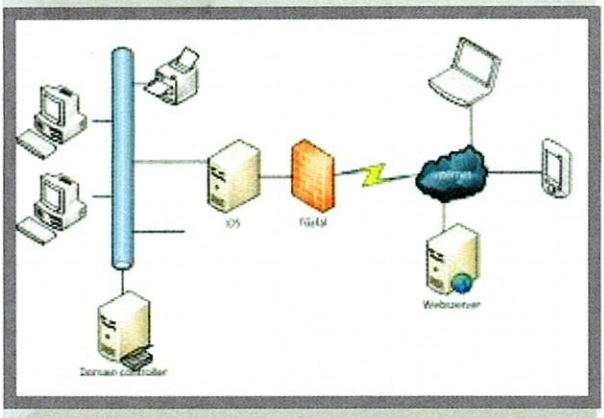
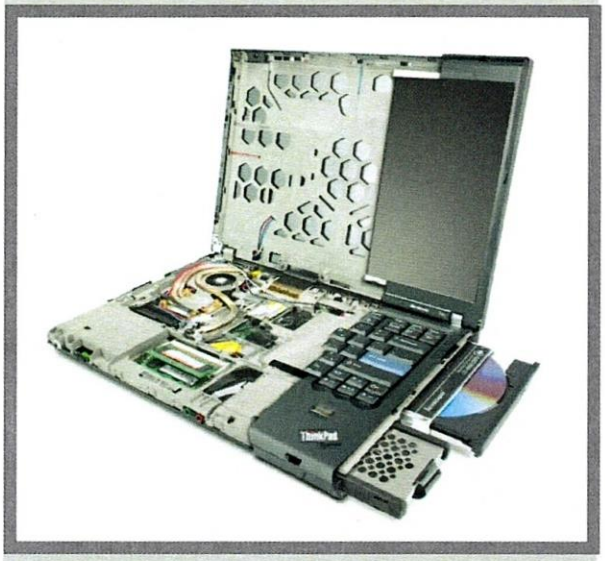
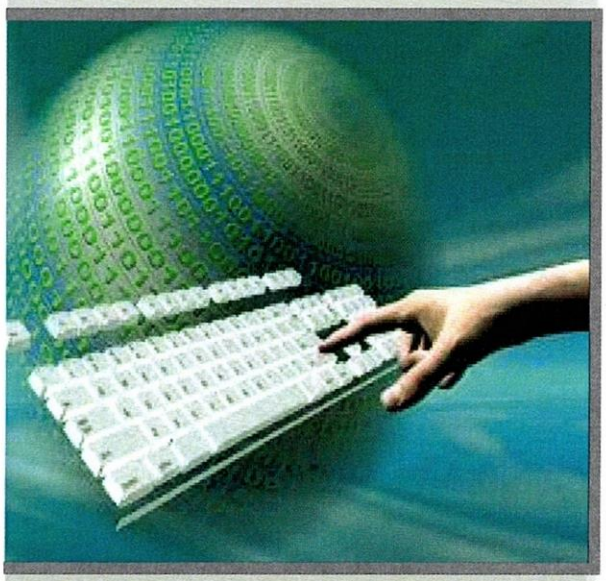


2017.

POLGÁRI POLGÁRMESTERI HIVATAL INFORMATIKAI BIZTONSÁGI SZABÁLYZATA





Hatályba lépés dátuma:

2018. április 24.

Jóváhagyta:

.....

Dr. Váliné Antal Mária

jegyző

ph.

POLGÁR VÁROS JEGYZŐJE HAJDÚ-BIHAR MEGYE

Tartalom

Módosítási jegyzőkönyv

Az Informatikai biztonsági szabályzat a fedő és záró rendelkezések lapon jóváhagyott napon lép érvénybe. Módosítása esetén a Módosítási jegyzőkönyv részben kerül rögzítésre. A jegyző által jóváhagyott módon a jelen jegyzőkönyvben kerül az időpont, az ok és a jóváhagyó rögzítésre.

Frissítés/Módosítás dátuma	Módosítás tartalma	Jóváhagyó
2013.10.30	Iktatás	jegyző
2014.06.25	Módosítás	jegyző
2017. december 10.	Frissítés, módosítás ***Oka:*** ASP csatlakozást megelőzően biztonsági szabályzás felülvizsgálata, szükséges módosítások, meglévő szabályzás és a követelményeknek való megfelelés érdekében: - frissített fedlap - módosítási jegyzék - jogszabályi háttér - fogalmak - ASP követelmények - célja - hatálya - szabályzások - eljárásrendek - mellékletek	jegyző
2018. március 20.	Frissítés ***Oka:*** Az ASP rendszerhez való csatlakozást követően az információs rendszert érintő jelentős változást követőn felül kell vizsgálni a szabályozást és szükség esetén rögzíteni a változásokat.	jegyző

A módosításokat minden alkalommal a Polgári Polgármesteri Hivatal jegyzője hagyja jóvá.

A dokumentum Hitelességét igazolom:
Polgár, 2018. április 24.

.....
Dr. Váliné Antal Mária
jegyző
ph.

1. Jogszabályi háttér

A Polgári Polgármesteri Hivatal (a továbbiakban: Hivatal) az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) követelményeire vonatkozóan a jogszabályi követelmények közül a következőket veszi a szabályozás kialakításában is követendőnek:

- A 73/2013. (XII. 4.) NFM rendelet és 77/2013. (XII. 19.) NFM rendelet hatályát vesztette, ezt nem tekinti érvényesnek, a további hatályban lévő szabályokat érvényesnek tekinti.
- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről
- 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
- 257/2016 (VIII.31.) Korm. rendelet az Önkormányzati ASP rendszerről, melynek szükséges részletszabályait az informatikai biztonsági szabályzatba rögzíteni kell.

Az Informatikai Biztonsági szabályzatra vonatkozóan (továbbiakban: IBSZ) a következő követelményeket fogalmazza meg:

3.1.1.1.	**Informatikai biztonsági szabályzat**
3.1.1.1.1.	*Az érintett szervezet:*
3.1.1.1.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonsági szabályzatot;
3.1.1.1.1.2.	más belső szabályozásában, vagy magában az informatikai biztonsági szabályzatban meghatározza az informatikai biztonsági szabályzat felülvizsgálatának és frissítésének gyakoriságát;
3.1.1.1.1.3.	gondoskodik arról, hogy az informatikai biztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.

3.1.1.1.2.	*Az informatikai biztonsági szabályzatban meg kell határozni:*
3.1.1.1.2.1.	a célokat, a szabályzat tárgyi és személyi (a szervezet jellegétől függően területi) hatályát;
3.1.1.1.2.2.	az elektronikus információbiztonsággal kapcsolatos szerepköröket;
3.1.1.1.2.3.	a szerepkörhöz rendelt tevékenységet;
3.1.1.1.2.4.	a tevékenységhez kapcsolódó felelősséget;
3.1.1.1.2.5.	az információbiztonság szervezetrendszerének belső együttműködését.
3.1.1.1.3.	*Az informatikai biztonsági szabályzat elsősorban a következő elektronikus információs rendszerbiztonsággal kapcsolatos területeket szabályozza:*
3.1.1.1.3.1.	kockázatelemzés (amely szorosan kapcsolódik a biztonsági osztályba és biztonsági szintbe soroláshoz);
3.1.1.1.3.2.	biztonsági helyzet-, és eseményértékelés eljárási rendje;
3.1.1.1.3.3.	az elektronikus információs rendszer (ideértve ezek elemeit is) és információtechnológiai szolgáltatás beszerzés (amennyiben az érintett szervezet ilyet végez, vagy végezhet);
3.1.1.1.3.4.	biztonsággal kapcsolatos tervezés (például: beszerzés, fejlesztés, eljárásrendek kialakítását);
3.1.1.1.3.5.	fizikai és környezeti védelem szabályai, jellemzői;
3.1.1.1.3.6.	az emberi erőforrásokban rejlő veszélyek megakadályozása (pl.: személyzeti felvételi- és kilépési eljárás során követendő szabályok, munkavégzésre irányuló szerződésben a személyes kötelmek rögzítése, a felelősség érvényesítése, stb.);
3.1.1.1.3.7.	az informatikai biztonság tudatosítására irányuló tevékenység és képzés az érintett szervezet összes közszolgálati, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekintetében;
3.1.1.1.3.8.	az érintett szervezetnél alkalmazott elektronikus információs rendszerek biztonsági beállításával kapcsolatos feladatok, elvárások, jogok (amennyiben az érintett szervezetnél ez értelmezhető);
3.1.1.1.3.9.	üzlet-, ügy- vagy üzemmenet folytonosság tervezése (így különösen a rendszerleállás során a kézi eljárásokra történő átállás, visszaállás az elektronikus rendszerre, adatok pótlása, stb.);

