BIHARNAGYBAJOM KÖZSÉGI ÖNKORMÁNYZAT

KÉPVISELŐ-TESTÜLETÉNEK

2018. június 26-án megtartott zárt rendkívüli ülésének

– jegyzőkönyve

– határozatai: 78., 79., 80., 81., 82., 83., 84., 85., 86., 87.

HATÁROZATOK

78/2018. (VI. 26.) számú KT határozat	a zárt rendkívüli képviselő-testületi ülés napirendjének elfogadásáról
79/2018. (VI. 26.) számú KT határozat	díszpolgári cím adományozásának elhatározásáról
80/2018. (VI. 26.) számú KT határozat	néhai Darabos Imre részére történő díszpolgári cím adományozásával kapcsolatban
81/2018. (VI. 26.) számú KT határozat	Dobos Sándor önkormányzati képviselő – személyes érintettség miatt – döntéshozatalból történő kizárásáról
82/2018. (VI. 26.) számú KT határozat	a Biharnagybajomi Önkéntes Tűzoltó Egyesület részére „Biharnagybajomért Emlékérem" adományozásáról
83/2018. (VI. 26.) számú KT határozat	néhai Darabos Imre részére posztumusz „Biharnagybajomért Emlékérem" adományozásáról
84/2018. (VI. 26.) számú KT határozat	Imre Lajosné részére díszpolgári cím adományozásáról
85/2018. (VI. 26.) számú KT határozat	Agócs Miklósné részére „Biharnagybajom Közszolgálatáért Elismerő Díj" adományozásáról
86/2018. (VI. 26.) számú KT határozat	Nagy Sándorné részére „Biharnagybajom Közszolgálatáért Elismerő Díj" adományozásáról
87/2018. (VI. 26.) számú KT határozat	Földi József „Biharnagybajom Sportjáért Elismerő Díj" adományozásáról

J E G Y Z Ő K Ö N Y V

Készült: Biharnagybajom Községi Önkormányzat Képviselő-testületének 2018. június 26-án a Biharnagybajomi Polgármesteri Hivatal tanácstermében megtartott – 16,30 órakor kezdődő – zárt rendkívüli ülésén.

Jelen vannak: Szitó Sándor polgármester
Dr. B. Csák István alpolgármester
B. Csák Imre
Dobos Sándor
Gazdag Endréné
Patakiné Darabos Zsuzsanna önkormányzati képviselők

Imre-Erdős Szilvia jegyző

Az ülésről távol maradt: Dul Sándor önkormányzati képviselő

Szitó Sándor polgármester
Köszöntöm a Képviselő-testület zárt ülésén jelenlévő képviselőket, jegyző asszonyt. Megállapítom, hogy Biharnagybajom Községi Önkormányzat Képviselő-testülete határozatképes, a 7 megválasztott önkormányzati képviselőből jelen van 6 képviselő.

Az ülés napirendjére a következő javaslatot teszem:
Előterjesztés helyi kitüntető címek adományozására
Előadó: Szitó Sándor polgármester

Aki a napirenddel egyetért, kérem kézfelnyújtással jelezze.
A határozathozatalban részt vett 6 képviselő.

A Képviselő-testület 6 igen szavazattal, ellenvélemény és tartózkodás nélkül meghozta határozatát:

78/2018. (VI. 26.) számú KT
HATÁROZAT
a képviselő-testületi ülés napirendjének elfogadásáról
Biharnagybajom Községi Önkormányzat Képviselő-testülete
a 2018. június 26-i zárt rendkívüli ülésének napirendjét a következők szerint fogadja el:

N a p i r e n d:
Előterjesztés helyi kitüntető címek adományozására
Előadó: Szitó Sándor polgármester
Véleményező bizottság: Népjóléti és Ügyrendi Bizottság

napirend

Előterjesztés helyi kitüntető címek adományozására

Előadó: Szitó Sándor polgármester

Véleményező bizottság: Népjóléti és Ügyrendi Bizottság

Szitó Sándor polgármester

Emlékeztetőül szeretném elmondani, hogy ki is kaphat díszpolgári címet: „Biharnagybajom Díszpolgára" cím adományozható annak a köztiszteletben álló magyar vagy külföldi állampolgárnak, aki egész életművével vagy valamely kiemelkedően jelentős munkájával olyan általános elismerést szerzett, amellyel hozzájárult a falu fejlődéséhez és jó hírnevének öregbítéséhez.

A cím önkormányzati ciklusonként egy személynek adományozható. A kitüntetéssel emlékérem és oklevél, valamint 500.000,- Ft bruttó pénzjutalom jár.

A javaslatok: B. Csák Imre, Darabos Imre, dr. Veréb Tibor, Nemes Sándor, Szitó Sándor. Tegnap a Népjóléti Bizottság ülésén az ajánlók képviselőjétől érkezett javaslat arra, hogy Imre Lajosnét Biharnagybajomért Emlékéremre javasolt személyek közül tegyük át a díszpolgári címre javasolt személyek közé. Így összesen 6 ajánlás van a díszpolgári címre. Vannak hosszabb-rövidebb ajánlások.

Legtöbb ajánlás – 44 db – Darabos Imrére érkezett, aki posztumusz került fel az ajánlottak közé. Az idősek korosztály vélhetőleg ismerte és tudja, hogy Ő gondnoka volt az egyháznak. A gondnoksága alatt betöltött fontos szerepéért javasolták, főleg egyházi körökből, de más személyektől is érkezett személyére javaslat.

Imre Lajosné sorakozott még fel ide az 50 db ajánlásával. Az előzőnek Czeglédi Péter Pál volt a fő ajánlásgyűjtője, Imre Lajosnénak Baloghné Kiss Katalin, aki az óvodai dolgozóktól, óvodával kapcsolatban lévőket keresett fel, de ott is van egy pár egyéb név is. Nagyjából beazonosítható ez a két kör, hogy az Óvoda és az Egyház.

B. Csák Imrét nem kell bemutatni, engem sem kell bemutatni. Nemes Sándorról tudjuk, hogy fafaragó, legutóbb a Szigetvári veszedelemmel kapcsolatos emlékművét avattuk fel, amit felajánlott. Veréb doktort mindenki ismerte. Hosszas beszélgetés után a Népjóléti és Ügyrendi Bizottság hozott egy javaslatot.

Patakiné Darabos Zsuzsanna Népjóléti és Ügyrendi Bizottság elnöke

A Népjóléti és Ügyrendi Bizottság díszpolgári címre az átcsoportosítás után Imre Lajosnét javasolta.

Szitó Sándor polgármester

A véleményező bizottságnak ismerjük a javaslatát, aki Imre Lajosnét javasolja díszpolgári címre. Ehhez képest kell a Testületnek vagy ezt jóváhagyni vagy pedig mást javasolni.

B. Csák Imre önkormányzati képviselő

Elhangzott, voltak, akik felvállalták, hogy egy-egy személy érdekében lobbizzanak, keressenek támogatókat. Én, amikor megnéztem a névsort, úgy is gondoltam, hogy igen, aki sok ajánlást, több ajánlást is kapott, az „viheti" is, hiszen valóban úgy néz ki, hogy nagyon sokan látványosan egyet is értenek vele. Most egy kicsit megkavarodtam. Ha valakit jelölnek mondjuk bronzfokozatra és a szervezet meg azt mondja, legyen belőle aranyfokozat. Imre Lajosnénak a jelentős előrelépése.

B. Csák Imre önkormányzati képviselő
Innentől kezdve, ha őt az emlékéremre javasoltak közül kivesszük, ha csak a Bizottságnak nincs javaslata, hogy Darabos Imre bácsit meg tegyük ide, ezért van nekem némi bizonytalanságom. Én magamban összeraktam, hogy első csoport, második csoport, harmadik csoport, ki az, akit én támogatok. Innentől kezdve, én nagyjából ahhoz tartom is magam.

Szitó Sándor polgármester
Szinte ugyanezen logikát követte alpolgármester úr tegnap. Ebből az apropóból a Biharnagybajomért Emlékéremre javasoltak közé bekerült tegnap Darabos Imre bácsi. Viszont ott nem Ő került javaslatra.
„Biharnagybajomért Emlékérem" kitüntetés adományozható annak a magyar állampolgárságú személynek, vagy társadalmi szervezetnek, aki élete vagy működése rövidebb-hosszabb szakaszában Biharnagybajom községhez kötődött és munkássága alkalmas a falu jó hírnevének öregbítéséhez vagy ha élete során nem Biharnagybajomhoz kötődött, a tevékenysége a települést gyarapítja. Önkormányzati ciklusonként egy vagy két kitüntetés adományozható. A kitüntetéssel emlékérem és oklevél, valamint 250.000,- Ft bruttó pénzjutalom jár.

Két civil szervezet is van javasolva ezen díjra. Egyik az Önkéntes Tűzoltó Egyesület, ott a 140 éves évforduló az, ami leginkább az apropó, a Református Férfikórusnál 10 éves évforduló van említve az ajánlásban. Ide átkerült Darabos Imre bácsi, alpolgármester úr javasolta tegnap a bizottsági ülésen, hogy kerüljön át ide, Hegyesi Béla fodrászt is javasolták. Imre Lajosné innen kikerült. Láposi Istvánnét mindenki ismeri. Nemes Sándorról már szó volt. És én vagyok még az ajánlottak között.

Patakiné Darabos Zsuzsanna Népjóléti és Ügyrendi Bizottság elnöke
A Népjóléti és Ügyrendi Bizottság „Biharnagybajomért Emlékérem"-re az Önkéntes Tűzoltó Egyesületet javasolta.

Szitó Sándor polgármester
Szavazásra én a Bizottság véleményét fogom elsőként feltenni. Ha nem fog eredmény születni, akkor fogjuk tovább tárgyalni. Azt gondolom, azért van a véleményező szerepe a Bizottságnak, hogy az ő véleményét kell a Testületnek vagy jóváhagyni vagy megmásítani.

Dr. B. Csák István alpolgármester
A posztumusz címmel jár pénzjutalom?

Szitó Sándor polgármester
Igen. Öt évvel ezelőtt, amikor posztumusz adtunk két személynek is – Szűcs Sándor és Juhász Sándor –, akkor a Szűcs Sándorét az ő hagyatékát ápoló kapta, a Juhász Sándorét pedig az élő örökösei.

„Biharnagybajom Díszpolgára" címre a Népjóléti és Ügyrendi Bizottság javaslata az volt, hogy Imre Lajosnénak adományozzuk ebben az évben. Aki ezzel egyetért, kézfelnyújtással jelezze.

