósított védelem teljes körű, a kockázatokkal arányos és időben folyamatosan biztosított legyen.

1.2 Az IBSZ hatálya

Az IBSZ **területi hatálya** kiterjed az Fejér Megyei Önkormányzati Hivatal – használatában lévő - helyiségeire.

AZ IBSZ **tárgyi hatálya** kiterjed a Hivatal teljes informatikai rendszerére – függetlenül annak megvalósítási eszközeitől, módszereitől – az információ feldolgozása teljes folyamatára, életciklusára. Kiterjed továbbá a Hivatal tulajdonában lévő, illetve bérelt (használt) berendezésekre, eszközökre.

Az IBSZ **személyi hatálya** kiterjed a Hivatal valamennyi – köztisztviselőjére és munkavállalójára és azon személyekre, akik a Hivatallal munkavégzésre irányuló egyéb jogviszonyban állnak, ideértve a megbízási szerződés alapján munkát végző személyeket is (a továbbiakban: munkavállalók), továbbá mindazokra, akik a hivataltól informatikai szolgáltatásokat vesznek igénybe.

1.3 AZ IBSZ alkalmazása

Az IBSZ tartalmát az IBSZ hatálya alá tartozó személyekkel meg kell ismertetni és annak végrehajtását (betartását) az adott szakterület vezetőnek folyamatosan ellenőriznie kell. Mulasztás, visszaélés esetén a munkajogi eljárási lehetőségek, valamint a vonatkozó jogszabályok keretein belül, a vétséggel arányos mértékben kell szankcionálni. Külső személyek esetében a munkavégzést szabályozó szerződésben kell intézkedni a megfelelő garanciák beépítéséről.

Az IBSZ-t évente felül kell vizsgálni és a gyakorlati tapasztalatok, előfordult biztonsági események, a jogszabályi környezet változásai, a technikai fejlődés, az alkalmazott új informatikai eszközök, új programrendszerek, fejlesztési és védelmi eljárások miatt szükségessé vált módosításokat el kell végezni. A felülvizsgálatok tervszerű lebonyolításáról gondoskodni kell.

2 Fogalmak és meghatározások az IBSZ alkalmazásában

Adat: Az információ megjelenési formája, értelmezhető (észlelhető, érzékelhető, felfogható és megérthető) ismeret.

Adatbiztonság: Az adatokhoz történő jogosulatlan hozzáférés, az adatok módosítása és tönkretétele elleni műszaki és szervezési intézkedések, illetve eljárások együttes rendszere.

Adatfeldolgozás: Az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

Adatkezelés: Az alkalmazott eljárástól függetlenül a személyes adatok felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítását és a nyilvánosságra hozatalt), törlése, illetve az adatok megváltoztatása és a további felhasználásuk megakadályozása.

Adattovábbítás: Ha az adatot meghatározott második személy számára hozzáférhetővé teszik.

Adattörlés: Az adatok felismerhetetlenné tétele oly módon, hogy helyreállításuk nem lehetséges.

Alkalmazói rendszer: Olyan program, amelyet az alkalmazó saját speciális céljai érdekében vezet be, és amely a hardver és az operációs rendszer funkcióit használja.

Bejelentkezés: Az informatikai rendszer és egy felhasználó között – ez utóbbi által – olyan kapcsolat kezdeményezése, amelynek során számára az informatikai rendszer funkcióinak használata lehetővé válik, valamint a felhasználó személy egyértelműen azonosítható.

Belépés: Személyek belépése olyan területekre, helyiségekbe, amelyekben az informatikai rendszert, illetve egyes elemeit tárolják vagy használják.

Bizalmasság: Annak biztosítása, hogy az információhoz és adatokhoz csak azok a meghatalmazottak férhessenek hozzá, akiknek hozzáférési joguk van.

Biztonság: Az informatikai rendszer olyan stabil állapota, amelyben a Hivatal számára kielégítő mértékig fennáll a rendszer működőképessége, és teljesül az információk rendelkezésre állására, sértetlenségére, valamint bizalmasságára vonatkozó elvárás. Ez az állapot tárt, teljes körű, folytonos és a kockázatokkal arányos védelem megvalósításával jön létre.

Biztonsági esemény: Minden olyan esemény, amely a biztonságra nézve fenyegetést jelent vagy jelenthet.

Egyenszilárdság: Olyan állapot, melynek fennállása esetén a védelmi rendszer bármely pontjának áttörése ugyanannyi „munkát” (időt, pénzt, illetve egyéb erőforrást) igényel.

Felhasználó: Az a személy, aki feladatai megoldásához rendelkezik azokkal a jogosultságokkal, melyek szükségesek ahhoz, hogy egy vagy több informatikai rendszerhez hozzáférjen.

Fenyegetés: Olyan körülmény vagy esemény, amely valamely informatikai rendszerben veszélyezteti, avagy veszélyeztetheti az adat, illetve információ, rendelkezésre állását, sértetlenségét, bizalmasságát vagy hitelességét, illetve a rendszernek és a rendszer elemeinek működőképességét.

Hálózat: Két vagy több számítógép, vagy általánosabban informatikai rendszer összekapcsolása, amely a rendszer komponensei között adatcserét és adattárolást tesz lehetővé.

Hálózati férgek: Olyan programtörzs, ami az informatikai hálózaton terjed, jut el egyik informatikai rendszerből a másikba, és fejt ki kártékony hatást.

Hardver: Az informatikai rendszer fizikai elemei.

Helyreállítás: Olyan munkafolyamat, melynek eredményeként a valamely katasztrófa következtében megsérült erőforrások eredeti állapotukba kerülnek.

Hibamentes állapot: Az a tényleges állapot, amikor információk vagy adatok elérhetősége és a rendszer rendelkezésre állása, sértetlensége, hitelessége vagy bizalmassága sem átmenetileg, sem tartósan nem korlátozott.

Hitelesség: Egy információ hiteles, ha minden kétséget kizáróan megállapítható annak előállítója és az a tény, hogy az előállítás óta változatlan maradt.

Hozzáférés: Olyan eljárás, amely a felhasználó számára – jogosultsága függvényében – meghatározott célra, adott helyen és időben elérhetővé teszi az informatikai rendszer erőforrásait.

Illetéktelen személy: Olyan személy, aki az adat megismerésére nem jogosult.

Információ: Jelentést hordozó adat vagy adathalmaz, amely mennyisége vagy minősége folytán az azt befogadó személy(ek)nek új ismeret(ek)et ad, illetve bizonytalanságot szüntet meg.

Információbiztonság: Az információ bizalmasságának, hitelességének, sértetlenségének és rendelkezésre állásának fenntartása.

Információ-kezelő eszközök: Olyan automatizált eszközök, illetve berendezések, melyek az információt feldolgozzák, tárolják, továbbítják.

Informatikai biztonság: Állapot, amely olyan előírások, szabványok betartásának eredménye, amelyek az információk elérhetőségét, sértetlenségét és megbízhatóságát érintik, és amelyeket az informatikai rendszerekben vagy komponenseikben, valamint az informatikai rendszerek vagy komponenseik alkalmazása során megelőző biztonsági intézkedésekkel lehet elérni.

Informatikai rendszer: A hardverek és szoftverek olyan kombinációjából álló rendszer, amit az adat-, illetve információ-feldolgozás, különböző feladatainak teljesítésére alkalmazunk.

Jelszó: Az a személy(ek)hez kötött titkosan kezelt (azonosító) karakter sorozat, amelynek a birtokában pontosan definiált jogok gyakorlása lehetséges – az adott informatikai rendszerben.

Közérdekű adat: Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv, illetve személy kezelésében lévő, a személyes adat fogalma alá nem eső és törvényben meghatározott kivételek körébe nem tartozó adat.

Kriptográfia: Azon algoritmikus módszerekkel és adatátviteli protokollokkal foglalkozó tudomány, amelynek módszereit alkalmazva megteremthető az üzenetek, illetve a tárolt információk titkossága, védettsége, hitelessége.

Kriptográfiai protokoll: Azon adatátviteli eljárások összessége, amelyek biztosítják a rejtjelező kulcsok, valamint az átvitt rejtjelezett adatok titkosságát, integritását, hitelességét és a rejtjelező rendszerek támadásokkal szembeni ellenállását.

Különleges adat: A faji eredetre a nemzeti, nemzetiségi és etnikai hovatartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más meggyőződésre, az egészségi állapotra, a kóros szenvedélyre, a szexuális életre, valamint a büntetett előéletre vonatkozó személyes adatok.

Külső személy, szervezet: Jogi és természetes személyek azon csoportja, akik a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban állnak.

Logikai bomba: A vírus olyan része, illetve szerkezete, amely időhöz, esemény bekövetkezéséhez, logikai változó adott értékéhez kötött módon aktivizálódik.

Minősített adat: Állam-, és szolgálati titokká minősített adatok.

Működőképesség: A rendszernek és elemeinek az elvárt és igényelt üzemelési állapotban való fennmaradása.