3.1.1.1.3.10. az elektronikus információs rendszerek karbantartásának rendje;

3.1.1.1.3.11. az adathordozók fizikai és logikai védelmének szabályozása;

3.1.1.1.3.12. az elektronikus információs rendszerhez való hozzáférés során követendő azonosítási és hitelesítési eljárás, és a hozzáférési szabályok betartásának ellenőrzése;

3.1.1.1.3.13. amennyiben az érintett szervezetnek erre lehetősége van, a rendszerek használatáról szóló rendszerbejegyzések értékelése, az értékelés eredményétől függő eljárások meghatározása;

3.1.1.1.3.14. az adatok mentésének, archiválásának rendje,

3.1.1.1.3.15. a biztonsági események - ideértve az adatok sérülését is - bekövetkeztekor követendő eljárás, ideértve a helyreállítást;

3.1.1.1.3.16. az elektronikus információs rendszerhez jogosultsággal (vagy jogosultság nélkül fizikailag) hozzáférő, nem az érintett szervezet tagjainak tevékenységét szabályozó (karbantartók, magán-, vagy polgári jogi szerződés alapján az érintett szervezet számára feladatokat végrehajtók), az elektronikus információbiztonságot érintő, szerződéskötés során érvényesítendő követelmények.

3.1.1.1.4. Az informatikai biztonsági szabályzat tartalmazza az érintett szervezet elvárt biztonsági szintjét, valamint az érintett szervezet egyes elektronikus információs rendszereinek elvárt biztonsági osztályát.

2. Személyi és tárgyi hatálya

2.1. Személyi hatálya

Az IBSZ személyi hatálya kiterjed a Hivatallal közszolgálati jogviszonyban álló vezetőkre, ügyintézőkre, valamint a munkaviszony keretében foglalkoztatott ügyviteli és fizikai alkalmazottakra, közszolgálati munkavállalókra, valamint a közfoglalkoztatásban alkalmazott munkavállalókra. **A szabályzatban foglaltak megismerésről a jegyző által jóváhagyott módon a jegyző gondoskodik, hogy illetéktelen és jogosulatlanok számára ne legyen megismerhető.** A Hivatal jegyzőjének döntése alá tartozik az informatikai biztonsági szabályzat és annak be nem tartásához kapcsolódó jogkövetkezmények kezelése.

A szabályzat személyi kifejezett kiterjed az *elektronikus információs rendszert* használó személyekre. Továbbá minden olyan személyre, vagy szervezetre, akik az elektronikus

információs rendszert közvetve vagy közvetlenül szerződéses úton kezelik, használják vagy módosításokat (létrehozás, törlés, módosítás) végeznek rajta. A hatály kiterjed mindazon személyekre is akik, közvetve vagy közvetlenül az elektronikus információs rendszerrel kapcsolatba kerülnek.

2.2. Tárgyi hatálya

Az IBSZ tárgyi hatálya a következőre is kiterjed:

- a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- a Hivatal tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre,
- valamint az informatikai eszközök műszaki dokumentációira,
- az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- a rendszer- és felhasználói programokra,
- az adatok felhasználására vonatkozó utasításokra,
- az adathordozók tárolására, felhasználására.

A szabályzat tárgya hatálya a Hivatal belső szervezeti egységei által vezetett nyilvántartások, adatbázisok és valamennyi egyedileg kezelt adat, elektronikus szolgáltatások illetőleg dokumentumok esetében is érvényesek. Az információ biztonság által előírt módon a jogszabályi követelményeknek megfelelően, a Hivatal védi és megfelelően a szervezeti infrastruktúrát, és kialakítja a szükséges intézkedéseket az informatikai rendszereket tartalmazó irodák védelmének érdekében.

3. Az IBSZ célja

Az IBSZ alapvető célja, hogy a **Polgári Polgármesteri Hivatal** és intézményeiben az alkalmazottai által kezelt adatok vonatkozásában, az informatikai rendszer használata során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát, továbbá a szervezet elektronikus információs rendszerének bizalmasságát, sértetlenségét, rendelkezésre állását biztosítsa.

Az IBSZ célja továbbá:

- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése,
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

A jelen IBSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét. A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzembe helyezésen keresztül az üzemeltetésig.

A szabályzat további célja a jogszabályi követelményeknek való megfelelésen túl, hogy egy jogszabályi alapú biztonságirányítási rendszer, kerüljön kialakításra, melynek az IBSZ az alapja, az alapvető kulcs eleme a biztonságos munkamenet és az emberek kockázati tényezők csökkentése között. Illetve amennyiben, az információs rendszereket érintő változás következik be, akkor a lehetséges fenyegetések elkerülése érdekében milyen szükséges szabályokat, eljárásrendeket kell használni, alkalmaznia a védelem fenntartása érdekében.

4. Fogalmak

A Hivatal a jogszabály által meghatározott elveket, fogalmakat beépíti az IBSZ szabályozásába, annak érdekében, hogy felhasználók tudatosan tudják használni és értelmezni, a Hivatali informatikai, információ biztonság kialakítása során.

Bizalmasság: A rendszerben tárolt adatok és információk jogosultság szerinti megismerése, felhasználása, az adatok megfelelőn történő rögzítése a jogosultságnak megfelelően.

Sértetlenség: Az adat származása (hiteles forrásból származik – hitelessége), az adat eredete ellenőrizhető (letagadhatatlan a forrás), a rendeltetésnek megfelelő használat jellemző rá.

Rendelkezésre állás: A rendszert, csak az arra jogosultak számára elérhető, az abban kezelt adatok, folyamatosan kiesés nélkül, megfelelően elérhetőek, használhatóak.

Adatgazda: Annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik.

Adatkezelő: Az a természetes vagy jogi személy, aki, vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bízhat meg.

Adatfeldolgozó: Az a természetes vagy jogi személy, aki, vagy amely az adatkezelő megbízásából adatok feldolgozását végzi.

Adatkezelés: Az alkalmazott eljárástól függetlenül az adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is;

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

Adattovábbítás: Ha az adatot meghatározott harmadik fél számára hozzáférhetővé teszik.

Nyilvánosságra hozatal: Ha az adatot bárki számára hozzáférhetővé teszik;

Adatbiztonság: Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

Biztonsági esemény: Nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen

helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.

Rendszergazda: A rendszerben lévő adatok védelméért felelős, a bizalmasság, sértetlenség és rendelkezésre állás technológiai megvalósításának szempontjából tartja karban az informatikai rendszert annak érdekében, hogy az adatgazdák által kezelt adatok biztonsági elvárásai megvalósításra kerüljenek.

