8/2014. Készült: 1 példányban

Mérk Nagyközség Képviselő-testületének 2014. július 16-én 15^{00} órai kezdettel megtartott ülésének

a.) jegyzőkönyve
b.) 53-58/2014.(VII.16.) határozata

Napirend:

1.Tájékoztató a lejárt határidejű határozatok végrehajtásáról, a két ülés közt végzett munkákról valamint a lakosság szélesebb körét érintő jogszabályokról

2. A szennyvízberuházás helyzetének áttekintése

3. A Széchenyi utcai szükséglakások helyzetének áttekintése

4. Mérki Közös Önkormányzati Hivatal Informatikai Biztonsági Szabályzata

5. Pénzeszköz biztosítása 2014. augusztus 16-án tartandó falunapra

6. Első lakáshoz jutók részére pénzeszköz biztosítása

Mérk, 2014. július 21.

Müller Istvánné
polgármester

Készült: Mérk Nagyközség Képviselő-testületének 2014. július 16-én 15^{00} órai kezdettel megtartott ülésén

Az ülés helye: Községháza Mérk

Jelen vannak: Müller Istvánné polgármester asszony
Haga Dezső, Jónás Ferenc, Magyarics Anita, Böszörményi Jánosné, Aradi Ferenc képviselők
Török László jegyző

Távolmaradását bejelentette: Reszlerné Pásztor Andrea képviselő

Meghívottak: Fülöp Tamás KEVIÉP Kft. Debrecen képviseletében

Müller Istvánné polgármester asszony köszönti a megjelenteket, megállapítja, hogy az ülés határozatképes, mivel a 7 főből 6 fő jelen van. Javaslatot tesz az alábbi napirend megtárgyalására, és jegyzőkönyv hitelesítőnek Magyarics Anita és Aradi Ferenc képviselőket javasolja.

Napirend:

1.Tájékoztató a lejárt határidejű határozatok végrehajtásáról, a két ülés közt végzett munkákról valamint a lakosság szélesebb körét érintő jogszabályokról

2. A szennyvízberuházás helyzetének áttekintése

3. A Széchenyi utcai szükséglakások helyzetének áttekintése

4. Mérki Közös Önkormányzati Hivatal Informatikai Biztonsági Szabályzata

5. Pénzeszköz biztosítása 2014. augusztus 16-án tartandó falunapra

6. Első lakáshoz jutók részére pénzeszköz biztosítása

Ezt követően a képviselő-testület 6 igen szavazattal, ellenszavazat és tartózkodás nélkül a javasolt napirend megtárgyalását, és jegyzőkönyv hitelesítőnek Magyarics Anita és Aradi Ferenc képviselőket elfogadta.

Tárgy / 1. tsp**.** / **Tájékoztató a lejárt határidejű határozatok végrehajtásáról, a két ülés közt végzett munkákról valamint a lakosság szélesebb körét érintő jogszabályokról**

Előadó: Müller Istvánné polgármester asszony

Előterjesztés jegyzőkönyvhöz csatolva.

Kérdés, hozzászólás nem hangzott el, rövid beszélgetést követően a képviselő-testület 6 igen szavazattal, ellenszavazat és tartózkodás nélkül az alábbi határozatot hozta:

Mérk Nagyközség Önkormányzat képviselő-testülete

53/2014 (VII.16.) határozata

A lejárt határidejű határozatok végrehajtásáról, a két ülés végzett munkáról, a lakosság szélesebb körét érintő jogszabályokról

A képviselő-testület!

A lejárt határidejű határozatok végrehajtásáról szóló előterjesztést és a 38-43/2014 (V.27.) és a 44-52/2014 (VI.17.) számú határozatokat végrehajtottá nyilvánítja, a két ülés között végzett munkáról, a lakosság szélesebb körét érintő jogszabályokról szóló tájékozatót tudomásul veszi.

Tárgy /2. tsp./ **A szennyvízberuházás helyzetének áttekintése**

Előadó: Müller Istvánné polgármester asszony

Előterjesztés jegyzőkönyvhöz csatolva.

Müller Istvánné polgármester asszony a településünkön megvalósuló szennyvízberuházás kapcsán tájékoztatja a jelenlévőket az alábbiakról:

Mérken a szennyvízberuházást két kivitelező cég végzi. Az egyik a KEVIÉP Kft. (Debrecen), a másik a KEVÍZ 21 zRt. (Nyíregyháza). A KEVIÉP Vállaj községről indította a beruházást. Mérken az alábbi utcák kiépítését végzi: Hunyadi a csorda kúti lejáróig, József Attila, Kinizsi, Árpád, Dózsa, Rákóczi, Béke, Bem, Bem köz, Ady, Bajcsy, Fenyő, Nefelejcs, Kiss József utca. A KEVÍZ 21 zRt. a szennyvíztelep komplett kivitelezője, de hozzájuk tartozik a Toldi, Wesselényi, Alkotmány, Klapka, Édesanyák, Petőfi, Kossuth, Liget, Mező, Vasvári, Somogyi Béla, Széchenyi, Táncsics utcák. A lakosság részéről nagy az elvárás. Nap mint nap szembesülünk különféle problémákkal, hogy a kivitelezés folyamán vízvezeték, kábel tv vezeték sérül stb. Folyamatosan kapcsolatot tartunk a kivitelezőkkel. Napi szinten folynak az ellenőrzések és a lakossági panaszok intézése.

Fülöp Tamás úr a KEVIÉP képviselője az elhangzottakra reagálva elmondja, hogy valóban egy ilyen nagy volumenű beruházás a kivitelezés során mindig okoz gondot, problémát. Tudni kell azt, hogy Mérken a 70-es években épült meg az ivóvíz rendszer azbeszt pala csővel, maga a rendszer elöregedett. Ebből az elöregedésből adódnak részint problémák, valamint a talajszerkezetből. Sok helyen az utcák szűk keresztmetszete is zavaróan hat a munkavégzésre. Anyagdeponálás, gépekkel való mozgás, közlekedés körülményes. Eddig 9 csőtörésük volt a munkaterületükön. Egy kivitelező céget, akinél 5 esetben fordult elő csőtörés elküldték, szerződést bontottak velük. A csőtörést sok esetben a talajszerkezet összetétele (szürke homok) okozza, a talaj megmozgatását követően a vízvezeték csövek alól a homok elfolyik, nem tart, emiatt következik be a törés. A vízügyesek segítségünkre vannak, az általuk kért technológiát tartva próbáljuk elkerülni ezeket a gondokat. Jó az együttműködés a Tiszamenti Regionális Vízművek Zrt.-vel, akik biztosítják a hibák elhárításához szükséges anyagokat.

A beruházással kapcsolatosan kérdést intézett Jónás Ferenc képviselő úr, Aradi Ferenc képviselő úr, Böszörményi Jánosné képviselő asszony, Török László jegyző úr.

A feltett kérdésre Fülöp Tamás mérnök úr, a KEVIÉP képviselője a kielégítő választ megadta. Kihangsúlyozta a beruházás megkezdése előtt videóval dokumentált helyzetfelmérés történt, a beruházást követően annak megfelelően kell az eredeti állapotot visszaállítani. A visszaállítást részben ők, részben a KEVÍZ 21 Zrt. fogja elvégezni. Azon vannak, hogy ez év október végére a beruházás befejeződjön, és a próbaüzemelés is minél előbb megtörténjen.

Müller Istvánné asszony összefoglalta az elhangzottakat, kihangsúlyozva, hogy az elkövetkezendő napokban a projekt műszaki ellenőrével folyamatos helyszíni bejárásokat fog tartani, hogy a beruházás mindenki megelégedésére jól valósuljon meg. Az itt elhangzott kérdések nem a kivitelezők ellen, hanem a jó munkavégzés megvalósítása érdekében hangoztak el. Kéri, hogy a lakosság tájékoztatása a kivitelezők és PR-os vállalkozók részéről sokkal pontosabban, hatékonyabban történjen meg.

Miután több kérdés, hozzászólás nem hangzott el a képviselő-testület 6 igen szavazattal, ellenszavazat és tartózkodás nélkül az alábbi határozatot hozta:

Mérk Nagyközség Önkormányzata képviselő-testülete

54/2014 (VII.16.) határozata

A szennyvízberuházás helyzetének áttekintéséről

A képviselő-testület!

Áttekintve a szennyvíz beruházás jelenlegi helyzetét, a kivitelezőtől kapott szóbeli tájékoztatás alapján elfogadja, tudomásul veszi.

Felhatalmazza polgármester asszonyt, hogy folyamatosan kísérje figyelemmel a projekt megvalósulását, és ha szükséges intézkedjen a kivitelezők felé a tervszerű pontos munka végzésére.

Tárgy /3.tsp./**A Széchenyi utcai szükséglakások helyzetének áttekintése**

Előadó: Török László jegyző úr

Előterjesztés jegyzőkönyvhöz csatolva.

Török László jegyző úr az előterjesztéssel kapcsolatosan kihangsúlyozza, hogy mindenképpen indokolt a Mérken lévő szükséglakások karbantartása. A Széchenyi utca 13. sz. alatti ikerlakás lelakott állapotban van, födém- és tetőszerkezete annyira sérült, hogy azt gazdaságosan felújítani nem célszerű. Ebben a lakásban lakik Virág Lajos egyedül. A Széchenyi utca 11. sz. alatti lakás (ikerlakás)

még gazdaságosan felújítható a Széchenyi utca 13. sz. alatti házból kinyert anyagokból. Javasolja a felújítást megszervezni és Virág Lajost Széchenyi utca 11. szám alatti lakásba elhelyezni.

Az előterjesztéssel kapcsolatosan kérdés nem hangzott el.

Böszörményi Jánosné képviselő asszony az előterjesztéssel egyetértve kihangsúlyozza, hogy a Széchenyi utca 11. szám alatti lakásban, mivel ott van egy üres lakásrész, Virág Lajos normális körülmények közé elhelyezhető.

Jónás Ferenc képviselő úr Virág Lajos elhelyezését a Széchenyi utca 11 szám alatti szükséglakásba támogatja azzal, hogy a jövőben, aki a szükséglakásban lakik, valamilyen összegű lakbért fizessen.

Rövid beszélgetés követően a képviselő-testület 6 igen szavazattal, ellenszavazat és tartózkodás nélkül az alábbi határozatot hozta:

Mérk Nagyközség Önkormányzata képviselő-testülete

55/2014 (VII.16) határozata

A Széchenyi utcai szükséglakások helyzetének áttekintéséről

A képviselő-testület!

A Mérk, Széchenyi utca 13. szám alatti szükséglakást megszüntetni rendeli. Az ott lakó Virág Lajos-t (Szül.: Mátészalka, 1966.05.21.; Anyja neve: Pintye Anna) az önkormányzat tulajdonát képező Mérk, Széchenyi utca 11. szám alatti lakásba helyezi el. Az elhelyezéssel egy időben a Széchenyi utca 11. szám alatti lakás felújítását biztosítja.

Felhatalmazza jegyző urat, hogy intézkedjen nevezett átköltözésére valamint arra, hogy az eddig ingyenesen használt lakásért az ott lakók bérleti díjat fizessenek.

A bérleti díj összegére a képviselő-testület később intézkedik.

Megbízza polgármester asszonyt, hogy saját hatáskörében intézkedjen a Széchenyi utca 11. szám alatti lakás soron kívüli karbantartására.

Határidő: 2014. december 15.
Felelős: polgármester asszony
jegyző úr

Tárgy /4. tsp./ **Mérki Közös Önkormányzati Hivatal Informatikai Biztonsági Szabályzata**

Előadó: Török László jegyző úr

Előterjesztés jegyzőkönyvhöz csatolva.

Kérdés, hozzászólás nem hangzott el. A képviselő-testület 6 igen szavazattal, ellenszavazat és tartózkodás nélkül az alábbi határozatot hozták:

Mérk Nagyközség Önkormányzatának képviselő-testülete

56/2014 (VII.16) határozata

Mérki Közös Önkormányzati Hivatal Informatikai Biztonsági Szabályzatáról

A képviselő-testület!

Mérki Közös Önkormányzati Hivatal Informatikai Biztonsági Szabályzatát ezen határozathoz csatolt tartalommal tudomásul veszi azzal, hogy annak végleges hatályba lépése 2016. december 31-ig fokozatosan történik meg.