Négy szem elve: Olyan tevékenység, amelyet csak két személy, egymást ellenőrizve végezhet.

Nyilvános rendszerek: Olyan információ-kezelő rendszerek, amelyek korlátozás nélkül, bárki számára hozzáférhetőek.

Nyilvánosságra hozatal: Ha az adatot bárki számára hozzáférhetővé teszik.

Program: eljárási leírás, amely valamely informatikai rendszer által közvetlenül, vagy átalakítást követően végrehajtható.

Rejtjelezés: Adatokon végzett olyan titkosító eljárás, melynek eredménye olyan kimenetet ad, mely az eredeti tartalmat lehetőség szerint semennyire sem tükrözi.

Rendelkezésre állás: Az a tényleges állapot, amikor is egy informatikai rendszer szolgáltatásai állandóan, illetve egy meghatározott időben a jogosult felhasználók számára igénybe vehetőek és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva.

Rendszerprogram (rendszerszoftver): Olyan alapszoftver, amelyre szükség van ahhoz, hogy valamely informatikai rendszer hardvereit használhassuk és az alkalmazói programokat működtessük. A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.

Sértetlenség: Annak az elvnek az érvényesülése, mely szerint az információkat, adatokat, illetve a programokat csak az arra jogosultak változtathatják meg, és azok véletlenül sem módosulhatnak, vagyis az információfeldolgozási folyamatok pontosságának és teljességének megvalósulása.

Személyes adat: A meghatározott természetes személlyel (továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható.

Szoftver: Az informatikai rendszer logikai eleme, amely a működtetés vezérléséhez szükséges.

Távdiagnosztikai port: Olyan távoli diagnosztikai eszköz, melyet a karbantartásért felelős szakemberek használnak az adott eszköz üzemeltetése során.

Távoli vezérlés: A távoli vezérlést biztosító modul központi vezérlést nyújt osztott környezetben.

Trójai faló: Olyan rosszindulatú programtörzs, amelyet készítője illegálisan épített be az általa készített programba, és a felhasználó szándéka ellenére és tudta nélkül hajt végre illegális feladatokat.

Tűzfal: Egy számítástechnikai eszköz, amely fizikailag és logikailag elválaszt egy hálózatot egy másiktól. Lehet forgalomszűrő a hálózati és transzport rétegben vagy alkalmazásszintű az alkalmazási rétegben.

Védelmi intézkedés: A fenyegetettség bekövetkezési valószínűségének, illetve a bekövetkezéskor jelentkező kár csökkentésére tett szervezési és/vagy technikai eszközökkel megvalósított intézkedések.

Védendő adat: Üzleti titok, valamint személyiségi jogokat érintő adatok.

Vírus: Olyan programtörzs, amely illegálisan készült egy felhasználói program részeként. A felhasznált program alkalmazása során átterjedhet, „megfertőzhet” más, az informatikai rendszerben lévő rendszer-, illetve felhasználói programot. Sokszorozva önmagát (lehet mutáns is) egy beépített feltételhez kötötten (pl. konkrét időpont, szabad lemezterület helyek száma, stb.) pusztító hatást indíthat el.

3 Biztonságpolitika

3.1 Az információbiztonsági irányelvek

A Hivatal működése, jó hírneve függ attól, hogy szolgáltatásait megbízhatóan, folyamatosan és zavartalan módon képes nyújtani. Így ezen állapot fenntartása a Hivatal alapvető érdeke.
A Hivatal információbiztonsági alapvetései:

- A Hivatal információ-kezelő eszközei, adatai rendkívül nagy értéket képviselnek. Emiatt a Hivatal e szakterület biztonsági kérdéseinek különös jelentőséget tulajdonít, azt kiemelten kezeli.
- Az információbiztonság kapcsán a Hivatal legfontosabbnak az információk funkcionalitásának, rendelkezésre állásának, bizalmasságának, integritásának, sértetlenségének, hitelességének megóvását tekinti. Ennek érdekében a Hivatal vezetői mindent megtesznek annak érdekében, hogy a kockázatokkal arányos és a törvényi előírásoknak is megfelelő védelmi intézkedésekkel és eszközökkel biztosítsák a rendszerek és adatok védelmét.
- Az információbiztonsági állapot elemzését, rendszerezett módszertanok, illetve szabványok alapján végzi és rendszeresen felülvizsgálja. (A biztonsági intézkedéseket és eljárásokat ezen elemzéseken nyugvó kockázatmenedzselésre alapozza.)
- A biztonság megteremtése érdekében tett intézkedések során fontos szempont, hogy a kockázatokat a pénzügyi erőforrások optimális felhasználása mellett csökkentse megfelelő szintre a Hivatal.

4 Elektronikus információs rendszer dokumentumai

A Hivatal biztonsági előírásait elsősorban jelen szabályzat rögzíti, de számos alacsonyabb rendű szabályozó dokumentum, és nyilvántartás tartalmaz olyan előírásokat, illetve leírásokat, melyek biztonsági szempontból kritikusak. Ezeknek a dokumentumoknak az ellenőrzését, az információ biztonsági felelős végzi. Elkészítésük, ill. a nyilvántartások vezetése az informatikus feladata.

A szabályzatban meghivatkozott eljárásrendek felülvizsgálati és ellenőrzési gyakoriságát a Hivatal 1 évben határozza meg – amennyiben ettől eltérő gyakoriság mellett dönt, a Hivatal vezetősége, az külön feltűntetésre kerül.

5 Szervezetbiztonság

5.1 Elektronikus információs rendszer biztonsági szervezete

A Hivatal vezetője, a Fejér Megye Jegyzőnek A 2013. évi L. törvény előírásainak megfelelően az elektronikus információs rendszer biztonságért felelős személyt bízott meg. A Hivatal mérete nem tette szükségessé külön szervezet kialakítását.

5.1.1 Elektronikus információs rendszer biztonságáért felelős személy

Az elektronikus információs rendszer biztonságáért felelős személy az információ biztonsági felelős.

A megbízott személy közvetlenül a Fejér Megye Jegyzőnek tartozik elszámolási kötelezettséggel, neki jelent és vele egyezteti feladatait, melyek a törvény előírásának megfelelően az alábbiak:

a) gondoskodik a Hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
b) elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
c) előkészíti a Hivatal elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
d) előkészíti a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását és a Hivatal biztonsági szintbe történő besorolását,
e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a Hivatal e tárgykört érintő szabályzatait és szerződéseit,
f) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal
g) 2013. évi L. törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet,
h) Az elektronikus információs rendszer biztonságáért felelős személy biztosítja a 2013. évi L. törvényben meghatározott követelmények teljesülését a Hivatal valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők – ha a Hivatal az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők a 2013. évi L. törvény hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.
i) Az elektronikus információs rendszer biztonságáért felelős személy feladatai és felelőssége más személyre nem átruházható.
j) Az elektronikus információs rendszer biztonságáért felelős személy jogosult a közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.

5.1.2 A Hivatal vezetője

A Hivatal vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről a következők szerint[1]:

a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
b) biztosítja a Hivatalra irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
c) az elektronikus információs rendszer biztonsági osztálya és a Hivatal biztonsági szintje alapján előírt követelményeknek megfelelően az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,
d) kiadja a Hivatal elektronikus információs rendszereire vonatkozó informatikai biztonságpolitikáját,
e) meghatározza a Hivatal elektronikus információs rendszereinek informatikai biztonsági stratégiáját,
f) meghatározza a Hivatal elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,
g) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a Hivatal munkatársai információbiztonsági ismereteinek szinten tartásáról,
h) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a Hivatal elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
i) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
j) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,
k) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
l) ha a Hivatal az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az 2013. évi. L. törvényben foglaltak szerződéses kötelemként teljesüljenek,
m) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,
n) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

Az előző pontokban meghatározott feladatokért a Hivatal vezetője a k) és l) pontjában meghatározott esetben is felelős, kivéve azokat az esetköröket, amikor jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót kell a Hivatalnak igénybe venni.

[1] a 2013. évi. törvény rendelkezéseinek megfelelően

A Hivatal vezetőjének a feladatok ellátása során a 2013. évi. L. törvény és egyéb jogszabályokban, rendeletekben meghatározott előírásokat is be kell tartania.

5.1.3 Az informatikai dolgozók

Az informatikai dolgozóknak a biztonsági előírások betartására különösen nagy hangsúlyt kell fektetniük. Legfontosabb biztonsági feladataik:

a) Részvétel a külső-, illetve belső vizsgálatok során feltárt kockázatok csökkentésében;
b) Informatikai rendszer rendelkezésre állásának biztosítása, növelése;
c) részvétel a felhasználók oktatásában;
d) rendszerdokumentációk készítése;
e) külső szakértők felügyeletének biztosítása;
f) A Hivatal biztonságát érintő eseményekről, helyzetekről tájékoztatja az információ biztonsági felelőst és a Hivatal vezetőjét.