5. Szerepkörök és tevékenységek, felelősségek

A Hivatal a jogszabály által meghatározott követelmények szerint meghatározta a Hivatal adatainak és az elektronikus információs rendszer szempontjából szükséges információ biztonságot érintő szerepköröket.

Szerepkörök:

- Hivatal vezetője
- Biztonsági felelős
- Adatvédelmi felelős

5.1 Hivatal vezetője, feladatai, felelőssége

A jogszabály által meghatározottan a következő szabályok vonatkoznak a Hivatal vezetőjére, az elektronikus információs rendszer és annak humán tényezőit érintő védelmét tekintve:

- Gondoskodik az információbiztonsági ismeretek szinten tartásáról, oktatásáról;
- Kialakítja az elektronikus információbiztonságot segítő belső szervezeti egységet.

A Hivatal belső szabályozását érintő feladatai:

- Informatikai biztonsági szabályzatot ad ki,
- Meghatározza a felelős(ök)re és a felhasználókra vonatkozó szabályokat.
- jóváhagyja a biztonsági osztályba sorolást, valamint a biztonsági szint meghatározását,

- Felel a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért,
- Felelős az eredmények biztonsági szabályzatba foglalásáért,
- Köteles meggyőződni arról, hogy a biztonság megfelel-e a jogszabályoknak és a kockázatoknak,

A Hivatal szervezeti működése szerint gondoskodik:

- Az eseményeinek nyomon követhetőségéről.
- Biztonsági események kezeléséről is rendelkezik:
- A gyors és hatékony reagálásról, kezeléséről,
- A lehetséges fenyegetésekre történő felhívással egyidejűleg haladéktalanul tájékoztatja az érintetteket.
- Hatósággal való együttműködésről
- Tájékoztatás céljából megküldi a szervezet informatikai biztonsági szabályzatát,
- Biztosítja az ellenőrzés lefolytatásához szükséges feltételeket.
- Az információ biztonság felügyeléről

Hivatal vezetőjének további felelőssége:

- Biztonsági kockázatok és a kockázatokkal arányos védelem meghatározása (védelem elvárt erőssége)
- Bizalmasság, sértetlenség, rendelkezésre állás vizsgálata alapján – minden egyes rendszerre vonatkozóan védelem kialakítása
- A lehetséges fenyegetettség mértékének azonosítása (bekövetkezési valószínűség, kármérték => kockázatok)
- A személyes adatok védelméért, az adatkezelés jogszerűségéért a jegyző felelős.

5.2. Információ biztonságért felelős feladatai, felelőssége

A jogszabályi követelményeken túl kiemelten következő szabályok vonatkoznak az információ biztonsági felelősre:

- Jogosult a szervezet vezetőjének közvetlenül tájékoztatást adni és jelentést tenni,

Belső szabályozás kialakítását tekintve:

- elvégzi vagy irányítja a tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
- támogatja az informatikai biztonsági szabályzatot előkészítését,
- véleményezi a szervezet tárgykört érintő szabályzatait és szerződéseit.

Információ biztonságért felelős felelőssége:

- támogatja a biztonsági osztályba sorolást és a biztonsági szintbe történő besorolást ,

5.3. Adatvédelemért felelős feladatai, felelőssége

A Hivatalban a belső szervezeti egység kialakítását és személyi állományát tekintve a Hivatal adatvédelmi felelőse az informatikus (rendszergazda). A jelen szabályzatban foglaltak szakszerű végrehajtásáról a Hivatal vezetőinek kell gondoskodnia. A Hivatal vezetői és informatikusa a szakszerű végrehajtás és szakmai döntés kialakításához külső szakértőt is alkalmazhat.

Amennyiben a Hivatal Informatikai vezetője az Adatvédelemért felelős, akkor a következő feladatokat látja el:

- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- javaslatot tesz a rendszer és a felmerülő kockázatok, szűk keresztmetszeteinek felszámolására.
- az adatgazdák segítségével, meghatározza a védett adatok körét,
- ellátja az adatkezelés és adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,

- az adatvédelmi feladatok ismertetése,
- ellenőri tevékenységét adminisztrálja.
- ellenőrzi a szoftverek használatának jogszerűségét

Az informatikai vezető ellenőri feladatai

- évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását,
- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
- előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

Az informatikai vezető jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a Hivatal vezetőjénél,
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,
- betekinthet valamennyi iratba, ami az informatikai feldolgozásokkal kapcsolatos,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

Amennyiben a Hivatali Adatvédelmi felelős feladatait a Rendszergazda látja el, akkor a következő feladatok kapcsolódnak hozzá:

- a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli,
- felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének folyamatos ellenőrzése,
- felelős a Hivatali informatikai rendszer hardver eszközeinek karbantartásáért,
- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- gondoskodik a folyamatos vírusvédelemről
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer adminisztrációját,

6. Információ biztonsági belső együttműködés

A Hivatal gondoskodik róla, hogy a szervezetben lévő szerepkörök között belső együttműködés alakuljon ki, a Hivatal informatikai, információ biztonságot, adatvédelmet és ügymenet folytonosságot érintő területeiken. A Hivatal kijelöli az információ és az informatikai biztonság szempontjából a biztonsággal összekapcsolódó szerepköröket (adatgazda, folyamatgazda). Emellett a Hivatal meghatározza, kik a folyamatgazdák, adatgazdák mellett érintett személyek vagy más szervezeti egységek.

A belső együttműködés során minden érintett munkavállaló és felhasználó kötelessége részt venni a belső együttműködésben (pl. tudatossági tájékoztatások, képzéseken, adatok biztonsági besorolása, információs rendszer biztonsági intézkedés végrehajtása). Ennek célja, az, hogy amennyiben az információ biztonságot érintő kérdés merül fel, megválaszolásához az adatkezelő, adatgazda együttműködése megteremhető legyen a szükséges védelmi intézkedés megtételéhez.

Az informatikai és az információ biztonság kialakítása során a Hivatalban nyilvántartott adatokat védeni kell különösen a **jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, sérülés, törlés vagy megsemmisülés ellen**. A Hivatal elektronikus és papír alapú iratokat, adatokat a munkaköri feladat ellátásán kívül a munkahelyről kivinni nem lehetséges! A munkahelyen kívül feldolgozni, tárolni csak a jegyző egyetértésével lehet, a megfelelő biztonsági intézkedés megtételét követően lehet, csak azzal a feltétellel, hogy az irat, adat tartalmát a jogosultsági szintnek betartása mellett, illetéktelen személy nem ismerheti meg. Az iratok tárolása, kezelése során fokozottan ügyelni kell arra, hogy illetéktelen személyek ne ismerhessék meg azok tartalmát. A munkavégzés céljára szolgáló irodákat távozáskor kulcsra kell zárni. Az irodahelyiségek nyitva tartása miatt, illetéktelen hozzáférés esetén az érintett fegyelmi felelősséggel tartozik. Az információs rendszerrel szemben elkövetett vétség esetén a ***Fegyelmi eljárásrendben*** meghatározott, tudatosító és tájékoztatásra szolgáló szabályok érvényesek, valamint a Btk. szerint meghatározottak.

A Hivatal a jogszabály által előírt információ biztonsági irányítási rendszer hatékony kialakítása érdekében, a rendszer, rendszerelemei, annak adatai és felhasználói védelmének érdekében meghatározza, kialakítja, felülvizsgálja és módosítja a folyamatokat, eljárásrendeket. Az eljárásrendekben rögzített folyamatok dokumentálását úgy kell megtenni, hogy abból az elvégzett kontroll tevékenység, intézkedés - ideértve annak egyes jellemzőit, részleteit, így különösen is az eljárás vagy a tevékenység tartalmi mélységét, az érintett

személyek és tárgyi hatókörét tekintve megállapítható legyen. pl. Tudatosság és képzési eljárásrendben rögzített képzési forma, annak dátuma, helye, résztvevői és témája rögzítésre kerül.