Mellékletek:
Besorolási nyilatkozat
Beszerzési és Karbantartási Szabályzat
Engedélyezési és Jogosultsági Szabályzat
Informatikai Biztonsági Szabályzat
Informatikai Biztonságpolitika
Kockázatkezelési Szabályzat

Besorolási Nyilatkozat

Mérki Közös Önkormányzati Hivatal nyilatkozatban rögzíti, hogy a 2014.07 hó időszakban külsős szakember által egy kockázatértékelés során végzett L_2013 tv. –nek való megfelelés vizsgálatának eredményeként a Hivatal biztonsági szintje:

2-es (azaz kettes) besorolású

Indoklás:

- A szervezet által működtetett és kockázatértékelés során vizsgált elektronikus információs rendszerek egyike sem magasabb a 2-es biztonsági osztálynál.
- Hivatalunkban az elektronikus információs rendszerek biztonságához kapcsolódó eljárások teljes kialakítására törekszünk, de ehhez belső forrásból sem megfelelő szaktudás, sem megfelelő eszközrendszer nem áll még rendelkezésünkre.
- Hivatalunkban az elektronikus információs rendszerek és szolgáltatások nyilvántartása nem teljes körű.
- Hivatalunkban a jogosultságkezelési folyamatok jelenleg nem kellőképpen kidolgozottak.
- Hivatalunkban az adathordozók nyilvántartása, kezelése, törlése nem teljes körű.
- Hivatalunkban az elektronikus információs rendszerek biztonsági felügyelete nem automatizált.
- Hivatalalunkban az elektronikus információs rendszerek előállítanak a biztonságra vonatkozó információkat, de azokat a szervezet nem elemzi.

Mérki Közös Önkormányzati Hivatal

Beszerzési és Karbantartási Szabályzata

Tartalomjegyzék

Általános rendelkezések

A szabályzat célja

Jelen szabályzat a(z) Mérki Közös Önkormányzati Hivatal (továbbiakban: Hivatal) az IT eszközök beszerzése, valamint azok karbantartása során betartandó szabályokról rendelkezik.

A szabályzat hatálya

A szabályzat érvényessége kiterjed a Hivatal valamennyi szervezeti egységére, funkciójára és folyamatára.

Eszköz beszerzések

Általános szabályok

a) Az informatikai eszközök és szoftverek beszerzésénél mindig az Hivatali beszerzésekre vonatkozó szabályok szerint kell eljárni. A beszerzett számítástechnikai eszközöket és szoftvereket nyilvántartásba kell venni.
b) Az IT referens egyeztetve az igénylő osztályok vezetőivel értékeli az igényeket, majd a jegyzővel való egyeztetés után, egy fontossági rangsort alkotva, beruházási igényként betervezik a költségvetésbe. Ha nincs az aktuális költségvetésben forrás a beruházásra, akkor nem tervezett beszerzés történik.
c) Az eszközök rendeltetésszerű használatáért a személyi leltár szerint használatra kijelölt köztisztviselő felelős.

Hardver beszerzés

A beszerzés és üzembe helyezés előtt a Hivatal Informatikai rendszeréhez való illeszthetőségi (kompatibilitási) vizsgálatát el kell végezni. Ezen felül törekedni kell az egységes (homogén) eszközpark kialakítására.

Szoftver beszerzés

A beszerzés és üzembe helyezés előtt a Hivatal Informatikai rendszeréhez való illeszthetőségi (kompatibilitási) vizsgálatát el kell végezni. Ingyenes (freeware) alkalmazások esetén ellenőrizni kell, hogy üzleti jellegű felhasználásra is szabadon használható-e. A szoftverkörnyezet kialakításánál is törekedni kell az egységességre (homogenitásra).

Kellékanyag beszerzés

Az informatikai üzemeltetéshez szükséges irodatechnikai eszközök megfelelő minőségben és mennyiségben történő készletezése a rendszergazdák feladata. Ezekből a kellékekből mindig akkora készlettel kell rendelkezni, mely biztosítja a folyamatos üzletmenetet.

Karbantartások

Általános szabályok

a) a számítástechnikai eszközökön javítást, módosítást, illetve új eszközök telepítését csak a rendszergazdák, vagy az általuk megbízott és ellenőrzött külső vállalkozó végezhet;
b) számítógépek esetében, ha a javítás külső helyszínen történik, az esetleges adattartalmat törölni, az el- és visszaszállítást pedig dokumentálni kell
c) a nem javítható eszközöket a leírtaknak megfelelően selejtezni kell, esetleges adattartalmukat pedig – szükség esetén véglegesen és helyreállíthatatlanul – törölni kell

d) a tervezett karbantartások mértéke és gyakorisága feleljen meg a gyártói előírásoknak és ajánlásoknak, de minimum évente egyszer legyen elvégezve;
e) minél nagyobb mértékben járuljon hozzá a kockázatok (a működési szabályok betartásával) csökkentéséhez, a helyes és rendszeres karbantartottság révén;

Tervezett karbantartások

A Hivatal az eszközparkot az alábbi gyakorisággal tartja (vagy tartatja) karban, melyek elvégezését és eredményét dokumentálja:

Számítógépek és szerverek: évenkénti karbantartás

Számítástechnikai hálózat: évenkénti karbantartás és tesztelés

Nyomtatók és egy eszközök: igény szerinti, de legalább évente

Mérki Közös Önkormányzati Hivatal

Engedélyezési és Jogosultsági Szabályzat

Tartalomjegyzék

Általános rendelkezések

A szabályzat célja

Jelen szabályzat rendelkezik a(z) Mérki Közös Önkormányzati Hivatal (továbbiakban: Hivatal) információs rendszereinek a szerepkörök és jogosultságok tekintetében támasztott elvárásairól, melyeket rendszertechnikailag meg kell valósítani.

A szabályzat hatálya

A szabályzat érvényessége kiterjed a Hivatal valamennyi szervezeti egységére, funkciójára és folyamatára.

A kockázatkezelés céljai

a) a Hivatalnál csak az arra jogosult személyek rendelkezhetnek hozzáféréssel a rendszerekhez és az információkhoz;
b) a vezetőknek és az alkalmazottaknak ismerniük kell a feladatokat és a szükséges jogokat;
c) valamennyi felhasználó személyre szóló felhasználói jogosultságot kell, hogy rendelkezzen;
d) kerülni kell az ellentmondó vagy egymást kioltó jogosultságokat, szerepköröket;
e) a jogosultságok igénylése, engedélyezése, visszavonása dokumentált kell, hogy legyen;

Definíciók

1. *felhasználói fiókok (user accountok):* a felhasználói fiókok a hálózatokon vagy alkalmazásokon belül a felhasználó egyértelmű beazonosítására szolgál. Egy felhasználói fiók több szerepkörhöz is tartozhat.

2. *szerepkörök:* tevékenységeik gyakorlásához a hivatali dolgozóknak feladataiknak megfelelő jogokra van szükségük. A csoportokban összefoglalt jogokat szerepköröknek nevezzük. Ez az összefoglalás csökkenti az operatív IT-kockázatokat és növeli a hatékonyságot a hozzáférési jogok adminisztrációja során

3. *szolgáltatás fiókok (service accountok):* a személyhez nem kötött felhasználó fiókokat szolgáltatás fióknak nevezzük. Elsősorban olyan funkciók és feladatok számára kerülnek bevetésre, amelyek nem igénylik a mindenkori felhasználó interaktív tevékenységét, hanem pl. az IT-rendszerek közötti adatcseréhez szükségesek

Felelősségek

A Hivatal vezetése

a) felelős a kritériumok meghatározásáért
b) kinevezi a fiók felelősöket, tevékenységüket felügyeli
c) dönt a szabályok elfogadásáról és a szükséges intézkedésekről
d) gondoskodik a szabályzás fontosságának tudatosításáról és annak betartatásáról

Az IT referens

a) felelős a jogosultságok kialakításáért és nyilvántartásáért
b) javaslatokat tesz a szabályok módosítására
c) felelős a szükséges oktatások megtartásáért, megtartatásáért
d) kezdeményezi az éves rendszeres felülvizsgálatokat

A munkatársak

Felelős a közzétett, illetve számukra kiadott előírások betartásáért

A fiókkezelés szabályozása

A fiókkezeléssel kapcsolatos elvárások

a) a rendszerek és információk elérése csak sikeres beazonosítást követően válhat lehetővé.
b) minden felhasználónak önálló, személyre szóló fiókot kell kapnia, amely egyértelműen beazonosítható
c) tiltott a más személyek felé, ill. más személyek által történő továbbadás vagy felhasználás
d) a felhasználói fiókokat egységes névkonvenció szerint javasolt létrehozni
e) privilegizált jogosultságokhoz, azaz olyan jogosultságokhoz, amelyek a vállalat szempontjából kritikus adattörzsekhez rendelkeznek hozzáféréssel, vagy amelyek IT-rendszerek rendszer-konfigurációját teszik lehetővé (pl. adminisztrátorok, adatbank-felhasználók vagy fejlesztők), külön felhasználói fiókot kell létesíteni, elkülönítve a normális jogosultságot igénylő feladatokhoz használt fióktól

f) minden szolgáltatás fiókot (service accountot) felelőshöz kell hozzárendelni, aki felelős a szolgáltatás fiók aktualizálásáért és törléséért, jelszavainak rendszeres megváltoztatásáért
g) biztosítani kell, hogy csak feljogosított dolgozók ismerjék a szolgáltatás fiókok (service accountok) jelszavát.
h) valamennyi felhasználói fiókot és annak módosítását dokumentálni kell. Ennek kapcsán figyelembe kell venni az ellenőrzési követelményeket is.

A fiókok elnevezési szabályai (névkonvenció)

A felhasználói fiókokat egyértelműen kell kiadni. Amennyiben technikailag lehetséges, úgy már a felhasználói elnevezésből világosan felismerhetőnek kell lennie, hogy az adott fiók rendelkezik-e privilegizált jogokkal (pl. „gipsz.j_admin“), továbbá az elnevezésből levezethetőnek kell lennie magának a felhasználónak (pl. „gipsz.j“) vagy szolgáltatás fiók esetén a feladatkörnek (pl. "daily_backup") is.

Fiókok létrehozása, módosítása, törlése

A felhasználói fiókok igénylésére, létrehozására és módosítására alkalmas eljárás minden esetben engedélyezési folyamatot tesz szükségessé. Ennek az engedélyezési folyamatnak mindenkor nyomon követhetően dokumentáltnak kell lennie oly módon, hogy vizsgálat esetén rövid időn belül és hiánytalanul igazolásokat lehessen felmutatni.

A felhasználói fiókok igénylését és engedélyezését a területen belül két különböző személynek kell végrehajtania. A felhasználói fiókok kezelése a rendszergazdák felelősségi köréhez tartozik.

Felhasználói fiókot csak olyan személyek részére szabad kiadni, akik elfogadják a Hivatal információbiztonsági szabályait. Az elfogadást írásos úton kell megadni és annak nyomon követően dokumentáltnak kell lennie, amely a szerződés mellékletét képezheti. Ez különösen a külső szolgáltatókra érvényes.

A már nem szükséges fiókokat inaktívvá kell változtatni és három hónap elteltével törölni kell. A törlés csak akkor megengedett, ha az üzlet szempontjából lényeges és megőrzés-köteles adatok ezzel nem mennek veszendőbe és ellenőrzési követelmények ezeket nem tiltják.

A jogosultságok szabályozása

A jogosultságokkal kapcsolatos elvárások

a) RBAC elv (role-based access control), (szerepkörökön alapuló hozzáférési ellenőrzés): a jogosultságokat lehetőleg csak szerepkörökön keresztül adjuk ki és kerüljük az egyéni joghozzárendeléseket. Amennyiben ez nem lehetséges, úgy az eltéréseket külön kell dokumentálni és az alkalmazásukat, valamint szükségességüket rendszeresen kell ellenőrizni.
b) legalacsonyabb privilégium elve: a mindenkori szerepkörhöz mindig csak azon jogosultságok kerülnek kiadásra, amelyekre a szerepkörnek a teljesítendő feladatkörön belül végzett tevékenységhez valóban szüksége van.
c) feladat- és/vagy funkció-szétválasztás elve: a hozzáférési jogok kiadásának a feladat- és/vagy funkció-szétválasztás elve szerint kell megtörténnie, azaz a szakterület részéről szakmailag meghatározott szétválasztásoknak a kiadott és rendszertechnikailag hozzárendelt jogokban kell visszatükröződniük.
d) kerülni kell az egymásnak ellentmondó, ill. egymást kioltó jogosultságokkal rendelkező szerepköröket. Az eltéréseket dokumentálni, indokolni és azokat kivételként engedélyezni kell.

