Kivonat Kunszentmárton Város Önkormányzata Képviselő-testületének
2015. október 29-én tartott soros ülésének jegyzőkönyvéből.

306/2015.(X.29.) határozat
Kunszentmárton Város Önkormányzata Informatikai Biztonsági Politikája dokumentum elfogadására.

Kunszentmárton Város Önkormányzatának Képviselő-testülete, a hatályos jogszabályok és ajánlások alapján, megtárgyalta és elfogadja a mellékletben szereplő „**Kunszentmárton Város Önkormányzata Informatikai Biztonsági Politikája**” dokumentumot.

A megfogalmazott biztonságpolitikai célok és feladatok kiterjednek az Önkormányzat valamennyi intézményére, azok vezetőiére, ügyintézőire, a rendszerek felhasználóira, fejlesztőire, üzemeltetőire.

Az Informatikai Biztonsági Politikája hatálya alá tartozók készítsék el saját **Informatikai Biztonsági Szabályzatukat.**

Felelős: Wenner-Várkonyi Attila polgármester
Dr. Hoffmann Zsolt jegyző
Intézményvezetők

Határidő: 2016. február 28.

Erről értesül:
- képviselő-testületi tagok
- Wenner-Várkonyi Attila polgármester
- Dr. Hoffmann Zsolt jegyző
- Kunszentmárton Város Önkormányzatának szervei

kmf.

/Wenner-Várkonyi Attila/ sk.
polgármester

/Dr. Hoffmann Zsolt/ sk.
jegyző

A kivonat hiteles: Kunszentmárton, 2015. október 30.

Mihályi Ferenc

Kunszentmárton Város Önkormányzatának Informatikai Biztonsági Politikája

Bevezetés

Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény alapján a helyi önkormányzás, a település helyi közügyeiben demokratikus módon, széles körű nyilvánosságot teremtve kifejezi és megvalósítja a helyi közakaratot.
Az információ-technológia széleskörű alkalmazásának eredményeként az Önkormányzat Hivatalának (továbbiakban: hivatal) és Intézményeinek adatvagyona meghatározó részben elektronikus formában áll rendelkezésre, a hivatali folyamatok informatikai struktúrára épülnek.
A Hivatal elektronikus informatikai rendszerei egyrészt a funkcionális területek működését segítik elő (iktatórendszer, elektronikus testületi rendszer, pénzügyi-számviteli alkalmazások, helyi adózási rendszer, nyilvántartások, kapcsolattartás más intézményekkel), másrészt a város életével, működésével kapcsolatos információkat szolgáltat a polgárok, érdeklődők, vállalkozók részére.
Az Önkormányzás egységes szemléletű, hatékony működéséhez elengedhetetlen, az információs rendszerek lehető, legteljesebb védelmének kialakítása, a jogszabályokkal összhangban történő megteremtése.

Az Informatikai Biztonsági Politika célja

Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme.

Az Informatikai Biztonsági Politika (a továbbiakban: IBP) az Önkormányzat akaratnyilvánítása a szervezet informatikai rendszerei által kezelt információvagyon bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzésére és fenntartására irányuló intézkedések bevezetésére.

Az IBP célja irányelveket adni a biztonságért felelős vezetők részére a biztonsági politikánál alacsonyabb szintű szabályozások kialakításához, a jelen és jövőbeli informatikai biztonsági döntéseik meghozatalához, illetve a biztonsági rendszer működtetői és a felhasználók számára a napi rendeltetésszerű tevékenységük gyakorlásához.

Az IBP hatálya kiterjed:

- Kunszentmárton Város Önkormányzatának szerveire, valamint Kunszentmárton Város Önkormányzatának Hivatalára.
- Az Önkormányzat és szervei valamennyi vezetőjére, ügyintézőjére, a rendszerek felhasználóira, fejlesztőire, üzemeltetőire.
- Az Önkormányzattal és szerveivel külső, megbízásos (szerződéses) eseti munkakapcsolatban lévő személyekre is, amelyeknek érvényesülését a fenti szerződések tartalmának megfelelő kialakításával kell biztosítani.
- Az Önkormányzat és szervei által használt valamennyi informatikai rendszerre, amely felhasználja, feldolgozza, illetve felügyeli, ellenőrzi a keletkező, illetve felhasznált adatokat, információkat.