Szavazásban részt vett 6 képviselő.
3 igen szavazat, ellenvélemény 0, tartózkodás 3.

Szitó Sándor polgármester
Nem született döntés, mert nincs meg a jelenlévő képviselők többségének az igen szavazata. Az SZMSZ-ünk szerint döntés hiányában a Képviselő-testületnek egyszerű szótöbbséggel, nyílt szavazással határozni kell a további eljárásról.
Azt gondolom, ha már ennyi ajánlás érkezett, akkor tudjunk választani, válasszunk díszpolgárt. Aki ezzel egyetért, kézfelnyújtással jelezze.

Szavazásban részt vett 6 képviselő.
A Képviselő-testület 6 igen szavazattal, ellenvélemény és tartózkodás nélkül meghozta határozatát:

79/2018. (VI. 26.) számú KT
HATÁROZAT
díszpolgári cím adományozásának elhatározásáról

Biharnagybajom Községi Önkormányzat Képviselő-testülete úgy határoz, hogy az ülésen dönt „Biharnagybajom Díszpolgára" cím adományozásáról.

Határidő: 2018. június 26.

Felelős: Szitó Sándor polgármester

Szitó Sándor polgármester
A díszpolgári cím adományozásával kapcsolatos döntés meghozatala érdekében kössünk valamilyen kompromisszumos megoldást, mindenképp próbálkozzunk meg egy döntéssel. A tartózkodókhoz fordulok. Mi az, amivel a tartózkodás feloldható, vagy ki az, akiben feloldható, beszélgessünk, én meggyőzhető vagyok.

B. Csák Imre önkormányzati képviselő
Felvállalták. Ha én nem akarom aláírni Darabos Imre bácsit, nem akarok aláírni. Én elolvastam az ajánlást is. Ha első sorban Koroknai András szerepel, ugyan így él az ajánlás. Ők tudják, hogy ebből Imre bácsi mit csinált. Az Egyház ilyen létszámban megtámogatta. Én ezt nagyon elfogadtam. Megkérdeztük a népet, a nép így gondolta. Az most egy dolog, ha most az önkéntes tűzoltó közül Tóth Imre vagy Dobos Sándor elindult, akkor ők tudtak volna 80 ajánlást összeszedni. Miért nem indultak el? Ezt tudhattuk, ha meghirdetjük, annak, hogy valakinek egy vagy ötven ajánlása van, annak súlya lesz. Tovább én nem is mérlegelem.

Dr. B. Csák István alpolgármester
Amikor megláttam az előterjesztést, én is ezen az álláspontón voltam. Ha látszik, hogy 1-2-3 név mellett sorakoztak fel nagyobb létszámban, akkor azokat nem tudom, hogy én felülbírálhatom-e, mivel a listán szereplő minden ember megérdemli vagy megérdemelheti a címet. Az én ajánlásom egy ajánlás lesz a 44 mellett vagy az 50 mellett. Én úgy érkeztem, hogy ekkora társadalmi nyomást nem bírálhatok felül.

Dobos Sándor önkormányzati képviselő
Ha erről szólt volna, akkor elindított volna mindenki mindenki vagy valaki mellett ajánlásgyűjtést. Így azonban átcsapott volna önkormányzati választásba. Nekem ez a korteshadjárat csípte a szememet.

Imre-Erdős Szilvia jegyző
Van olyan, aki úgy gyűjtötte, hogy behozott 50 vagy akárhány ajánlólapot, és van, aki külön, de egybe hozták be. Ki hogy értelmezte. Valaki pedig aláírást gyűjtött. A rendeletünk erről nem rendelkezik.

Dr. B. Csák István alpolgármester
A lehetőség mindenki előtt ott volt, volt, aki élt vele, volt, aki nem.

B. Csák Imre önkormányzati képviselő
Ha magunkra akarjuk venni, akkor ennek a kis cikknek a végének az kellett volna lenni, hogy dönt a Képviselő-testület a javasolt személyekről. Döntésénél az ajánlók számát figyelembe fogja venni vagy nem fogja figyelembe venni. Elég egy embernek ajánlani valakit, mert az pont olyan súlyú, mintha százan ajánlanák.

Imre-Erdős Szilvia jegyző
Erről nem rendelkezik a rendeletünk.

B. Csák Imre önkormányzati képviselő
Találkoztunk egy jelenséggel. Kell a jövőre nézve is gondolkodni.

Szitó Sándor polgármester
Több észrevétel is van, amit már most helyre kellene tenni. Jelenleg van egy rendeletünk, azon, ha módosítunk, az már csak a jövőre nézve lehet érdemleges. Jelenleg abból kell okosnak vagy legalább is bölcsnek lenni, ami előttünk van.

Kérdezem a két képviselőt, hogy az elhangzottak függvényében a döntéshez tudnak-e felcsatlakozni valamilyen indokkal, vagy kitartanak az álláspontotok mellett.

Patakiné Darabos Zsuzsanna Népjóléti és Ügyrendi Bizottság elnöke
Én igen.

Gazdag Endréné önkormányzati képviselő
Én ismertem Imre bácsit, tényleg egy köztiszteletben álló ember volt, de a mai fiatalok nem ismerik. Imrénét viszont ismerik, aki tényleg jó példa, élő példa lehet arra, ahogy Ő dolgozott.

Szitó Sándor polgármester
Nekem is az a véleményem, hogy díszpolgárnak olyan személyt javasoljunk, aki tényleg követendő példa tud lenni életében még. Nem megbántva Darabos Imrét, aki biztos sok mindent tett. Az ajánlása nagyon szépen, nagyon korrektül megvan fogalmazva, tetszetős is. Annyi a problémám, hogy nekem nem jelenik meg a szemem előtt, de ez az én problémám, nem a másé.

Dr. B. Csák István alpolgármester
Juhász Sándort sem ismerték a mai fiatalok. Az emlékversenyen él a példája, ugyan úgy, mint Darabos Imre bácsinak az egyházon belül. Nem vitathatjuk ezt el.

Szitó Sándor polgármester
Ez az én mérlegelésemnél volt mérvadóbb kicsit.

Dr. B. Csák István alpolgármester
Én Imre Lajosnét is ugyan úgy támogatom, nekem nem is volt ez kérdés, amikor megkaptam a listát. Azzal, hogy összekavartuk, engedtük, hogy átcsoportosíthatók legyenek emberek, az én meglátásomból ezzel borult fel az egész metodikám. Én úgy gondoltam, hogy ez itt nem is lesz kérdés, olyan egyértelmű. Engem a Darabos Imrét indítók, érte lobbizók megkerestek, én felvállaltam, aláírtam. Én is méltónak találtam Őt arra. Én mind a kettőre igennel szavaznék, azért tartózkodom.
Imre Lajosné ajánlását elindító pontosan a Népjóléti Bizottság tagja, Ő indítványozza, hogy léptessük elő. Nem mindenkinek volt ilyenre lehetősége. Ha most mindenkit ide becitáltunk volna, ők is lehet, hogy ide-oda felosztogatták volna. Én mind a két személyt támogatom. Én bennem ez kavart, ezen sajnos nem tudok továbblépni, ez megköt.

Dobos Sándor önkormányzati képviselő
Nekem az bántja a szemem, hogy nem volt tudatosítva, hogy lehet ajánlószelvényeket gyűjteni.

Imre-Erdős Szilvia jegyző
De nem lehet, de nem tiltja semmi, erről a rendelet nem rendelkezik. Élelmes emberek ezt kitalálták. Van, aki behozta a sok szavazólapot és van, aki csak az ajánlóívet. Ezt sem egyformán csinálták.

B. Csák Imre önkormányzati képviselő
De le lehet ezt adott esetben úgy is egyszerűsíteni, nem a Testület vagy a Bizottság kerül kellemetlen helyzetbe, hogy valaki hiába hoz 50 ajánlást, egy személy egy ajánlás, az 50 is egyet ér.

Imre-Erdős Szilvia jegyző
A rendeletünkben le kell szabályozni.

Dr. B. Csák István alpolgármester
Nem tudom milyen megfontolásból az anyag készítője döntött úgy, hogy ezeknek az ajánlásoknak súlyt ad. Ha nem írja ide a nevekhez, nincs ez. Valahol ez szándék volt, hogy ez jelentkezzen. Ha nincs odaírva, akkor nincs is vita benne. Csak a személyről, mint magáról és nem a társadalmi csoportosulásról mondunk véleményt.

Szitó Sándor polgármester
Ez én vagyok. Ha alpolgármester úr lett volna az anyag készítője, nem írta volna oda? Azon is gondolkodtam, hogy odategyem-e az ajánlószelvényeket. Úgy gondoltam látni kell, hogy valakit mennyien ajánlottak. Én ezért tettem oda.
Aki egyetért azzal, hogy Darabos Imre kapja a díszpolgári címet, kérem kézfelnyújtással jelezze.

Szavazásban részt vett 6 képviselő.
A Képviselő-testület 2 igen szavazat, 3 tartózkodás, 1 ellenvélemény alapján meghozta határozatát:

80/2018. (VI. 26.) számú KT
HATÁROZAT
néhai Darabos Imre részére történő díszpolgári cím adományozásával kapcsolatban

Biharnagybajom Községi Önkormányzat Képviselő-testülete úgy határoz, hogy néhai Darabos Imre részére „Biharnagybajom Díszpolgára" címet nem adományoz.

Határidő: 2018. június 26.

Felelős: Szitó Sándor polgármester

Szitó Sándor polgármester
Azt gondolom, hogy ne bővítsük a kört. Én magamat nem fogom feltenni szavazásra, B. Csák Imrét nem gondolom, hogy feltesszük, Veréb doktor úr a beszélgetés során nem vetődött fel. Azt gondolom továbbra is azon megy a vita, hogy akkor Imre Lajosné, ha már felkerült ide bizottsági ülésen.
Jegyző asszonnyal már a legeslegelején – amikor nevekről még nem is volt szó – abban nem értettünk egyet a rendeletünk értelmezése során, hogy a Bizottságnak és a Testületnek mi a szerepe. Én azt mondtam, hogy bekerültek a nevek, a Bizottság véleményez, a Testület dönt. Jegyző asszony meg azt mondta, hogy nem, mert minden egyes előterjesztésnél van módosítási lehetősége a Bizottságnak, illetve a Testületnek.

Imre-Erdős Szilvia jegyző
Mert mindig is így volt.