A jogosultságok elnevezési szabályai (névkonvenció)

Valamennyi meghatározott szerepkört és jogosultságot egységes elnevezési szabály szerint kell névvel ellátni, amely szabály a hozzátartozó feladatterületeket és jogokat egyértelműen felismerhetővé teszi. Ez az előírás érvényes a szerepkörök és a jogosultságok rendszertechnikai leképezésére is, amennyiben ez technikailag lehetséges.

A szerepkörök és jogosultságok megváltoztatása

A szerepkörök és jogosultságok változtatását meghatározott eljárás szerint a változáskezelés keretében kell végrehajtani. Ennek során az alábbi folyamatokat kell figyelembe venni:

a) a mindenkori felhasználó belépése az adott feladatkörbe (pl. munkaviszony létesítése, osztályváltás vagy átszervezés következtében).
b) a mindenkori felhasználó kilépése az adott feladatkörből (pl. nyugdíjba vonuláskor, osztályváltás vagy átszervezés következtében).

c) változtatások a feladatkörben, amelyek következményeként változtatások válnak szükségessé a jogosultságokban, vagy amelyek következményeként jogosultságok kerülnek megszüntetésre.

A személyzeti osztálynak és a szakterületnek kell funkciójuk keretében valamennyi személyi változást és a jogosultságok ebből eredő változásait a felelős adminisztrátorok felé a jogosultságok minél korábbi illesztése érdekében közvetlenül lejelenteni.

Ennek során főként azt kell biztosítani, hogy a már nem szükséges jogosultságok rövid időn belül bevonásra kerüljenek, azaz amint azokra a mindenkori feladatkörön belüli teljesítéshez már nincs szükség.

A szerepkörök és jogosultságok ellenőrzése

Valamennyi szerepkört és kiadott jogosultságot legalább évente egy alkalommal kell felülvizsgálni. Az osztályvezetők kötelesek meggyőződni a meghonosított szerepkörök megfelelőségéről, a szerepkörök hozzárendelésének megfelelőségéről és esetleg a felhasználók járulékos egyéni jogosultságainak helyességéről. Az eltéréseket jelenteni kell az IT referensnek.

Egyéb rendelkezések

Fiókok és jogosultságok dokumentálása

A rendszergazdák a felhasználókról és jogosultságaikról nyilvántartást vezet, mely tartalmazza:

a) a jogosult nevét, szervezeti egységét
b) a jogosultság tárgyát vagy a szerepkört
c) a jogosultság időtartamát (ha szükséges)

Egyéb biztonsági követelmények, ajánlások

a) az információbiztonság garantálása céljából valamennyi hozzáférési kísérletet naplózni kell
b) többszöri sikertelen bejelentkezési kísérletet követően az érintett fiókot automatikusan zárolni kell (a zárolás feloldásának módja lehet automatikus, vagy manuális is)
c) az inaktív munkameneteket meghatározott idő után zárolni kell, vagy meg kell szakítani
d) minden szolgáltatás esetében törekedni kell a központosított hitelesítésre (pl. LDAP)
e) törekedés a 4 szem-elvre: a jogosultságok engedélyezése és azok rendszertechnikai felvétele legalább +1 fő ellenőrzése mellett történjen meg

Általános korlátozások

Az információs rendszer nem használható az alábbi tevékenységekre:

a) az érvényes magyar jogszabályokba ütköző cselekmények, mint pl.: a szerzői jogok megsértése; szoftverek szándékos és tudatos illegális használata, terjesztése, stb.
b) haszonszerzést célzó, közvetlen üzleti célú tevékenység, reklámok terjesztése
c) az információs rendszer, illetve erőforrásai szabályos működését megzavaró, veszélyeztető, vagy erőforrásait pazarló tevékenységek, mint pl.: kéretlen levelek, elektronikus játékok, stb.
d) az információs rendszer erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére irányuló bármilyen tevékenység
e) vallási, etnikai, politikai, erkölcsi vagy más jellegű érzékenységet sértő, másokra nézve sértő, esetleg másokat zaklató tevékenység (pl. szélsőséges nézeteket képviselő, fajgyűlölő, vagy pornográf anyagok megtekintése, tárolása, közzététele vagy továbbítása)

Mérki Közös Önkormányzati Hivatal

Informatikai Biztonsági Szabályzat

Tartalomjegyzék

1.1 Az Informatikai Biztonsági Szabályzat

Az állami és a hivatali szervek elektronikus biztonságáról szóló 2013 évi L Tv. 15. § (1) bekezdés d) pontjában az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII tv. 24 § (3) bekezdésében, valamint a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992 évi LXVI 30. § (1) bekezdésében kapott felhatalmazás alapján

a(z) Mérki Közös Önkormányzati Hivatal (továbbiakban: Hivatal) informatikai biztonsági szabályzatát az alábbiakban határozza meg.

a) meghatározza a célokat, a szabályzat tárgyi és személyi (a Hivatal jellegétől függően területi) hatályát,
b) az elektronikus információbiztonsággal kapcsolatos szerepköröket,
c) a szerepkörökhöz rendelt tevékenységeket,
d) a tevékenységekhez kapcsolódó felelősségeket,
e) az információbiztonság hivatalrendszerének belső együttműködését

Az Informatikai Biztonsági Szabályzat összhangban van a Hivatal minőségirányítási rendszerét leíró dokumentumokkal.

1.1.1 A dokumentum célja

A szabályzat célja, hogy az adatbiztonság érvényesítése, az egyes szoftverekhez való hozzáférési jogok meghatározása, az ellenőrzési mechanizmusok meghatározása, a felelősségi viszonyok tisztázása, az egyes adatkezelő műveletek részletezése az adatvédelmi és az iratkezelési szabályzattal, illetve a vonatkozó jogszabályi előírásokkal összhangban történjen.

1.1.2 A dokumentum hatálya

A szabályzat tárgyi hatálya kiterjed a Hivatal tevékenysége során keletkezett, kezelt, feldolgozott, tárolt adatokra és információkra, a számítástechnikai eszközökre, dokumentációikra, és az azokat körülvevő környezetre, valamint a szoftverekre, adatbázisokra, a kapcsolódó dokumentációkra és az adatbiztonsági nyilvántartásokra.

A szabályzat személyi hatálya kiterjed a Hivatal köztisztviselőire, ügykezelőire, munkavállalóira, illetve egyéb munkavégzésre irányuló, egyéb jogviszonyban álló személyekre, továbbá a választott képviselőkre és a Hivatallal szerződéses kapcsolatban álló vállalkozóira és azok alkalmazottaira.

1.1.3 Alapfogalmak

1. *adat:* az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;

2. *adatfeldolgozás:* az adatkezeléshez kapcsolódó technikai feladatok elvégzése;

3. *adatfeldolgozó:* az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az adatkezelő részére adatfeldolgozást végez;

4. *adatkezelés:* az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása;

5. *adatkezelő:* az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az adatkezelést végzi;

6. *adminisztratív védelem:* a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;

7. *auditálás:* előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;

8. *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;

9. *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;

10. *biztonsági esemény kezelése:* az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;

11. *biztonsági osztály:* az elektronikus információs rendszer védelmének elvárt erőssége;

12. *biztonsági osztályba sorolás:* a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;

13. *biztonsági szint:* a Hivatal felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

14. *biztonsági szintbe sorolás:* a Hivatal felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

15. *elektronikus információs rendszer 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;

16. *életciklus:* az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;

17. *észlelés:* a biztonsági esemény bekövetkezésének felismerése;

18. *felhasználó:* egy adott elektronikus információs rendszert igénybe vevők köre;

19. *fenyegetés:* olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

20. *fizikai védelem:* a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;

21. *folytonos védelem:* az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;

22. *globális kibertér:* a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese;

23. *informatikai biztonságpolitika:* a biztonsági célok, alapelvek és a Hivatal vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására;

24. *informatikai biztonsági stratégia:* az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere;

25. *információ:* bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;

26. *kiberbiztonság:* a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez;

27. *kibervédelem:* a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését;

28. *kockázat:* a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;

29. *kockázatelemzés:* az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

30. *kockázatkezelés:* az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;

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

32. *korai figyelmeztetés:* valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;

33. *létfontosságú információs rendszerelem:* az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené;

34. *logikai védelem:* az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;

35. *magyar kibertér:* a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne;

36. *megelőzés:* a fenyegetés hatása bekövetkezésének elkerülése;

37. *reagálás:* a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;

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

39. *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;

40. *sérülékenység:* az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

41. *sérülékenység vizsgálat:* az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;

42. *számítógépes incidenskezelő központ:* az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott hivatalokban tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)];

43. *Hivatal:* az adatkezelést vagy adatfeldolgozást végző jogi személy, valamint jogi személyiséggel nem rendelkező gazdasági társaság, egyéni vállalkozó;

44. *teljes körű védelem:* az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;

45. *üzemeltető:* az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság agy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

46. *védelmi feladatok:* megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;

47. *zárt célú elektronikus információs rendszer:* jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer;

48. *zárt védelem:* az összes számításba vehető fenyegetést figyelembe vevő védelem.

1.1.4 Szerepkörök

A Polgármesteri hivatal a részletes hivatali szerepköröket a Szervezeti és Működési Szabályzatban rögzítette.

Polgármesteri hivatal (képviselő testület, jegyző, polgármester): az Informatikabiztonsági feladatokkal kapcsolatban kitűzi a célokat, programokat, stratégiát, politikát határoz meg, felügyeli ezek megvalósulását, forrást biztosít a megvalósításokhoz.

Informatikai referens: az informatikabiztonsággal kapcsolatban szervezi, és szakmai kompetenciájának megfelelően végrehajtja a Polgármesteri hivatal által meghatározott politikát, célokat, stratégiát. Kapcsolatot tart és felügyeli a feladatok végrehajtásával megbízott személyt, vagy személyeket.

Informatikabiztonsági felelős- az a szakember, aki szakmailag kompetens és ellátja az informatikabiztonsággal kapcsolatos törvényi feladatokat.

Beosztottak, alkalmazottak, köztisztviselők: végrehajtják és betartják az utasításokat, szabályokat. Magatartásukkal segítik a hatékony és biztonságos informatikabiztonság megteremtését.

1.1.5 Tevékenységek

A polgármesteri hivatal a tv.-ben meghatározott alaptevékenységét a Szervezeti és Működési Szabályzatban rögzítette.

1.1.6 Hivatalrendszer belső együttműködése

A polgármesteri hivatal a belső együttműködését a Szervezeti és Működési Szabályzatban rögzítette.

2.1 Besorolási Nyilatkozat

Mérki Közös Önkormányzati Hivatal nyilatkozatban rögzíti, hogy a 2014.07 hó időszakban külsős szakember által egy kockázatértékelés során végzett L_2013 tv. –nek való megfelelés vizsgálatának eredményeként a Hivatal biztonsági szintje:

2-es (azaz kettes) besorolású

Indoklás:

- A szervezet által működtetett és kockázatértékelés során vizsgált elektronikus információs rendszerek egyike sem magasabb a 2-es biztonsági osztálynál.
- Hivatalunkban az elektronikus információs rendszerek biztonságához kapcsolódó eljárások teljes kialakítására törekszünk, de ehhez belső forrásból sem megfelelő szaktudás, sem megfelelő eszközrendszer nem áll még rendelkezésünkre.
- Hivatalunkban az elektronikus információs rendszerek és szolgáltatások nyilvántartása nem teljes körű.
- Hivatalunkban a jogosultságkezelési folyamatok jelenleg nem kellőképpen kidolgozottak.
- Hivatalunkban az adathordozók nyilvántartása, kezelése, törlése nem teljes körű.
- Hivatalunkban az elektronikus információs rendszerek biztonsági felügyelete nem automatizált.