Értelmező rendelkezések

- Adat: Értelmezhető, elemi ismeret, amely az információt ábrázolja.
- Információs vagyon: Adatok, információk, szellemi, erkölcsi javak összessége.
- Adatbiztonság: Az adatokba történő betekintés, az adatok megszerzése, módosítása és

tönkretétele ellen műszaki és szervezési intézkedések és eljárások együttes rendszere.

- Adatbiztonság megsértése: Az a cselekmény vagy mulasztás, amely következményei az adatot veszélyeztetik.
- Adatfeldolgozás: Az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül végrehajtásához alkalmazott módszertől és eszköztől.
- Adatkezelés: Az alkalmazott eljárástól függetlenül az adatok gyűjtése, felvétele, tárolása, feldolgozása, hasznosítása. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is.
- Adatvédelem: Az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás, amely az adatok előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségére vonatkozik.
- Biztonsági követelmények: A biztonsági követelmények azok a biztonsági elvárások, amelyeket a fenyegetések határoznak meg.
- Biztonsági esemény: Az informatikai rendszer biztonságában beállt olyan kedvezőtlen változás vagy bekövetkező jelentős hatású zavaró esemény, amely rontja az informatikai szolgáltatás minőségét és veszélyezteti a rendszer biztonságát.
- Folyamatos ügyvitel biztosítása: Az informatikai rendszerek folyamatos rendelkezésre állása.
- Hozzáférés: az informatikai rendszer védelmi mechanizmusa által biztosított erőforrás-használat.
- Informatikai biztonság: az információs rendszer tulajdonsága, amely a rendszer biztonsági követelményeinek és céljainak teljesülését mutatja. Előírások, szabványok betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és bizalmasságát eredményezik, amelyeket az informatikai rendszerekben vagy komponenseikben, valamint az informatikai rendszerek vagy komponenseik alkalmazása során biztonsági megelőző intézkedésekkel lehet elérni.
- Informatikai biztonsági utasítások, eljárások: A kritikus alrendszer területek egyes üzemeltetési eljárásainak részletes leírásai.
- Katasztrófakezelés, tervezés: Lehetővé teszi, hogy egy esetleges katasztrófa bekövetkezte után az informatikai szolgáltatások ellenőrzött módon, egy előre megállapított szinten helyreállíthatók legyenek.
- Kontrollok-óvintézkedések: Mindazok a fizikai, adminisztratív, technikai technológiai módok, eljárások, amelyeket védelmi célból terveztek és a kockázatot csökkentik.
- Informatikai infrastruktúra: a Hivatalhoz kapcsolódó, feladatokat ellátó, illetve a hivatali hálózatba kapcsolt hardverelemek, az azokon futó szoftverek és a rajtuk megtalálható adatok együttese.
- Rendszergazda: az informatikai infrastruktúra hardver- és szoftverelemeinek, valamint szolgáltatásainak működését technikailag biztosító felelős.
- Üzemeltető: az adott szoftver-, vagy hardverelemet a Hivatal nevében üzembe állító és üzemeltető rendszergazda.
- Felhasználó: az a személy, aki a Hivatal informatikai infrastruktúrájának vagy szolgáltatásainak valamely elemét igénybe veszi.
- Hivatali felhasználó: olyan felhasználó, aki a Hivatallal munkavállalói jogviszonyban van.
- Szolgáltatás: az informatikai infrastruktúra olyan részhalmaza, amely a hivatali felhasználó számára meghatározott funkcionalitást nyújt.
- Publikus szolgáltatás: olyan szolgáltatás, amelyet a hivatali felhasználókon kívül mások is - korlátozottan vagy korlátozás nélkül - igénybe vehetnek.
- Szerver: olyan feladatokat ellátó számítógép, amely a hivatali hálózatra kapcsolódik és felhasználói köre számára szolgáltatást nyújt.
- Munkaállomás: a hivatali hálózathoz kapcsolt olyan számítógép, amely nem tekinthető szervernek és egyértelműen valamely hivatali felhasználóhoz vagy hivatali felhasználói

csoporthoz rendelhető.
- Külső munkaállomás: a hivatali hálózathoz kapcsolt olyan számítógép, amely nem tekinthető szervernek és egyértelműen nem rendelhető valamely hivatali felhasználóhoz vagy hivatali felhasználói csoporthoz.