5.2 Együttműködés külső szervezetekkel

Külső személyek számára védett információt csak a titokvédelmi jogszabályok és belső előírások betartásával lehet kiadni. Ezt az információszolgáltatást a munkához elengedhetetlenül szükséges információkra kell korlátozni.
Titoktartási nyilatkozatot minden a Hivatallal kapcsolatba kerülő olyan személlyel alá kell íratni, aki munkavégzése során védendő információk, adatok birtokába jut, vagy juthat.

5.2.1 Az információbiztonság független vizsgálata

Vizsgálni kell, hogy a Hivatalnál közzétett információbiztonsági irányelvek, információbiztonsági szabályai betartásra, illetve betarttatásra kerültek-e. A vizsgálatok egy résztét az információ biztonsági felelős végzi, de a Hivatal vezetőjének gondoskodnia kell rendszeres, független szakértői vizsgálatokról is.

5.2.2 Helyszíni tevékenységet végző külső vállalkozók

Külső személyek, szervezetek adathozzáférése a Hivatal információkezelő eszközeihez fokozott kockázatot hordoz magában. Alapszabály, hogy informatikai eszközhöz harmadik fél csak felügyelettel férhet hozzá, ettől eltérni csak a Fejér Megye Jegyző írásos engedélye alapján lehetséges.

5.2.3 A külső személyek, szervezetek által történő adathozzáférések

A kockázatok minimalizálására a Hivatal az alábbi követelményeket határozza meg:

- Harmadik féllel kötött szolgáltatási szerződéseknek tartalmaznia kell szolgáltatás szint megállapodásokat, egyéb szerződések esetén pedig a garanciális feltételeket.
- A Hivatal külső személyek, szervezetek alkalmazásakor a Hivatallal kapcsolatba hozható információk kényszerű vagy szükségszerű felfedését, illetve kiadását a lehető legszükségesebbre korlátozza.
- Külső személy – pl. karbantartás, javítás céljából – az információkezelő eszközökhöz csak úgy férhet hozzá, hogy a kezelt védett vagy minősített adatokat ne ismerhesse meg.

5.2.4 Külső személyek hozzáférésének engedélyezése, ellenőrzése

Külső hozzáféréssel a rendszerhez kizárólag érvényes szerződéssel rendelkező szervezet/vállalat dolgozói férhetnek hozzá. A hozzáférőknek titoktartási nyilatkozatot kell aláírniuk, felelősséggel tartoznak továbbá a jelszavak védelméért.

5.2.5 Információbiztonsági követelmények a külső személlyel kötött szerződésekben

Amennyiben a Hivatal és a külső személyek közötti szerződésnek információbiztonsági vonatkozása is van, akkor azt egyeztetni kell azt az információ biztonsági felelőssel.
A szerződés megkötésekor az alábbi szempontokat kell minimálisan figyelembe venni, amennyiben az adott feltétel értelmezhető az adott szerződésre nézve.
A megállapodásban/szerződésben kötelezően meg kell határozni:

- a külső személy által hozzáférhetővé védendő értékeket (hardver, szoftver, információ, adat),
- a helyszínt, ahol a megrendelt tevékenység történik,
- az adatok, információk felhasználási célját, illetve, hogy a külső a szolgáltató felelősséget vállal a megfelelő vezetői ellenőrzési és a biztonsági intézkedések végrehajtásáért,
- a külső személy által elérhető alkalmazások meghatározását, illetve a hozzáférési jogosultságokat,
- a külső személy anyagi és erkölcsi felelősségvállalását bármilyen káresetért vagy negatív következményét, amely a szerződéses előírások be nem tartásából fakad,
- a szükséges fizikai védelem szabályozásait.

6 Kockázatelemzési módszertana

A Hivatal a kockázatelemzést a NIST 800-30-as publikációja alapján végzi, illetve végezteti – a pontos módszertant a megbízott dolgozó vagy szervezet készíti el, melyet az információ biztonsági felelős hagy jóvá. A Hivatal kockázatelemzési stratégiát készít, melynek minimálisan az alábbiakat kell terjednie:

- a lehetséges kockázatok felmérésére;
- a kockázatok kezelésének felelősségére;
- a kockázatok kezelésének elvárt minőségére;
- az eljárásrendben meg kell határoznia az átfogó kockázatelemzés gyakoriságát;
- az eljárásrendben tartalmaznia kell azokat az eseményeket melyeknél kockázatelemzést kell végezni. Ezek minimálisan
    - jelentős változás áll be az elektronikus információs rendszerben vagy annak működési környezetében,
    - új fenyegetések jelennek meg,
    - olyan körülmény jön létre, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát,

Egyéb rendelkezések:

- A kockázatok elemzésének feltétele (ill. annak első lépése) a rendszerek biztonsági osztályba sorolása,
- A Hivatal vezetője felelős azért, hogy a kockázat elemzésről készített jelentést/jegyzőkönyvet az érintettek megismerjék.
- A Hivatal vezetője a jelentés szétküldését követően összehívja az informatikai vezetőt és az információ biztonsági felelőst, akikkel közösen meghatározzák a kockázatok csökkentésének módját (intézkedési tervet készítenek). A Hivatal vezetője felelősöket és a határidőket a szab meg.

7 A vagyon osztályozása és ellenőrzése

7.1 Adatok besorolása

Az elektronikus információs rendszeren tárolt adatokat besorolásuknak megfelelően védeni kell. Az adatok besorolását és az adatokhoz való hozzáférés jóváhagyását az adatgazdák végzik. Az adatgazda kinevezése a Hivatal vezetőjének jogkörébe tartozik.

7.2 Elektronikus információs rendszer osztályba sorolása

Az elektronikus rendszerek osztályba sorolását a rajta tárolt adatok besorolása alapján, illetve az általuk biztosított szolgáltatások rendelkezésre állásának fontossága alapján sorolja be a Hivatal.

A szervezet vezetője által jóváhagyott besorolás az alábbi:

ID	Megnevezés	Biztonsági osztály		
		R	S	B
1	Számítás-technikai rendszerek és hálózatok	2-es	2-es	2-es
2	Levelező rendszer	2-es	2-es	2-es
3	Elektronikus információ biztonsági rendszerek	2-es	2-es	2-es
4	Beléptető és kamera rendszer	1-es	2-es	2-es
5	Fájlszerver	2-es	2-es	2-es
6	Iktató rendszer	2-es	2-es	2-es

7.3 Szervezet biztonsági szintje

A kockázatelemzés eredménye, és a rendszerbesorolás alapján a Szervezet biztonsági szintje:2-es.

8 Emberi tényezők az információbiztonságban

A Hivatal különös figyelmet fordít munkavállalóinak kiválasztására, oktatására, ellenőrzésére, a Hivatal szervezeti struktúrájának biztonságos kialakítására, fejlesztésére.

8.1 Információbiztonsági követelmények érvényesítése a munkaköri leírásokban

Minden munkavállalónak rendelkeznie kell részletes és egyértelmű munkaköri leírással, amelyben a feladatok és felelősségek félreérthetetlenül meghatározottak.

8.1.1 Ellenőrzés belépéskor

Felvétel előtt az alábbiakat mindenképpen ellenőrizni kell

- személyazonosság,
- szakmai önéletrajz,
- véleményezett működési bizonyítvány.
- szakmai végzettséget tanúsító diplomák, oklevelek eredeti példányai,
- hatósági erkölcsi bizonyítvány – ha a Hivatal vezetője az adott pozíció esetén ezt szükségesnek tartja.

8.1.2 Titoktartási nyilatkozat

A Hivatal működése és ügyvitele során nem zárható ki, hogy alkalmazottaknak, illetve külső személyeknek védendő adatokat, információkat (pl. személyiségi jogokat érintő adatok) kell kezelnie, ezért valamennyi érintettet a védendő adat, információ minősítése érvényességi idejének megfelelő titoktartási kötelezettség terheli ezen adatok bizalmasságának megőrzését illetően. E titoktartási kötelezettség vállalása a Hivatallal történő munkaviszony, szerződéses jogviszony létesítésének és fenntartásának egyik alapvető feltétele.

8.2 Felhasználói képzés

A belépést követően a felhasználók rövid informatikai képzésen vesznek részt, mely kitér az egyes információk tárolási helyére, az incidensek bejelentésének módjára és a legfontosabb biztonsági tudnivalók ismertetésére.

Ezen túlmenően az információ biztonsági felelős köteles évente átfogó oktatást tartani a dolgozóknak a biztonság növelése érdekében. A biztonsági oktatáson való részvétel minden dolgozónak köztelező, melyet a jelenlévők aláírásukkal igazolnak.

8.3 Biztonsági események és üzemzavarok kezelése

8.3.1 Biztonsági események és a biztonsági rendszerek hiányosságainak jelentése

A Hivatal biztonságát veszélyeztető eseményeket minden munkavállalónak a felismerést követően, a lehető legrövidebb időn belül jelentenie kell felettesének vagy az információ biztonsági felelősnek.

Az informatikai rendszerben keletkező üzemzavarok kapcsán bekövetkező eseményeket az informatikus kezeli és dokumentálja.