- Hivatalalunkban az elektronikus információs rendszerek előállítanak a biztonságra vonatkozó információkat, de azokat a szervezet nem elemzi.

Az informatikai biztonsági szabályzat elsősorban a következő, az érvényes rendeletben meghatározott elektronikus információs rendszerbiztonsággal kapcsolatos területeket szabályozza:

Adminisztratív Védelmi Intézkedések

Szervezeti szintű alapfeladatok

Informatikai biztonságpolitika

A Hivatal megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonságpolitikát. Az informatikai biztonságpolitikát a Hivatal vezető testülete hagyja jóvá.

A Hivatal vezető testülete a biztonságpolitikában kiberbiztonsági célokat határoz meg, felállítja az informatikai biztonságpolitika hivatali szempontú alapelveit, bemutatja az érintett hivatal vezető beosztású tagjainak elkötelezettségét a biztonsági feladatok irányítására és támogatására, kifejti az érintett hivatalban alkalmazott biztonsági alapelveket és megfelelőségi követelményeket. Az informatikai biztonságpolitikát szükség szerint, de legalább évente egyszer az informatika biztonsági rendszer felülvizsgálata során (belső audit) a Hivatal felülvizsgálja, szükség szerint módosítja. Az informatikabiztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor a biztonságpolitikát újra vizsgálja, szükség szerinti módosítja.

A Hivatal a részletes informatikai biztonságpolitikát egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(Informatikai Biztonságpolitika)* kezeli.

Informatikai biztonsági stratégia

A Hivatal megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonsági stratégiát. Az informatikai biztonsági stratégiát a Hivatal vezető testülete hagyja jóvá.

A Hivatal vezető testülete az informatikai biztonsági stratégiában a rövid, közép és hosszú távú célokat határozza meg. Az informatikai biztonsági stratégia illeszkedik az érintett hivatal más stratégiáihoz (így különösen az informatikai biztonságpolitikához, a költségvetési és humánerőforrás tervezéshez, valamint a tevékenységi kör változásához, fejlesztéshez), jövőképéhez. Az informatikai biztonsági stratégiát szükség szerint, de legalább évente egyszer az informatika biztonsági rendszer felülvizsgálata során (belső audit) a Hivatal felülvizsgálja, szükség szerint módosítja. Az informatikabiztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor az informatikai biztonsági stratégiát újra vizsgálja, szükség szerinti módosítja.

A Hivatal a részletes informatikai biztonsági stratégiát egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(Informatikai Biztonsági Stratégia)* kezeli.

Informatikai biztonsági szabályzat

A Hivatal megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonsági szabályzatát. Az informatikai biztonsági szabályzat a Hivatal, vezető testülete hagyja jóvá.

Az informatikai biztonsági szabályzatát szükség szerint, de legalább évente egyszer az informatika biztonsági rendszer felülvizsgálata során (belső audit) a Hivatal felülvizsgálja, szükség szerint módosítja. Az informatikabiztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor az informatikai biztonsági szabályzatot újra vizsgálja, szükség szerinti módosítja. A Hivatal az „informatikai biztonsági jelentésben” rögzíti az érintett hivatal elvárt biztonsági szintjét, valamint az érintett hivatal egyes elektronikus információs rendszereinek elvárt biztonsági osztályát.

A Hivatal a részletes informatikai biztonsági szabályzat egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(Informatikai Biztonsági Szabályzat)* kezeli.

Az elektronikus információs rendszerek biztonságáért felelős személy

A Hivatal vezetője az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg (külsős alvállalkozó), aki: ellátja az állami és hivatali szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott feladatokat. A Hivatal vezetője gondoskodik (alvállalkozó esetén szerződésben elvárja) a biztonságért felelős személy képzettségéről az idevonatkozó rendeletnek megfelelően.

Pénzügyi erőforrások biztosítása

A Hivatal vezetése a költségvetés tervezése és a beruházások, beszerzések során az ide vonatkozó törvényben meghatározott határidőkkel tervezi az informatikai biztonsági stratégia megvalósításához szükséges forrásokat. Intézkedik a terveknek megfelelő kiadásokhoz szükséges erőforrások rendelkezésre állásáról. Dokumentálja e követelmény alá eső kivételeket.

Intézkedési terv és mérföldkövei

A Hivatal vezetése intézkedési tervet készít az elektronikus információbiztonsági stratégia megvalósításához az ide vonatkozó törvényben meghatározott határidőkkel, és ebben mérföldköveket határoz meg. Az így elkészített intézkedési tervet meghatározott időnként felülvizsgálja és karbantartja a kockázatkezelési stratégia és a kockázatokra adott válaszok, tevékenységek prioritása alapján. Ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál (belső vagy külső vizsgálat során) hiányosságot állapítanak meg, vagy a meghatározott biztonsági szint alacsonyabb, mint az érintett hivatalra érvényes szint, akkor a Hivatal vezetése a vizsgálatot követő 90 napon belül felülvizsgálatot készít a hiányosság megszüntetése érdekében.

A Hivatal a részéletes intézkedési tervet egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(Informatikai Biztonsági Stratégia)* kezeli.

Az elektronikus információs rendszerek nyilvántartása

A Hivatal az elektronikus információs rendszereiről, minden rendszerre nézve nyilvántartást vezet, azt szükség szerint aktualizálja. A nyilvántartás tartalmazza:

a) a rendszerek alapfeladatait;
b) a rendszerek által biztosítandó szolgáltatásokat;
c) az érintett rendszerekhez tartozó licenc számot (amennyiben azok az érintett Hivatal kezelésében vannak);
d) a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;
e) a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

A Hivatal az elektronikus rendszerek nyilvántartását egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(Elektronikus Információs Rendszerelem Leltár)* kezeli.

3.1.1.10 Kockázatkezelési stratégia

A Hivatal vezetése megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a kockázatkezelési stratégiát. A kockázatkezelési stratégiát szükség szerint, de legalább évente egyszer az informatika biztonsági rendszer felülvizsgálata során (belső audit) a Hivatal felülvizsgálja, szükség szerint módosítja. Az informatikabiztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor a kockázatkezelési stratégiát újra vizsgálja, szükség szerinti módosítja.

A stratégia kiterjed:

a) a lehetséges kockázatok felmérésére;
b) a kockázatok kezelésének felelősségére;
c) a kockázatok kezelésének elvárt minőségére.

A Hivatal a részéletes kockázatkezelési stratégiát és módszertant egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(Kockázatkezelési Szabályzat)* kezeli.

3.1.1.11 Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

A Hivatal vezetése megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési eljárási folyamatokat. Felügyeli az elektronikus információs rendszer és környezet biztonsági állapotát, meghatározza az információbiztonsággal összefüggő szerepköröket és felelősségeket, kijelöli az ezeket betöltő személyeket, integrálja az elektronikus információbiztonsági engedélyezési folyamatokat a Hivatali szintű kockázatkezelési eljárásba, összhangban az informatikai biztonsági szabályzattal.

Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, az érintett Hivatal hatókörébe tartozó:

a) emberi, fizikai és logikai erőforrásra,
b) eljárási és védelmi szintre és folyamatra

A Hivatal az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárást egy külön dokumentumban *(Engedélyezési és Jogosultsági Szabályzat)* kezeli.

3.1.2 Kockázatelemzés

3.1.2.1 Kockázatelemzési eljárásrend

A Hivatal vezetése megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a kockázatelemzési eljárásrendet, mely a kockázatelemzési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő.

A Hivatal a részletes kockázatkezelési eljárást és módszertant egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(Kockázatkezelési szabályzat)* kezeli.

3.1.2.2 Biztonsági osztályba sorolás

A Hivatal jogszabályban meghatározott szempontok alapján megvizsgálja (alvállalkozó igénybevétele esetén megvizsgáltatja) elektronikus információs rendszereit, és a 3.1.1.7 pont szerinti nyilvántartás alapján meghatározza, hogy azok melyik biztonsági osztályba sorolandók.

A Hivatal vezetése jóváhagyja a biztonsági osztályba sorolást, és dokumentumban *(Informatikai Biztonsági Szabályzat)* rögzíti annak eredményét.

A biztonsági osztályba sorolást az elektronikus információs rendszereket érintő változások után ismételten elvégzi.

3.1.2.3 Kockázatelemzés

A Hivatal végrehajtja a biztonsági kockázatelemzéseket és rögzíti azok eredményét *(a NEIH módszertani segédletben)*. A kockázatkezelési szabályzatnak megfelelően felülvizsgálja a kockázatelemzések eredményét és megismerteti a kockázatelemzés eredményét az érintettekkel.

Amikor változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát, ismételt kockázatelemzést hajt végre a Hivatal.

A Hivatal gondoskodik arról, hogy a kockázatelemzési eredmények a jogosulatlanok számára ne legyenek hozzáférhetőek, megismerhetőek. A kockázatelemzési eredményeket bizalmasan kezeli.

3.1.3 Tervezés

3.1.3.1 Biztonságtervezési eljárásrend

Biztonságtervezési szempontból a Hivatal az alábbi időszakokat definiálja az információs rendszerek életciklusának tekintetében:

a) követelmény meghatározás;

b) fejlesztés vagy beszerzés;
c) megvalósítás vagy értékelés;
d) üzemeltetés és fenntartás;
e) kivonás (archiválás, megsemmisítés).

A rendszerbiztonság tervezésekor a Hivatal az információs rendszerek valamennyi életciklusára vonatkozóan szem előtt tartja az Informatikai Biztonságpolitikában megfogalmazott célokat és követelményeket, valamint a gyártói és iparági előírásokat, ajánlásokat.

3.1.3.2 Rendszerbiztonsági terv

A Hivatal vezetése az elektronikus információs rendszereihez rendszerbiztonsági tervet készíttet, amely:

a) összhangban áll az Informatikai Biztonságpolitikával és a Biztonságtervezési Eljárásrenddel, valamint igazodik a szervezet felépítéséhez és architektúrájához,
b) meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait (biztosítandó szolgáltatásait és azok elvárt szolgáltatási szintjeit [angolul SLA]), biztonságkritikus elemeit és alapfunkcióit;
c) meghatározza az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát;
d) meghatározza az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;
e) a vonatkozó rendszerdokumentáció keretébe foglalja az elektronikus információs rendszer biztonsági követelményeit (naplózás, mentés és helyreállítás, üzletmenet-folytonosság);
f) meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és azok bővítését, végrehajtja a jogszabály szerinti biztonsági feladatokat;
g) gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is);
h) belső szabályozásában, vagy a rendszerbiztonsági tervben meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszer rendszerbiztonsági tervét (belső audit);
i) frissíti a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások, és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;
j) elvégzi a szükséges belső egyeztetéseket;
k) gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

3.1.3.2.1 Kivételek

Ha egy adott információs rendszer jelentősége nem indokolja, vagy a különböző jogi, szabályozási, vagy üzemeltetési körülmények nem teszik lehetővé, a Hivatal vezetése eltekint a rendszerbiztonsági terv megkövetelésétől.

3.1.3.3 Személyi biztonság

A Hivatal:

a) megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat a rájuk vonatkozó szabályokat, felelősségüket az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet;
b) Az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja;
c) meghatározott gyakorisággal felülvizsgálja és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat a rájuk vonatkozó szabályokat, felelősségüket az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet a viselkedési szabályok betartását;
d) gondoskodik arról, hogy a c) pont szerinti változás esetén a hozzáféréssel rendelkezők tekintetében a b) pont szerinti eljárás megtörténjen;
e) meghatározza az érintett szervezeten kívüli irányban megvalósuló követelményeket;

A Hivatal az elektronikus információbiztonsággal kapcsolatos engedélyezési és hozzáférési szabályokat egy külön dokumentumban *(Engedélyezési és jogosultsági szabályzat)* kezeli.

3.1.3.3.2 Viselkedési szabályok az interneten

A Hivatal:

a) tiltja és számon kéri a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét;
b) tiltja a belső szabályzatában meghatározott, interneten megvalósuló tevékenységeket (pl.: chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták, stb.);
c) tilthatja a közösségi oldalak használatát, magánpostafiók elérését, és más, a Hivataltól idegen tevékenységet.