Az Informatikai Biztonsági Politikával kapcsolatos alapelvek

Információvédelem területei

Információvédelem területei az alábbiak:
a) Azonosítás, hitelesítés;
b) Jogosultság kiosztás, ellenőrzés;
c) Hitelesség garantálása;
d) Sértetlenség garantálása;
e) Bizonyítékok rendszerének és folyamatának kialakítása.

Alapvető elektronikus információbiztonsági követelmények

A**z** elektronikus információs rendszerek teljes életciklusában meg kell valósítani, és biztosítani kell
a) az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint
b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

Az elektronikus információs rendszernek az előző pontban meghatározott feltételeknek megfelelő védelme körében a szervezetnek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják:
a) a megelőzést és a korai figyelmeztetést,
b)-az észlelést,
c) a reagálást,
d) a biztonsági események kezelését.

A biztonságpolitikai alapelvek és védelmi célkitűzések

Az Önkormányzat és szervei az informatikai biztonság területén az alábbi alapelveket és védelmi célkitűzéseket kívánják következetesen érvényesíteni:

- Bizalmasság biztosítása az Önkormányzat és szervei által kezelt, felhasznált adatokhoz való hozzáférés tekintetében, elsősorban a szervereken és a felhasználói munkaállomásokon történő adathozzáférések és az adatkezeléseknél felhasznált adathordozók kezelése, valamint a kommunikáció során.
- Sértetlenség biztosítása az Önkormányzat és szervei teljes adatvagyonára vonatkozóan az adatkezelés, adattárolás és a kommunikáció során.
- Az Önkormányzatnál és szerveinél történő adatkezelések és feldolgozások során követelmény, hogy a pontos és helyes információkat dolgozzák fel, az adatok sértetlenségét megőrizzék a feldolgozás előtt, közben és után.
- Rendelkezésre állás fenntartása elsősorban az Önkormányzat és szervei adatvagyonára vonatkozóan, amelyet biztosítani kell mind a külső, mind pedig a belső adatkérések során.
- Működőképesség fenntartása az Önkormányzat és szervei informatikai rendszereire és rendszerelemeire vonatkozóan, amely az adott informatikai eszköz vagy rendszer elvárt és igényelt üzemelési állapotban való fennmaradását jelenti. Ennek elérése céljából biztosítani kell a megfelelően képzett személyzetet, technikai és anyagi feltételeket.

Az Informatikai Biztonsági Politika az Önkormányzat tevékenységének szolgálatában

Az Önkormányzat és szervei kezelésében, valamint felügyeletében működő és ezen intézményeket kiszolgáló kommunikációs és informatikai rendszereket az adatok titkosságára, bizalmas jellegére és biztonságára vonatkozó törvényeknek megfelelően kell üzemeltetni.

Az informatikai rendszerekben az adatot, információt és egyéb szellemi tulajdont, az intézmény számára jelentkező értékével és a személyiségi jogok biztosításával arányosan kell védeni az illetéktelen betekintéstől, a módosítástól, a sérüléstől, megsemmisüléstől és a nyilvánosságra kerüléstől.

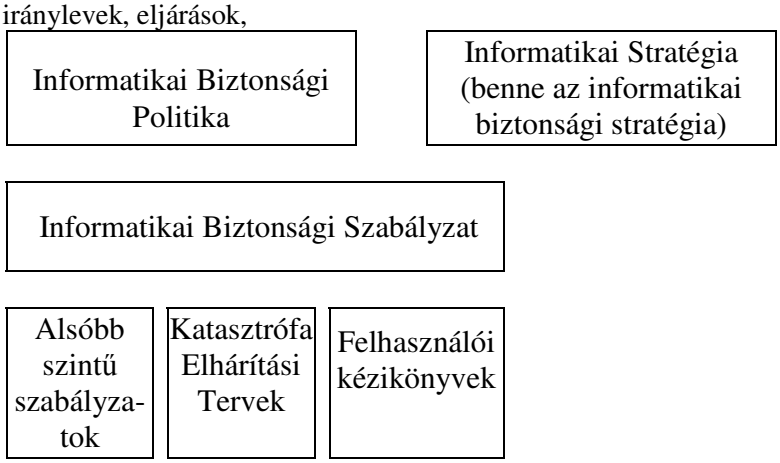
A védelem megvalósítása érdekében a tervezés során a költségvetésben biztosítani kell azokat az anyagi feltételeket, amelyek lehetővé teszik a megfelelő színvonalú technika, valamint a speciális felkészültséget igénylő személyi feltételek megteremtését és folyamatos fenntartását.