Szitó Sándor polgármester
Ezért lehetett tegnap a Bizottság ülésén módosítással élni.
Alpolgármester úrnak tegnap az volt a javaslata, hogy cseréljünk, Imre Lajosné legyen a díszpolgár, viszont akkor Darabos Imre bácsi kapja a Biharnagybajomért Emlékérmet. Volt egy ilyen javaslat is.
Én mindenkinek a személyét tudom támogatni, felül tudok emelkedni azon is, hogy posztumusz kapja. A javasolt emberek közül – jómagam kivételével – mindenki megérdemli. Én fel tudok csatlakozni bárkihez. Imre Lajosné azért volt egy kicsit közelebb hozzám, mert nem posztumusz.

Szitó Sándor polgármester
„Biharnagybajomért Emlékérem"-re van javasolva a Biharnagybajomi Önkéntes Tűzoltó Egyesület.

Dobos Sándor önkormányzati képviselő
Évekig az Egyesület elnöke voltam, érintett vagyok, ezért kérem a szavazásból történő kizárásomat.

Szitó Sándor polgármester
Aki egyetért azzal, hogy Dobos Sándort kizárjuk a szavazásból, kérem kézfelnyújtással jelezze.

Szavazásban részt vett 6 képviselő.
A Képviselő-testület egyhangúlag, 6 igen szavazattal meghozta határozatát:

81/2018. (VI. 26.) számú KT
HATÁROZAT
Dobos Sándor önkormányzati képviselő – személyes érintettség miatt – döntéshozatalból történő kizárásáról

Biharnagybajom Községi Önkormányzat Képviselő-testülete Dobos Sándor önkormányzati képviselő személyes érintettségének bejelentésével kapcsolatban az alábbiakat határozza el:

A Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 49. § (1) bekezdésében és a 60. §-ban foglaltak alapján a Biharnagybajomi Önkéntes Tűzoltó Egyesület részére adományozandó kitüntetéssel kapcsolatos döntés meghozatalakor – Dobos Sándor önkormányzati képviselő bejelentésére tekintettel – kizáró oknak tekinti a személyes érintettségét, ezért Dobos Sándort a döntéshozatalból kizárja.

Határidő: 2018. június 26.
Felelős: Szitó Sándor polgármester

Szitó Sándor polgármester
Aki egyetért azzal, hogy „Biharnagybajomért Emlékérem"-et a Biharnagybajomi Önkéntes Tűzoltó Egyesület kapja, kézfelnyújtással jelezze.

Szavazásban részt vett 5 képviselő.
A Képviselő-testület 4 igen szavazattal és 1 tartózkodással meghozta határozatát:

82/2018. (VI. 26.) számú KT
HATÁROZAT
a Biharnagybajomi Önkéntes Tűzoltó Egyesület részére „Biharnagybajomért Emlékérem" adományozásáról

Biharnagybajom Községi Önkormányzat Képviselő-testülete úgy határoz, hogy a Biharnagybajomi Önkéntes Tűzoltó Egyesület részére – a 140 éven át tartó, település szolgálatában végzett áldozatos munkájáért – BIHARNAGYBAJOMÉRT EMLÉKÉRMET és oklevelet adományoz.

A díjjal járó emlékérem és oklevél, valamint pénzjutalom a 2018. július 13-án tartandó ünnepi képviselő-testületi ülésen kerül átadásra.

Határidő: 2018. július 13.

Felelős: Szitó Sándor polgármester

Szitó Sándor polgármester
A zárt ülést megelőzően született tartott nyilvános ülésen módosítottuk a rendeletünket, mely szerint a „Biharnagybajomért Emlékérem"-ből kettő is adományozható. Javaslom, hogy posztumusz „Biharnagybajomért Emlékem" kerüljön adományozásra néhai Darabos Imre részére. Aki ezzel egyetért, kézfelnyújtással jelezze.

Szavazásban részt vett 6 képviselő.
A Képviselő-testület 5 igen szavazattal, ellenvélemény nélkül, 1 tartózkodással meghozta határozatát:

83/2018. (VI. 26.) számú KT
HATÁROZAT
néhai Darabos Imre részére posztumusz „Biharnagybajomért Emlékérem" adományozásáról

Biharnagybajom Községi Önkormányzat Képviselő-testülete úgy határoz, hogy néhai Darabos Imre részére – a Biharnagybajomi Református Egyházközség gondnokaként végzett sok éves kimagasló munkájáért, mellyel a település javát szolgálta – posztumusz BIHARNAGYBAJOMÉRT EMLÉKÉRMET és oklevelet adományoz.

A díjjal járó emlékérem és oklevél, valamint pénzjutalom a 2018. július 13-án tartandó ünnepi képviselő-testületi ülésen kerül átadásra.

Határidő: 2018. július 13.

Felelős: Szitó Sándor polgármester

Szitó Sándor polgármester
Visszakanyarodunk a díszpolgári címhez. Meg fogom ismételni a Népjóléti Bizottság javaslatát. Aki tudja ismételten, újból vagy újra, esetleg először támogatni Imre Lajosnét, kérem kézfelnyújtással jelezze.

Szavazásban részt vett 6 képviselő.
A Képviselő-testület 5 igen szavazattal és 1 tartózkodással meghozta határozatát:

84/2018. (VI. 26.) számú KT
HATÁROZAT
Imre Lajosné részére díszpolgári cím adományozásáról

Biharnagybajom Községi Önkormányzat Képviselő-testülete úgy határoz, hogy Imre Lajosné (Biharnagybajom, Posta u. 5.) részére – aki az óvodai nevelés területén végzett kiemelkedő szakmai munkájával és jelentős közéleti tevékenységével hozzájárult a falu fejlődéséhez és a település hírnevének öregbítéséhez – BIHARNAGYBAJOM DÍSZPOLGÁRA kitüntető címet és oklevelet adományoz.

A díjjal járó emlékérem és oklevél, valamint pénzjutalom a 2018. július 13-án tartandó ünnepi képviselő-testületi ülésen kerül átadásra.

Határidő: 2018. július 13.

Felelős: Szitó Sándor polgármester

Szitó Sándor polgármester
„Biharnagybajom Közszolgálatáért Elismerő Díj" adományozható azoknak a személyeknek, akik szakterületükön tartósan kiemelkedő eredményt nyújtanak valamint, akik hosszú időn át közmegelégedésre látják el a közalkalmazotti, köztisztviselői feladataikat. Önkormányzati ciklusonként két kitüntetés adományozható. A kitüntetéssel emlékérem és oklevél, valamint 250.000,- Ft bruttó pénzjutalom jár.
Három név van javasolva: Agócs Miklósné, aki jövőre megy nyugdíjba, Nagy Sándorné, aki szintén jövőre megy nyugdíjba, valamint Nemes-Lajsz Julianna.

Nagy dilemmában voltunk, mert Juhászné Hegedűs Mária nyugdíjba megy pár napon belül. Azt gondoltuk, hogy őt egy magasabb és szakmai elismerésre terjesztjük fel. A Képviselő-testület hozott is döntést ezzel kapcsolatban, melyet megküldtünk az illetékes minisztériumnak, ahonnan még semmilyen értesítést nem kaptunk. Országgyűlési képviselő úrtól is kértünk ezzel kapcsolatban segítséget, aki megtette, amit tudott és türelmünket kérte. A helyi kitüntetések odaítélésével nem tudunk tovább várni. Nem szeretnénk, ha Juhászné Hegedűs Mária elismerés nélkül hagyná el a Biharnagybajomi Polgármesteri Hivatalt.

Patakiné Darabos Zsuzsanna Népjóléti és Ügyrendi Bizottság elnöke
A Népjóléti és Ügyrendi Bizottság úgy döntött, hogy bízva a minisztérium jóindulatában, a helyi kitüntető díjra, a „Biharnagybajom Közszolgálatáért Elismerő Díj"-ra Agócs Miklósnét és Nagy Sándornét javasolta.

B. Csák Imre önkormányzati képviselő
Ha nem kap Juhászné Hegedűs Mária miniszteri kitüntetést, akkor mi van? Mi a B-terv?

Szitó Sándor polgármester
Akkor leghamarabb jövőre kaphat.

Imre-Erdős Szilvia jegyző
Tegnap bizottsági ülésen is azt kértem és most is azt kérem, hogy egyet ítéljünk oda most és eggyel pedig várjunk. Én is azt gondolom és úgy gondolom, hogy abban mindannyian egyetértünk, hogy Marikát nem szabad elengedni kitüntetés nélkül. A felterjesztéskor meg kellett jelölni az átadás napját, július 14-ét jelöltük meg.

B. Csák Imre önkormányzati képviselő
azt is meg lehet csinálni, hogy év végén dönteni és átadni, mert addig kiderül.
A rendeletet a Képviselő-testület alkotja. Ha megvan a módosítási szándék, akkor év végén is átadható a díj.

Szitó Sándor polgármester
Lehet módosítani a rendeletet. Én most a Bizottság javaslatát tartanám követendőnek.
A képviselő úr javaslata egy életképes javaslat. A decemberi időpont nekem tetszik B-tervnek.

„Biharnagybajom Közszolgálatáért Elismerő Díj"-ra javasolt személy Agócs Miklósné. Aki egyetért a javaslattal, kérem kézfelnyújtással jelezze.

Szavazásban részt vett 6 képviselő.
A Képviselő-testület egyhangúlag, 6 igen szavazattal, ellenvélemény és tartózkodás nélkül meghozta határozatát:

85/2018. (VI. 26.) számú KT
HATÁROZAT
Agócs Miklósné részére „Biharnagybajom Közszolgálatáért Elismerő Díj" adományozásáról

Biharnagybajom Községi Önkormányzat Képviselő-testülete úgy határoz, hogy Agócs Miklósné (Biharnagybajom, Bajcsy-Zs. u. 25.) részére – aki kiemelkedő köztisztviselői tevékenységét hosszú időn át közmegelégedésre látta el – BIHARNAGYBAJOM KÖZSZOLGÁLATÁÉRT ELISMERŐ DÍJAT és oklevelet adományoz.

A díjjal járó emlékérem és oklevél, valamint pénzjutalom a 2018. július 13-án tartandó ünnepi képviselő-testületi ülésen kerül átadásra.

Határidő: 2018. július 13.

Felelős: Szitó Sándor polgármester

Szitó Sándor polgármester
Aki egyetért Nagy Sándorné részére történő „Biharnagybajom Közszolgálatáért Elismerő Díj" adományozásával, kérem kézfelnyújtással jelezze.