A Hivatal az elektronikus információbiztonsággal kapcsolatos engedélyezési és hozzáférési szabályokat egy külön dokumentumban *(Engedélyezési és jogosultsági szabályzat)* kezeli.

3.1.4 Rendszer és szolgáltatás beszerzés

3.1.4.2 Beszerzési eljárásrend

A Hivatal vezetése megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a beszerzési eljárásrendet *(Beszerzési és karbantartási szabályzat)*, mely az érintett Hivatal elektronikus információs rendszerére, az ezekhez kapcsolódó szolgáltatások és információs rendszer biztonsági eszközök beszerzésére vonatkozó szabályait fogalmazza meg és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő. A szabályzatot a szükséges mértékben és meghatározott gyakorisággal felülvizsgálja.

3.1.4.4 A rendszer fejlesztési életciklusa

A Hivatal az elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri informatikai biztonsági helyzetüket.

A Hivatal a fejlesztési életciklus egészére meghatározza és dokumentáltatja az információbiztonsági szerepköröket és felelősségeket.

A Hivatal meghatározza és a Hivatalra érvényes szabályok szerint kijelöli az információbiztonsági szerepköröket betöltő, felelős személyeket.

3.1.4.4.2 A rendszer életciklus szakaszai a következők:

a) követelmény meghatározás;
b) fejlesztés vagy beszerzés;
c) megvalósítás vagy értékelés;
d) üzemeltetés és fenntartás;
e) kivonás (archiválás, megsemmisítés).

3.1.4.8 Külső elektronikus információs rendszerek szolgáltatásai

A Hivatal:

a) szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek az érintett Hivatal elektronikus információbiztonsági követelményeinek;
b) meghatározza és dokumentáltatja az érintett Hivatal felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban;
c) külső és belső ellenőrzési eszközökkel ellenőrizteti, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

3.1.6 Emberi tényezőket figyelembe vevő – személy – biztonság

3.1.6.5 Eljárás jogviszony megszűnésekor

A Hivatal:

a) megszünteti, vagy visszaveszi a személy egyéni hitelesítő eszközeit;
b) tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető a jogviszony megszűnése után is fennálló kötelezettségekről;

c) visszaveszi az érintett hivatal elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt;
d) megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és a Hivatali információkhoz;
e) az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket;
f) a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik;
g) a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzi.

3.1.6.8 Fegyelmi intézkedések

A Hivatal fenntartja magának a jogot, hogy a jelen IBSZ-t megsértőkkel szemben eljárjon. Az eljárást a Hivatal jegyzője vagy az IT referens kezdeményezheti. A kezdeményezést a Hivatal vezetője felülvizsgálja, a szükséges intézkedéseket elrendelheti. Az IBSZ megsértése esetén az intézmény megvonhatja a hálózat, illetve a gépek használatának jogát határozott időre, vagy határozatlan időre, visszavonásig.

Ha az IBSZ megsértése kismértékű, vagy nem tekinthető szándékosnak, akkor az elkövetőt írásban figyelmeztetni kell. A figyelmeztetés utáni ismételt elkövetést szándékosnak kell tekinteni. Különösen súlyos esetben, illetve szándékosság esetén a rendszergazdák a használati jogot megvonhatják és az IBSZ megsértője a teljes információs rendszerből kitiltható. Ha szükséges, az intézmény fegyelmi eljárást, polgári jogi pert is indíthat. Amennyiben az elkövetett vétség a Büntető Törvénykönyv szerint bűncselekménynek minősül, a Hivatal vezetője köteles a szabályszegővel szemben feljelentést tenni, és a rendelkezésre álló bizonyítékokat az eljáró hatóságok részére átadni.

3.1.7 Tudatosság és képzés

3.1.7.1 Képzési eljárásrend

A Hivatal rendszeres képzésben részesíti az információs rendszer felhasználóit. A képzések gyakoriságát az információs rendszerek változásainak és egyéb igényeknek a figyelembevételével kell meghatározni, de évente legalább egyszer továbbképzésen kell részt vennie minden munkavállalónak. A szervezetbe újonnan belépő munkavállalókat a lehető leghamarabb alapképzésben kell részesíteni.

A Hivatal vezetése:

a) felelős a képzési kritériumok meghatározásáért
b) biztosítja a képzéshez a szükséges erőforrásokat
c) gondoskodik a képzések fontosságának tudatosításáról a teljes szervezetben

Az IT referens:

a) felelős a képzési rendszer kialakításáért, fenntartásáért
b) felelős a szükséges oktatások megtartásáért, megtartatásáért

A munkatársak:

a) felelősek a képzési előírások betartásáért, a képzések során leadott anyagok elsajátításáért

3.1.7.2 Biztonságtudatossági képzés

A Hivatal annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára:

a) az új felhasználók kezdeti képzésének részeként;
b) amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
c) a Hivatal vezetése által meghatározott gyakorisággal, de minimum évente egyszer

Fizikai Védelmi Intézkedések

3.2.1 Fizikai és környezeti védelem

3.2.1.2 Fizikai védelmi eljárásrend

A Hivatal azon helyiségeibe, ahol információs rendszerek (pl. szerverek) vagy rendszerelemek (pl. számítógépek) találhatóak, vagy ahonnan bármilyen jellegű hozzáférés lehetséges a rendszerekhez vagy rendszerelemekhez, csak az arra jogosultak léphetnek be, meghatározott szabályok szerint.

A szabályok és korlátozások nem vonatkoznak a létesítmény bárki által szabadon látogatható vagy igénybe vehető helyiségeire.

3.2.1.3 Fizikai belépési engedélyek

A Hivatal:

a) összeállítja, jóváhagyja és kezeli az elektronikus információs rendszereknek helyt adó létesítményekbe belépésre jogosultak listáját;
b) a belépési jogosultságot igazoló dokumentumokat (pl. kitűzők, azonosító kártyák, intelligens kártyák) bocsát ki a belépéshez a belépni szándékozó részére;
c) rendszeresen felülvizsgálja a belépésre jogosult személyek listáját;
d) eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése nem indokolt;
e) intézkedik a b) pont szerinti dokumentumok visszavonása, érvénytelenítése, törlése, megsemmisítése iránt.

3.2.1.4 A fizikai belépés ellenőrzése

A Hivatal:

a) kizárólag a szervezet által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést;
b) naplózza a fizikai belépéseket;
c) ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;
d) kíséri a létesítménybe ad-hoc belépésre jogosultakat és figyelemmel követi a tevékenységüket;
e) megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközt;
f) nyilvántartást vezet a fizikai belépést ellenőrző eszközről;
g) meghatározott rendszerességgel változtatja meg a hozzáférési kódokat és kulcsokat, vagy azonnal, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az adott személy elveszti a belépési jogosultságát;
h) az egyéni belépési engedélyeket a belépési pontokon ellenőrzi;
i) a kijelölt pontokon való átjutást felügyeli a szervezet által meghatározott fizikai belépést ellenőrző rendszerrel, vagy eszközzel;
j) felhívja a szervezet tagjainak figyelmét a rendellenességek jelentésére.

Logikai Védelmi Intézkedések

3.3.1 Konfigurációkezelés

3.3.1.1 Konfigurációkezelési eljárásrend

A konfigurációkezelés célja az informatikai infrastruktúra adatainak kézben tartása, az egyes komponensek beazonosítása, figyelemmel követése és karbantartása. A szolgáltatásokról, a szoftver és hardver konfigurációkról és azok dokumentációjáról központilag tárol információkat így segíti az incidensfelügyeletet, problémakezelést, változáskezelést és a verziókövetést.

3.3.1.2 Alapkonfiguráció

Azon információs rendszereknél, ahol indokolt és technikailag lehetséges, a Hivatal egy-egy alapkonfigurációt fejleszt ki, dokumentáltatja és karbantartatja azt, valamint leltárba foglalja a rendszer lényeges elemeit.

3.3.1.8 Elektronikus információs rendszerelem leltár

A Hivatal leltárt készít az elektronikus információs rendszer elemeiről, amit naprakészen tart annak érdekében, hogy:

a) pontosan tükrözze az elektronikus információs rendszer aktuális állapotát,
b) az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet, valamint azok licenceit tartalmazza;
c) legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez.

3.3.1.10 A szoftverhasználat korlátozásai

A Hivatal:

a) kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi, vagy más jogszabályoknak;
b) a másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát;
c) ellenőrzi és dokumentálja az állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

A Hivatal az elektronikus információbiztonsággal, rendszer- és szoftverhasználattal kapcsolatos szabályait egy külön dokumentumban *(Engedélyezési és jogosultsági szabályzat)* kezeli.

3.3.1.11 A felhasználó által telepített szoftverek

A Hivatal információs rendszereire, valamint azok számítógépeire és egyéb komponenseire csak a rendszergazdák telepíthetnek szoftvereket, valamint azok rendszerszintű beállításait is csak ők (vagy az általuk megbízott külsős szakértők) jogosultak megváltoztatni.

3.3.2 Üzletmenet- (ügymenet-) folytonosság tervezése

3.3.2.1 Üzletmenet-folytonosságra vonatkozó eljárásrend

Az információk védelmének és a megfelelő rendelkezésre állásának biztosítása érdekében a Hivatal az alábbi elvárásokat fogalmazza meg az üzletmenet-folytonossági tervekkel szemben:

a) biztosítsák, hogy a kockázatok esetleges bekövetkezésekor a szolgáltatás kiesés ne legyen nagyobb a tervezetnél (ne sérüljön az SLA);
b) adjanak megfelelő alapot a kockázatok csökkentésére irányuló hatékony intézkedések végrehajtásához és eredményességük nyomon követéséhez;
c) határozzák meg azokat az intézkedéseket, amelyek ahhoz szükségesek, hogy a Hivatal folyamatos működése biztosítva legyen;
d) határozzák meg azokat az intézkedéseket, feladatokat, melyeket az esetleges folytonosság megszakadásra felkészülésként, illetve bekövetkezésekor a kár enyhítéseként, illetve a helyreállításért kell tenni;
e) biztosítsák, hogy az üzletmenet-folytonosság és a szolgáltatások rendelkezésre állása személyes felelősséghez köthető legyen;
f) illeszkedjenek a Hivatal közép és hosszú távú stratégiáihoz és céljaihoz;

3.3.2.2 Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

A Hivatal vezetése által az elektronikus információs rendszerekhez készíttetett rendszerbiztonsági terveknek tartalmazniuk kell az adott elektronikus rendszer (szolgáltatás) üzletmenet-folytonossági tervét is, amely:

a) összhangban áll az Informatikai Biztonságpolitikával és a Biztonságtervezési Eljárásrenddel, valamint igazodik a szervezet felépítéséhez és architektúrájához;
b) összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;
c) meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági tervet;
d) az elektronikus információs rendszer vagy a működtetési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálja az üzletmenet-folytonossági tervet;
e) tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, személyeket és Hivatali egységeket;

f) gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható;
g) meghatározza az alapfeladatokat (a biztosítandó szolgáltatásokat és azok elvárt szolgáltatási szintjét [angolul SLA]) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;
h) rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről;
i) jelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket;
j) fenntartja a Hivatal által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is;
k) kidolgozza a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

A Hivatal az elektronikus információbiztonsággal kapcsolatos üzletmenet-folytonossági terveket rendszerenként külön dokumentumban *(Rendszerbiztonsági terv)* és mellékleteiben kezeli.

3.3.2.8 Az elektronikus információs rendszer mentései

A Hivatal a rendszerbiztonsági és üzletmenet-folytonossági elvárásokkal összhangban:

a) meghatározott gyakorisággal mentést végez az elektronikus információs rendszerben tárolt felhasználószintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;
b) meghatározott gyakorisággal elmenti az elektronikus információs rendszerben tárolt rendszerszintű információkat, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;
c) meghatározott gyakorisággal elmenti az elektronikus információs rendszer dokumentációját, köztük a biztonságra vonatkozókat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;
d) megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen.

A Hivatal az információs rendszerek mentésével kapcsolatos elvárásait (mentések gyakorisága a tolerálható adatvesztés függvényében, elvárt helyreállítási idő, megőrzési idő, offsite példányok, stb.) rendszerenként külön dokumentumban *(Rendszerbiztonsági terv)* és mellékleteiben kezeli.

