Szabadszállási
Polgármesteri
Hivatal

Informatikai Biztonságpolitika

Storchné Somogyi Eszter

Jegyző

2015.07.01.

Tartalomjegyzék

I. Az Informatikai Biztonságpolitika

Az Informatikai Biztonságpolitika (továbbiakban: IBP) célja, hogy a Szabadszállási Polgármesteri Hivatal (továbbiakban: Hivatal) elektronikus információs rendszereiben kezelt adatok védelme az Európai Unió és Magyarország hatályos jogszabályaival, az informatikai biztonságra vonatkozó nemzetközi és hazai szabványokkal, ajánlásokkal és a Hivatal belső rendelkezéseivel összhangban legyen.

A Hivatal informatikai biztonsága a bizalmasság, sértetlenség és rendelkezésre állás szempontjából úgy kerüljön kialakításra, hogy a védelem az elektronikus információs rendszerre és környezetére nézve teljes körű, zárt szabályozási ciklusú és a kockázatokkal arányos legyen, és a megvalósított védelmi képességek az elektronikus információs rendszer teljes életciklusában folytonosan működjenek. A Hivatal célja, hogy a megvalósított védelemmel biztosítsa a megbízhatóság és az adatbiztonság elvárásait.

II. Az elektronikus információs rendszerek biztonságához kapcsolódó fogalmak

Az elektronikus információs rendszerek biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

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

Folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem.

Informatikai biztonsági irányítási rendszer (IBIR): Az IBIR egy általános irányítási rendszer, amely az üzleti kockázat elemzésen alapul, megállapítja, megvalósítja, üzemelteti, ellenőrzi, karbantartja és javítja az informatikai biztonságot. Az irányítási rendszer magában foglalja a szervezetet, a struktúrát, a szabályzatokat, a tervezési

tevékenységeket, a felelősségeket, a gyakorlatokat, az eljárásokat, a folyamatokat és az erőforrásokat.

Kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.

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

Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

Teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem.

Vagyonleltár: A Hivatal elektronikus információbiztonságának kialakításához nélkülözhetetlen egy információbiztonsági vagyonleltár, mely a következő csoportosítás szerint tartalmazza a Hivatal eszközeit:

a) **Információ-vagyon:** az adatok, adatbázisok, szoftver-kezelési kézikönyvek, oktatási, üzemviteli, üzemeltetési, biztonsági segédletek és nyilvántartások.

b) **Szoftver-vagyon:** rendszerszoftverek, alkalmazói szoftverek, fejlesztő-eszközök és szolgáltatások.

c) **Fizikai-vagyon:** hardver (számítógépek, perifériák, mobil számítástechnikai eszközök), kommunikációs eszközök (telefonok, faxok, modemek, hálózati csatoló eszközök, telefonalközpontok), adathordozók és egyéb műszaki berendezések (szünetmentes tápegység, légkondicionáló berendezés, villámhárító, stb.).

Zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.

III. IBP hatálya

1. Szervezeti-személyi hatály

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

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

a) a polgármesterre, az alpolgármesterre,

b) a választott képviselőkre,

c) a külsős bizottsági tagokra,

d) a közszolgálati tisztviselői jogviszony alapján foglalkoztatott köztisztviselőkre,

e) a munkaviszony alapján foglalkoztatott munkatársakra,

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

g) más szervezetek képviseletében a Hivatal munkahelyein tartózkodó személyekre.

2. Tárgyi hatály

Az IBP tárgyi hatálya kiterjed a Hivatal adataival és adatainak kezelésével összefüggésben használt bármilyen adatrögzítésre, tárolásra, feldolgozásra vagy továbbításra képes infokommunikációs eszközre és ezek működési környezetére.

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

3. Időbeli hatály

Jelen IBP a kiadás napján lép hatályba.

IV. Az IBP felülvizsgálata

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

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

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

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

V. Megfelelés a jogszabályoknak

A Hivatal célul tűzi ki a teljekörű megfelelést a mindenkori jogszabályi követelményeknek mind az elektronikus informatikai biztonság, mind az adatvédelem területén.