Az informatikus feladata az informatikai rendszerekkel kapcsolatos napi problémák bejelentésének kezelése, regisztrálása, továbbítása.

A biztonsági esemény kezelése során az információ biztonsági felelős és az informatikus felelőssége, hogy a Hivatal vezetőjét tájékoztatása. A biztonsági incidenseket az „Üzletmenet folytonosság menedzsment” fejezetben megfogalmazott irányelveknek megfelelően kell kezelni.

9 Fizikai és környezeti biztonság

Az információbiztonság vonatkozásában a fizikai és környezeti biztonság az alábbi legfontosabb védelmi területeket jelenti:

- fizikai hozzáférés elleni védelem (behatolás detektálás, videó-felügyelet, beléptető rendszer),
- tűzvédelem,
- sugárzott és vezetett zavarvédelem,
- első és másodlagos villámvédelem,
- túl áram és túlfeszültség védelem,
- elektrosztatikus védelem,
- zavartalan szünetmentes áramellátás,
- légkondicionálás (hőmérséklet, páratartalom, pormentesség),
- rezgésvédelem.

A védelem differenciált módon kiterjed a szerverteremre, az információkezelő eszközökkel ellátott irodákra, kommunikációs és diszpécserközpontokra.

9.1 Biztonsági szegmensek

9.1.1 A beléptetés fizikai eszközei

A beléptetést a portaszolgálat végzi, azokat a helyiségeket melyekben bizalmas adatok találhatóak nem hagyhatóak őrizet nélkül. A Hivatal épületébe vendég csak úgynevezett vendégkártyával léphet, és közlekedhet. Minden dolgozó felelőssége az ismeretlen személyek megállítása és szükség esetén elkísérése a portaszolgálathoz, ha nem rendelkezik az illető vendégkártyával.

A Hivatalnál két biztonsági zóna került kialakításra, melyek jogosultsága külön szabályozható:

I. zóna Címerterem, előtér, Elnöki Iroda, Titkárság, Alelnöki Iroda, 4 iroda

II. zóna 8 iroda, Megyei Jegyzői Iroda, Megyei Jegyzői Tárgyaló, Megyei Jegyzői Titkárság, Aljegyzői Iroda, Tárgyaló

Megjegyzés: a Vendégkártyák nem nyitják a biztonsági zónákat leválasztó ajtókat.

A szerverszoba ajtaját mindig kulccsal kell zárni, az informatika feladata nyilvántartani azokat a személyeket, akik rendelkeznek kulccsal a szerverszobához – kulcsot a szerverszobához csak a Hivatal vezetőjének engedélyével lehet kiadni.

9.1.2 Tűzvédelem

A tűzvédelem részletes előírásait a Hivatal tűzvédelmi szabályzata tartalmazza.

9.1.3 Elektrosztatikus védelem

A szerverteremben elhelyezett nagy kiterjedésű fém eszközöket egyen potenciálra kell hozni az EMC szabványok figyelembevételével. A padlóburkolatok, berendezési tárgyak antisztatikus kivitelűeknek kell lenni.

9.1.4 Légkondicionálás (hőmérséklet, páratartalom, pormentesség)

A számítógépterem jelenleg nem klimatizált, de amennyiben a Hivatal a kialakítása mellett dönt, az alábbiakat kell figyelembe venni: a helyiségek hőmérséklete, szélsőséges külső hőmérsékleti viszonyok mellett is 18-25 °C között, páratartalma 60%±10% relatív

páratartalom között legyen. A folyamatos üzemelést monitorozással, illetve redundanciával kell biztosítani.

9.1.5 Munkavégzés a szerverszobában

A szerverszobában történő munkavégzés kifejezett engedélyhez kötött tevékenység, melyet a Hivatal vezetője engedélyezhet. Harmadik fél belépését minden esetben a belépési naplóban kell rögzíteni.

9.1.6 Energiaellátás

Az esetleges áramkimaradások okozta kiesések csökkentése, és a hálózati zavarok szűrése érdekében a szervereket szünetmentes tápegységről kell üzemeltetni, az eszközöket rendszeresen tesztelni kell és karban kell őket tartani.

9.2 Általános védelmi intézkedések

9.2.1 Nyomtatott papír alapú dokumentumok

- Minden nyomtatott, bizalmas adatot tartalmazó papír alapú dokumentumot elzártan kell tárolni, csak a legszükségesebbek lehetnek az asztalon.
- Munkaidő végén minden bizalmas adatot tartalmazó dokumentumot el kell zárni, a selejtezésre váró dokumentumokat selejtezésükig besorolásuknak megfelelően kell tárolni, majd el kell szállíttatni a selejtezés szabályinak megfelelően.
- Tilos közös használatú helyiségekben, illetve eszközökben védett adatokat tartalmazó dokumentumokat őrizetlenül hagyni.
- Védett adatokat tartalmazó dokumentumokat kizárólag megsemmisíteni lehet, újrafelhasználása (csomagolás, nyomtatás a hátoldalra, stb.) tilos. A megsemmisítés történhet helyi iratmegsemmisítő használatával, illetve központilag kezelt módon (égetés, bezúzás).

9.2.2 Képernyő-kezelési irányelvek

A számítógépek képernyőjének védelmét úgy kell beállítani, hogy ha nem történik munkavégzés, akkor automatikusan zárolja a képernyőt és a géphez történő hozzáférés lehetőségét és csak a jelszó ismételt megadásával lehessen azt újra használni. E funkciót a felhasználóknak késleltetés nélkül is aktiválni kell, ha gépüket bejelentkezve őrizetlenül hagyják. Az automatikus képernyőzár késleltetési ideje nem lehet hosszabb, mint 15 perc. A képernyőzár központi beállítása az informatikus feladata.

9.2.3 Eszközök átvétele

A személyhez rendelt informatikai eszközöket (személyi számítógépeket, notebookokat, tableteket, stb.) a felhasználónak át kell vennie, és a leltárban fel kell tűntetni, hogy melyik felhasználónak került átadásra.

9.2.4 Eszközök kivitele

A Hivatal épületéből információkezelő eszközöket kivinni csak engedélyével szabad – a mobil eszközök átvételekor, az átadás engedélynek minősül, így a megkötés azokra az esetekre vonatkozik, mikor nem mobil eszközt szeretne valaki kivinni az épületből.

Egy csoporthoz rendelt hordozható személyi számítógép a Hivatal területről történő kivitelét az adott szakterületi vezető engedélyezheti.

9.3 Eszközök karbantartása, garanciája

Az informatika felelőssége az egyes eszközök garanciális állapotának nyomon követése. Az informatikai eszközök besorolását követően az információ biztonsági felelős és a Hivatal vezetője közösen meghatározza azokat a feltételeket, melyekkel megvalósítható az elvárható biztonsági szint. Jelen szabályzat az irányelveket tartalmazza:

- 3-es vagy annál magasabb besorolást kapott informatikai rendszernek gyártói/szállítói garanciával kell rendelkeznie. A megkötés vonatkozik az aktív eszközökre is, melyek a szolgáltatás, adat elérés biztosításában részt vesznek.
- 4-es vagy annál magasabb besorolást kapott informatikai rendszerre gyártói/szállítói karbantartási és szerződést kell kötni.
- az informatika felelőssége, hogy az eszközök állapotát nyomon kövesse a legfontosabb karbantartási feladatokat elvégezze, vagy elvégeztesse, ennek megfelelően köteles kidolgozni a pontos eljárási rendet.
- A szünetmentes tápegységeket legalább évente egyszer felül kell vizsgálni/vizsgáltatni. A vizsgálattal egy időben az eszközök dokumentált karbantartását is el kell végezni.
- A légkondicionálókat legalább évente egyszer felül kell vizsgálni/vizsgáltatni. A vizsgálattal egy időben az eszközök dokumentált karbantartását is el kell végezni.

10 Konfigurációkezelés

10.1 Alap konfiguráció

Az informatika feladata összeállítani egy-egy egységes alap konfigurációt a munkaállomás-, és a szerver típusokra. Az alap konfigurációnak tartalmazni kell azokat az alkalmazásokat, melyek az eszköz használatához, illetve a munkavégzéshez szükségesek – megteremtik továbbá a biztonság elvárt szintjét (pl. vírusirtó).

Az alapkonfigurációk kialakítása és karbantartása az informatikus feladata a konfigurációk kezelését a konfigurációkezelési eljárásrend tartalmazza.

10.2 Üzemeltetési eljárások és felelősségek

10.2.1 Az üzemeltetési eljárások dokumentációja

Annak érdekében, hogy az üzemeltetett rendszerről minden szükséges és lényeges információ dokumentált formában megtalálható legyen, Üzemeltetési kézikönyveket kell készíteni.

Az informatikus feladata a dokumentumok elkészítése, illetve elkészíttetése, karbantartása és megfelelőségének ellenőrzése.

10.2.2 Konfigurációkezelés az üzemeltetés során

Az éles üzemű eszközökön végezett minden változás csak kellő körültekintéssel, és kizárólag az informatikus által végezhető.