3.3.2.9 Az elektronikus információs rendszer helyreállítása és újraindítása

A Hivatal gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

A Hivatal az elektronikus információbiztonsággal kapcsolatos helyreállítási szabályokat, valamint az elektronikus információs rendszer helyreállításának, újraindításának menetét az érintett rendszerre vonatkozó dokumentumban *(Rendszerbiztonsági terv)* és mellékleteiben kezeli.

3.3.3 Karbantartás

3.3.3.1 Rendszer karbantartási eljárásrend

A Hivatal vezetése megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a rendszer karbantartási eljárásrendet, mely a rendszer karbantartási kezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

A Hivatal az elektronikus információbiztonsággal kapcsolatos karbantartási szabályokat egy külön dokumentumban *(Beszerzési és Karbantartási Szabályzat)* kezeli.

3.3.3.2 Rendszeres karbantartás

A Hivatal által megbízott személyek vagy vállalkozók:

a) a karbantartásokat és javításokat ütemezetten hajtatja végre, dokumentáltatja és felülvizsgáltatja a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a Hivatal követelményeinek megfelelően;
b) jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;
c) az ezért felelős személyek jóváhagyásához köti az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a Hivatali létesítményből;

d) az elszállítás előtt minden adatot és információt – mentést követően – töröl a berendezésről;
e) ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;
f) csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási nyilvántartáshoz.

A Hivatal az elektronikus információbiztonsággal kapcsolatos karbantartási szabályokat egy külön dokumentumban *(Beszerzési és Karbantartási Szabályzat)* kezeli.

3.3.4 Adathordozók védelme

3.3.4.1 Adathordozók védelmére vonatkozó eljárásrend

Az adathordózónak minősülő olyan eszközök (pl. floppy, CD, USB eszközök, külső merevlemezek, stb.) kezelésének általános irányelvei:

a) minél nagyobb mértékben járuljon hozzá az adathordozók kezeléséből eredő kockázatok csökkentéséhez;
b) tegye lehetővé valamennyi, a tevékenységet érintő adathordozók kezelésével kapcsolatos fenyegető esemény azonosítását;

3.3.4.2 Hozzáférés az adathordozókhoz

A Hivatal dokumentálja az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, valamint jogosítványuk tartalmát, időtartamát.

3.3.4.6 Adathordozók törlése

A Hivatal a helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törli az elektronikus információs rendszer meghatározott adathordozóit a leselejtezés, a hivatali ellenőrzés megszűnte, vagy újrafelhasználásra való kibocsátás előtt. A törlési mechanizmusokat az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően alkalmazza.

3.3.4.7 Adathordozók használata

A Hivatal engedélyezi az adathordozók használatát, és dokumentálja az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, valamint jogosítványuk tartalmát, időtartamát.

3.3.5 Azonosítás és hitelesítés

3.3.5.1 Azonosítási és hitelesítési eljárásrend

A Hivatal vezetése megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az azonosítási és hitelesítésre vonatkozó eljárásrendet, mely az azonosítási és hitelesítési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

A Hivatal az elektronikus információbiztonsággal kapcsolatos engedélyezési és hozzáférési szabályokat egy külön dokumentumban *(Engedélyezési és jogosultsági szabályzat)* kezeli.

3.3.5.2 Azonosítás és hitelesítés (szervezeten belüli felhasználók)

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a Hivatal felhasználóit, a felhasználók által végzett tevékenységet.

3.3.5.4 Azonosító kezelés

A Hivatal:

a) az egyéni-, csoport-, szerepkör- vagy eszközazonosítók kijelölését a Hivatal által meghatározott személyek vagy szerepkörök jogosultságához köti;
b) hozzárendeli az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz vagy eszközhöz;
c) meghatározott időtartamig megakadályozza az azonosítók ismételt felhasználását;
d) meghatározott időtartamú inaktivitás esetén letiltja az azonosítót.

3.3.5.5 A hitelesítésre szolgáló eszközök kezelése

A Hivatal vezetése által kijelölt személy:

a) ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát;
b) meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;
c) biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;
d) dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket;
e) megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során;
f) meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;
g) a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket;
h) megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;
i) megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;
j) lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

3.3.5.6 A hitelesítésre szolgáló eszköz visszacsatolása

Az elektronikus információs rendszer fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

3.3.5.8 Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

A szervezet jelenleg egyik rendszeréhez sem biztosít hozzáférést külső felhasználók számára.

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti az érintett hivatalon kívüli felhasználókat és tevékenységüket.

3.3.5.8.2 Hitelesítés szolgáltatók tanúsítványának elfogadása

Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat fogadhatja el az érintett szervezeten kívüli felhasználók hitelesítéséhez.

3.3.6 Hozzáférés ellenőrzése

3.3.6.1 Hozzáférés ellenőrzési eljárásrend

A Hivatal vezetése megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a hozzáférés ellenőrzési eljárásrendet, mely a hozzáférés ellenőrzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

A Hivatal az elektronikus információbiztonsággal kapcsolatos engedélyezési és hozzáférési szabályokat egy külön dokumentumban *(Engedélyezési és jogosultsági szabályzat)* kezeli.

3.3.6.2 Felhasználói fiókok kezelése

A Hivatal:

a) meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait és ezek típusait;
b) kijelöli a felhasználói fiókok fiókkezelőit;
c) kialakítja a csoport- és szerepkör tagsági feltételeket;
d) meghatározza az elektronikus információs rendszer jogosult felhasználóit, a csoport- és szerepkör tagságot és a hozzáférési jogosultságokat, valamint (szükség esetén) az egyes felhasználói fiókok további jellemzőit;
e) létrehozza, engedélyezi, módosítja, letiltja és eltávolítja a felhasználói fiókokat a meghatározott eljárásokkal vagy feltételekkel összhangban;
f) ellenőrzi a felhasználói fiókok használatát;

…értesíti a fiókkezelőket, ha:

a) a felhasználói fiókokra már nincsen szükség;
b) a felhasználók kiléptek vagy áthelyezésre kerültek;
c) az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak;

…feljogosít az elektronikus információs rendszerhez való hozzáférésre:

a) az érvényes hozzáférési engedély,
b) a tervezett rendszerhasználat,
c) az alapfeladatok és funkcióik alapján;

A Hivatal meghatározott gyakorisággal felülvizsgálja a felhasználói fiókokat, a fiókkezelési követelményekkel való összhangot.

A megbízott személy kialakít egy folyamatot a megosztott vagy csoport felhasználói fiókokhoz tartozó hitelesítő eszközök, adatok újra kibocsátására (ha ilyet alkalmaznak), a csoport tagjainak változása esetére.

3.3.6.3 Hozzáférés ellenőrzés érvényesítése

Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

3.3.6.12 Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

Nincsenek olyan felhasználói tevékenységek, melyeket az elektronikus információs rendszerben azonosítás vagy hitelesítés nélkül végre lehetne hajtani.

3.3.6.16 Külső elektronikus információs rendszerek használata

A Hivatal meghatározza, hogy:

a) milyen feltételek és szabályok betartása mellett jogosult a felhasználó egy külső rendszerből hozzáférni az elektronikus információs rendszerhez;
b) külső elektronikus információs rendszerek segítségével hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani a Hivatal által ellenőrzött információkat.

3.3.6.18 Nyilvánosan elérhető tartalom

A Hivatal:

a) kijelöli azokat a személyeket, akik jogosultak a nyilvánosan hozzáférhető elektronikus információs rendszeren az érintett Hivataltól kapcsolatos bármely információ közzétételére;
b) a kijelölt személyeket képzésben részesíti annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat;
c) közzététel előtt átvizsgálja a javasolt tartalmat;
d) meghatározott gyakorisággal átvizsgálja a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a nem nyilvános információk tekintetében és eltávolítja azokat.

3.3.7 Rendszer- és információsértetlenség

3.3.7.2 Rendszer- és információsértetlenségére vonatkozó eljárásrend

A rendszer- és információsértetlenség megvalósítása során a Hivatal az informatikai biztonságpolitikában meghatározott célok és követelmények szerint jár el, valamint alkalmazza a biztonságtervezési eljárásrendben foglaltakat.

A fentieken túlmenően – de azokkal összhangban – a Hivatal az alábbi követelményeket fogalmazza meg a rendszerek és információk sértetlenségének megőrzése érdekében:

3.3.7.3 Hibajavítás

A Hivatal:

a) azonosítja, belső eljárásrendje alapján jelenti és kijavítja, vagy kijavíttatja az elektronikus információs rendszer hibáit;

b) telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket a szervezet feladatellátásának hatékonysága, az előre nem látható következmények szempontjából;
c) a biztonságkritikus szoftvereket frissítésük kiadását követő 1 hónapon belül telepíti, vagy telepítteti;
d) beépíti a hibajavítást a konfigurációkezelési folyamatba.

3.3.7.4 Kártékony kódok elleni védelem

A Hivatal:

a) az elektronikus információs rendszerét annak belépési és kilépési pontjain védi a kártékony kódok ellen, felderíti és megsemmisíti azokat.
b) frissíti a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg;

…konfigurálja a kártékony kódok elleni védelmi mechanizmusokat úgy, hogy a védelem eszköze:

a) rendszeres ellenőrzéseket hajt végre az elektronikus információs rendszeren és végrehajtja a külső forrásokból származó fájlok valós idejű ellenőrzését a végpontokon a hálózati belépési, vagy kilépési pontokon a biztonsági szabályzatnak megfelelően, amikor a fájlokat letöltik, megnyitják, vagy elindítják;
b) a kártékony kód észlelése esetén blokkolja vagy karanténba helyezi azt; és riassza a rendszeradminisztrátort és az érintett Hivatal által meghatározott további személy(eke)t;
c) ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az elektronikus információs rendszer rendelkezésre állására.

3.3.7.5 Az elektronikus információs rendszer felügyelete

A Hivatal:

a) felügyeli az elektronikus információs rendszert, hogy észlelje a kibertámadásokat, vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat;
b) azonosítja az elektronikus információs rendszer jogosulatlan használatát;
c) felügyeleti eszközöket alkalmaz a meghatározott alapvető információk gyűjtésére és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére;
d) védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;
e) erősíti az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel;
f) meghatározott gyakorisággal biztosítja az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek.

3.3.7.6 A kimeneti információ kezelése és megőrzése

A Hivatal az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

3.3.8 Naplózás és elszámoltathatóság

3.3.8.1 Naplózási eljárásrend

A Hivatal az elektronikus információbiztonsággal kapcsolatos naplózási szabályokat rendszerenként külön dokumentumban *(Rendszerbiztonsági terv)* és mellékleteiben határozza meg, az alábbi általános követelmények figyelembevételével:

3.3.8.2 Naplózható események

A Hivatal az érintett elektronikus információs rendszerre vonatkozó rendszerbiztonsági tervben:

a) meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét.
b) egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő Hivatali egységgel, hogy növelje a kölcsönös támogatást, és hogy iránymutatással segítse a naplózható események kiválasztását;
c) megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

3.3.8.3 Naplóbejegyzések tartalma

Az elektronikus információs rendszer a naplóbejegyzésekből gyűjt elegendő információt ahhoz, hogy ki lehessen mutatni, milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

3.3.8.8 Időbélyegek

Az elektronikus információs rendszer belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához. Időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz – úgynevezett UTC – vagy a Greenwichi középidőhöz – úgynevezett GMT – rendelhető módon, megfelelve a Hivatal által meghatározott időmérési pontosságnak.

3.3.8.9 A napló információk védelme

Az elektronikus információs rendszer megvédi a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

3.3.8.11 A naplóbejegyzések megőrzése

A Hivatal a naplóbejegyzéseket meghatározott – a jogszabályi és az érintett szervezeten belüli információ megőrzési követelményeknek megfelelő – időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

3.3.8.12 Naplógenerálás

Az elektronikus információs rendszer:

a) biztosítja a naplóbejegyzés generálási lehetőségét a 3.3.8.2 pontban meghatározott, naplózható eseményekre;
b) lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire;
c) naplóbejegyzéseket állít elő a 3.3.8.2 pont szerinti eseményekre, a 3.3.8.3 pontban meghatározott tartalommal.