Ennek érdekében a Hivatal informatikai biztonsági céljainak megvalósítása során

a) az állami és önkormányzati szervek elektronikus informatikai biztonságáról szóló 2013. évi L. törvény,

b) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény,

c) valamint a MSZ ISO/IEC 27001:2006 szabvány Közigazgatási Informatikai Bizottság 25. és 28. számú ajánlásait veszi alapul.

VI. Vezetőségi szándéknyilatkozat

A Hivatal vezetése jelen IBP kiadásával elkötelezi magát a Hivatal informatikai biztonságának megteremtésére és fenntartására, illetve támogatja az informatikai biztonságot érintő kockázatarányos intézkedéseket.

A Hivatal vezetése tudatosan törekszik az informatikai biztonság szintjének folyamatos szinten tartására, az adatvédelem bővülő elvárásainak és a változó szabályozásoknak való megfelelésre és a mind újabb technikai kihívások gyors kezelésére, ezért rendszeresen felülvizsgálja, korszerűsíti informatikai biztonsági irányítási rendszerét.

VII. Az Informatikai Biztonsági szabályozó rendszer

Az informatikai biztonsági szabályozó rendszer három szintre tagolódik:

Stratégiai szint

Legfelső szint, a Hivatal jegyzőjének akaratnyilvánítása.

- kiadja: Jegyző
- felülvizsgálat: szükség szerint, de legalább évente
- dokumentumok: Informatikai Biztonsági Politika, Informatikai Biztonsági Stratégia

Szabályozási szint

A politikában megfogalmazott elvek leképezésére, a követelmények meghatározására szolgáló szabályzatok.

- kiadja: Jegyző
- felülvizsgálat: szükség szerint, de legalább évente
- dokumentumok: Informatikai Biztonsági Szabályzat, Felhasználói Informatikai Biztonsági Házirend

Eljárásrendek

A szabályzatokban meghatározott követelményeket az adott területen eljárásrendekben kell részletesen kidolgozni.

- kiadja: a folyamatért felelős vezető
- felülvizsgálat: szükség szerint, de legalább évente
- dokumentumok: technológiai vhr által előírt eljárásrendek.

VIII. A Hivatalban kezelt adatok érzékenysége

A Hivatal a feladatellátás módjától függően az elektronikus információs rendszereiben többféle típusú és érzékenységű adatot kezel:

Alaptevékenység ellátása érdekében kezelt adatok

A Hivatal a rá vonatkozó jogszabályok alapján alaptevékenysége ellátása érdekében a következő adatfajtákat kezeli:

- belső döntés-előkészítő adatok, tervezetek (nem nyilvános),
- személyes adatok.

Alaptevékenység támogató folyamatai által kezelt adatok

A Hivatal funkcionális tevékenysége során a következő adatfajtákat kezeli:

- köztisztviselők személyes adatai,
- pénzügyi-számviteli adatok,
- elektronikus információs rendszerek dokumentációi.

Különös védelmet igénylő adatok

A fenti adatfajták közül informatikai biztonsági szempontból különösen védendőek

a) személyes adatok.

IX. Informatikai biztonsági alapelvek

Az informatikai biztonsági környezetet a hatályos jogszabályok vonatkozó követelményeinek maximális figyelembevételével szükséges kialakítani.

Az informatikai biztonsági intézkedéseket az informatikai biztonsági kockázatok rendszeres felülvizsgálatával kell alátámasztani.

Az informatikai biztonsági intézkedéseket, a Hivatal adatait és elektronikus információs rendszereit veszélyeztető kockázati tényezőkre megfelelő, kockázatarányos ellenintézkedéseket a rendszer minden elemére, és azok életciklusának - fejlesztés, bevezetés, üzemeltetés, kivezetés - teljes tartalmában, teljes körűen érvényre kell juttatni.

Az informatikai biztonságot a szabályozás, eszközök, eljárások és emberi tényezők oldaláról egyaránt kezelni kell.

A Hivatal elektronikus információs rendszereihez való hozzáférések szintjét úgy kell megállapítani, hogy az igénylő minden jogosultságot és információt megkapjon, ami a munkájához szükséges, ugyanakkor csak annyit kapjon meg amennyi a munkájához feltétlenül szükséges.