Szavazásban részt vett 6 képviselő.
A Képviselő-testület egyhangúlag, 6 igen szavazattal, ellenvélemény és tartózkodás nélkül meghozta határozatát:

86/2018. (VI. 26.) számú KT
HATÁROZAT
Nagy Sándorné részére „Biharnagybajom Közszolgálatáért Elismerő Díj" adományozásáról

Biharnagybajom Községi Önkormányzat Képviselő-testülete úgy határoz, hogy Nagy Sándorné (Biharnagybajom, Sirály u. 13.) részére – aki kiemelkedő ápolónői tevékenységét hosszú időn át közmegelégedésre látta el – BIHARNAGYBAJOM KÖZSZOLGÁLATÁÉRT ELISMERŐ DÍJAT és oklevelet adományoz.

A díjjal járó emlékérem és oklevél, valamint pénzjutalom a 2018. július 13-án tartandó ünnepi képviselő-testületi ülésen kerül átadásra.

Határidő: 2018. július 13.

Felelős: Szitó Sándor polgármester

Szitó Sándor polgármester
„Biharnagybajom Sportjáért Elismerő Díj" adományozható azoknak a személyeknek és egyesületeknek, akik/amelyek a testnevelés és a sport népszerűsítésében, a diák-, a tömeg- és/vagy a versenysport szervezésében, valamint a lakosság fizikai és egészségi állapotának fejlesztésében kimagasló munkát végeztek, továbbá olyan hazai és/vagy nemzetközi sporteredményeket értek el, amellyel hozzájárultak a község hírnevének öregbítéséhez. Önkormányzati ciklusonként legfeljebb egy kitüntetés adományozható. A kitüntetéssel emlékérem és oklevél, valamint 250.000,- Ft bruttó pénzjutalom jár.
Kettő ajánlásunk van, Földi József és Macskinné Pór Erzsébet. földi József a súlyemelőknek az edzője, számos elismerést kaptak versenyzői, már most határon túlról is. Macskinné Pór Erzsébet a mazsorettesek művészeti vezetője már 15 éve, több generációt kinevelt. Határon belülről és határon túlról is kaptak szebbnél szebb elismeréseket.

Patakiné Darabos Zsuzsanna Népjóléti és Ügyrendi Bizottság elnöke
A Népjóléti és Ügyrendi Bizottság Macskinné Pór Erzsébetet javasolta a „Biharnagybajom Sportjáért Elismerő Díj"-ra.

Dr. B. Csák István alpolgármester
Az anyagot olvasva elgondolkoztam rajta, hogy „Biharnagybajom sportjáért Elismerő Díj"-at kiknek lehetne még adni. Jelenleg ez a két terület van, ahol országos eredményeket tudnak felmutatni. Most jubilálnak a mazsorettesek. Ott gondolkodtam azon, hogy kinek, mit jelent ez a díj. Mind a ketten ugyan úgy megérdemlik a munkájuk alapján. A mazsorett csoport hatalmas gyermekbázissal rendelkezik, több évfolyammal, több csoporttal.

Dr. B. Csák István alpolgármester
Ez egy hatalmas elismerése a vezető hölgynek, de megvan az utánpótlás. Úgy látom, hogy a másik oldalt viszont a súlyemelés az sosem volt, sosem lesz egy nagyon szimpatikus sportág. Ott az edző keresi fel, kutatja fel a gyerekeket, akiket erre az útra készít. Kinek mit jelentene ez a díj, hogyha megkapná, kinek mekkora lökést adna ez, ha ad lökést. Én mind a kettőt támogatom, támogatni tudom.

Gazdag Endréné önkormányzati képviselő
Én is elismerem mind a kettőjük munkáját. Ha azt nézzük, hogy a Macskinné Pór Erzsébet munkája mögött ott van egy akkor szülői bázis és akkora anyagi segítséggel, mindennel, de tudom, hogy Földi József milyen, azonban rendszeresen járnak versenyre, országos versenyt bonyolít le – nem egy versenyen voltam ott – és nincs mellette senki. Olyan gyerekeket visz versenyre, akik az életben Bajomból ki sem jutottak volna soha, ha nem viszi őket, szerintem. Ismerem a Macskinné Pór Erzsébet munkáját is.

B. Csák Imre önkormányzati képviselő
Én úgy jöttem ide, hogy Földi Józsefet támogatom.

Dr. B. Csák István alpolgármester
Ha a következő ciklusban is úgy dönt a Képviselő-testület, hogy kiosztja ezeket a díjakat, nem hiszem, hogy a két név mellé fel tudna zárkózni valaki jelenleg. Ezen két személy mögött több tízéves múlt van, sikerekben eltöltött. Kinek adna nagyobb lökést, kinek adna nagyobb stabilitást, ha segít a működésben, kit segít jobban, én emiatt hajlok egy kicsit Földi József felé. A mazsorett egy olyan divatos sportág, ahol mindig lesz gyermek, mindig lesz ember, aki foglalkozzon velük. Én attól félek, ha Földi József egyszer abbahagyja, akkor azzal eltűnik a Súlyemelő Szakosztály is. Az idő előrehaladtával, korából kifolyólag előbb-utóbb el fog következni.

Dobos Sándor önkormányzati képviselő
Az egyértelmű, hogy Macskinné Pór Erzsébet hatalmas tömeget mozgat meg, látványos dolgokat csinál. De ha azt nézzük, hogy a Hajdú-Bihari Naplóban megjelenik, hogy első, második, harmadik helyezést értek el a súlyemelők országos szinten, akkor ez is nagy dolog.

Szitó Sándor polgármester
Aki egyetért azzal, hogy „Biharnagybajom Sportjáért Elismerő Díj"-at a Népjóléti és Ügyrendi Bizottság javaslata alapján Macskinné Pór Erzsébet kapja, kérem kézfelnyújtással jelezze.

Szavazásban részt vett 6 képviselő.
2 igen szavazat és 4 tartózkodás alapján nem született döntés.

Szitó Sándor polgármester
Aki egyetért azzal, hogy „Biharnagybajom Sportjáért Elismerő Díj"-at Földi József kapja, az kérem kézfelnyújtással jelezze.

Szavazásban részt vett 6 képviselő.
A Képviselő-testület 4 igen szavazattal, ellenvélemény nélkül, 2 tartózkodással meghozta határozatát:

87/2018. (VI. 26.) számú KT
HATÁROZAT
Földi József „Biharnagybajom Sportjáért Elismerő Díj" adományozásáról

Biharnagybajom Községi Önkormányzat Képviselő-testülete úgy határoz, hogy Földi József (Biharnagybajom, Bacsó B. u. 1.) részére – a Biharnagybajom Sportegyesület Súlyemelő Szakosztályában végzett kiemelkedő edzői tevékenységéért, mellyel hozzájárult a település hírnevének öregbítéséhez, a sportág népszerűsítéséhez – BIHARNAGYBAJOM SPORTJÁÉRT ELISMERŐ DÍJAT és oklevelet adományoz.

A díjjal járó emlékérem és oklevél, valamint pénzjutalom a 2018. július 13-án tartandó ünnepi képviselő-testületi ülésen kerül átadásra.

Határidő: 2018. július 13.

Felelős: Szitó Sándor polgármester

A Képviselő-testület zárt ülésén több napirendi pont tárgyalására nem került sor. Polgármester úr mindenkinek megköszönte a részvételt, az ülést 17,10 órakor bezárta.

k. m. f.

Szitó Sándor
polgármester

BIHARNAGYBAJOM RÉSZSÉGI ÖNKORMÁNYZAT 3.

Imre-Erdős Szilvia
jegyző

JELENLÉTI ÍV

a Képviselő-testület 2018. június 26-án megtartott

zárt ülésén jelenlévő önkormányzati képviselőkről

Szitó Sándor .....

B Csák Imre .....

Dr. B. Csák István .....

Dobos Sándor .....

Dul Sándor .....

Gazdag Endréné .....

Patakiné Darabos Zsuzsanna .....

Biharnagybajom Községi Önkormányzat
P o l g á r m e s t e r é t ő l

M E G H Í V Ó

Biharnagybajom Község Önkormányzatának Képviselő-testülete

2018. június 26-án kedden

a nyilvános ülést követően rendkívüli ZÁRT ÜLÉST tart,

melyre Önt tisztelettel meghívom.

N a p i r e n d:

Előterjesztés helyi kitüntető címek adományozására

Előadó: Szitó Sándor polgármester

Véleményező bizottság: Népjóléti és Ügyrendi Bizottság

Biharnagybajom, 2018. június 22.

Szitó Sándor s.k.
polgármester

Biharnagybajom Községi Önkormányzat
P o l g á r m e s t e r é t ő l

Előterjesztés

a Képviselő-testület 2018. június 26-án tartandó rendkívüli ülésére
helyi kitüntető címek adományozására

Tisztelt Képviselő-testület!

A kitüntetések alapításáról és adományozásának rendjéről szóló 18/2010. (XII. 20.) számú önkormányzati rendelet alapján Biharnagybajom Községi Önkormányzat Képviselő-testülete azoknak a személyeknek, szervezeteknek, közösségeknek, akik (amelyek) az országos vagy helyi társadalmi, gazdasági, kulturális életben a község és a lakossága javára eredményes és sikeres tevékenységet folytattak, ezzel az utókor számára példát mutattak (követendő példával szolgáltak) kitüntetéseket, elismeréseket alapított.

Az elismerések fajtái:

- Biharnagybajom Díszpolgára
- Biharnagybajomért Emlékérem
- Biharnagybajom Közszolgálatáért Elismerő Díj
- Biharnagybajom Sportjáért Elismerő Díj

A kitüntetések önkormányzati ciklusonként egy alkalommal ítélhetőek oda, átadásukra pedig a falunap alkalmával kerül sor.

A képviselő-testület ez évben tervezi odaítélni az arra alkalmasoknak a helyi kitüntetéseket, ezért az ez évi költségvetésben már biztosította a fedezetet a kitüntetésekkel járó pénzjutalom összegére, továbbá a rendelet értelmében a lakosság minél szélesebb körű tájékoztatása érdekében a javaslattételi felhívás közzé lett téve a Bajomi Hírlevél tárgyévi első számában.