7. ASP rendszerhez való csatlakozás követelményei

A Hivatal a jogszabály által meghatározottak szerint rögzíti az ASP csatlakozáshoz kapcsolódó követelményeket. Az elektronikus információs rendszereket érintő legfontosabb követelmények, melyek a Hivatal munkavállalói számára is kötelezően követendő. Ezek a biztonsági követelmények a következők:

- Az ASP Központtól kapott szoftveres tanúsítvány és annak jelszava nem adható át az ASP Központ által nem feljogosított személynek.
- Az önkormányzati ASP rendszerben csak a „257/2016. (VIII. 31.) Korm. rendelet az önkormányzati ASP rendszerről" jogszabályban említett szereplők végeznek, illetve végeztetnek központilag fejlesztői, üzemeltetői, működtetői tevékenységet. Bárminemű fejlesztői tevékenységet az ASP Központ vezetője engedélyez írásban.
- Az önkormányzati ASP rendszerben tesztelést végezni csak az idézett Korm. rendeletben meghatározott felek jogosultak.
- Azokon az eszközökön, amelyeken önkormányzati ASP rendszer van használatban, vagy adat továbbítódik rá, tilos olyan alkalmazást használni, amely az eszközt az ASP Központon kívüli harmadik féllel köti össze, és amellyel lehetőség van távoli támogatásra, vezérlésre, távoli hozzáférésre, képernyő átvételére stb.
- • A tenant adminisztrátornak törekednie kell a legkisebb jogosultság kiosztásához a felhasználók körében. A jogosultságok kiosztásánál javasolt figyelembe venni a szervezeti és működési szabályzatot, amely nem kerülhet ellentmondásba sem a Hivatali IBSZ-szel, sem e Tájékoztatóval.
- Az ASP Központ egy esetleges biztonsági incidens során a tenant adminisztrátoroknak privilégiumokkal járó jogosultság-kiosztását számon kérheti.
- Biztonsági audit során, ha az indokoltnál magasabb hozzáférés állapítható meg egyes felhasználók esetében, annak oka jegyzőkönyvben kell, hogy szerepeljen.
- Általánosságban megállapítható, hogy a jogosultságok kiosztója is felelőssé tehető a gondatlanságból bekövetkezett biztonsági események kapcsán.
- A Korm. rendelet szerinti üzemeltető és működtető felek a Hatóság kérésére, utasítására is leállíthatják az önkormányzati ASP rendszert, vagy annak bizonyos elemeit (pl. kibertámadás esetén). Ebben az esetben az ASP Központ tájékoztatása addig nem fog

megtörténni, amíg az incidens kiváltója, okozója, felderítése akadályokba ütközhet, azaz a Hatóság írásbeli engedélyezéséig.

- A jogszabály elvárja az önkormányzati ASP-hez történő csatlakozás után az IBSZ és az eljárásrendek esetleges felülvizsgálatát, ismételt kihirdetését, ahol az értelmezhető.

8. Biztonsági eseménykezelés

A Hivatalban történő biztonsági incidensek, annak kezelésére (dokumentálás, eljárások, ellenőrzés, utóvizsgálat stb.) vonatkozó részletszabályokat a Hivatal a ***Biztonsági események kezelési eljárásrendben*** rögzíti.

Biztonsági incidensek esetén a Hivatal IBSZ-ben hivatkozott eljárásrend szerint kell eljárni, azonban az önkormányzati ASP-t ért incidensek észlelését jelenteni kell az ASP Központ felé is a Kormányzati Eseménykezelő Központ mellett (utóbbi esetén az észlelés nem feltétlenül jelentkezik a Hivataloknál, de kizárni sem lehet).

A jelentés nem tartalmazhat olyan szenzitív adatot (pl. személyes adatot), elemeket, amelyet harmadik fél nem ismerhet meg.

Az incidens nem feltétlenül a kliens oldali eszközön jelentkezett, még ha azt az ASP rendszer felhasználója úgy véli, fontos meghatározni hogy az incidens mikor és kinek kell jelenteni, továbbítani. Ennek bejelentési felülete a hibabejelentő rendszer. Az ASP Központ a bejelentéseket fogadja, továbbítja az illetékes terület felé és a jogszabály szerinti lépéseket megteszi. A Hivatalnak további kötelezettségei is vannak biztonsági incidensek kapcsán (pl. Kormányzati Eseménykezelő Központtal történő kapcsolatfelvétel), melyet a jogszabályok részleteznek.

9. Biztonsági esemény kezelését követő helyreállítás

A Hivatalban a biztonsági esemény bekövetkezését követően meghatározásra kerül a kár mértéke, és a szükséges akcióterv, hogy melyik Ügymenet folytonossági terv az, amely segítségével a helyreállítást minél hamarabb lehetővé tehető. A Hivatal ***Biztonsági eseménykezelési eljárásrendje*** a szükséges részletszabályokat rögzíti (természeti katasztrófa, áramszünet, áramkimaradás, emberi károkozás) de az elektronikus információs rendszer és annak rendszerelemeinek helyreállítását illetően a mindenkori Katasztrófa és az Informatikai Katasztrófa elhárítási eljárásrend rendelkezik.

10. Biztonsági helyzet- és eseményértékelés

Amennyiben a Hivatalban olyan eset történik, amiből az eljárásrendben megfogalmazott vagy a jogszabályban rögzített eseményre lehet következtetni, akkor a Hivatal **jegyzőjének** a jogköre az adott helyzetben eljárni, döntést hozni és kijelölni a felelősöket és felülvizsgálni a körülményeket, és meghozni a szükséges reagáló intézkedését az Ügymenet folytonossági tervnek megfelelően. Az incidensekről az eljárásrendben rögzített jelentést kell készíteni. A rögzítés célja, annak igazolása, hogy a Hivatal a bekövetkezett biztonsági események esetén, a szükséges védelmi intézkedések vizsgálatát elvégezte, lehetőségeket mérlegelve a helyesbítő intézkedést hajtott végre a kockázatok csökkentésére.

11. Elektronikus információs rendszer és annak szolgáltatásai

A Hivatal elektronikus információs rendszerei és annak elemei esetében nem szolgáltat és nem végez Hivatali tevékenységen kívüli műveleteket. Kizárólag a Hivatal tevékenységeinek és ügymeneteinek ellátására alkalmazza a Hivatal vezetősége által jóváhagyott elektronikus információs rendszereket.

12. Biztonsággal kapcsolatos tervezés

A Hivatal kialakítja a szükséges biztonság irányítási rendszert a szervezet megfelelő biztonságának beszerzése, tervezése, fejlesztése, karbantartása során. A Hivatal tevékenysége során nem végez beszerzési tevékenységet. A Hivatal rendszerfejlesztési tevékenységei közé értendő a kis értékű, és kereskedelmi forgalomban kapható általában irodai alkalmazásokat, szoftvereket, vagy azokat a hardver beszerzéseket, amelyek jellemzően a tönkrement eszközök pótlása, vagy az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából történnek, valamint a javítás, karbantartás céljára történő beszerzéseket végez kizárólagosan.

A biztonsággal kapcsolatos tervezés során a tervezés, végrehajtás, ellenőrzés, reagáló tevékenységet alkalmazza a biztonsági irányítási rendszer működtetése érdekében. Amennyiben, szükséges külön részletszabályokat határoz meg a Hivatali vezetőség jóváhagyását követően, a szükséges teendők végrehajtásához. Az információ biztonság felügyelete a Hivatal vezetősége által jóváhagyott módon meghatározott időszakonként történik.