A Hivatal munkafolyamatainak szervezése során a visszaélések megelőzése és észlelése érdekében a kritikus felelősségi köröket szét kell választani, lehetővé téve a másodlagos ellenőrzést, illetve felülvizsgálatot.

Az IBP iránymutatásainak be kell épülniük az Hivatal mindennapi életébe, működési folyamataiba. A szervezeti kultúrának és a dolgozók tudatos viselkedésének részévé kell válnia, ezért kellőképpen kommunikálni, és oktatni szükséges.

Meg kell valósítani a biztonsági intézkedések, funkciók működésének az ellenőrzését és visszacsatolását, biztosítva, hogy a hiányosságok szankcionálva legyenek.

Az informatikai biztonság és a működési folyamatok kialakítása (átalakítása) során az alábbi elveket kell érvényesíteni. Az elvekhez kapcsolódóan pontos követelményeket, rendszereket, kontrol funkciókat szükséges kialakítani.

Kockázatarányos védelem elve

A jogszabályi környezet egyre szigorúbb előírásokat fogalmaz meg az információk kezelésére, védelmére vonatkozóan. Ezért a Hivatal az informatikai biztonsági irányítási rendszerét és az elektronikus információs rendszereit

- a jogszabályoknak és belső szabályozóinak,
- a felügyeleti szervek írásban rögzített utasításainak,
- szerződéses kötelezettségeinek,
- a szakmai igényeinek, valamint
- az informatikai biztonsági kockázatok, figyelembevételével alakítja ki.

Az informatikai biztonsági kockázatelemzést lehetőleg a teljes szervezetre kell elvégezni. A kockázatelemzés informatikai részében az elektronikus információs rendszer minden elemcsoportjára (hardver, szoftver, adat, emberi erőforrás, és iroda (épület, objektum)) kiterjedő felmérést kell végezni. Meg kell határozni a fenyegetettségek teljes körét, valamint a kockázatok mértékét (a biztonsági esemény valószínűségének és következményének kombinációja).

A kockázatelemzés elvégzése után - a feltárt kockázat mérséklése érdekében - meg kell tervezni a reális és kockázatarányos biztonsági intézkedéseket, a szükséges fejlesztéseket, valamint dokumentálni kell a megmaradó kockázatokat.

Az informatikai biztonság a kockázatkezelés által épül be minden, informatikai eszközzel támogatott szervezeti folyamatba.

A teljes körű védelem elve

A Hivatal az adatokat és az elektronikus információs rendszereket veszélyeztető minden kockázati tényezőre megfelelő választ és kezelést biztosít, valamint az informatikai biztonságot az informatikai életciklus (fejlesztés, bevezetés, üzemeltetés, kivezetés) minden pontján érvényre juttatja, az eszköz, az eljárás és a humánerőforrás oldalról egyaránt kezeli.

A szükséges és elégséges hozzáférés elve

Figyelembe véve a Hivatal tevékenységét, az adatokhoz való hozzáférési jogosultságokat és jogosultsági szinteket úgy kell meghatározni, hogy a felhasználó számára minden információ elérhető legyen, ami feladatának ellátásához szükséges. Ugyanakkor biztosítani kell, hogy a felhasználó ne férjen hozzá olyan adatokhoz, amelyek nem tartoznak a feladatának ellátásához.

A négy szem elv

A szakmai és szervezeti kockázatok figyelembevétele mellett, az adatkezelés folyamatába (adatbevitel, adatmódosítás, adatfeldolgozás, stb.) meghatározott pontokon ellenőrzéseket, felülvizsgálatokat kell beépíteni. Az ellenőrzés elve, hogy a folyamatokat végrehajtó és azokat ellenőrző személyek ne legyenek ugyanazon személyek.

X. Alapvető Informatikai biztonsági követelmények

A Hivatal elektronikus információs rendszerei teljes életciklusában meg kell valósítani és biztosítani kell

- az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint
- az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása

zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

Az elektronikus információs rendszernek a fentieknek megfelelő védelme körében a szervezetnek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják:

- a megelőzést és a korai figyelmeztetést,
- az észlelést,
- a reagálást,
- a biztonsági események kezelését.