10.2.3 A feladatkörök biztonsági szétválasztása

Az információbiztonsággal kapcsolatos szerepkörök feladatainak és felelősségeinek meghatározásakor az alábbi követelményt figyelembe kell venni:

Nem rendelkezhet egy azon személy egy területen belül végrehajtói és ellenőri jogkörrel.

10.3 Szoftverek, alkalmazások és hardver elemek, IT szolgáltatások beszerzése

Valamennyi hardver és szoftver eszköz, alkalmazás és információtechnológiai szolgáltatás beszerzése/igénybevétele csak az informatikussal egyeztetve a hivatalvezető engedélyével indítható[2].
Csak olyan beszerzés indítható, amelyek:

- Megfelelnek a specifikált követelményeknek,
- Igény szerinti terméktámogatását a gyártó vállalja,
- Illeszkedik a használt platformhoz,
- A rendszerkörnyezetbe való beillesztése nem ütközik kompatibilitási problémákba,
- Illeszkedik az egységes informatikai elképzelésekhez.

A szoftverlicence lejártával, vagy engedély nélküli szoftverek használatával a szoftverfrissítést, terméktámogatást visszautasíthatja a szolgáltató cég, valamint a szoftverek licence nélkül, vagy azzal ellentétes módon történő használatával olyan jogsértő helyzet állhat elő, mely informatikai biztonsági szempontból nem engedhető meg. Ezért a szoftverek és alkalmazások beszerzése és használata során a törvényeknek való megfelelés, valamint a folyamatos terméktámogatás céljából szigorúan be kell

[2] Jelen szabályzat nem mondja ki, hogy elegendő a informatikai vezetőnek engedélyeznie a beszerzést, de kimondja, hogy az ő jóváhagyása minden esetben szükséges.

tartani a végfelhasználói licence megállapodásokat. A szoftverek és alkalmazások jogtisztaságáért az informatikai vezető felelős. Ennek megfelelően

- Minden használatban lévő szoftver és alkalmazásnak rendelkeznie kell megfelelő számú érvényes licensszel,
- Időben korlátos licenszek lejárata után, ha még szükség van a programokra, a licence megújításáról gondoskodni kell – illetve el kell távolítani őket a rendszerről.

Az új szoftverek és alkalmazások installálását körültekintően kell megtervezni és kezelni, biztosítva, hogy a megnövekedett kockázatokat a tevékenység során az alkalmazott eljárások és biztonsági kontrollok segítségével (pl. tesztelés) kezelhetővé tegyék. (Részleteket a változáskezelési eljárásrend tartalmazza).
Az informatikai szolgáltatások igénybevételénél a szakmai követelmények összeállításáért az informatikus felel, így minden esetben be kell vonni a beszerzés folyamatába. Az informatikusszükség esetén bevonhatja a folyamatba az információ biztonsági felelőst is.
A Fejér Megye Jegyző felelőssége, hogy a beszerzési eljárásrendekbe a fenti követelmények érvényesüljenek.

10.4 A rendszer tervezése és átvétele

10.4.1 Kapacitástervezés

Az informatikai rendszer kihasználtságát, terhelését folyamatos vizsgálat alatt kell tartani. A vizsgálatok eredményeinek figyelembevételével kell tervezni a beruházásokat, szabad igénybe venni szolgáltatásokat.

10.4.2 Rendszermonitorozás folyamata

Az informatikus feladata a proaktív üzemeltetés megvalósítása. Az informatikus feladata az eszközök rendszeres ellenőrzése, mely történhet ütemezetten kézzel, vagy automatikus eszközzel.

10.4.3 A rendszer átvétele

Az átadás/átvételi eljárásnak biztosítani kell, hogy az átvevő meggyőződjön arról, hogy a fejlesztés/implementálás során teljesültek-e mind a folyamatra, mind a környezetre vonatkozó, a tervezéskor meghatározott és jóváhagyott szakmai és biztonsági követelmények.

10.4.4 Az informatikai rendszer dokumentációjának biztonsága

Az informatikai rendszerről készített minden dokumentáció bizalmasan kezelendő, harmadik félnek csak az információ biztonsági felelős jóváhagyásával adhatóak át.

10.5 Védelem a rosszindulatú programok ellen

A Hivatal információs rendszere – mint minden a külvilág számára nyitott rendszer – kitett a különböző rosszindulatú programok által okozott káreseményeknek. Megfelelő intézkedésekkel meg kell akadályozni és ki kell szűrni a számítógép-vírusok, hálózati férgek, trójai programok egyéb rosszindulatú kódok bejutását a rendszerbe.

10.6 Adathordozók védelme

10.6.1 Adathordozók szállítása

Az adathordozók szállítására vonatkozó eljárásoknak az alábbi követelményeknek kell megfelelniük:

- Épületen kívüli szállítás esetén a legrövidebb és leggyorsabb útvonalat kell választani.

- Az adatokat titkosítás nélkül csak fokozott biztonsági intézkedések mellett szabad szállítani
- Tömegközlekedési eszközön – lehetőség szerint – ne történjen az adathordozó szállítása.
- Az adathordozókat tilos őrizetlenül hagyni.
- Az adathordozókat óvni kell a fizikai sérülésektől, mechanikai behatásoktól, valamint az egyéb szennyeződésektől (nedvesség, por, csapadék, sugárzó hő, stb.).

10.6.2 Adathordozók címkézése

A mentési adathordozók esetén nyilván kell tartani, hogy milyen adat található rajtuk, és az mikori állapotot tükröz.

Optikai adathordozók esetén mindenképpen fel kell tűntetni azt is, hogy a rajta lévő adatok bizalmasak-e. Az adathordozókat a besorolásuknak megfelelő mértékben, és módon kell védeni.

10.6.3 Adathordozók megsemmisítése

Azt a javíthatatlan fizikai adathordozót, melyet akár üzem közben, vagy másolatként károsodás ért, vagy a megengedett hibahatárt elérte, selejtezni kell. Selejtezés során biztosítani kell az adatok megsemmisítését is. Bizalmas adatot tároló adathordozó Hivatalon kívüli újrahasznosítása csak az információ biztonsági felelős által jóváhagyott módszerrel történt törlést/felülírást követően hasznosítható.

10.6.4 Adathordozók használata

A Hivatal munkaállomásaihoz csak abban az esetben csatlakoztatható adathordozó, ha az a munka elvégzéséhez szükséges. Az eszközök csatlakoztatását a felettes, vagy az információ biztonsági felelős megtilthatja.

Tilos magántulajdonban lévő eszközre a Hivatal bármilyen adatát felmásolni – kivéve, ha az publikus besorolást kapott.

10.7 Információcsere

A Hivatalon belüli és a külvilággal történő adatforgalom és kommunikáció során a munkavállalók csak azokat a kommunikációs csatornákat és infrastruktúrát használhatják, amelyeket a Hivatal engedélyezett.

10.7.1 Az elektronikus levelezés biztonsága

A Hivatal támogatja, hogy a munkavállalók a kapott feladataik hatékonyabb elvégzéséhez a szükséges mértékben és módon igénybe vegyék a Hivatal elektronikus levelező rendszerét.

A levelek küldése során minden felhasználónak felelőssége az erőforrások ésszerű használata, és a Hivatal jó hírének védelme.

A Hivatal dolgozói számára a magáncélú levelezés használata korlátozott mértékben engedélyezett, de csak abban az esetben, ha ez nem jelent üzleti célú felhasználást.

10.7.2 Faxok, fénymásolok használata

A Hivatalnál elhelyezett fénymásolókat és nyomtatókat, kizárólag a hálózatban reigisztrált felhasználók használhatják. A nyomtatók / fénymásolok kizárólag munkavégzésre használhatóak. A Hivatal 3 központi nyomtatóval rendelkezik:

1. Elnöki Titkárság, Megyei Jegyzői Titkárság, Hivatali folyosó.

2. F Használat után minden esetben ellenőrizni kell, hogy maradtak-e dokumentumok az eszközök környezetében. Az őrizetlenül hagyott dokumentumokat el kell juttatni az

információ biztonsági felelősnek, aki a dokumentumok tartalmának megfelelően dönt azok további kezeléséről.

10.7.3 Nyilvánosan hozzáférhető rendszerek

A weboldal szerkesztését a Neosoft Informatikai Szolgáltató Kft. végzi (székhely: 8000 Székesfehérvár, Távírda u. 2/A.) Tartalmának feltöltését dedikált személy végzi.
A nyilvánosan elérhető rendszerek esetén általános követelmény, hogy a hozzáférést a biztonság érdekében a lehető legnagyobb mértékben korlátozni kell. Meg kell továbbá akadályozni azt, hogy esetlegesen sikeres támadás hozzáférést biztosítson a Hivatal egyéb rendszereihez.