Az Informatikai Biztonsági Politika helye az informatikai biztonsággal foglalkozó dokumentumok rendszerében

Az Önkormányzat és szerveinek vezetői az informatikai rendszerek, illetve rendszerelemek teljes életciklusára, az informatikai biztonság elviselhető kockázati szinten tartása érdekében kialakítják az informatikai biztonsági dokumentációs rendszert. Minden intézménynek ki kell alakítania a dokumentációs rendszerben az Informatikai Biztonsági Politika alatt elhelyezkedő dokumentumokat a saját informatikai rendszereikre vonatkozóan.

Az Önkormányzat és szervei informatikai biztonságával kapcsolatos szabályokat és elvárásokat az informatikai biztonsági dokumentációs rendszer tartalmazza. Részei:

- törvényi előírások és egyéb jogszabályok,
- biztonsági iránylevek, eljárások,



Az informatikai biztonsági feladatok végrehajtásához szükséges feltételek megteremtését az informatikai biztonsági stratégiában (az Informatikai Stratégia részeként) is szerepeltetni kell.

A Önkormányzat és szervei viszonya az informatikai biztonság tekintetében

- Az Önkormányzat és szervei önállóan alakítják ki informatikai biztonsági szabályrendszerüket, azonban ezen szabályok nem mondhatnak ellent a vonatkozó törvényi, jogszabályi előírásoknak.
- Az Önkormányzat szervei, a hivatal és az intézmények elkészítik saját informatikai biztonsági szabályzatukat, saját, működő rendszerük tekintetében.
- Az Önkormányzat és szervei informatikai kapcsolatainak kialakítására illetve biztosítására csak olyan technikai és adminisztratív intézkedések engedélyezhetők, ill. valósíthatók meg, amelyekkel a jogszabályi és egyéb előírásoknak megfelelően biztosítják az informatikai rendszereik védelmét.

Az Önkormányzat és szervei informatikai biztonságának területeire vonatkozó alapelvek, követelmények

Számítógép-hálózati biztonság

Az Önkormányzat és szervei az informatikai rendszereiket logikai, technikai és adminisztratív eszközökkel védik az érkező támadások ellen.

Hozzáférés szabályozás

- Az Önkormányzatnál és szerveinél a felhasználók csak ellenőrzött körülmények között, a szükséges felhasználói jogosultságokkal férhetnek hozzá az informatikai rendszerekhez és szolgáltatásokhoz.
- A külső felek nem férhetnek hozzá a számítógépes rendszerekhez, számítógépekhez.
- A hozzáférések szabályainak kialakításánál a felhasználói profilokat rendszerenként kell meghatározni a szükségesnél nem több hozzáférési jogosultság elve alapján, és ehhez kell a személyeket hozzárendelni.
- A felhasználói hozzáférések kezelésére szóló eljárást, a felhasználónak a rendszerbeli teljes életciklusára kell megfogalmazni.

Adattovábbítás elektronikus úton:

A bizalmas tranzakciók adatainak cseréje a jogszabályokban meghatározottak szerint csak megbízható csatornákon történhet.

Adatok sértetlenségének, konzisztenciájának biztosítása

Az adatok bevitele során biztosítani kell a forrás dokumentumok, az adatbeviteli munkakörök és munkaállomások biztonságát és azonosíthatóságát, valamint a bevitt adat ellenőrzését és hibás bemeneti adatok kezelését.

a) Az informatikai rendszerek üzemeltetése során biztosítani kell a kezelt adatok, információk rendszeres biztonsági mentését.

b) Az Önkormányzatnál és szerveinél megfelelő eljárásokat kell kidolgozni az adathordozók kezelésére, tárolására, nyilvántartására, annak rendszeres, naprakész aktualizálására, valamint ezek megsemmisüléstől és illetéktelen hozzáféréstől történő védelmére.
Az adathordozók elhelyezése során biztosítani kell, hogy az elhelyezés feltételei megfeleljenek

az adatok, információk biztonsági osztályba sorolási modelljében meghatározott követelményeknek.