12.1 Tervezés és előkészítés során előforduló veszélyforrások

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit.
- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

12.2. A rendszerek megvalósítása során előforduló veszélyforrások

- hibás adatállomány működése,
- helytelen adatkezelés,
- programtesztelés elhagyása.

12.3. A működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság,
- szervezetlenség,
- képzetlenség,
- szándékosan elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

13. Kockázatelemzés

A hivatal megvizsgálja a szervezet elektronikus információs rendszereit és annak fizikai és logikai környezetét érő kockázatokat. A Hivatal kockázatelemzése szorosan kapcsolódik a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolásához és annak védelmi intézkedéseihez.

A kockázatelemzés részletszabályait és annak eredményét (kockázatok, sebezhetőségek, kockázatgazdák, felelősök, beépített ellenőrzési pontok) a Hivatal ***Kockázatkezelési eljárásrendje*** rögzíti. A kockázat elemzést az 5. sz. Mellékletben meghatározott kárértékek szerint vizsgálja meg.

14. Fizikai védelmi eljárásrend

A Hivatal meghatározza és ismerteti az IBSZ-be a fizikai védelmet érintő káreseteket, illetve az emberi tényezőre vonatkozó eseteket. Ennek célja az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások megismerése, azért, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

14.1. Fizikai védelmet érintő káresetek

- elemi csapás:
- földrengés,
- árvíz,
- tűz,
- villámcsapás, stb.
- környezeti kár:
- légszennyezettség,
- nagy teljesítményű elektromágneses térerő,
- elektrosztatikus feltöltődés,
- a levegő nedvességtartalmának felszökése vagy leesése,
- piszkolódás (pl. por).
- közüzemi szolgáltatásba bekövetkező zavarok:
- feszültség-kimaradás,
- feszültségingadozás,
- elektromos zárlat,
- csőtörés.

14.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a megváltozott körülmények figyelmen kívül hagyása,
- vírusfertőzött adathordozó behozatala,

- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

14.3. Tűzvédelem

A gépterem illetve kiszolgáló helyiség a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent. A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell. A hivatal géptermeibe, szerverszobáiba minimum 1-1 db tűzoltó készüléket kell elhelyezni. A hivatal géptermeiben, szerverszobáiban elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni. **A nagy fontosságú, pl. törzsadat-állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni. (Ezen adatállományok kijelölése az informatikai vezető feladata.)**

A Hivatal a további Fizikai védelmet érintő részletszabályokat, eseteit a ***Fizikai védelmi eljárásrendben*** szabályozza.

15. Az emberi erőforrásokban rejlő veszélyek megakadályozása

A Hivatal gondoskodik róla, hogy, az elektronikus információs rendszert használó személyek, megfelelő tájékoztatást kapjanak a rendszer használatát illetően. Ennek részletszabályait a Tudatosság és képzés eljárásrenden beleül a Biztonságtudatossági képzés szabályaiban rögzíti. A szabályokat a belépő felhasználók esetében is ismerteti. Továbbá a kilépő felhasználók esetében az ***Eljárás jogviszony megszűnése*** eljárásrendet alkalmazza. A Hivatal elektronikus információs rendszereivel szemben felmerülő személyi veszélyek megakadályozása és tájékoztatását a ***Fegyelmi intézkedések eljárásrendben*** rögzíti.

16. Tudatosság

A Hivatal gondoskodik róla, hogy a Hivatali biztonságtudatosságát növelje. Az informatikai és információ biztonságot érintő tudatossági képzéseket, tájékoztatásokat,

rendszeres biztonsági értekezleteket a Hivatal ***Tudatosság és képzés eljárásrendje*** rögzíti, szabályozza.

17. Biztonsággal összefüggő feladatok, tevékenységek

A Hivatal elektronikus információs rendszereit tekintve a Hivatal meghatározza a biztonsággal kapcsolatos feladatokat, elvárásokat, jogokat. Ezeket a szabályokat a Hivatal vezetősége és az mindenkori üzemeltetésért felelős vezető/rendszergazda alakítja ki a helyi infrastrukturális követelményeknek megfelelően. Első sorban a Hivatal rendszereinek bizalmasságát, sértetlenségét, rendelkezésre állását illetően határozza meg a védelem kialakítása szempontjából szükséges teendőket. Ezeket a teendőket az érintett szervezeti munkavállalókkal egyezteti, a Hivatali munkamenetnek és az ügymenet folytonosságnak megfelelően kezeli és rögzíti. Továbbá a feladatokhoz szükséges eszközök, informatikai beállítások megfelelő kezelésének, tárolásának rendjét is meghatározza.

18. Ügymenet, (üzletmenet-) folytonosság

A Hivatal ügymenet, üzletmenet folytonosságra vonatkozó szabályait, a Hivatal ***Ügymenet folytonossági terv*** eljárásrendre szabályozza. Kifejezett képen a rendszerleállásokra és kézi megoldásokra, adatok helyreállítására, az elektronikus információs rendszer megfelelő működéséhez történő átállásra vonatkozó részletszabályokat is tartalmazza. Kivételt képez a korábban is említett informatikai rendszerek üzemeltetési helyreállítása, katasztrófa terve.

19. Karbantartási rend

A Hivatal elektronikus információs rendszereinek rendszeres és meghatározott Karbantartási tevékenységét és annak részletszabályait a Hivatal ***Karbantartási eljárásrendje*** szabályozza. Továbbá meghatározza a karbantartást végző szervezetet/személyeket is, melyben a jogosultságok és a hozzáférések is rögzítésre kerülnek. Ennek eredményét csatolja a karbantartási eljárásrendhez.

20. Adathordozók fizikai hozzáférésnek védelme

Elemi csapás (vagy más ok) esetén a számítógépekben, vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

20.1. Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell. A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése. Az üzemeltetést, karbantartást és szervizelést az informatikusok végzik. Alapgép megbontását (kivéve a garanciális gépeket) csak informatikus végezheti el.

A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlatait,
- a tapasztalatokat.

20.2. Vagyonvédelmi előírások

A Hivatal az elektronikus információs rendszerek esetén és a fizikai vagyontárgyakkal kapcsolatban a következő vagyonvédelmi előírásokat határozza meg:

- a géptermek külső és belső helyiségeit biztonsági zárakkal kell felszerelni,
- a gépterembe való be- és kilépés rendjét szabályozni kell,
- a gépterembe, szerverterembe történő illetéktelen behatolás tényét a hivatal vezetőjének azonnal jelenteni kell,
- az informatikai eszközöket csak a hivatal arra felhatalmazott alkalmazottai használhatják,
- **az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.**

20.3. Adathordozók

A Hivatal az adathordozók esetén a következő részletszabályokat határozza meg:

- a Hivatalban csak a vagyonleltárában lévő belső Hivatali adathordozó használata engedélyezett
- a használni kívánt adathordozót a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni,
- könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
- a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek, (tiszta asztal)
- adathordozót másnak átadni csak engedéllyel szabad, (vezetői jóváhagyás)
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

20.4. Az adathordozók nyilvántartása

Az adathordozókról az egységeknek nyilvántartást kell vezetni. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval (sorszámmal) kell ellátni.

20.5. Adathordozók tárolása

Az adathordozók tárolására műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

20.6. Az adathordozók megőrzése

Az adathordozók megőrzési idejét a törvényekben meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani.

20.7. Selejtezés, sokszorosítás, másolás

A selejtezést a Hivatal ***Selejtezi eljárásrendje***, szabályzata alapján kell lefolytatni. Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni. Az adathordozók megsemmisítésére vonatkozó selejtezési szabályokat az eljárásrend szabályozza. Biztonsági illetve archív adatállomány előállítása másolásnak számít.