10.7.4 Az információcsere egyéb formái

Az élőszóban és telekommunikációs eszközökön történő információközlés veszélyes pontját jelentik a mindkét fél halló-, illetve látótávolságon belül tartózkodó illetéktelen személyek.
Az információ védelmének érdekében a következő irányelveket mindenképpen követni kell:

- Bizalmas megbeszélés nem történhetnek nyilvános helyen, nyitott irodákban vagy vékony falú helyiségekben.
- Telefonbeszélgetés során kerülni kell a lehallgatás lehetőségét. Veszélyt jelenthetnek a telefon fogadó oldalán tartózkodó személyek is.
- Üzenetrögzítőn nem hagyhatóak védett adatokat tartalmazó üzenetek.

11 Jogosultságok kezelése

A Hivatal informatikai rendszerét minden munkavállaló, feladatának ellátásához szükséges mértékig, az ennek megfelelő jogosultságokkal és a szükséges időtartamig használhatja.
A Hivatal törekszik arra, hogy ahol a technikai feltételek ezt lehetővé teszik, kizárólag nevesített felhasználói fiókkal lehessen hozzáférni az informatikai rendszerhez.

11.1 Hozzáférések nyilvántartása

Napra kész nyilvántartás kell vezetni minden személyről, aki az alkalmazáshoz valamilyen hozzáférési jogosultsággal rendelkezik. Meg kell valósítani az alábbi ellenőrzési funkciókat:

- A jogosultságokat évente legalább egyszer felül kell vizsgálni.
- Szintén évente egyszer felül kell vizsgálni a szerepköröket és a hozzájuk kapcsolódó jogosultságokat, annak ellenőrzésére, hogy a megadott hozzáférési szint megfelelő a működési célra,
- Havonta felül kell vizsgálni a jogosultság-nyilvántartási rendszert és az inaktív (két hónapja be nem jelentkezett) felhasználói azonosítókat fel kell függeszteni.
- Az ellenőrzés eredményeit a Hivatal vezetője megvizsgálja és szükség esetén –a területi vezető(k) bevonásával – dönt a jogok visszavonásáról, illetve módosításáról.

11.2 Hálózathoz való hozzáférések ellenőrzése

11.2.1 Hálózati szolgáltatások használatának irányelvei

Az informatika feladata a felhasználói csoportok számára elérhető hálózati szolgáltatások meghatározása és biztosítása.
Egy hálózati szolgáltatáshoz hozzáférési jogot az az alkalmazott kaphat:

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

11.3 Bejelentkezési eljárások

A felhasználói munkaállomásokról csak biztonságos beléptetési folyamat során lehet elérni a Hivatal információkezelő eszközeit.
Az informatikai rendszerekbe való belépésnek legalább az alábbi követelményeket kell teljesítenie:

- a rendszer a belépés előtt a lehető legkevesebb információt szolgáltassa a technológiáról,
- sikertelen belépés esetén a rendszer nem jelölheti meg, hogy a megadott adatok melyike volt hibás,
- nem ad a rendszer súgó üzeneteket a bejelentkezési folyamat alatt, amelyek a jogosulatlan felhasználókat támogatná,
- limitálni kell a sikertelen belépések számát és a belépési folyamat maximális idejét.
- limitálni kell a sikertelen belépések számát és a belépési folyamat maximális számát,
- régi jelszavak egy éven belüli újrafelhasználását az operációs rendszernek meg kell akadályoznia.

11.4 Adathozzáférés korlátozása

A felhasználók hozzáférését az alkalmazói rendszerekben alkalmazási, menü, illetve objektum szintre kell korlátozni. Rendszerfunkciókat, parancsokat, melyekhez a felhasználónak a közvetlen munkájához nem szükségesek, le kell tiltani – amennyiben erre van lehetőség. Az adott alkalmazói rendszer gyártó által biztosított, ajánlott felhasználói azonosítókat le kell tiltani, a kötelező felhasználói azonosítók jelszavát meg kell változtatni.

További védelmi elem a következtetési lehetőségek kizárásának mechanizmusa (inference control). Ez a mechanizmus azt kívánja megakadályozni, hogy jogosult adatok alapján ne lehessen nem jogosult adatokra következtetni.

11.5 Hozzáférés a monitorozó rendszerhez és a rendszer használata

11.5.1 Események naplózása

A hozzáférési irányelvektől való eltéréseket figyelemmel kell kísérni, hogy az adott esetben bizonyítékként szolgáljanak a biztonsági események kivizsgálásához.

Az operációs rendszer szintjén rendelkezésre álló biztonsági ellenőrzéseket fel kell használni az információkezelő eszközökhöz való hozzáférések korlátozásánál.

11.5.2 Eseménynaplók értékelése

Az adatok összegyűjtése és kiértékelése az informatikus feladata. Ha ennek során a biztonságot érintő eseményre derül fény, akkor azt haladéktalanul tudatni kell a Hivatal vezetőjével és az információ biztonsági felelőssel, akik kivizsgálják az esetet.

Az eseménynaplók speciális hozzáférési szabályokkal rendelkeznek, törlésük és módosításuk tilos!

11.5.3 Egyéb elvégzendő feladatok

Az informatikusnak időszakosan ellenőriznie kell a rendszer normális üzemét, és ha rendellenességet tapasztal, a rendszer működését meg kell állítania.

11.6 Dátum és időbeállítás

A monitorozás elengedhetetlen kelléke a rendszerelemek órájának helyes beállítása, hogy a kiértékelésnél pontos adatok kerüljenek kivizsgálásra, ezért NTP szervert kell alkalmazni.

11.7 Eszközök hálózatra csatlakoztatása

Idegen tulajdonú hordozható számítógépek csatlakoztatása a LAN hálózatra csak a Hivatal vezetőjének írásos engedélyével történhet.

A megkötés nem vonatkozik a publikus WiFi hálózatra – mely külön alhálózatban található.

11.8 Hordozható informatikai eszközök

11.8.1 A hordozható informatikai eszközök mozgatása

A notebookokat, tableteket és egyéb hordozható berendezéseket szállító személyek:

- A szállítás során a szállító személy felel azért, hogy biztosítsa az eszköz folyamatos felügyeletét.
- Repülés vagy vonatút alatt a személyi számítógépet kézipoggyászként kell szállítani.
- Az eszközöket tilos a járműben hagyni.
- Azokban az esetekben, amikor az eszközöket nem a Hivatal tulajdonában lévő telephelyein kell hagyni, fokozott figyelmet kell fordítani a jogosulatlan hozzáférés, az adatok esetleges módosítása, megrongálása vagy ellopása elleni védelemnek.

11.8.2 Az eszköz tárolása

A berendezés gyártójának a berendezés védelmére vonatkozó útmutatásait kötelező követni.

11.8.3 Mi a teendő, ha a számítógépet ellopták

- Jelenteni a számítógép ellopásának tényét a hivatal vezetőjének, az informatikusnak és az információ biztonsági felelősnek.
- Bejelentést kell tenni a rendőrségen.
- Értesíteni kell az ingatlan üzemeltetőt, ha a számítógépet a Hivatalon kívüli ingatlanból lopták el.
- Valamennyi jegyzőkönyvet, jelentést meg kell őrizni, az információ biztonsági felelős részére át kell adni**.**

12 Rendszerfejlesztések és azok karbantartása

12.1 A rendszerek biztonsági követelményei

12.1.1 A biztonsági követelmények meghatározása és elemzése

A fejlesztési feladatokat megelőzően a Hivatal igénye szerinti követelmény-specifikáció alapján össze kell állítani a kiinduló védelmi, biztonsági követelményeket, amelyekhez:

- Meg kell határozni az alkalmazói rendszerek kritikusságát az általa támogatott folyamatok üzletmenet-folytonossági szempontból történt besorolásának megfelelően.
- Fel kell mérni, hogy hol kezelne védett adatokat, amelyhez hozzáférési jogok meghatározása szükséges.
- Fel kell mérni, hogy melyek azok a funkciók, illetve folyamatok, amelyekhez csak a megfelelős jogosultsággal rendelkező személyek férhetnek hozzá.
- Meg kell határozni, hogy hol vannak betörésre alkalmat adó pontok.
- Meg kell vizsgálni, hogy megfelelően vannak-e dokumentálva a folyamatok.
- Fel kell mérni, hogy ki van-e dolgozva a biztonsági mentés folyamata.
- Fel kell mérni, hogy gondoskodnak-e a mentési adathordozók biztonságos tárolásáról.

A biztonsági követelmények érvényesítése a tervezés során az informatikai dolgozók feladata. A tervezés során figyelembe kell venni az üzletmenet folytonossági tervek kialakítása során készített hatáselemzéseket tartalmazó tanulmányokat.