Szoftverkezelés biztonsága

Az Önkormányzat és szervei informatikai rendszereiben kizárólag jogtiszta, az üzemeltetéshez, adatfeldolgozáshoz szükséges, engedélyezett alapprogramok, irodai szoftvercsomagok és feldolgozó programok futtathatók.

Rosszindulatú szoftverek elleni védekezés

A rossz szándékú szoftverek kártételeinek megelőzésre megfelelő megelőző, észlelési és korrekciós mechanizmusokat kell alkalmazni.

Tűzfalas védelem

Az internetet és az elektronikus levelezést a felhasználók csak a szervezettel kapcsolatos feladataik végzéséhez használhatják.
Az internet használat, levelezés létesítése és üzemeltetése vonatkozásában megfelelő védelmet kell kialakítani a külső támadások, illetve a belső erőforrásokhoz történő jogtalan külső hozzáférések megakadályozása érdekében.
A tűzfalnak el kell rejtenie a belső hálózat struktúráját.
Minden alkalmazással, illetve infrastruktúrával kapcsolatos tevékenységhez kötődő információáramlásnak át kell haladnia a tűzfalon.
A rendszerbe csak az engedélyezett forgalom léphet be.
A szervezet kiszolgáló gépeit, amelyek a nyilvános hálózatból érkező szolgáltatási kérelmeket kezelik, ún. demilitarizált zónában (DMZ) kell elhelyezni.

Fizikai védelem

Illetéktelen hozzáférés megakadályozása

Az Önkormányzat és szerveinél az infrastrukturális elemek kialakítása során figyelembe kell venni az Informatikai Biztonsági Szabályzatban meghatározott szempontokat is.

Az informatikai rendszer környezeti feltételeinek biztosítása

Az informatikai rendszerek külső környezeti hatásoktól való védelmét úgy kell kialakítani, hogy a szervezet vagyona és az ügymenet folytonossága ne legyen veszélyeztetve. A védelemnek biztonsági osztályba sorolástól függően ki kell terjednie a biztonságos elektromos ellátás, a klímatizálás, a tűz- és villámvédelem biztosítására is.

Adminisztratív védelem aktualizálása, karbantartása

Az informatikai rendszerben bekövetkezett változásokat és alkalmazott problémakezelési eljárásokat (tervezés, létrehozás, üzemeltetés-karbantartás, megszüntetés) dokumentált formában, kell végezni.
Az informatikai biztonsági dokumentációs rendszer aktualitásának fenntartása érdekében a dokumentumok rendszeres karbantartást igényelnek.
A dokumentációs rendszer dokumentumait felül kell vizsgálni a következő esetekben:

- a szervezet igényei, céljai megváltoznak,
- új területek, szolgáltatások jelennek meg,
- informatikai szolgáltatások szűnnek meg,
- új informatikai technológiák kerülnek bevezetése,
- informatikai technológiák alkalmazása szűnik meg,

- a kockázatelemzés következtében új, lényeges változtatások válnak szükségszerűvé.

Az IBP szervezete

Informatikai biztonsággal kapcsolatos feladatkörök meghatározása

A felső vezetésnek a szervezeten belül, hogy a dolgozók csak a munkakörükhöz, illetve beosztásukhoz tartozó feladatokat lássák el, mindenkit tájékoztatni kell arról, hogy milyen mértékű belső ellenőrzési és biztonsági felelősséggel tartozik.

Informatikai biztonsági szervezet

Az informatikai biztonság tervezése, alapkövetelményeinek lefektetése, bevezetése és ellenőrzése a szervezet vezetőinek a feladata.

Személyekre vonatkozó biztonsági megállapítások

A Önkormányzat és szerveinél az informatikai biztonsági követelmények és annak betartásának követelményeit a dolgozóval ismertetni kell.

Mindezek kapcsán az Informatikai Biztonsági Szabályzatban részletesen szabályozni kell a következő területeket:

1. informatikai funkciók meghatározása;
2. munkavállalókkal szembeni követelmények;

Egyéb területek

Oktatás, képzés és a biztonságtudatosság fokozása

A Önkormányzat és szervei az informatikai biztonsági dokumentációs rendszerben foglaltak érvényre juttatásának érdekében fontosnak tekintik az informatikai biztonsági képzést, oktatást, az informatikai biztonság tudatosítását.