A felhívásra a következő javaslatok érkeztek:

- „Biharnagybajom Díszpolgára" elismerésre javasolt személyek
    - B.Csák Imre – 2 db ajánlás
    - Darabos Imre (1912-1993) – 44 db ajánlás
    - Dr. Veréb Tibor – 1 db ajánlás
    - Nemes Sándor (fafaragó) – 1 db ajánlás
    - Szitó Sándor – 1 db ajánlás

- „Biharnagybajomért Emlékérem" elismerésre javasolt személyek
    - Biharnagybajomi Önkéntes Tűzoltó Egyesület – 2 db ajánlás
    - Biharnagybajomi Református Férfikórus – 1 db ajánlás

- Hegyesi Béla (fodrász) – 1 db ajánlás
- Imre Lajosné – 50 db ajánlás
- Láposi Istvánné – 1 db ajánlás
- Nemes Sándor (fafaragó) – 1 db ajánlás
- Szitó Sándor – 1 db ajánlás

- „Biharnagybajom Közszolgálatáért Elismerő Díj" elismerésre javasolt személyek

  - Agócs Miklósné – 12 db ajánlás
  - Nagy Sándorné – 1 db ajánlás
  - Nemes-Lajsz Julianna – 2 db ajánlás

- „Biharnagybajom Sportjáért Elismerő Díj" elismerésre javasolt személyek

  - Földi József – 2 db ajánlás
  - Macskinné Pór Erzsébet – 2 db ajánlás

A kitüntetésre vonatkozó javaslatokat május 31-ig kellett írásban beterjeszteni hozzám, melyet a Népjóléti és Ügyrendi Bizottság véleményez a képviselő-testületi döntés előtt.

Előterjesztésemhez mellékelem a korábbi kitüntetettek névsorát.

Kérem a Tisztelt Képviselő-testületet tárgyalja meg az előterjesztést, és hozza meg döntését.

Biharnagybajom, 2018. június 19.

Szitó Sándor s.k.
polgármester

Eddigi kitüntetettjeink:

1991.

„Biharnagybajomért emlékérem"
· Nemes Antal kovácsmester

Biharnagybajom Önkormányzat Nívódíjasai:
· Papp László nyugalmazott tanár
· néhai Dr. Darabos Pálné nyugalmazott tanítónő
· Gorzsás Sándorné ápolónő
· Gy. Kiss Lajos Önkéntes Tűzoltó Egyesület parancsnok
· Juhász Istvánné gyékénykötő
· Makra Lászlóné tanítónő
· Nemes Barnabásné tanárnő

1992.

„Biharnagybajom Díszpolgára"
· Jeney Lajos építész

„Biharnagybajomért emlékérem"
· Nemes Antal nyugalmazott tanár

Biharnagybajom Önkormányzat Nívódíjasai
· Gál Gyuláné köztisztviselő
· Máthé Sándorné gyékénykötő
· Nemes Benjáminné nyugalmazott tanítónő
· Nemes Sándor fafaragó
· Dr. Veréb Tibor háziorvos

1994.

„Biharnagybajom Díszpolgára"
· Dr. Somogyi Éva idegsebészeti szemész

„Biharnagybajomért emlékérem"
· Dr. Szűrös Mátyás országgyűlési képviselő

Biharnagybajom Önkormányzat Nívódíjasai
· Kiss Imréné köztisztviselő
· id. Veress Sándor asztalos
· Hajdu Gyula vőfély
· Nemes István zenetanár
· Dr. Hubert Zoltán háziorvos

1997.

„Biharnagybajom Díszpolgára"
· Kacska Zoltán polgármester

2008.

„Biharnagybajom Díszpolgára"
· Nemes István

„Biharnagybajomért emlékérem"
· Furka Albertné Báthori Ágnes

Biharnagybajom Önkormányzat Elismerő Díja
· Bagdi Imréné Fórián Eszter

2009.

„Biharnagybajomért emlékérem"
· Kalmár Gyula

Biharnagybajom Önkormányzat Elismerő Díja
· Tóth Imre
· Láposi Gyuláné Gali Jolán
· Nagy Andrásné Gyimesi Judit

2013.

„Biharnagybajom Díszpolgára"
· Szűcs Sándor (posztumusz)

„Biharnagybajomért emlékérem"
· Sperlágh házaspár

„Biharnagybajom Közszolgálatáért Elismerő Díj"
· Láposi Márton Zoltán
· Gyügyei Katalin

„Biharnagybajom Sportjáért Elismerő Díj"
· Juhász Sándor (posztumusz)

BIZALMAS INFORMÁCIÓT TARTALMAZ!

Informatikai Biztonsági Szabályzat

Hatályba lépés dátuma: 2014. június 25.

Készítette, dokumentum változástörténet

Dátum	Szerző	Verzió	Módosítás tárgya
2014.06.19	Biró Gergely Ganev Attila	1.0	Átadott verzió
2016.07.07.	Biró Gergely Ganev Attila	1.1	Törvényi változások alapján felülvizsgált verzió
2016.12.09.	Biró Gergely Ganev Attila	1.2	NEIH előírások alapján felülvizsgált verzió
2018.04.09.	Biró Gergely Ganev Attila	1.3	Hivatali informatikai változásai alapján felülvizsgált verzió

Ellenőrizte

Dátum	Név	Verzió	Aláírás

Jóváhagyta

Dátum	Név	Verzió	Aláírás

TARTALOMJEGYZÉK

1. INFORMÁCIÓ BIZTONSÁG

1.1. AZ IBSZ HATÁLYA

Az Informatikai Biztonsági Szabályzat (továbbiakban IBSZ vagy szabályzat) hatálya kiterjed a Biharnagybajomi Polgármesteri Hivatalra (a továbbiakban: Hivatal) és minden alkalmazottjára, továbbá azon személyekre, akik a Hivataltól kapott megbízásuknál fogva a Hivatal Informatikai Biztonsági Szabályzatában előírt rendelkezésekkel kapcsolatba kerülnek (a továbbiakban: munkatársak).

Az IBSZ tárgyi hatálya kiterjed a Hivatal tulajdonát képező, továbbá a Hivatal által használt épületekben lévő:

- Irodák, személyek rendelkezésére bocsátott, vagy általuk tárolt valamennyi informatikai berendezésre, beleértve a berendezések műszaki dokumentációját is,
- Rendszerprogramokra és a felhasználói programokra,
- Elektronikus adatok teljes körére, keletkezésük és felhasználásuk, valamint feldolgozásuk helyétől, továbbá a megjelenési formájuktól függetlenül,
- Adathordozókra, azok tárolására és felhasználására, beleértve a feldolgozásra beérkezés és a felhasználókhoz történő eljuttatás folyamatait is,
- Az informatikai folyamatban szereplő valamennyi dokumentációra.

1.2. AZ IBSZ CÉLJA

Az IBSZ célja a Hivatal tulajdonában lévő informatikai eszköz- és adatvagyon védelmének szabályozása, a 2013 évi L törvény (továbbiakban Informatikai biztonsági Törvény vagy IBTV) 2. biztonsági osztálya szerint.

A 2013. évi L. törvény, valamint a 41/2015 BM rendelet alapján lefolyatott vizsgálat alapján a Hivatal informatikai rendszerei nem teljesítik a jogszabályok által előírt 2. biztonsági osztály előírásait.

A Hivatalnak, a használt informatikai rendszerek és a kezelt adatok vizsgálata alapján, a jogszabály által meghatározott 3. biztonsági szintet kell teljesítenie.

Az IBSZ célja a Hivatal tulajdonában lévő informatikai eszköz- és adatvagyon védelmének szabályozása, a 2013 évi L törvény (továbbiakban Informatikai biztonsági Törvény vagy IBTV) 2. biztonsági osztálya szerint. A Hivatal több alkalmazást is használ, amelyeket a kezelt adatok alapján a 41/2015 BM rendelet 2. biztonsági osztálya szerinti előírások szerint kell védeni. A központilag biztosított adatkezelő

szolgáltatások esetében (ASP szakrendszerek) a Hivatalnak csak a saját informatikai infrastruktúrájában a 2. biztonsági osztály előírásait kell teljesítenie.

A Hivatal célja, a jogszabályi előírások szerinti 2. biztonsági osztály és 3. biztonsági szint elérése, ezért a törvényi előírásoknak nem megfelelő szabályzatok javítására és a szükséges feladatok elvégzésére Cselekvési tervet készít.

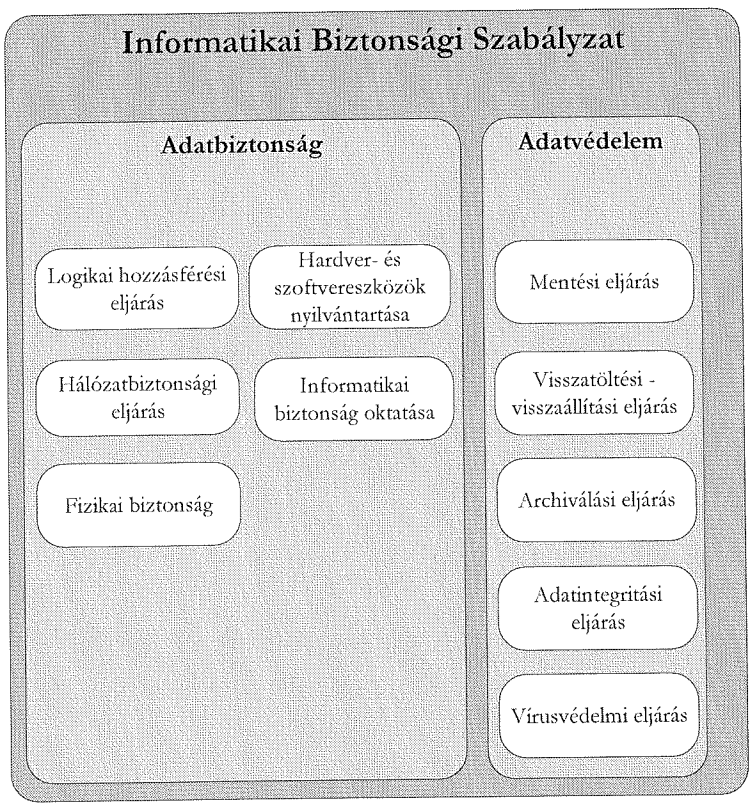
A jelen Informatikai Biztonsági Szabályzat meghatározza a biztonsági intézkedéseket a Hivatalnál működtetett informatikai rendszerre vonatkozóan, valamint az adatbiztonság és adatvédelem szemszögéből eljárásokat és feladatokat határoz meg az adatok osztályozására; a logikai és fizikai hozzáférésre; mentési, archiválási, visszatöltési és adatintegritási eljárásokra vonatkozóan.

Az IBSZ meghatározza a számítástechnikai eszközök beszerzésének és használatának, a szoftverkészítés és alkalmazás, az adatkezelés folyamatának biztonsági szabályait, továbbá az informatikai szerepköröket, és előírja az egyes érintett személyek informatikai biztonságot érintő feladatait.

A célok elérése érdekében a védelemnek működnie kell az egyes rendszerelemek fennállásának teljes ciklusa alatt – a megtervezéstől az alkalmazáson (üzemeltetésen) keresztül a felszámolásukig.

Az Informatikai Biztonsági Szabályzatot rendszeresen, évente legalább egy alkalommal felül kell vizsgálni.