12.2 Alkalmazói rendszerek biztonsága

12.2.1 A bemenő adatok hitelességének ellenőrzése

Az alkalmazói rendszerek fejlesztésekor figyelembe kell venni, hogy a bemenő adatok hitelességének ellenőrzése az adatok keletkezési helyén kell, hogy történjen.
A bemenő adatok hitelességének biztosítása érdekében a fejlesztés során kockázatkezelés alapján kell meghatározni, hogy milyen funkciók bevezetése szükséges az adott fejlesztés során. Például

- A felhasználó személyeknek azonosíthatósága.
- A beviteli mezők adattípusonkénti specifikálhatósága (szöveges, numerikus, dátum, stb.).
- Beviteli mezők maszkolhatósága.
- Mezők közötti konzisztencia vizsgálat beállíthatósága.
- Mezők közötti konzisztencia vizsgálat beállíthatósága.
- Kötelezően kitöltendő mezők definiálhatósága.
- „Négy szem” elv érvényesíthetősége

Az információ biztonsági felelős felelőssége, hogy a fenti követelmények érvényesítésre kerüljenek a fejlesztések során.

12.2.2 Az adatfeldolgozás ellenőrzése

Az alkalmazói rendszerek fejlesztésekor, kialakításakor figyelembe kell venni azt a követelményt, hogy a rendszerben megfelelő kontrollokat alakítsanak ki a szükséges

kontrollokat a fejlesztési igény ismeretében a kockázatok elemzését követően kell meghatározni.
Az információ biztonsági felelős feladata, hogy a fenti követelmények érvényesítésre kerüljenek a fejlesztések során. A követelményeknek való megfelelést a fejlesztést indító Szervezeti egység ellenőrzi.

13 Kriptográfiai óvintézkedések

13.1 A kriptográfiai óvintézkedések használatának szabályozása

Kriptográfiai óvintézkedéseket kell alkalmazni a védett adatok elektronikus tárolásakor és átvitelekor. A kriptográfiai óvintézkedések erősségét a fenyegetettségek függvényében kell meghatározni. A kriptográfiai eszközök kiválasztásakor az alábbi szempontokat kell figyelembe venni:

- Adatátviteli rendszer esetén
    - A rendszer által kezelt védett adatok típusa
    - A rendszer által kezelt védett adatok körének nagysága
    - Átviteli közeg sávszélessége, minősége
    - Visszafejtési időkorlát
    - Felhasználói kör összetétele
    - Kulcskezelési lehetőségek
- Adattároló egységek esetén
    - A rendszer által kezelt védett adatok típusa
    - A rendszer által kezelt védett adatok körének nagysága

13.2 Titkosítás

Az adatok és információk idegen kézbe kerülésének megakadályozása érdekében titkosításokat kell alkalmazni az adatállományok, információk tárolásakor és továbbításakor.
3-as vagy magasabb besorolású adat nem továbbítható nyilvános csatornán keresztül, csak titkosított formában. A titkosításhoz AES titkosítást minimum 256 bit hosszúságú kulcsot és erős jelszót kell alkalmazni. A jelszót minden esetben más csatornán kell eljuttatni a félhez, mint amilyen csatornán a csatolmányt küldtük (email csatolmány esetén pl. sms-ben küldhető a jelszó)

13.3 Digitális aláírás

Az elektronikus adatok hitelességét biztosító digitális aláírás szükségességéről a Hivatal vezetője dönt. A megfelelő rendszer kiválasztása a beszerzési folyamatoknak megfelelően történik.

13.3.1 Kulcsmenedzsment

Azoknál az informatikai rendszereknél, amelyeknél biztonsági követelményként a vezetőség titkosítást határozott meg, a kulcsok biztonságos kezelése érdekében a rendszernek az alábbi követelményeknek kell megfelelnie:

- Minden kulcsot védeni kell a módosítás és megsemmisülés ellen, valamint a titkos és privát kulcsokat a jogosulatlan nyilvánosságra hozás ellen. A fizikai védelemnek pedig a kulcsokat előállító, tároló és archiváló eszközök védelmére kell irányulnia.
- Szimmetrikus kulcsú titkosításnál a kockázatok mértékétől függően négy-szem elvének megfelelően kell biztosítani, hogy egy személy ne rendelkezzen hozzáféréshez az adatokhoz.
- A kulcsok nyilvánosságra hozásának, ismertté válásának elkerülése érdekében minden kulcsot meghatározott időpontban aktiválni és deaktiválni kell, és használatukat egy meghatározott időtartamra kell korlátozni, ezen időtartam hosszát pedig a kriptográfiai

védelem alkalmazásának körülményeitől és a lehetséges fenyegetésektől kell függővé tenni.

- A kriptográfiai szolgáltatások külső szolgáltatóival kötött szerződéseknek és szolgáltatás szint megállapodásoknak tartalmazniuk kell a kötelezettségvállalásra, a szolgáltatás megbízhatóságára és a szolgáltatás nyújtásának reakcióidejére vonatkozó körülményeket is.

14 Üzletmenet folytonosság menedzsment

Az informatikai rendszerek megbízható működése területén meghatározó tényező az üzletmenet folytonosság biztosítása. Alapvető célja, hogy a Hivatal a folyamatait támogató informatikai erőforrásai a rendelkezésre álló időben a lehető legjobb időkihasználással és a legmagasabb funkcionalitási szinten működjenek – figyelembe véve az üzemzavari és katasztrófa események széles skáláját – annak érdekében, hogy a folyamatok zavara által okozott közvetlen és közvetett károk minimálisak legyenek.

A Hivatal jelenleg nem rendelkezik üzletmenet folytonossági szabályzattal az IBSZ a legfontosabb célokat határozza meg, melyek figyelembevételével kell kialakítani a szabályzatot.

14.1 Üzletmenet folytonosság menedzsment területei

Az üzletmenet folytonosság tervezésének célja, hogy előre meghatározott lépések végrehajtásával lehetővé tegye a Hivatal kritikus folyamatainak folyamatos vagy minimális leállással járó működését abban az esetben is, ha bármilyen nem normális működés, illetve katasztrófa helyzet fordulna elő.

Az üzletmenet folytonossági tervet az elektronikus információs rendszer vagy a működtetési környezet változásai esetén felül kell vizsgálni és aktualizálni kell. A tesztelés során felmerült problémák kezelése érdekében a terveket szintén aktualizálni kell. A változásokról értesíteni kell minden személyt, akik jogosultak a terv megismerésére.

A tervnek ki kell térnie minimálisan:

- Az alap funkciókra illetve ezek kapcsolódó vészhelyzeti követelményeket
- helyreállítási feladatokra, ill. ezek prioritására
- a helyreállítás során végzendő feladatok mellé felelősöket kell rendelni
- az adatok/rendszerek sérülése esetén végrehajtandó lépésekre

14.1.1 Üzletmenet folytonosság menedzsment

A Hivatal kríziskezelő Szervezete az alábbi szinteken valósul meg:

- Kríziskezelő Szervezet

A kríziskezelő Hivatal munkáját felügyeli, gondoskodik arról, hogy az üzletmenet folytonosságát védő folyamat összhangban legyen a Hivatal stratégiájával.

- Operatív Kríziskezelő Testület

Naprakészen tartja az üzletmenet folytonossági tervet, értékeli a krízishelyzetre utaló jelzéseket, szükség esetén elvégzi a krízishelyzet eszkalációját.

- Kríziskezelő Csoportok

Személyi összetételük és struktúrájuk a naprakész üzletmenet folytonossági tervben van meghatározva. tevékenységüket a tervben foglaltak alapján az Operatív kríziskezelő Testület felügyeletével, irányításával végzik.

14.1.2 Üzletmenet folytonosság és a hatásvizsgálat

A hatásvizsgálat célja, hogy a Hivatal folyamatainak, ill. a funkciók pontos feltérképezését követően azoknak a mennyiségi és minőségi jellemzőkkel kifejezett hatásoknak a vizsgálata, elemzése, amelyet a folyamatok más egyéb folyamatokra, üzleti komponensekre és

szereplőkre gyakorolnak. Ennek megfelelően meg kell határozni, hogy milyen hatást (pénzügyi, működési, jogi, hírnév) gyakorolna a Hivatalra az egyes folyamatok és rendszerek esetlegesen bekövetkező leállása.
E fázis eredményeként meg kell határozni:

- az egyes folyamatok prioritását,
- a kritikus feladatokat, és az ahhoz kapcsolódó folyamatokat,
- a folyamatok közötti függőségeket,
- a maximálisan megengedhető kiesés időket,
- a kritikus folyamatok és rendszerek egymásnak történő megfeleltetését.

14.1.3 Katasztrófa elhárítása

Abban az esetben, ha az elektronikus rendszer összeomlik, kompromittálódik vagy meghibásodik, gondoskodni kell az ismert állapotba történő helyreállításról és a rendszerek újraindításáról.