20.8. Leltározás

A szoftvereket és adathordozókat a ***Leltározási Szabályzatban*** foglaltaknak megfelelően kell leltározni.

21. Elektronikus információs rendszer

21.1. Rendszerszoftver védelem

Az informatikai vezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

21.2. Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni. Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek. Az elektronikus információs rendszerek esetén felül kell vizsgálja, a jogosultságokat és mindenkinek a legkisebb jogosultsági elv szerint kell hozzáférnie az aktuális információs rendszerhez.

A szoftverek használatára vonatkozó jogosultság kezelés a jegyző által jóváhagyott módon az informatikus/rendszergazda/üzemeltetési vezető/felelős által kerül végrehajtásra. A részletszabályokat (a jogosultságokat kezelését és a szoftverekhez tartozó jogosultságokat) a ***Hozzáférési eljárásrend*** szabályozza, rögzíti.

21.3. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől. A központi gépek háttértárairól folyamatosan biztonsági mentést kell készíteni. Ennek részletszabályait a Mentési rend eljárásrend szabályozza. Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni. A vásárolt szoftverekről biztonsági másolatot kell készíteni. A működésbiztonság részletszabályait az ***Informatikai katasztrófa elhárítási*** eljárásrend szabályozza.

A felhasználók munkaállomás használata során a következő követendő szabályok betartása követendő:

- Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
- Vírusfertőzés gyanúja esetén az informatikusokat/rendszergazdát/adatgazdát azonnal értesíteni kell az incidens kivizsgálása és a reagálása érdekében.
- Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.
- A hivatal informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.
- A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni.
- A hálózat vezetékének megbontása szigorúan tilos.
- Az informatikai eszközt és tartozékait helyéről elvinni csak az eszköz leltárfelelőse tudtával és engedélyével szabad.

22. Rendszerbejegyzések értékelése

A Hivatal vezetősége meghatározza a mindenkori üzemeltetési vezető/rendszergazdával együttműködve az elektronikus információs rendszerben lévő rendszerbejegyzések szükségességét. Továbbá arról is rendelkezik, hogy melyek azok, amiket rendszeresen kell naplózni, felülvizsgálni vagy reagáló intézkedést tenni a megfelelő ügymenet folytonosság és a rendszer bizalmasságának, sértetlenségének, rendelkezésre állásának fenntartása érdekében.

23. Elektronikus információs rendszerek nyilvántartása

A Hivatal meghatározza, nyilván tartja a használt elektronikus információs rendszereket. Annak változásait, alapfeladatait, fejlesztőit, a szolgáltatást végző szervezet és az üzemeltetésért felelős szervezetet megnevezését rögzíti.

24. Ellenőrzés

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése illetve annak megakadályozása, hogy az megismétlődjön. A munkafolyamatba épített ellenőrzés során az IBSZ rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

25. Mentési és archiválási rend

A Hivatal a rendszerek és a benne tárolt adatok biztonságára vonatkozó mentési eljárásrendet a ***Mentési eljárásrendben*** foglaltaknak megfelelően végzik el. A mentés készítésre vonatkozó kiemelten fontos korábban meghatározott szabályok a következőek:

A Hivatal kiemelt rendszer- és felhasználói programjairól napi, heti, valamint éves mentés készül.

Az adatfeldolgozás után biztosítani kell az adatok mentését. **A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata.** A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az adatok archiválásban az informatikusok segítséget nyújtanak. A DMS (Dokumentum Menedzsment Rendszer) - ASP szolgáltatás (Application Service Providing - magyarul alkalmazás-szolgáltatás) keretén belül történő adatok esetén a mentés nem a hivatal rendszerein belül történik. Archiválási célból a tárgy év utolsó mentésének (az éves mentés) megtörténte után a NAS adattároló eszköz tükör merevlemeze cserélődik, egy új merevlemezre. A mentést tartalmazó HDD a jegyzői titkárságon páncélszekrényben kerül elhelyezésre.

a. Adatvesztés, elemi kár, bármilyen, adatokat érintő probléma esetén követendő eljárás

(1) Az adatkezelő munkatárs az adatok épségét, hozzáférhetetlenségét veszélyeztető legapróbb jelet észlelve köteles értesíteni az érintett személyeket.

(2) Az adatkezelő munkatárs a veszély legapróbb jelét észlelve azonnal abbahagyja a munkát, az elmentetlen dokumentumokat elmenti és az adatvédelmi felelős további utasításági nem nyúl sem a számítógéphez, sem a biztonsági másolatokat tartalmazó merevlemezhez.

(3) Az adatvédelmi felelős (amennyiben nem azonos a rendszergazdával) saját hatáskörében és az adatkezelő munkatárs jelzésére is dönthet úgy, hogy az adatok biztonságára nézve veszélyhelyzetnek értékeli a jeleket és tüneteket.

(4) Az adatvédelmi felelős (amennyiben nem azonos a rendszergazdával) haladéktalanul értesíti a Hivatal rendszergazdáját.

(5) A rendszergazda kiérkezéséig az adatvédelmi felelős biztosítja az érintett számítástechnikai eszközök elkülönítését (senki nem nyúlhat hozzá, még az adatvédelmi felelős sem).

b. Adatok visszatöltése, adatmentési pontok visszaállítása

A napi és heti rendszerességgel mentett adatokat csak az adatvédelmi felelős tudtával és írásbeli beleegyezésével szabad visszatölteni. Az adatok visszatöltéséről jegyzőkönyvet kell készíteni.

26. Jogosultság nélküli hozzáférés

A Hivatal gondoskodik róla, hogy az elektronikus információs rendszerekhez jogosultsággal (vagy jogosultság nélkül fizikailag) hozzáférő személyek, akik nem az érintett szervezet tagjai, de a szervezet által megbízott tevékenységét végeznek el, azokra vonatkozólag megfelelően kialakított hozzáférési szabályokat határoz meg.

Ide tartozhatnak például a karbantartók, magán-, vagy polgári jogi szerződés alapján az érintett szervezet számára feladatokat végrehajtó személyek, továbbá az elektronikus információbiztonságot érintő, a szerződéskötés során érvényesítendő lehetséges követelmények.

27. Biztonsági szint és osztály

A Hivatal a jogszabályi követelménynek megfelelően meghatározta a szervezet biztonsági szintjét, illetve az elektronikus információs rendszer felmérése – jogszabály által előírt határidőre – megtörtént. A Hivatal a jogszabály által előírt követelmények szerint meghatározza, Hivatal vezetője által jóváhagyja a Hivatal biztonsági szintbe sorolását, továbbá a Hivatal elektronikus információs rendszereinek az osztályba sorolását is elvégzi. Az osztályba sorolást és annak eredményét az IBSZ mellékletei között rögzíti.

A Hivatal adatai különböző biztonsági fokozatba tartozhatnak, melyet a szabályzat mellékletei részleteznek. A hivatal vezetője a biztonsági osztályba sorolást jóváhagyta. Mivel a felmérés során meghatározott biztonsági szint alacsonyabb, mint az érintett szervezetre érvényes szint, a vizsgálatot követő **90 napon belül cselekvési tervet** kell készíteni. A biztonsági osztályba sorolást az elektronikus információs rendszereket érintő változások után ismételten el kell végezni. A biztonsági osztályba sorolást a jegyző által jóváhagyott módon történik a jogszabályi követelményeknek megfelelően.

28. Kapcsolódó szabályozások

A Hivatal gondoskodik róla, hogy a Hivatal elektronikus információs rendszerei és annak szabályai a Hivatal legfontosabb biztonságot érintő szabályaival összhangban legyenek.