3.3.9 Rendszer- és kommunikációvédelem

3.3.9.1 Rendszer- és kommunikációvédelmi eljárásrend

A rendszer- és kommunikációvédelem megvalósítása során a Hivatal az informatikai biztonságpolitikában meghatározott célok és követelmények szerint jár el, valamint alkalmazza a biztonságtervezési eljárásrendben foglaltakat.

A fentieken túlmenően – de azokkal összhangban – a Hivatal az alábbi követelményeket fogalmazza meg a rendszer- és kommunikációvédelem érdekében:

3.3.9.6 A határok védelme

Az elektronikus információs rendszer:

a) felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt;
b) a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a Hivatal belső hálózatától;
c) csak a Hivatal biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

3.3.9.10 Kriptográfiai kulcs előállítása és kezelése

A Hivatal előállítja és kezeli az elektronikus információs rendszerben alkalmazott kriptográfiához szükséges kriptográfiai kulcsokat a kulcsok előállítására, szétosztására, tárolására, hozzáférésére és megsemmisítésére vonatkozó belső szabályozásnak megfelelően.

3.3.9.11 Kriptográfiai védelem

Az elektronikus információs rendszer szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg.

3.3.9.12 Együttműködésen alapuló számítástechnikai eszközök

Az elektronikus információs rendszer meggátolja az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha az érintett Hivatal engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a személyeknek, akik fizikailag jelen vannak az eszköznél.

Mérki Közös Önkormányzati Hivatal

Informatikai Biztonságpolitika

Tartalomjegyzék

Általános rendelkezések

Az intézkedés célja

a) Az Informatikai Biztonságpolitika (a továbbiakban: IBP) a Hivatal vezetésének akaratnyilvánítása a szervezet informatikai rendszerei által kezelt információs vagyon bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzésére és fenntartására irányuló intézkedések bevezetésére, megfelelés a 2013. évi L. törvénynek (az állami és önkormányzati szervek elektronikus információbiztonságáról).

b) 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, továbbá az elektronikus információs rendszerek rendszer működtetői és a felhasználók számára a napi rendeltetésszerű tevékenységük gyakorlásához.

Az intézkedés hatálya

a) Mérki Közös Önkormányzati Hivatal (a továbbiakban: Hivatal). valamint a Szervezeti és Működési Szabályzat szerinti szervezeteire.

b) A Hivatal és szervezetei valamennyi vezetőjére, ügyintézőjére, a rendszerek felhasználóira, üzemeltetőire.

c) A Hivatallal és szervezeteivel külső, megbízásos (szerződéses) eseti munkakapcsolatban lévő személyekre is, amelyeknek érvényesülését a fenti szerződések tartalmának megfelelő kialakításával kell biztosítani.

d) A Hivatal és szervezetei által használt valamennyi informatikai rendszerre, amely felhasználja, feldolgozza, illetve felügyeli, ellenőrzi a keletkező, illetve felhasznált adatokat, információkat.

Informatikai Biztonságpolitikával kapcsolatos alapelvek

Információvédelem területei

A 77_2013 (XII.19.) NFM rendeletben megfogalmazott elvárásoknak azon fejezetei, amelyek kielégítik a Hivatalra vonatkozó biztonsági osztályba sorolási szintet.

Az Informatikai Biztonságpolitika a Hivatal szolgálatában

a) A Hivatal és szervezetei kezelésében, valamint felügyeletében működő és ezeket az intézményeket kiszolgáló kommunikációs és informatikai rendszereket az adatok titkosságára, bizalmas jellégére és biztonságára vonatkozó törvényeknek megfelelően kell üzemeltetni.

b) Az informatikai rendszerekben adatot, információt és egyéb szellemi tulajdont az intézmény számára jelentkező értékével arányosan kell védeni az illetéktelen betekintéstől, a módosítástól, a sérüléstől, megsemmisüléstől és a nyilvánosságra kerüléstől. A védelemnek biztosítani kell az informatikai rendszer megbízható működését fenyegető káresemények elhárítását, illetve hatásuk minimalizálását a megadott biztonsági követelmények szintjén. A biztonsági szabályok megsértése esetén az IBP hatálya alá eső személyekkel szemben felelősségre vonási eljárást kell kezdeményezni.

c) 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 Biztonságpolitika helye az informatikai biztonsággal foglalkozó dokumentumok rendszerében

a) A Hivatal és szervezeteinek vezetői az informatikai rendszerek, illetve rendszerelemek teljes életciklusára, az informatikai biztonság elviselhető kockázati szinten tartása érdekében kialakítják (szükség szerint külső segítség igénybevételével) az informatikai biztonsági dokumentációs rendszert.

b) A Hivatal és szervezetei informatikai biztonságával kapcsolatos szabályokat és elvárásokat az informatikai biztonsági dokumentációs rendszer tartalmazza, úgymint:

- törvényi előírások és egyéb jogszabályok,
- biztonsági iránylevek, eljárások,
- az Informatikai Biztonságpolitika,
- az Informatikai Biztonsági Szabályzat,
- alsóbb szintű informatikai biztonsági szabályzatok, eljárásrendek
- rendszerbiztonsági tervek (üzletmenet-folytonosság, mentés, naplózás)
- biztonsági nyilvántartások, sémák, tervek, vázlatrajzok, űrlapok.

c) Az informatikai biztonsági feladatok végrehajtásához szükséges feltételek megteremtését az informatikai biztonsági stratégiában szerepeltetni kell.

A biztonságpolitikai alapelvek és védelmi célkitűzések

A Hivatal és szervezetei az informatikai biztonság területén az alábbi alapelveket és védelmi célkitűzéseket kívánják következetesen érvényesíteni:

a) Bizalmasság biztosítása a Hivatal és szervezetei 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.

b) Sértetlenség biztosítása a Hivatal és szervezetei teljes adatvagyonára vonatkozóan az adatkezelés, adattárolás és a kommunikáció során.

c) A Hivatalnál és szervezeteinél történő adatkezelések és feldolgozások során követelmény, hogy a pontos és helyes információkat dolgozzák fel, az adatok sértetlenségét megőrizzék a feldolgozás előtt, közben és után.

d) Rendelkezésre állás fenntartása elsősorban a Hivatal és szervezetei adatvagyonára vonatkozóan, amelyet biztosítani kell mind a külső, mind pedig a belső adatkérések során.

e) Működőképesség fenntartása a Hivatal és szervezetei 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 és technikai feltételeket.

Tartalmi követelmények

A Hivatal és szervezeteinek vezető beosztású tagjainak elkötelezettsége

a) A Hivatal és szervezetei önállóan alakítják ki informatikai biztonsági szabályrendszerüket, azonban ezen szabályok nem mondhatnak ellent a vonatkozó törvényi előírásoknak és az Informatikai Biztonsági Politikájának.

b) A Hivatal megfogalmazza az Informatikai Biztonsági Szabályzat, és további kötelezően előírt szabályzatok készítésének alapelveit, amely alapelvek alapján a hivatal és az intézmények elkészítik saját informatikai biztonsági szabályzatukat a saját, működő rendszerük tekintetében.

c) A Hivatal és szervezetei 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.

A Hivatal és szervezetei informatikai biztonságának területeire vonatkozó alapelvek és követelmények

Az adminisztratív és fizikai védelemi feladatok tekintetében

a) A Hivatal a rendeletnek megfelelően kialakítja az elvárt dokumentációs rendszert, köztük a politikát, célokat és terveket alkot, és olyan nyilvántartásokat vezet be és tart fenn, amely alapja egy pontos és helyes szakmai kockázatelvű vizsgálatnak.

b) Kockázatelemzést véges a veszélyek, fenyegetettségek feltérképezésére és az intézkedések sorrendjének gazdasági megalapozására.

c) Terveket alkot az elvégzendő feladatok követésére.

d) Felügyeli a rendszer és szolgáltatás beszerzését, engedélyezését.

e) 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.

f) Informatikai biztonsági szervezet informatikai biztonsági tervezése, alapkövetelményeinek lefektetése, bevezetése és ellenőrzése a szervezet vezetőinek a feladata.

A vezetők igénybe vehetnek biztonsági szakértőket annak érdekében, hogy megfelelő információkkal rendelkezzenek a szervezetük informatikai biztonsági helyzetéről. A szakértők feladata továbbá, hogy gondoskodjanak a különböző szabványok és ajánlások alkalmazásáról. A vezetők igénybe vehetik a szakértőket a biztonsági események kivizsgálása és értékelése során is.

g) Személyekre vonatkozó biztonsági megállapításoknál a Hivatal és szervezeteinél az informatikai biztonsági követelmények és annak betartásának követelményeit a dolgozóval ismertetni kell, ezért az Informatikai Biztonsági Szabályzatban részletesen szabályozni kell a következő területeket:

- informatikai funkciók meghatározása,
- munkavállalókkal szembeni követelmények,
- titoktartási nyilatkozatok.

h) Illetéktelen hozzáférés megakadályozása, továbbá a Hivatalnál és szervezeteinél az infrastrukturális elemek (pl.: kábelhálózat, szerverszobák) kialakítása során figyelembe kell venni az Informatikai Biztonsági Szabályzatban meghatározott szempontokat is.

i) Az informatikai rendszer környezeti feltételeinek biztosítása.

Az informatikai rendszerek külső környezeti hatásoktól való védelme úgy, 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 klimatizálás, a tűz- és villámvédelem biztosítására is.

j) Adminisztratív védelem aktualizálása, karbantartása úgy, hogy az informatikai rendszerben bekövetkezett változásokat és alkalmazott problémakezelési eljárásokat (tervezés, létrehozás, üzemeltetés-karbantartás, megszüntetés) dokumentált formában, a szabályozó előírásoknak megfelelően kell végezni.

Az informatikai biztonsági dokumentációs rendszer aktualitásának fenntartása érdekében a rendszerben található 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.

k) Oktatás, képzés és a biztonságtudatosság fokozása

A Hivatal és szervezetei az informatikai biztonsági dokumentációs rendszerben foglaltaknak megfelelően. Ennek érdekében fontosnak tekintjük az informatikai biztonsági képzést, oktatást, az informatikai biztonság tudatosítását.

A biztonsági követelmények maradéktalan teljesülése érdekében oktatást, képzést kell biztosítani minden informatikai szereplő számára az informatikai biztonságtudatosságának fejlesztésével kapcsolatban, valamint a rendszerek üzemeltetéséhez és rendeltetésszerű használatához szükséges biztonsági követelmények elsajátítása érdekében.

A logikai védelemi feladatok tekintetében

a) Számítógép-hálózati biztonságánál a Hivatal és szervezetei az informatikai rendszereiket logikai, technikai és adminisztratív eszközökkel védik a külső kapcsolatok, egyéb szervezetek és az Internet felől érkező támadások ellen.

b) Hozzáférés szabályozás

A Hivatalnál és szervezeteinél 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 életciklusán keresztül kell érvényesíteni. (Az új felhasználók felvételétől, a felhasználó kilépéskor történő jogosultságainak megszüntetéséig.)

c) Adattovábbítás elektronikus úton a bizalmas tranzakciók adatainak cseréje a jogszabályokban meghatározottak szerint csak megbízható csatornákon történhet.

A bizalmas információk közé tartoznak a biztonsági eljárásokhoz kapcsolódó információk, a bizalmas tranzakciók adatai, a jelszavak és a kriptográfiai kulcsok. Ezek továbbítására a hagyományos eljárási rend, illetve elektronikus úton való továbbításukhoz megbízható csatornák kialakítására van szükség, amely a különböző felhasználók és a rendszerek, valamint a különböző rendszerek közötti rejtjelezéssel valósítható meg.

d) 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.

Az informatikai rendszer üzemeltetése során biztosítani kell a kezelt adatok, információk rendszeres biztonsági mentését. Rendszeres visszaállítási teszteket kell végezni és mindezeket dokumentálni kell.

A Hivatalnál és szervezeteinél megfelelő eljárásokat kell kidolgozni az adathordozók kezelésére, tárolására, nyilvántartására, annak rendszeres, naprakész aktualizálására, valamint ezek megsemmisüléstől és illetéktelen hozzáféréstől történő védelmére. Az eljárások kidolgozásának célja, az ügymenet folytonosságának fenntartása és a szervezet vagyonának megóvása.