14.1.4 Üzletmenet folytonossági terv kidolgozása

A Hivatal számára a hatáselemzés által meghatározott folyamatokra el kell készíteni a szükséges akciótervek. A tervekben részletezésre kerülnek a folyamatokat támogató erőforrások kiesésekor alkalmazandó alternatív megoldások, az ezekre való felkészülési, illetve a visszaállításhoz szükséges lépések. Meghatározásra kerültek továbbá a szükséghelyzeti erőforrás igények, illetve az erőforrások kiesésekor értesítendő személyek, Szervezetek és az alternatív megoldás megvalósításában résztvevő személyek köre is.
A tervet a nagyobb rendszerváltozások esetén, ill. évente felül kell vizsgálni

14.1.5 A terv tesztelése

Az üzletmenet folytonossági terv tesztelése az a folyamat, amellyel a terv helyessége megvizsgálható és igazolható, hogy egy katasztrófa szituációban, a tervben specifikált körülmények biztosításával, a rögzített teendők végrehajtásával a tervben vállalt időtartamon belül helyreállítható. A tesztelés alapvető célja:

- a végrehajthatóság ellenőrzése,
- hiányosságok felderítése,
- szűk keresztmetszetek meghatározása,
- hibák feltárása,
- a terv végrehajtásának begyakorolása.

Fentiek értelmében az elkészült üzletmenet folytonossági tervet – átvételkor, majd legalább kétévente egyszer, illetve a jelentősebb változásokat követően – tesztelni kell.

15 Megfelelés a jogszabályoknak és a belső biztonsági szabályzatoknak

15.1 Megfelelés a jogi követelményeknek

Szigorúan be kell tartani és tartatni a vonatkozó jogszabályokat, belső utasításokat. A jogszabályok előírásainak betartatása a szakterület vezetők feladata és felelőssége. A Hivatalra vonatkozó jogszabályok összegyűjtése, illetve betarttatásának ellenőrzése a Hivatal vezetőjének felelőssége.

A megfelelés során elektronikus információs rendszerek szempontjából különös hangsúlyt kell fektetni az adatvédelmi törvényre és az illegális adattartalom, és szoftverek elleni intézkedésekre.

15.2 Szellemi tulajdonjogok

A törvény szerint az eredeti számítógépes program az azt létrehozó személy vagy szervezet (intézmény) szellemi tulajdona. A számítógépes programokat a szerzői jogi törvény védi, amely kimondja, hogy az ilyen művek engedély nélküli másolása, a másolat tárolása, használata jogkövetkezményekkel járhat.

15.3 Szerzői jogok

A szerzői jogról szóló törvény kimondja, hogy szerzői jogi védelem alá tartozik az irodalom, a tudomány és a művészet minden alkotása. Ebből következően a szerző hozzájárulása kell ahhoz, hogy az felhasználásra kerülhessen (hozzáférhető legyen).

15.4 Szoftver szerzői jogok

Egy adott szoftver esetében a licenc szerződés határozza meg a szerzői jog tulajdonosa által megengedett szoftver használat feltételeit. A szoftverhez adott licencszerződésre külön utalás történik a szoftver dokumentációjában, vagy a program indításakor megjelenő képernyőn is. A szoftver ára tartalmazza a szoftver licencét, és megfizetése kötelezi a vevőt, hogy a szoftver kizárólag a licencszerződésben leírtak szerint használja.

A szoftver licencszerződés, amennyiben eltérően nem rendelkezik, a vevőnek csak egyetlen „biztonsági” másolat készítését engedélyezi arra az esetre, ha az eredeti szoftver lemeze meghibásodna, vagy megsemmisülne. Az eredeti szoftver bármely további másolása jogosulatlan másolásnak minősül és megsérti a szoftvert védő és használatát szabályozó licencszerződést, valamint a szerzői jogi törvényt.

Minden Internetről letöltött anyag használata során a letöltő személynek gondosan meg kell néznie, hogy mit tartalmaz a licenc egyezmény.

A Hivatal vezetése kizárólag jogtiszta szoftver használatát engedélyezi. A szoftverkészlet nyilvántartásának folyamatos karbantartásáról az informatikus köteles gondoskodni.

15.5 A Hivatal adatainak biztonsága

15.5.1 Titokvédelem

A biztonsági követelmények érvényre juttatása érdekében biztosítani kell, hogy a Hivatal információkezelő eszközeiben kezelt adatok minden esetben besorolásra kerüljenek. Ezt követően az adatok bizalmassági besorolásuknak megfelelően, illetve a törvényben előírt módon kell védeni.

15.5.2 Személyes adatok védelme

Az Info tv. értelmében személyes adatokat kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet és az adatkezelésnek az adatkezelés során mindvégig meg kell felelnie a kitűzött célnak. Az adatkezelés csak a cél eléréséhez szükséges mértékig és ideig történhet.[3]

15.5.3 A bizonyítékok gyűjtése

A Hivatalon belül több eljárás alapján lehet információbiztonságot megszegő bizonyítékokat gyűjteni.

Az információ biztonsági felelős ellenőrizheti a védett adatok biztonságát és az adatokhoz kapcsolódó adatkezelése jogszerűségét. Ezen ellenőrzéseket nem szükséges előre jelezni a vizsgálandó szakterületnek.

15.6 Az információbiztonság irányelveinek és a műszaki követelményeknek való megfelelés

15.6.1 Az információbiztonság ellenőrzési rendje

Az információbiztonsági ellenőrzéseket az információ biztonsági felelős – szükség esetén szakértői szervezet(ek) bevonásával – végzi.

Az ellenőrzéseknek egységesnek, kellően részletesnek és teljes körűnek kell lenniük. Ki kell terjedniük valamennyi fontos és ellenőrzendő információbiztonsági eszközre, folyamatra, eljárása. Az ellenőrzés folyamata a tervezéstől a kapcsolódó intézkedésekig, illetve az utóellenőrzésekig módszertanilag támogatott kell, hogy legyen. Az információbiztonsági ellenőrzéseket egységes formában kell dokumentálni.

Az ellenőrzések az alábbiak lehetnek:

- Célvizsgálat: egy adott információbiztonsági részterület jellemzően tervezett ellenőrzése egy vagy több helyszínen, eszközön vagy folyamaton.
- átfogó vizsgálat: az információbiztonsági szakterülethez tartozó valamennyi részterület, jellemzően tervezett ellenőrzése egy vagy több helyszínen, eszközön vagy folyamaton.
- Ad hoc vizsgálat: konkrét eseményhez vagy vezetői döntéshez kötődő, jellemzően nem tervezett vizsgálat.

Az ellenőrzések folyamata:

- tervezés
- felkészülés az ellenőrzésre
- ellenőrzés
- megállapítások
- esetlege megoldási javaslatok
- az ellenőrzés eredményeinek jegyzőkönyvezése (megállapítások, javaslatok)
- utóellenőrzés

Az ellenőrzésről készült dokumentumokat a Hivatal vezetőjének kell átadni.

Az ellenőrzések során a vonatkozó szabályok cím fejezetben meghatározott jogszabályokat, szabványokat és szabályzatokat kell figyelembe venni az információkezelő eszközök felülvizsgálatánál, illetve az ellenőrzés módszertani támogatásakor.

---

[3] a törvény további előírásokat is meghatároz, melyek nem lettek átemelve jelen fejezetbe.

15.6.2 Műszaki követelményeknek való megfelelés

Az informatikai rendszereket rendszeres időközönként át kell vizsgálni. A vizsgálatoknak a műszaki (hardver, szoftver, alkalmazás) követelményeknek való megfelelésre és ezen belül a biztonságra kell irányulnia.

Felülvizsgálatnak a Hivatal folyamatainak ellátáshoz szükséges számítógépekre, informatikai eszközökre, szoftverekre, valamint a szolgáltatások folytonosságát biztosító tartalék berendezésekre, az adatátviteli hálózatra kell kitérnie.

A biztonsági vizsgálat lefolytatása során az informatika köteles támogatást adni.

A vizsgálat során feltárt műszaki hiányosságokat jegyzőkönyvbe kell venni, majd a jegyzőkönyvet el kell juttatni a Hivatal vezetőjének.

15.6.3 Rendszerek auditálási megfontolásai

Az ellenőrzéseknél kettős célt kell szem előtt tartani, melyben az első szempont az, hogy az ellenőrzés tárgyát képező rendszer/folyamat hiányosságát fel lehessen tárni. Másik szempont, hogy a vizsgálat során a legkisebb behatás érje a vizsgálandó rendszert, így minimális esélye legyen egy véletlenszerű károkozásnak.

16 Záró rendelkezések

Jelen szabályzat hatálybalépésének dátuma: 2015. május 1. . A szabályzatban foglalt azon előírásoknak, melyeknek a Hivatal a hatályba lépéskor még nem felel meg és melyek beruházásokat, fejlesztéseke igényelnek, azok megvalósítására intézkedési tervet kell készíteni. Ezen Intézkedési terv végrehajtásának eredményeképpen a szabályzat előírásait a 2013. évi L törvény előírásaival összhangban el kell végezni.
Jelen szabályzat rendelkezéseit szükség esetén, de legalább évente felül kell vizsgálni és a szükséges módosításokat el kell végezni. E karbantartás az információ biztonsági felelős felelőssége.

A szabályzat betartatásáért valamennyi szakterület-vezető felelős.
A szabályzatban nem érintett kérdésekben a hatályos jogszabályok szerint kell eljárni.

Kelt:Székesfehérvár, 2015. április 30..

Dr. Kovács Zoltán
megyei jegyző