A Hivatal működése szempontjából a legfontosabb szabályozások, amik az IBSZ előírásaival összhangban vannak:

- Szervezeti és Működési Szabályzatával
- Informatikai Katasztrófa Tervével
- Ügymenet folytonossági terv

29. Frissítési gyakoriság

A szabályzat frissítése a **jegyző** által jóváhagyott módon történik, amennyiben azt jogszabályi változás, szervezetben történő változás, átszervezés vagy más követelmény teszi szükségessé. A módosításokat a szabályzat elején lévő ***Módosítások jegyzéke*** részben rögzítenek, majd azt a szervezet érintett munkavállalóival megismertetik, az illetékes személyek által kihirdetésre kerül.

A szabályzat módosítását szükség szerint a Hivatal jegyző által jóváhagyott kinevezett személy felelős kezdeményezhet, melyet a **jegyző** hagy jóvá. Az IBSZ folyamatos karbantartása a jegyző által kinevezett felelős feladata.

30. Záró rendelkezés

A korábban elfogadott (2013. sz. Képviselő-testület a által jóváhagyott) Szabályzat hatályát veszti, kivételt képeznek az Adatvédelemre és az közérdekű adatok közzétételére, megismerésére vonatkozó szabályok. A jelenlegi szabályzás 2018. április 24. napján lép hatályba. Az informatikai biztonsági szabályzatot a szervezetre érvényes rendelkezések szerint az erre jogosult vezetőnek, jegyzőnek kell jóváhagynia.

A szabályzat a **jegyző** által jóváhagyott módon kerül kihirdetésre az illetékes személyek, munkavállalók számára, akik aláírással igazolják a szabályzat megismerését és annak betartását.

A szabályzat érvénybe léptetéséről a **jegyző** gondoskodik, továbbá a megismerést követően jóváhagyja, az érintettek megismerték és aláírással igazolták a szabályzatban leírtak. (1. Sz. Melléklet)

Polgár, 2018. április 24.

.....

Dr. Váliné Antal Mária
címzetes főjegyző

POLGÁR VÁROS JEGYZŐJE
HAJDÚ-BIHAR MEGYE

31.MELLÉKLETEK

1. sz. Melléklet - Megismerési nyilatkozat

Aláírásommal igazolom, hogy a **Polgári Polgármesteri Hivatal Informatikai Biztonsági** Szabályzatban lévő Hivatali politikát elolvastam, megismertem, magamra nézve követendőnek, kötelezőnek ismerem el, tekintem.

Ssz.	Név	Aláírás
1.	dr. Váliné Antal Mária címzetes főjegyző	
2.	Albeczné Kajatin Krisztina	
3.	Andorkó Mihályné	
4.	Brieger Sándor Lajos	
5.	Csépányiné Bartók Margit	
6.	Elek Zoltánné	
7.	Gyüge Szilvia	
8.	Kiss Anita	
9.	Kiss Balázsné	
10.	Léka Gyuláné	
11.	Lukácsné Oláh Kornélia	
12.	Makó Sándorné	
13.	Makóné Erős Anikó	
14.	Mecsei Dezsőné	
15.	Mezei Judit	
16.	Molnár Jánosné	
17.	Nagyné Szurkos Anikó	
18.	Német Máté Tibor	
19.	Renténé Horváth Gizella	
20.	Répási Antal	
21.	Szabó Bartalanné	
22.	Tanyi Tiborné	
23.	Vámosi Tamás	
24.	Vígné Varga Katalin	

Aláírásommal igazolom, hogy a Polgári Polgármesteri Hivatalban az Informatikai Biztonsági Szabályzat kihirdetésre, tájékoztatásra került, minden érintett munkavállaló részé, akik aláírással igazolják, annak megismerését, betartását.

Dátum: Polgár, 2018. április 24.
A dokumentum hitelességét igazolom:

.....
Dr. Váliné Antal Mária
címzetes főjegyző

2. sz. Melléklet – Szervezeti szintbe sorolása

Polgármesteri Hivatal			
Pont	Kérdés	Igaz-e	Szint
1.1.	A szervezet nem üzemeltet és nem fejleszt elektronikus információs rendszert, és saját hatáskörben erre más szervezetet, vagy szolgáltatót (ide nem értve a telekommunikációs szolgáltatót) sem vesz igénybe.	Igen	1
	Az adatfeldolgozás módját nem maga határozza meg.	Igen	
	Az adatkezelés tekintetében technikai, vagy információtechnológiai döntést nem hoz.	Nem	
	A használt elektronikus információs infrastruktúra kialakítása tekintetében döntési jogköre - ide nem értve a szervezet munkavégzését érintő informatikai rendszerelemek elhelyezését - nincs.	Nem	
	Egyedi adatokat és információkat kezel, vagy dolgoz fel.	Igen	
	Kritikus adatot nem kezel.	Nem	
	A szervezet információbiztonsági tevékenysége elsődlegesen az elektronikus információs rendszerrel kapcsolatba kerülő személyek információbiztonsággal kapcsolatos kötelezettségeinek szabályozására, számonkérésére terjed ki, addig a mértékig, ameddig a szervezet, vagy az egyes személyek tevékenysége az elektronikus információs rendszerre hatást tud gyakorolni.	Igen	
2.1.	A szervezet vagy szervezeti egység olyan elektronikus információs rendszert használ, amely személyes adatokat kezel.	Igen	2
	A szervezet jogszabály alapján kijelölt szolgáltatót vesz igénybe.	Igen	
3.1.	A szervezet vagy szervezeti egység szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt.	Nem	3
	A szervezet kritikus adatot, nem minősített, de nem közérdekű, vagy közérdekből nyilvános adatot kezel.	Nem	
	Központi üzemeltetésű, és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszerek vagy zárt célú elektronikus információs rendszer felhasználója.	Igen	
	Feladatai támogatására más külső szolgáltatót vesz igénybe.	Igen	
4.1.	A szervezet vagy szervezeti egység elektronikus információs rendszert vagy zárt célú elektronikus információs rendszert üzemeltet, vagy fejleszt.	Nem	4
5.1.	A szervezet vagy szervezeti egység európai létfontosságú rendszerelemmé vagy nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek elektronikus információs rendszereinek üzemeltetője, fejlesztője.	Nem	5
	Az információbiztonsági ellenőrzések, tesztelések végrehajtására jogosult szervezet vagy szervezeti egység.	Nem	

3. sz. Melléklet - Osztályba sorolás

Polgári Polgármesteri Hivatal					
Pont	Kérdés	Bizalmasság	Sértetlenség	Rendelkezésre állás	Osztály
2.2.1.	az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot;	Nem	Nem	Nem	1
2.2.2.	nincs bizalomvesztés, a probléma az érintett szervezeten belül marad, és azon belül meg is oldható;	Nem	Nem	Nem	
2.2.3.	a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez képest jelentéktelen;	Nem	Nem	Nem	
2.3.1.	személyes adat sérülhet;	Igen	Igen	Igen	2
2.3.2.	az érintett szervezet üzlet-, vagy ügymenete szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat, vagy elektronikus információs rendszer sérülhet;	Igen	Igen	Igen	
2.3.3.	a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;	Igen	Igen	Igen	
2.3.4.	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át.	Igen	Igen	Igen	
2.4.1.	különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek;	Nem	Nem	Nem	3
2.4.2.	az érintett szervezet üzlet-, vagy ügymenete szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat sérülhet;	Nem	Nem	Nem	
2.4.3.	a lehetséges társadalmi-politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek;	Nem	Nem	Nem	
2.4.4.	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 5%-át.	Nem	Nem	Nem	
2.5.1.	különleges személyes adat nagy mennyiségben sérülhet;	Nem	Nem	Nem	4