A folyamatos működés biztosítása

A folyamatos működés tervezésének és biztosításának célja, hogy az ügymenet tevékenységében bekövetkezett zavarokat ellensúlyozni lehessen és a kritikus folyamatok védettek legyenek, a nagyobb hibák és katasztrófák következményeitől.

A Katasztrófa Elhárítási Terv fejlesztésével és bevezetésével kell biztosítani, hogy az ügymenet szempontjából kritikus folyamatok visszaállíthatóak legyenek egy meghatározott időintervallumon belül. Az ügymenet folyamatos működésének biztosításába bele kell érteni a katasztrófa események következményeinek azonosítását és a rájuk történő reagálást, valamint a legszükségesebb alkalmazások meghatározott időn belüli visszaállítását.

Informatikai biztonsági események észlelése és kezelése

Az Önkormányzatnak és szerveinek érdeke, hogy a szervezet informatikai biztonságáért felelős vezetői mielőbb értesüljenek a bekövetkezett biztonsági eseményekről. Minden alkalmazottnak (külső vagy belső) ismernie kell azt az eljárást, amelyben jelenthetik az általuk felismert biztonsági eseményeket.

Ennek érdekében:

Informatikai biztonsági esemény bekövetkezésekor, arról a közvetlen munkahelyi vezetőt és az Informatikusokat kell értesíteni, valamint foganatosítani kell a megfelelő válaszintézkedéseket.

Rendszerfejlesztések biztonsági követelményei

A rendszerek biztonsági követelményeinek meghatározása során, rendszer alatt értjük az infrastrukturális elemeket, objektumokat, alkalmazásokat stb. Biztonsági szempontból kiemelkedő, hogy a biztonság, mint kritérium jelen legyen az alkalmazások és szolgáltatások tervezésétől kezdődően az ügymenet folyamataiba történő implementálásig.

Mobil eszközök használata

Felkészülve a jövő kihívásaira és reagálva az információtechnológiai eszközök fejlődésére és megjelenésére az Önkormányzat és szervei informatikai infrastruktúrájában szabályozni kell a mobil eszközök használatát.

A mobil eszközök használata során az eszközök jellegüknél fogva speciális kockázatokat hordoznak magukban. A mobil eszközökön történő munkavégzés során nem biztosított a megfelelő védelemmel ellátott környezet, ezért ilyen esetekben speciális védelmet kell biztosítani.

Az információ biztonság fenntartása

Az információ biztonsági irányítási rendszer fenntartása alapvetően fontos stratégiai cél. A stratégiában és az IBSZ-ben előírt feladatok végrehajtásához szükséges feltételek biztosításáért a jegyző felel.

Az információ biztonság szintjei, definíciója

Az információ biztonság szintjei

Az informatikai biztonsági szint besorolását a 2013. évi L törvény, valamint 41/2015. (VII. 15.) BM rendelet 4. melléklete szerint kell alkalmazni.

Értelmező rendelkezések

Az IBP-ben használt fogalmak és definíciók értelmezését a 2013. évi L törvény fogalmaival és definícióival azonosak.

Kunszentmárton, 2015. ……

1. számú melléklet

Vonatkozó jogszabályok

- 2004. évi CXL. Törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól
- 2009. évi CLV. Törvény a minősített adat védelméről
- 2011. évi CXII. Törvény az információs önrendelkezési jogról és az információszabadságról
- 2013. évi CCXX. Törvény az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól
- 2013. évi L. törvény - az állami és önkormányzati szervek elektronikus információbiztonságáról
- 38/2011. (III. 22.) Korm. rendelet - a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról
- 84/2012. (IV. 21.) Korm. Rendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről
- 85/2012. (IV. 21.) Korm. Rendelet az elektronikus ügyintézés részletes szabályairól
- 73/2013. (XII. 4.) NFM rendelet - az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről
- 1139/2013. (III. 21.) Korm. Határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről
- 142/2015. (VI. 12.) Korm. Rendelet az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól szóló 2013. évi CCXX. törvényvégrehajtásáról
- Közigazgatási Informatikai Bizottság 25. számú ajánlása