1.3. A SZABÁLYRENDSZER FELÉPÍTÉSE



1.4. FOGALMAK, MEGHATÁROZÁSOK

Az IBSZ-ben használt fogalmak meghatározásait az alábbi táblázat tartalmazza.

Fogalom	*Definíció*
Adat	Jelen szabályzat adatnak tekinti azokat a dokumentumokat, jelentéseket, információkat, leveleket stb., amelyek az informatikai rendszerben elektronikusan tárolódnak.
Adatgazda	Felelős az egyes adatcsoportokhoz történő hozzáférési jogosultságok meghatározásáért. A Hivatal informatikai rendszereiben kezelt adatcsoportjait határozza meg.
Adathordozó	Adathordozónak nevezzük az informatikai rendszertől elválasztható adattároló eszközöket. (CD, DVD, mobil merevlemez)
Mobil eszköz	Minden olyan informatikai eszköz, mely adat továbbításra, feldolgozásra, tárolásra alkalmas. (okostelefon, laptop, tablet)
Bizalmasság	Annak biztosítása, hogy az információhoz csak azok férhessenek hozzá, akik arra jogosultak.
Dokumentum	Számítástechnikai eszközökkel készített irat (fájl), ilyen lehet például Word szövegszerkesztővel vagy Excel táblázatkezelővel készített állomány, stb.
Éles környezet	Számítógépes rendszerek azon részei, ahol a tényleges szolgáltatásokat nyújtó szoftverek üzemelnek.
Esemény	Az esemény a felhasználó által érzékelt váratlan jelenség, amely károsan hat az informatikai biztonságra, ezen keresztül az informatikai szolgáltatásokra.
Felhasználó	Mindazok, akik az informatikai szolgáltatásokat használják, beleértve az informatikai fejlesztői csoportot.
Hitelesség	Egy információ hiteles, ha minden kétséget kizáróan megállapítható annak előállítója és az a tény, hogy az előállítás óta változatlan maradt.
Hozzáférés	Olyan eljárás, amely lehetővé teszi valamely informatikai rendszer használója számára, hogy a rendszerben lévő adatokat elérje (írás, olvasás, módosítás, törlés, stb.).

Információ	Az információk az informatikai rendszerekben adatok formájában jelennek meg.
Informatikai katasztrófa	Egy olyan nem kívánt esemény, amely az adattovábbító, -tároló és -feldolgozó képesség elvesztését okozza hosszabb időre, vagy fizikailag megsemmisül.
Informatikai katasztrófahelyzet kezelési terv	Eljárás vagy tevékenység, lépések sorozata annak biztosítására, hogy az informatikai rendszer kritikus információ feldolgozó képességeit helyre lehessen állítani elfogadhatóan rövid idő alatt a szükséges aktuális adatokkal katasztrófa után.
Informatikai katasztrófahelyzet	Az az állapot, amikor az informatikai rendszer utolsó működőképes állapotát az üzemeltetési szabályok előírásszerű betartásával és végrehajtásával, a meghatározott erőforrások felhasználásával a megállapított helyreállítási időn belül nem lehet visszaállítani.
Informatikai vészhelyzet	Egy olyan nem kívánt állapot, amely az informatikai rendszerhez kapcsolódó üzemeltetési szabályok előírásszerű betartásával és végrehajtásával, a meghatározott erőforrások felhasználásával meghatározott időn belül megoldható.
Internet	Világméretű számítógép-hálózat, amely a különböző rendszerű számítógép-hálózatok ezrei között egy egységes „hálózati társalgási nyelv" – az Internet Protocol – segítségével kommunikációt tesz lehetővé.
Katasztrófa elhárítás tervezés	Lehetővé teszi, hogy egy esetleges katasztrófa bekövetkezte után az informatikai szolgáltatásokat ellenőrzött módon, egy előre megállapított szinten helyreállítják, oly módon, hogy előre meghatározzák a helyreállítás során érvényes személyi felelősségeket, illetve a követendő tevékenységeket.
Kockázatelemzés	Az információs folyamatokra és az információra hatással lévő fenyegetettségek felmérése, bekövetkezési valószínűség és lehetséges hatásuk felmérése. A kockázatfelmérés és kockázatfelbecsülés általános folyamata.

On-line vírusellenőrzés	A valósidejű vagy on-line ellenőrzés feladata a számítógépes rendszer rendeltetésszerű használata közben használatba vett állományok és más objektumok valósidőben, közvetlenül a felhasználás előtt történő ellenőrzése. Ez képezi a rendszer legerősebb védelmi vonalát, és általánosan arra kell törekedni, hogy ez a vonal ne sérüljön, illetve ne inaktiválódhasson.
Off-line vírusellenőrzés	Az off-line, vagy passzív ellenőrzés feladata a teljes állományrendszer átvizsgálása, tekintet nélkül az állományok korára, illetve felhasználásuk gyakoriságára. Ez az üzemmód másodlagos védelmi vonalat képez, redundancia növelő tényező. Alkalmazása feltétlenül szükséges a víruskereső rendszer részeinek, vagy egészének frissítését követően, mivel ez biztosítja a frissítés által megnövekedett vírusismeret azonnali alkalmazását.
Rendelkezésre állás	Biztosítani az arra jogosult felhasználók és feldolgozó erőforrásokhoz való hozzáférését a megfelelő helyen és időben.
Rendszermonitorozó eszközök	Az egész rendszerről gyűjtenek információt és valamilyen csoportosító szempont alapján megjelenítik ezeket.
Informatikus	Legfontosabb feladatai: a Hivatal informatikai és távközlési eszközeinek folyamatos és üzembiztos működtetése, informatikai rendszerekkel kapcsolatos üzemeltetési feladatok elvégzése a lokális hálózatok és munkaállomások, szerverek üzemeltetése.
Rendszerprogram	Olyan alapszoftver, de nem operációs rendszer, mely biztosítja, hogy valamely informatikai rendszer hardvereit használhassuk és az alkalmazói programokat működtessük.
Sértetlenség (Integritás)	Az információ és feldolgozási folyamatok pontosságának és teljességének biztosítása.
Teszt-környezet	Olyan hardver és szoftverkörnyezet, melyen az éles kiadás terítése előtti program,- illetve rendszer-tesztelések zajlanak az éles környezethez hasonló körülmények között.

Tűzfal (firewall)	A tűzfal akadályt jelent a helyi és a külső hálózat között, melyen bizonyos forgalom egyik vagy mindkét irányban nem mehet keresztül, ill. valamilyen további ellenőrzésen megy keresztül. A tűzfalak rendszerint folyamatosan jegyzik a forgalom bizonyos adatait, a bejelentkező gépek, felhasználók azonosítóit, rendkívüli és kétes eseményeket, továbbá riasztásokat is adhatnak.
Virtualizáció	A virtualizáció egy keret rendszer vagy módszer, a számítógép erőforrásainak felosztására, egy többszörös megvalósító környezetre, alkalmazva egy vagy több koncepciót vagy technológiát.
Visszatöltés	Ezzel a funkcióval a korábban a "Mentés" funkcióval lementett adatokat állíthatók helyre. Ilyenkor visszaáll az adatbázis mentéskori állapota, az azóta bevitt adatok, módosítások elvesznek!

1.5. BELSŐ SZERVEZET FELÉPÍTÉSE

Az IBSZ-ben a Hivatal szervezeti felépítésével összhangban a következő főbb felelősségi körök jelennek meg:

- Jegyző

  A jegyző biztosítja a Hivatal információbiztonsági rendszer működtetéséhez szükséges erőforrásokat, jóváhagyja a szabályozásokat és intézkedéseket. Feladata az informatikusok koordinálása, engedélyezi és felügyeli az informatikai rendszer változásait.

- Az adatgazda

  Az informatikai rendszerben rögzített és kezelt adatok tulajdonosa. Felelős az adatok hitelességéért, védelméért, hozzáférési jogosultságok kiosztásáért.

- Az informatikus

  Az informatikus kiemelt jogosultságokkal rendelkező felhasználó, aki működteti az informatikai rendszereket és alkalmazza az előírt biztonsági intézkedéseket, javaslatokat tesz változtatásokra, amivel az információbiztonság hatékonysága javítható.

- A felhasználó

  A felhasználó az informatikai rendszerekhez hozzáféréssel rendelkező munkatárs, aki alkalmazza az IBSZ-ben és egyéb kapcsolódó szabályzatokban meghatározott biztonsági intézkedéseket.

- Informatikai biztonsági felelős

  Feladata a Hivatal informatikai biztonságának és szabályzatainak időszakos felülvizsgálata a 2013 év L törvény 13§, a 41/2015 BM rendelet valamint a Hivatal Informatikai biztonsági szabályzatában található biztonsági követelmények érvényesülésére.

1.5.1. FELELŐSSÉGI KÖRÖK ÖSSZEFÉRHETETLENSÉGI

Az informatikai biztonsági felelős független, szervezetileg nem tartozik a Hivatal által irányított szervezeti egységek egyikéhez sem.

Egyazon személy nem lehet felelős a rendszer beállításáért, ellenőrzéséért.

1.6. BESZÁLLÍTÓK

A Hivatal egyes, nagybiztonságú információs rendszerei, adatai – szerződéses kötelezettségekből eredően – harmadik fél számára is hozzáférhetőek lehetnek.

A Hivatal beszállítókkal szembeni kötelezettségeit a 1.6.1 Biztonsági intézkedések harmadik féllel való együttműködés során fejezet tartalmazza.

A beszállítókkal szemben támasztott követelményeket a beszállítókkal kötött szerződésekben kell megfogalmazni. A 1.6.2 Biztonsági intézkedések kezelése harmadik féllel kötött megállapodásokban fejezet tartalmazza a beszállítókkal kapcsolatos főbb biztonsági kérdések kezelésének módját.

Minden beszállító köteles, a munkájához használt számítógépeken naprakész operációs rendszert és aktív vírusirtó alkalmazást használni.

A 2013 évi L törvény értelmében, a nemzeti adatvagyon védelme érdekében csak Magyarországon üzemeltett szervereken tárolható adat. Harmadik fél által nyújtott adatfeldolgozó szolgáltatást (e-mail, fájl tárhely, stb.) szolgáltatást csak akkor szabad használni, ha az adatokat tartalmazó fizikai szerver Magyarországon található. Az adatok tárolási helyéről a szolgáltatónak a szolgáltatási szerződés megkötése előtt és a szolgáltatási szerződésben is nyilatkoznia kell.

1.6.1. BIZTONSÁGI INTÉZKEDÉSEK HARMADIK FÉLLEL VALÓ EGYÜTTMŰKÖDÉS SORÁN

A Hivatal egyes, nagybiztonságú információs rendszerei – szerződéses kötelezettségekből eredően – harmadik fél számára is hozzáférhetőek lehetnek.