Informatikai biztonság szervezete

A Hivatalban biztosítani kell, hogy

a feladat-, felelősség- és hatáskörök az egyes szervezeti egységek, illetve személyek között jól elkülönüljenek,

a feladatokhoz és felelősségekhez mindig megfelelő hatáskört kell társítani, és ezeket az elveket az informatikai biztonság területén érvényesíteni kell!

Informatikai biztonsági tevékenységek

A Hivatalban a következő informatikai biztonsági tevékenységeket kell ellátni:

- a Hivatal biztonsági szintjének megállapítása,
- a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása,
- informatikai biztonsági szabályozó rendszer kidolgozása, felülvizsgálata,
- informatikai kockázatelemzés és kezelés,
- elektronikus információs rendszerek biztonsági felügyelete,
- új elektronikus információs rendszerek informatikai biztonsági véleményezése és elfogadása,
- informatikai biztonsági tudatosság fokozása, képzések,
- kapcsolattartás a hatóságokkal,
- az informatikai biztonság független felülvizsgálata.

Az informatikai biztonsági felelősségi rend meghatározása

Az informatikai biztonság megteremtése és fenntartása olyan alapvető felelősség, amely szerint nem tartozhat egyszemélyi felelősségi és hatáskörbe az elektronikus információs rendszerek tervezése, fejlesztése, üzemeltetése és felügyelete. Az informatikai biztonság megvalósítását, fenntartását és ellenőrzését a Hivatal a feladatok és felelősség szempontjából egymástól elhatárolt szervezeti keretek között valósítja meg.

Az elektronikus információs rendszerek biztonságával összefüggő szerepkörök a következők:

- Jegyző
- IBF
- Adatgazdák
- Rendszergazda
- Felhasználók

Külső felek kezelése

Valamennyi külső fél részére - a rájuk vonatkozó mértékig - meg kell ismertetni az informatikai biztonsági előírások rájuk vonatkozó részeit.

Gondoskodni kell arról, hogy az informatikai biztonsági érdekek már a szerződéskötés megkötése előtti fázisban bevonásra kerüljenek a folyamatba, annak érdekében, hogy a szükséges kontrollok beépítésre kerüljenek a szerződésbe.

A külső feleket nyilatkoztatni kell arról, hogy a rájuk vonatkozó informatikai biztonsági előírásokat megismerték, megértették, és hogy annak betartásával végzik munkájukat.

Folyamatos ellenőrzéssel biztosítani kell az előírások betartását.

A Hivatal biztonsági szintjének meghatározása

A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a Hivatal szervezetét, a külön jogszabályban meghatározott szempontok szerint 1 -5-ig terjedő skálán biztonsági szintbe kell sorolni.

A Hivatal minimális biztonsági szintje a jogszabályok alapján 2-es szint.

A Hivatalnak meg kell vizsgálnia, hogy a vizsgálat elvégzésének a pillanatában melyik biztonsági szintnek felel meg, és ha nem éri el a jogszabályban meghatározott minimum biztonsági szintet, akkor cselekvési tervet kell készítenie a következő biztonsági szint elérésére.

A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása

A Hivatalnak el kell készítenie az elektronikus információs rendszereinek vagyonleltárát.

A Hivatalnak külön-külön, öt fokozatú skálán biztonsági osztályba kell sorolnia valamennyi elektronikus információs rendszerét a rendszerben kezelt adat bizalmasságának, sértetlenségének és rendelkezésre állásából, valamint a rendszer sértetlenségének és rendelkezésre állásának elvesztéséből fakadó kár szerint.

A Hivatalban elektronikusan kezelt adatok vonatkozásában adatgazdákat kell kijelölni, akik felelősek az adatok biztonsági osztályba sorolásáért.

A fentiek végrehajtása érdekében a Hivatalnak ki kell dolgoznia az elektronikus biztonsági osztályba sorolás módszertanát.