Az adathordozók elhelyezése során biztosítani kell, hogy az elhelyezés feltételei megfeleljenek az adatok, információk biztonsági osztályba sorolási modelljében meghatározott követelményeknek.

e) Szoftverkezelés biztonságánál a Hivatal és szervezetei informatikai rendszereiben kizárólag jogtiszta, az üzemeltetéshez, adatfeldolgozáshoz szükséges, engedélyezett alapprogramok, irodai szoftvercsomagok és feldolgozó programok futtathatók.

f) Rosszindulatú szoftverek elleni védekezés

A szoftverek és informatikai rendszerek sebezhetőek a rendszerbe bejutó rosszindulatú szoftverek (vírusok, trójai falovak) által.

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

Egyéb feladatok tekintetében

a) 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 (üzletmenet-folytonosság).

Le kell vonni a bekövetkezett katasztrófák következményeit, vizsgálni kell a szolgáltatások kiesését és a biztonság sérülését.

b) Informatikai biztonsági események észlelése és kezelése

A Hivatalnak és szervezeteinek 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.

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

Az informatikai biztonság terén a védekezés szempontjából fontos, hogy a korábban történt informatikai biztonsági eseményeket időben visszamenőleg tételesen, minden technikai körülményükkel együtt fel lehessen dolgozni (naplózás).

c) 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.

Mérki Közös Önkormányzati Hivatal

Kockázatkezelési Szabályzat

Tartalomjegyzék

Általános rendelkezések

A szabályzat célja

Jelen szabályzat a(z) Mérki Közös Önkormányzati Hivatal (továbbiakban: Hivatal) információbiztonsági céljait támogatja az információk, eszközök és folyamatok védelmének értékként történő felmérése, vizsgálata és értékelésének biztosítása érdekében

A szabályzat hatálya

A kockázatkezelési szabályzat érvényessége kiterjed a Hivatal valamennyi szervezeti egységére, funkciójára és folyamatára.

A kockázatkezelés céljai

f) megfelelően teljesítse a Hivatal 2013_L tv.-ben meghatározott elvárásokat;
g) minél nagyobb mértékben járuljon hozzá a kockázatok (bekövetkezési valószínűségük és/vagy hatásuk) csökkentéséhez;
h) illeszkedjen a közép-, illetve a hosszabb távú a Hivatal által meghatározott stratégiai és folyamat célok rendszeréhez;
i) tegye lehetővé valamennyi, a célok elérését fenyegető releváns kockázat azonosítását;
j) biztosítsa a kockázatok egységes értékelését;
k) vegye figyelembe mindazokat a kockázati tényezőket, melyeket az elvégzett belső, illetve külső ellenőrzések során már feltártak;
l) megfelelő alapot adjon a kockázatokkal arányos kontrollok azonosításához, megtervezéséhez, értékeléséhez, bevezetéséhez, működtetéséhez és ellenőrzéséhez;
m) tegye lehetővé a kockázatokban és kontrollokban bekövetkező változások nyomon követését, a kockázatok és kontrollok újraértékelését;
n) adjon megfelelő alapot a magas kockázatok csökkentésére irányuló hatékony intézkedések időbeni meghozatalához, végrehajtásához és eredményességük nyomon követéséhez;
o) a kockázatkezelés személyes felelősséghez köthető legyen;

Alapfogalmak

1. *kockázat:* mindazon események, amelyek bekövetkezése negatív hatással lehet a szervezet által kitűzött célok elérésére

2. *kockázat azonosítás, elemzés:* az információ módszeres felhasználása a kockázat forrásának azonosítására és a kockázatbecslésre

3. *kockázat értékelés:* a becsült kockázat és az adott kockázati kritérium összehasonlításának folyamata a kockázat jelentőségének meghatározására

4. *kockázat felmérés:* a kockázatelemzés és kockázatértékelés átfogó folyamata

5. *kockázat kezelése:* folyamat az intézkedések kiválasztására és végrehajtására a kockázat csökkentése érdekében

6. *információs rendszer:* olyan elektronikus rendszer, amely a Hivatal alaptevékenységeit hivatott támogatni és/vagy kritikus adatokat kezel (fogad, tárol, feldolgoz vagy továbbít)

Felelősségek

A Hivatal vezetése

e) felelős a kockázatkezelési rendszer(ek) kialakításáért, működtetéséért
f) felelős a kockázatkezelési kritériumok azonosításáért
g) kinevezi a kockázatfelmérésért felelősöket, tevékenységüket felügyeli
h) gondoskodik a kockázatkezelési irányelvek betartásáról
i) biztosítja a kockázatfelméréshez és –kezeléshez a szükséges erőforrásokat
j) dönt a kockázatfelmérés elfogadásáról, kockázatok elfogadásáról, az elfogadható kockázati szintről, a szükséges intézkedésekről, figyelemmel kísérési feladatokról
k) gondoskodik a kockázatkezelés fontosságának tudatosításáról a teljes szervezetben

A kockázatfelmérésért felelős

A működési és az informatikavédelmi kockázatfelmérésért a jogszabályban meghatározott képzettséggel, tapasztalattal rendelkező belső vagy külső (megbízott) a felelős. (Az IT referens kapcsolattartóként felügyeli és ellenőrzi a munkáját.) Felelősségi köre:

a) felelős a kockázat-felmérési módszertan (ok) kialakításáért, jóváhagyatásáért
b) kezdeményezi az éves rendszeres felmérés indítását
c) koordinálja a kockázat-felmérési tevékenységeket
d) javaslatokat tesz kockázatkezelési, javítási intézkedésekre
e) gondoskodik a kockázatkezelési intézkedések, kontrollok szabályozásokba, dokumentációs rendszerbe illesztéséről
f) rendszeresen tájékoztatja az IT referensen keresztül a Hivatal vezetését a kockázati szint alakulásáról, bekövetkezett kockázati eseményekről
g) felelős a szükséges oktatások megtartásáért, megtartatásáért

Az IT referens

e) a kockázatfelmérésért felelős segítségével azonosítja, felméri, értékeli a területére vonatkozó kockázatokat
f) javaslatot tesz a magas kockázatok kezelésére a saját területére vonatkozóan
g) intézkedik a saját hatáskörükben kezelhető kockázatok csökkentésére, kezelésére
h) felelős a területére eső kockázatok figyelemmel kíséréséért, kezeléséért
i) a kockázatok változása, újak felmerülése esetén aktualizálja a felmérést, tájékoztatja a kockázatfelmérésért felelőst

A munkatársak

a) felelősek a közzétett, kiadott kockázatkezelési előírások betartásáért
b) feladatuk a nem kezelt, illetve az új vagy változó kockázatok jelzése közvetlen vezetőjüknek és/vagy a kockázatfelmérésért felelősnek.

A végrehajtás szabályai

A kockázatok kezelésének folyamata

A kockázat-felmérési módszertan és a kockázatmenedzsment rendszer kialakítása során figyelembe vettük a vonatkozó jogszabályok (77_2013 (XII.19.) NFM rendelet), szabványok és a kapcsolódó útmutatók előírásait.

A kockázatok azonosítása, felmérése

A kockázatok azonosítása és felmérése információs rendszerenként történik, a Hivatal szolgáltatás katalógusa vagy információs rendszerelem leltárja alapján. (Amennyiben ilyen dokumentációk nem állnak rendelkezésre, az információs rendszerek egyedileg kerülnek meghatározásra az IT referens által.)

A kockázatok értékelése

A kockázatok értékelése a vonatkozó jogszabályok (77_2013 (XII.19.) NFM rendelet) alapján, a valószínűsíthető káresemény (közvetett és közvetlen) nagysága és annak a szervezetre gyakorolt, becsült hatása alapján történik.

A kockázatok kezelése

A Hivatal a feltárt kockázatokra a vonatkozó jogszabályban (77_2013 (XII.19.) NFM rendelet) meghatározott biztonsági intézkedések mielőbbi megvalósításával reagál.

A megvalósítandó biztonsági intézkedéseket, és azok megvalósításának sorrendjét a kívánt biztonsági osztály (biztonsági szint) elérésére megalkotott Intézkedési Tervben kell meghatározni.

Tárgy /5. tsp./ **Pénzeszköz biztosítása 2014. augusztus 16-án tartandó falunapra**

Előadó: Müller Istvánné polgármester asszony

Előterjesztés jegyzőkönyvhöz csatolva.

Kérdés nem hangzott el.

Aradi Ferenc képviselő úr egyetért az előterjesztővel, a Kinizsi Erőemelő SE nevében felajánlja segítségüket a rendezvény sikeres végrehajtásához.
Jónás Ferenc képviselő úr szintén támogatja a falunap megszervezését. Véleménye, hogy a színpadra elfogadható áron kell fellépőket szerződtetni, ugyanakkor a szokásos tűzijáték is legyen része a programnak.
Müller Istvánné polgármester asszony összefoglalja az elhangzottakat és javasolja, hogy augusztus 16-án legyen megtartva a mérki sportpályán a falunap, amelyre 1.000.000 –Ft-ot javasol elkülöníteni, mivel belépőjegy árusítását nem támogatja, hogy a településen élők közül minél többen részt vehessenek a rendezvényen. Miután több hozzászólás nem hangzott el, a képviselő-testület 6 igen szavazattal, ellenszavazat és tartózkodás nélkül az alábbi határozatot hozta:

Mérk Nagyközség Önkormányzata képviselő-testületének

57/2014 (VII.16.) határozata

Pénzeszköz biztosításáról 2014. augusztus 16-án tartandó falunapra

A képviselő-testület!

2014. augusztus 16-án a mérki sportpályán falunapot tart.
A falunapra 1.000.000 –Ft pénzeszközt biztosít.
Megbízza a Művelődési Ház munkatársát a falunap megszervezésével.

Felkéri jegyző urat, hogy ezen pénzeszköz átvezetéséről rendeleti úton gondoskodjon.

Felelős: polgármester asszony
jegyző úr
Határidő: augusztus 16.

Tárgy /6.tsp./ **Első lakáshoz jutók részére pénzeszköz biztosítása**

Előadó: Török László jegyző úr

Előterjesztés jegyzőkönyvhöz csatolva.

Kérdés nem hangzott el.

Müller Istvánné polgármester asszony javasolja, hogy kerüljön visszaállításra az első lakáshoz jutók támogatása. E célra erre az évre 300.000 –Ft-ot javasol felhasználni.

Jónás Ferenc javasolja visszaállítani ezen támogatási formát egyúttal javasolja, hogy az idősebb generáció is részesülhessen ebből a támogatási formából.

Miután több kérdés, hozzászólás nem hangzott el, a képviselő-testület 6 igen szavazattal, ellenszavazat és tartózkodás nélkül az alábbi határozatot hozta:

Mérk Nagyközség Önkormányzat képviselő-testülete

58/2014 (VII.16.) határozata

Első lakáshoz jutók részére pénzeszköz biztosításáról

A képviselő-testület!

2014. évre első lakáshoz jutók részére 300.000 –Ft pénzügyi fedezetet biztosít.

Felkéri jegyző urat, hogy a lakosság részére ezen döntést prolongálja, majd a beérkezett igényeket terjessze a képviselő-testület elé.

Megbízza továbbá, hogy ezen döntés pénzügyi átvezetéséről rendeleti úton módon gondoskodjon.

Határidő: október 1.

Felelős: jegyző úr

A tárgysorozati pontok megtárgyalását követően Török László jegyző úr ismertette Rettegi István mérki lakos kérelmét, aki az önkormányzat tulajdonát képező gát területén kecskéket kíván legeltetni. Rövid beszélgetés követően a képviselő-testület határozathozatal mellőzésével a gáton való legeltetést nem támogatja, mert az a gát oldalszerkezetének eróziójához vezet.

Miután több hozzászólás, kérdés nem volt, Müller Istvánné polgármester asszony megköszönve a megjelenést a képviselő-testületi ülést 16^{05} órakor bezárta.

k.m.f.

Müller Istvánné
polgármester

Török László
jegyző

Magyarics Anita
képviselő, jkv. hit.

Aradi Ferenc
képviselő, jkv. hit.