A külső informatikai kapcsolatok általános biztonsági követelményei az alábbiak:

- A külső partnernek titoktartási nyilatkozat aláírásával írásban is meg kell erősítenie, hogy a Hivatal titkait a Hivatal előírásai, a jogszabályoknak és a titokvédelmi szabályoknak megfelelően kezeli.
- Minden Hivatalon kívüli jogi és természetes személy számára biztosítani kell az adatok minősítésének feltüntetését az ***Információ védelmi szabályzat***nak ***(1. számú melléklet)*** megfelelően.
- Különös gondossággal kell eljárni olyan harmadik féllel szemben, amelynek személyzete nem tartózkodik állandóan a Hivatal irodájában, de időszakos fizikai és logikai hozzáférést kap az információs rendszerhez. Ilyenek lehetnek a hardver és szoftver támogatók, karbantartók stb.

Minden olyan esetben, amikor harmadik fél kapcsolódhat be a Hivatal informatikai rendszerébe, kockázatbecslést kell elvégezni, hogy a szükségessé váló különleges óvintézkedéseket meghatározzák.

Külön ki kell értékelni biztonsági szempontból, hogy a külső fejlesztő vagy szállító mennyiben rendelkezik lehetőségekkel a rendszer későbbi veszélyeztetéséhez.

Minden olyan esetben, amikor a Hivatal külső informatikai szolgáltatást vesz igénybe, köteles rendszeresen ellenőrizni, a szolgáltatás során az elvárható és a szerződésben szereplő védelmi intézkedések teljesülését.

Naprakész nyilvántartást kell vezetni, a harmadik fél által elérhető rendszerekről, modulokról. A nyilvántartásnak tartalmaznia kell a beszállító részére létrehozott hozzáférési adatait, jogosultságát. A szerződés lejárta után a hozzáférést meg kell szüntetni. A nyilvántartást rendszeresen, évente legalább egy alkalommal felül kell vizsgálni.

1.6.2. BIZTONSÁGI INTÉZKEDÉSEK KEZELÉSE HARMADIK FÉLLEL KÖTÖTT MEGÁLLAPODÁSOKBAN

A harmadik féllel kötött szerződésekben amennyiben az elkerülhetetlen, a távolról történő hibafelismerést, hibakezelést és diagnosztikai lehetőségeket éles üzemű rendszerek esetében, külön szabályozni kell, pontosan meghatározva az engedélyezett beavatkozások jellegét, körülményeit, korlátozását, kontrollját és az ezzel járó felelősségeket.

A hivatal informatikai eszközeinek beszállítók általi elérése csak biztonságos SSL védett csatornán lehetséges, amelyhez csak megbízható tanúsítvány használható. A távoli elérést minden esetben naplózni kell, a naplónak az alábbiakat kell minimálisan tartalmaznia:

- kapcsolódás ideje,
- forrás IP cím,
- bejelentkezéshez használt felhasználónév,
- kapcsolat bontásának ideje.

- A szolgáltatások külső (nem Hivatal szervezetéhez tartozó) informatikai kapcsolódási pontjaira vonatkozó biztonsági szabályokat meg kell határozni, és a betartásukat ellenőrizni kell.

A biztonsági követelményekről, a biztonsági ellenőrzések körülményeiről és a kapcsolódó intézkedésekről az együttműködési (beszállítói, szolgáltatói stb.) szerződésekben vagy az ezekhez kötött külön megállapodásokban rendelkezni kell.

A helyszínre települt külső személyek kockázatot jelentenek, ezért, a harmadik féllel kötött szerződésben a hozzáféréséből eredő valamennyi biztonsági követelményt és kötelezettséget fel kell tüntetni az elmulasztás következményeivel és a felelősségekkel együtt.

Indokolt esetben titoktartási megállapodást kell kötni a harmadik féllel az információk és az informatikai rendszerek védelme céljából (jellemzően a tartós, nagy értékű és (vagy) a kiterjedt hatókörű együttműködések esetén.

Indokolt esetben fenyegetés mentességi nyilatkozatot kell ellenjegyeztetni a harmadik féllel nyilatkoztatva, hogy az általa szállított termékek, megoldások nem tartalmaznak rosszindulatú kódokat, a fejlesztői jogosultságokat visszavonta és jogtiszta szoftvereket használt.

2. VAGYONTÁRGYAK KEZELÉSE

Az informatikai rendszerekkel kapcsolatos vagyontárgyak a szabvány szerint, a következők:

- információ-vagyontárgyak: adatbázisok és adatállományok, rendszerdokumentáció, használói/kezelői kézikönyvek, oktatási anyagok, üzemviteli, üzemeltetési és támogató eljárások, tartalékolási berendezések, archivált információ;
- szoftver-vagyontárgyak: alkalmazási szoftverek, rendszerszoftver, stb;
- fizikai vagyontárgyak: számítógépek és tartozékegységeik, monitorok, hordozható számítógépek (laptopok), modemek; a távközlési berendezések, mint útvonalválasztók (routerek), alközpontok (PABX-ek), fax-gépek, telefon hívásfogadó és válaszoló berendezések; egyéb műszaki berendezések, mint a tápáramellátó vagy a légkondicionáló egységek; a bútorok és az egyéb kiszolgáló helyiségek berendezései, stb;
- szolgáltatások: számítástechnikai és távközlési ("számítógépes" és "kommunikációs") szolgáltatások

2.1. ADATOK OSZTÁLYOZÁSA

Az adatok osztályozását kockázat elemzés eredménye alapján kell elvégezni. Az adatok osztályozásának kategóriáit, jelölésének és kezelésének módját az ***Információ védelmi szabályzat (1. számú melléklet)*** tartalmazza.

2.2. HARDVER- ÉS SZOFTVERESZKÖZÖK NYILVÁNTARTÁSA, KEZELÉSE

2.2.1. HARDVER- ÉS SZOFTVERNYILVÁNTARTÁS

2.2.1.1. A NYILVÁNTARTÁS TARTALMÁNAK MEGHATÁROZÁSA

Minden a Hivatal tulajdonába kerülő hardverről illetve szoftverről nyilvántartást kell vezetni.

A hardver eszközöket használatba vétel előtt el kell látni azonosító címkével (leltári számmal) és a nyilvántartásba fel kell jegyezni legalább:

- eszköz gyártója, típusa, sorozatszáma
- eszköz leltári száma
- beszerzés ideje

- garancia lejárata
- eszköz állapota (raktárban, selejt, felhasználónak kiadva)
- telepített szoftverek

A szoftverekről az alábbi adatokat kell nyilvántartani:

- szoftver gyártója, típusa
- szoftver sorozat száma
- beszerzés dátuma
- licensz mennyisége
- felhasznált licenszek hozzárendelése a hardverhez

A Hivatal által használt valamennyi szerver és kliens számítógépen meghatározott időközönként, de legalább évente ellenőrizni kell a telepített szoftverek jogtisztaságát, és licensz szerződés szerinti mennyiségét.

A hardver- és szoftvernyilvántartást meghatározott időközönként, de évente legalább egyszer felül kell vizsgálni.

2.2.1.2. ESZKÖZÖK BIZTONSÁGI OSZTÁLYOZÁSA ÉS KEZELÉSE

Hivatal számítástechnikai eszközeit, a hardvereket védelmi osztályokba kell sorolni az ***Információ védelmi szabályzat (1. számú melléklet)*** rendelkezései szerint, és a használat vagy kezelés során az osztályba sorolás szerinti védelmi követelményeket kell alkalmazni. A védelmi osztályok szerinti besorolásokat a ***Besorolási ív (4. számú melléklet)*** tartalmazza.

Azokat az eszközöket, amelyek (biztonsági szempontból) osztályozott adatot, szoftvert, alkalmazást tárolnak, az osztályozással megegyező módon kell kezelni.

Az osztályozott eszközöket más helyiségbe áthelyezni, vagy a Hivatal területéről kivinni csak az arra felhatalmazott személy engedélyével lehet.

Az osztályozott eszközöket az ***Selejtezési Szabályzat (2. számú melléklet)*** szerint kell selejtezni.

Az adatokat és az adatokat kezelő alkalmazásokat a 41/2015 BM rendelet előírásai alapján biztonsági osztályba kell sorolni és gondoskodni kell azok jogszabálynak megfelelő védelméről.

2.3. HARDVER- ÉS SZOFTVER ESZKÖZÖK BESZERZÉSÉNEK SZABÁLYAI

Beszerzés esetén a Hivatal az ***Informatikai Beszerzési Szabályzat***a alapján folytatja le a beszerzést.

Az *Informatikai Beszerzési Szabályzat*ot rendszeresen, de évente legalább egy alkalommal felül kell vizsgálni.

2.4. HARDVER- ÉS SZOFTVER ESZKÖZÖK SELEJTEZÉSE ÉS ÚJRAFELHASZNÁLÁSA

Az informatikai berendezéseken tárolt információk kikerülése akkor is veszélyeztetheti a Hivatal érdekeit, ha egy bizonyos eszközt (például merevlemezt, mágnesszalagot, stb.) ideiglenesen, vagy véglegesen kivonnak a használatból. Ezért ezekről az eszközökről az eszközök tárolásra való felkészítésekor, az irodából való kikerülés előtt, az adatokat az informatikusnak véglegesen, visszaállíthatatlanul törölnie kell.

Kiemelten védendő kategóriába sorolt adathordozót úgy kell megsemmisíteni, hogy arról adat, vagy adatok ne legyenek kinyerhetők, lemásolhatók, helyreállíthatók. (5.9.4 Selejtezés)

A feleslegesnek ítélt eszközöket el kell különíteni és az eszközöket jegyzékbe kell foglalni. A jegyző a véleményezteti az eszközöket, és a hasznosítási javaslatot vagy engedélyezi, vagy elutasítja.

A feleslegessé minősítés megtörténte után haladéktalanul meg kell kísérelni a felesleges vagyontárgyak hasznosítását, ami történhet értékesítés, vagy térítés nélküli átadás formájában.

A felesleges vagyontárgyak értékesítését a jegyző engedélyezheti. A térítés mértékében, az átadás időpontjában, a fizetés módjában és határidejében - az általános pénzforgalmi előírások keretén belül - a felek szabadon állapodhatnak meg. A jegyző által megbízott személy feladata az értékesítést alátámasztó Átadás-átvételi jegyzőkönyvek és kapcsolódó dokumentumok iktatása.

A felesleges eszközök térítés nélkül is hasznosíthatók.