A Hivatalnak külön jogszabályban meghatározott szempontok szerint meg kell vizsgálnia, hogy az elektronikus információs rendszerei melyik biztonsági osztálynak felelnek meg.

Abban az esetben, hogy ha az elektronikus információs rendszer logikai védelmi intézkedései nem érik el a biztonsági osztályba sorolás során megállapított osztályt, akkor a Hivatalnak cselekvési tervet kell készítenie a következő biztonsági osztály elérése érdekében. A következő biztonsági osztály elérésére 2 év áll a rendelkezésre.

Amennyiben valamely elektronikus információs rendszer biztonsági osztálya meghaladja a meghatározott minimum biztonsági szintet, akkor a Hivatal szervezetének biztonsági szintje automatikusan arra a biztonsági szintre emelkedik.

A cselekvési tervek kezelése

A cselekvési tervet a Hivatal Informatikai Biztonsági Stratégiájában meghatározott célok figyelembevételével, annak részeként kell kezelni.

Elektronikus információs rendszerek biztonságáért felelős személy

A Hivatalnak az informatikai biztonsági irányítási rendszerének megtervezése, bevezetése, működtetése és felülvizsgálata érdekében elektronikus információs rendszerek biztonságáért felelős személyt (továbbiakban: IBF) kell alkalmaznia, akinek

a képzettsége és szakképzettsége megfelel a külön jogszabályban meghatározott követelményeknek.

A Hivatalban el kell kerülni, hogy az IBF tekintetében mind a feladatellátása, mind a szervezeti tagozódása vonatkozásában informatikai biztonsági szempontból összeférhetetlen állapot alakuljon ki.

Ennek érdekében az IBF

- nem végezhet a Hivatalnál informatikai üzemeltetési és informatikai fejlesztési feladatokat,
- szervezetileg közvetlenül a jegyző alá tartozik, és kizárólag neki tartozik beszámolással. Az IBF feladat- és hatáskörét az Informatikai Biztonsági Szabályzat tartalmazza.

Kockázatelemzés

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

Ki kell dolgozni a Hivatal kockázatelemzési és kezelési eljárásrendjét, majd évente kockázatelemzéseket kell végezni az elektronikus információs rendszerek és az azokban kezelt adatok sérülékenységeinek minimalizálása érdekében.

Meg kell határozni a Hivatal által el nem fogadható kockázatok szintjét, a Hivatal által alkalmazott kockázatkezelési módszereket és **intézkedési terveket kell kidolgozni a kockázatok kezelésére.**

Az intézkedési tervnek tartalmaznia kell az adott kockázat ismertetését, a kockázat kezelésének módját, eszközét, illetve az intézkedés végrehajtásának felelősét, határidejét és költségeit.

A Hivatal kockázatelemzési és kezelési eljárásrendjét az Informatikai Biztonsági Szabályzat melléklete tartalmazza.

14.1. Informatikai biztonsági képzés

A Hivatal *{14.2 Az informatikai biztonsági felelősségi rend meghatározása}* **pontban meghatározott dolgozóinak** külön jogszabályban meghatározott **képzésen, továbbképzésen és éves továbbképzésen** kell részt venniük, melyet a Hivatal éves képzési tervének kialakításakor figyelembe kell venni.

14.2. Biztonsági események kezelése

Biztonsági eseményeket kezelő eljárásrendet kell kidolgozni annak érdekében, hogy a bekövetkező informatikai biztonsági események korai felfedezése, az érintettek tájékoztatása és az esemény minél előbbi elhárítása biztosított legyen.

14.3. Informatikai biztonsági ellenőrzés rendszere

A Hivatal informatikai biztonsági irányítási rendszerének és az elektronikus információs rendszerei biztonságának ellenőrzése többszintű feladat.