2.5.2.	személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket);	Nem	Nem	Nem	
2.5.3.	az érintett szervezet üzlet-, vagy ügymenete szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet;	Nem	Nem	Nem	
2.5.4.	a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, vagy vezetésében személyi felelősségre vonást kell alkalmazni;	Nem	Nem	Nem	
2.5.5.	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 10%-át.	Nem	Nem	Nem	
2.6.1.	különleges személyes adat kiemelten nagy mennyiségben sérülhet;	Nem	Nem	Nem	5
2.6.2.	emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;	Nem	Nem	Nem	
2.6.3.	a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;	Nem	Nem	Nem	
2.6.4.	az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;	Nem	Nem	Nem	
2.6.5.	a lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;	Nem	Nem	Nem	
2.6.6.	az érintett szervezet üzlet- vagy ügymenete szempontjából nagy értékű üzleti titkot, vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet;	Nem	Nem	Nem	
2.6.7.	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át.	Nem	Nem	Nem	

4. sz. A Hivatal biztonsági osztályba sorolása

(2013. évi IBSZ-ben meghatározott követelményrenszer, előzmények)

A Hivatal adatai különböző biztonsági fokozatba tartozhatnak, melyet a szabályzat mellékletei részleteznek. Az elektronikus információs rendszerek és a szervezet biztonságpolitikai felmérése – a jogszabály által előírt határidőre – megtörtént.

Biztonsági osztályok

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) szerint a besorolás elvégzése a következő elvek figyelembevételével az érintett szervezet felelőssége, az alábbiak a döntéshez csak szempontokat jelentenek:

A Polgármesteri Hivatal biztonsági osztályba sorolási szintje: **2. biztonsági osztály**

A 2. biztonsági osztály esetében **csekély káresemény** következhet be, mivel

- személyes adat sérülhet;
- az üzlet-, vagy ügymenet szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat, vagy elektronikus információs rendszer sérülhet;
- a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest csekély.

Mivel a felmérés során meghatározott biztonsági szint alacsonyabb, mint az érintett szervezetre érvényes szint, a vizsgálatot követő **90 napon belül cselekvési tervet** kell készíteni.

A Polgári Polgármesteri Hivatal biztonsági osztályba sorolása

a 77/2013. (XII. 19.) NFM rendelet 1. számú melléklete alapján

Az elektronikus információs rendszerek biztonsági osztályba sorolása

- Általános irányelvek
- Az érintett szervezet az elektronikus információs rendszere biztonsági osztályba sorolásakor a bizalmasság, sértetlenség és rendelkezésre állás követelményét a rendszer funkciójára tekintettel, ahhoz igazodó súllyal érvényesíti, így például
    - a nemzeti adatvagyont kezelő rendszerek esetében a sértetlenség követelményét emeli ki;
    - a létfontosságú információs rendszerelemek esetében a rendelkezésre állást követeli meg elsődlegesen;
    - a különleges személyes adatokkal kapcsolatban alapvető igényként fogalmazza meg a bizalmasság fenntartását.
- Az elektronikus információs rendszerek biztonsági osztályba sorolását kockázatelemzés alapján kell elvégezni, amit az érintett szervezet vezetője hagy jóvá. A kockázatelemzés során ajánlott a nemzetközi vagy hazai szabványok, ajánlások, legjobb gyakorlatok figyelembevétele.

- Az adatok és az adott információs rendszer jellegéből kiindulva a kockázatelemezés alapját
    - az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, és az elektronikus információs rendszerelemek sértetlenségének és rendelkezésre állásának sérüléséből, elvesztéséből bekövetkező kár, vagy káros hatás, terjedelme, nagysága;
    - a kár bekövetkezésének, vagy a kárral, káros hatással fenyegető veszély mértéke, becsült valószínűsége képezi.
- A biztonsági osztályba sorolásnál nem a lehetséges legnagyobb kárértéket, hanem a releváns, bekövetkezési valószínűséggel korrigált fenyegetések által okozható kárt, káros hatást kell figyelembe venni.
- Az elektronikus információs rendszerek biztonsági osztályai meghatározásához az alábbi - az érintett szervezetnél szóba jöhető - közvetett, vagy közvetlen kárt okozó hatásokat, veszélyeket és károkat kell - az érintett szervezet jellemzőire tekintettel - figyelembe venni:
    - társadalmi-politikai káros hatásokat, károkat vagy a jogsértésből, kötelezettség elmulasztásából fakadó káros hatásokat, károkat (így pl. alaptevékenységek akadályozása, különösen a létfontosságú információs rendszerelemek működési zavarai, a nemzeti adatvagyon sérülései, jogszabályok és egyéb szabályozások megsértése, jogszabály által védett adatokkal történő visszaélés vagy azok sérülése, a közérdekűség követelményének sérülése, személyiséghez fűződő jogok megsértése, bizalomvesztés hatóságokkal, felügyeleti szervekkel szemben, az ország jogrendjének sérülése, vagy ennek lehetővé tétele);
    - személyeket, csoportokat érintő károk, káros hatások (pl. különleges személyes adatok, banktitkok, üzleti titkok megsértése, szervezet, személyek vagy csoportok jó hírének károsodása, személyi sérülések, vagy haláleset bekövetkeztének - ideértve az elektronikus információs rendszer működésének zavara, vagy információhiány miatt kialakult veszélyhelyzetet - veszélye);
    - közvetlen anyagi károk (az infrastruktúrát, az elektronikus információs rendszert ért károk, és ezek rendelkezésre állásának elvesztése miatti pénzügyi veszteség, adatok sértetlenségének, rendelkezésre állásának elvesztése miatti költségek, dologi kár);
    - közvetett anyagi károk (pl. helyreállítási költségek, elmaradt haszonnal arányos költségek, a környezet biztonságának veszélyeztetése, perköltségek).
- A veszélyeztetettségnek a bekövetkezés valószínűségének megfelelő kárérték szinteknek megfelelő biztonsági osztályba sorolásakor a bizalmasság, sértetlenség és rendelkezésre állás követelménye külön-külön értékelendő.

5. sz. Melléklet - Kárérték-táblázatok

A Hivatal az informatikai, információ biztonságot érintő kockázatok esetében a korábban meghatározott kárértékeket veszi figyelembe, követendőnek. Továbbá a kockázatelemzési eljárásrendben meghatározott szabályok szerint jár el.

Bizalmasság kárérték táblázata

Az informatikai rendszer vagy az abban tárolt adat bizalmasságának sérülése esetén a kár mértéke:

Kárérték szint/Kárfajta	Közvetlen anyagi kár	Társadalmi-politikai hatás	Jogi következmény
2. / csekély kár	1.000.000 Ft-ig	Kínos helyzet a szervezeten belül	Belső szabályozóval védett adat vagy néhány személyes adat bizalmassága sérül

Sértetlenség kárérték táblázata

Az informatikai rendszer vagy az abban tárolt adat pontatlansága esetén a kár mértéke:

Kárérték szint/Kárfajta	Közvetlen anyagi kár	Közvetett anyagi kár	Társadalmi-politikai hatás
2. / csekély kár	1.000.000 Ft-ig	1 embernappal állítható helyre	Kínos helyzet a szervezeten belül

Rendelkezésre állás kárérték táblázata

Az informatikai rendszer vagy az abban tárolt adatok rendelkezésre állásának elvesztése esetén (nem elérhető a rendszer vagy az adat) a kár mértéke:

Kárérték szint/Kárfajta	Közvetlen anyagi kár	Közvetett anyagi kár	Társadalmi-politikai hatás	Szolgáltatási időszak (nap x óra)	Szolgáltatási szint (heti maximum kiesési idő)
2. / csekély kár	1.000.000 Ft-ig	1 embernappal állítható helyre	Kínos helyzet a szervezeten belül	5x8	96,5% hetente 1,5 óra