14.11.1. IBF ellenőrzései

Az IBF **éves ellenőrzési tervet** állít össze, melyet a jegyző hagy jóvá. Az ellenőrzési terv minimálisan a következő területekre terjed ki:

a) Informatikai biztonsági szabályozó rendszer

b) Vagyonleltár

c) Szervezet biztonsági szintje

d) Elektronikus információs rendszerek biztonsági osztályba sorolása

e) Kockázatok felülvizsgálata

f) Fizikai biztonság (gépterem, beléptetés ellenőrzése)

g) Határvédelem

h) Vírusvédelem

i) Biztonsági
frissítések j)
Mentések

k) Hozzáférések kezelése

Az elvégzett ellenőrzésekről jegyzőkönyvet készít, melyet a jegyző részére további intézkedések elrendelése érdekében benyújt.

14.11.2. Sérülékenység-vizsgálat

Magyarország állami szervei elektronikus információs rendszereit érő folyamatos támadásokra tekintettel időszakos **sérülékenység-vizsgálatokkal minimalizálni kell a Hivatal elektronikus információs rendszereinek műszaki sérülékenységeit.**

14.11.3. A Hatóság ellenőrzése

A jogszabályban meghatározottak szerint a **Nemzeti Elektronikus Információbiztonsági Hatóság ellenőrzi a Hivatalban a jogszabályokban előírt követelmények teljesítését.**

14.12. Kapcsolattartás a hatóságokkal

A Hivatal nevében a jogszabályokban meghatározott esetekben az IBF kapcsolatot tart

a) a Nemzeti Elektronikus Információbiztonsági Hatósággal,

b) a Nemzeti Biztonsági Felügyelettel és

c) a Kormányzati Eseménykezelő Központtal.

XII. VÉDELMI INTÉZKEDÉSEK

A Hivatal elektronikus információs rendszereinek jogszabályokban meghatározott védelmének megvalósítása érdekében adminisztratív, fizikai és logikai védelmi intézkedéseket alkalmaz.

A **Hivatalban alkalmazott adminisztratív és fizikai védelmi intézkedéseket a Hivatal szervezetének biztonsági szintje, az elektronikus információs rendszerekkel szemben támasztott logikai biztonsági követelményeket pedig az adott elektronikus információs rendszer biztonsági osztálya határozza meg.**

A Hivatal az adminisztratív, fizikai és logikai védelmi intézkedéseit a vonatkozó jogszabályok, a hazai, illetve nemzetközi szabványok, ajánlások alapján valósítja meg.

A védelmi intézkedések az Informatikai Biztonsági Szabályzatban, rendszerszintű informatikai biztonsági szabályzatokban, illetve eljárásrendekben kerülnek megfogalmazásra.

XIII. KAPCSOLÓDÓ DOKUMENTUMOK

15. Jogszabályok

a) 2012. évi I. törvény a munka törvénykönyvéről

b) 2012. évi C. törvény a Büntető Törvénykönyvről

c) 2013. évi V. törvény a Polgári Törvénykönyvről

d) 2013. évi L. törvény az állami és önkormányzati szervek elektronikus informatikai biztonságáról (továbbiakban: Ibtv.)

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

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

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

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

i) 1999. évi LXXVI. törvény a szerzői jogról

j) 2001. évi XXXV. törvény az elektronikus aláírásról

k) 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól

l) 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

m) 233/2013. (VI. 30.) Korm. rendelet az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről

n) 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus informatikai biztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

o) 83/2012. (IV. 21.) Korm. rendelet a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról

p) 83/2012. (IV. 21.) Korm. rendelet a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról

q) 84/2012. (IV. 21.) Korm. rendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről

r) 85/2012. (IV. 21.) Korm. rendelet az elektronikus ügyintézés részletes szabályairól

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

t) 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

16. Kapcsolódó szabványok, ajánlások

a) MSZ ISO/IEC 17799:2002: Az informatikai biztonság menedzselésének eljárásrendje

b) MSZE 17799-2:2004: Az információvédelem irányítási rendszerei. Előírás és használati útmutató

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

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

17. Az IBP-hez kapcsolódó belső dokumentumok

Az IBP-hez a következő Hivatali szabályzatok kapcsolódnak:

a) Szervezeti és Működési Szabályzat

b) Informatikai Biztonsági Stratégia

c) Informatikai Biztonsági Szabályzat

d) Adatvédelmi és Adatbiztonsági Szabályzat