3. EMBERI ERŐFORRÁSOK BIZTONSÁGA

A humánbiztonság-kezelés az emberi tényezőkkel kapcsolatos kockázatok megelőzésére, kiszűrésére, csökkentésére irányul, amelyhez elsősorban nem adminisztratív eszközöket (a szabályok merev alkalmazását) kell alkalmazni, hanem a humánerőforrás-kezelő folyamatokba kell beépíteni a biztonsági követelményeket is figyelembe vevő egységesített eljárásokat; vagyis a humán menedzsment folyamatokat ki kell egészíteni a biztonsági szempontokkal és követelményekkel.

A humánbiztonság-kezelés tehát az emberi tényezőkkel kapcsolatos kockázatok megelőzésére, kiszűrésére, csökkentésére irányul.

A humánbiztonság-kezeléssel kapcsolatban az alábbi alapvető (stratégiai szintű) követelmények fogalmazhatók meg:

- Teljes körű védelem: a védelem terjedjen ki minden minősített adatot előállító, felhasználó és kezelő, személyre, illetve azokra a személyekre, akik az ilyen adatot tároló, feldolgozó és továbbító információs rendszerrel kapcsolatban állnak.
- Zárt védelem: a humánbiztonsági eljárások során ki kell szűrni minden olyan személyt, akinek alkalmazása veszélyeztetheti az információs rendszer biztonságát, és a Hivatal jogi környezete tegye lehetővé az ilyen személyek eltávolítását is.
- Szabályozott védelem: például a hozzáférési és kezelői jogokat az "ismerete szükséges" (need-to-know) elv alapján kell kiosztani.
- Folytonos védelem: a védelem terjedjen ki az emberi erőforrás-fejlesztés teljes életciklusára.
- Kockázatokkal arányos védelem: a humánpolitikai védelmi ráfordítások (pl. a kompetencia-vizsgálat mélysége) arányosak legyenek a biztonsági kockázatokkal.

3.1.1.1. A HOZZÁFÉRÉSI RENDSZER KÖVETELMÉNYEI

Az informatikus, valamint a széles körű hozzáférései jogokat nyert felhasználók neveit és jelszavait minősítetten kell kezelni, esetükben az azonosítás és a hitelesítés kötelező.

Az azonosítás és a hitelesítés folyamatainak meg kell előznie az információs rendszerrel kapcsolatos bármilyen más engedélyezett beavatkozást.

A kliens-szerver alkalmazásoknál az azonosításnak és a hitelesítésnek mind a kliens, mind a szerver oldalon meg kell történnie, amelynek erőssége különböző lehet.

A hozzáférési jogosultságokat folyamatosan aktualizálni kell.

A felhasználói azonosítást egyértelműen kell hozzárendelni minden egyes személyhez, azaz nem létezhet több személy azonos, közös jelöléssel.

A hozzáférési jogok odaítélése, változtatása vagy megvonása csak arra feljogosított és hitelesített személyek által engedélyezett.

A hozzáférési jogosultságok tekintetében a szükséges minimális jogok odaítélésére kell törekedni.

Ki kell dolgozni a hozzáférési jogok nyilvántartási rendszerét, amely rendszerenként, szerepkörönként, személyenként, tartalmazza a szükséges adatokat.

Rendszerenként meg kell határozni, hogy normális üzemben és kivételes helyzetek esetén milyen eseményeket lehet, és melyeket kell naplózni (például a rendszerhez való hozzájutás, adatállományokhoz való hozzájutás, napló-nyomtatás, programlehívások, eredménytelen kísérletek).

Hivataltól távozó alkalmazottak hozzáférési jogait inaktívvá kell tenni.

A hibás vagy sikertelen kísérletekre megfelelő óvó- és ellen intézkedésekkel kell reagálni.

Az információs rendszer minden meghatározó eleme rendelkezzen olyan védelmi mechanizmusokkal, amely megakadályozza illetéktelen személyek logikai hozzáférését a védett rendszerhez.

Az adatkezelési biztonsági rendszer moduláris legyen így biztosítsa, hogy különféle hozzáférési kritériumok alapján meg lehessen határozni, az adatbázisok tartalmához, dokumentumokhoz, szolgáltatásokhoz történő hozzáférés jogosultsági szintjeit (írás, olvasás, törlés, stb.).

Az operációs rendszer rendelkezzen megfelelő hozzáférés-ellenőrzési, naplózási funkciókkal.

Az operációs rendszer védelmi erejének az alkalmazáshoz illeszkedő, lehető legnagyobb logikai védelmet biztosítania kell.

3.1.1.2. HOZZÁFÉRÉSI JOGOSULTSÁGOK NYILVÁNTARTÁSA

Az informatikus feladata a 3.2.2 Felhasználói jogosultságok létrehozása 3.2.3 Felhasználói jogosultságok megszüntetése, megváltoztatása fejezetek szerint a jogosultságok kezelése, és az elkészült jogosultság beállításról visszajelzést küldése az igénylőnek.

Az informatikus feladata a *Jogosultság nyilvántartást (3. számú melléklet)* aktualizálni és egy példányát zárható helyen köteles tárolni.

3.2. INFORMATIKAI BIZTONSÁGI KÖVETELMÉNYEK A MUNKASZERZŐDÉSBEN

A munkaszerződésekben rögzíteni kell munkavállalók felelősségének körét, a jogviszony fennállása utáni kötelezettségeket és ezek megsértése esetén a fegyelmi és felelősségre vonási eljárásokat.

A fejezet tartalmazza a munkavállalók be és kiléptetésének szabályait, valamint a munkavállalókkal szemben elvárt felelősségeket, kötelességeket.

A munkavállalót a munkaszerződés megkötésekor tájékoztatni kell a kötelezettségeiről, felelősségeiről, és a felelősségre vonás szabályairól. A munkavállalónak ki kell töltenie és alá kell írnia az ***5. sz. melléklet - Alkalmazotti nyilatkozat*** dokumentumot. Az alkalmazotti nyilatkozatokat a jegyző által megbízott személy köteles tárolni.

3.2.1. MUNKATÁRSAK INFORMATIKAI BIZTONSÁGI KÉPESÍTÉSI KÖVETELMÉNYEINEK MEGHATÁROZÁSA

Alapvető követelmény, hogy valamennyi munkatárs rendelkezzen a munkája ellátásához szükséges felkészültséggel.

A képesítési követelmények alapdokumentumai a munkaköri leírások, amelyek minden új munkakör létrehozásakor, illetve már meglévő munkakörök változásaikor szükségszerűen elkészülnek, ezért mindenkor az aktuális állapotot rögzítik.

3.2.2. FELHASZNÁLÓI JOGOSULTSÁGOK LÉTREHOZÁSA

Új dolgozó belépésekor, vagy ha egy dolgozó új munkakörbe kerül, vagy a munkakörhöz tartozó feladatokkal kapcsolatban ez szükségessé válik, a dolgozó vezetője (magasabb beosztású vezető) megigényli a dolgozó felhasználói azonosítójának/azonosítóinak, valamint a leendő munkahelyi környezetének létrehozását. Ehhez kitölti a ***Felhasználói jogosultság igénylő lap (8. számú melléklet)*** és ***Munkahelyi környezet létrehozása/megszüntetése (7. számú melléklet)*** formanyomtatványokat az adott dolgozó számára a munkaköri feladatainak az ellátásához. A felhasználói jogosultságot igénylő vezető feladata a csoportba sorolás és a csoport jogosultságon felüli jogok meghatározása.

Az informatikus kitöltött igénylőlap alapján létrehozza a rendszerekben az igényelt azonosítókat, kialakítja a munkahelyi környezetet, amit aláírásával igazol, és frissíti a jogosultság nyilvántartást. ***3. számú melléklet –Jogosultság kiosztási nyilvántartás)***

A ***Felhasználói jogosultság igénylő lap (8. számú melléklet)*** és ***Munkahelyi környezet létrehozása/megszüntetése (7. számú melléklet)*** igénylőlapokat az informatikus tárolni köteles.

3.2.3. FELHASZNÁLÓI JOGOSULTSÁGOK MEGSZÜNTETÉSE, MEGVÁLTOZTATÁSA

Ha egy dolgozó valamely vagy összes munkaköre megszűnik (áthelyezés, felmondás stb. során), a felhasználói azonosítóit, valamint a munkahelyi környezethez kapcsolódó hálózati hozzáféréseket haladéktalanul le kell tiltani, majd amennyiben lehetséges, meg kell szüntetni. A dolgozó vezetője megigényli a dolgozó felhasználói azonosítójának/azonosítóinak, valamint a munkahelyi környezetének megszüntetését. Ehhez kitölti a ***Felhasználói jogosultság igénylő lap (8. számú melléklet)*** és ***Munkahelyi környezet létrehozása/megszüntetése (7. számú melléklet)*** című formanyomtatványokat. A kitöltött igénylőlapok alapján az informatikus megszünteti a megfelelő rendszerekben az igényelt azonosítókat, a munkahelyi környezetet, amelyet az aláírásával igazol.

A jegyző jogosult arra, hogy bármely munkatárs valamely vagy összes érvényben lévő felhasználói azonosítóját azonnali hatállyal letiltathassa. A szükséges adminisztrációt ebben az esetben is el kell végezni, azonban ebben az esetben elegendő utólag elvégezni a dokumentációt.

Az adatok megőrzésének módját, illetve a megőrzés idejét és a megőrzendő adatok védelmét a dolgozó felettes vezetője határozza meg.

Egy dolgozó jogviszonyának megszűnéséről a felettes vezetőjét valamint a jogviszony megszűntetését végző informatikust is értesíteni kell. A kilépő dolgozó munkaügyi papírjait csak a felhasználói azonosítóinak letiltása vagy törlése után szabad átadni.

3.2.4. FELHASZNÁLÓK LOGIKAI HOZZÁFÉRÉSSEL KAPCSOLATOS KÖTELESSÉGEI, FELELŐSSÉGE

A felhasználóknak ismerniük kell a jelszavak, illetve a kezelésükben lévő berendezések használatára vonatkozó előírásokat.

A Hivatal informatikai rendszerének használatával kapcsolatos felhasználói feladatok:

- A felhasználói jelszavak titkosan kezelendők.
- A jelszó elfelejtése esetén a felhasználó az informatikustól igényelhet ideiglenes jelszót. Az ideiglenes jelszót az első bejelentkezés alkalmával kötelező megváltoztatni.
- A jelszó megválasztására, és a jelszavak kezelésére vonatkozó szabályokat a 6.1.1.1 Jelszómenedzsment fejezet tartalmazza.
- A jelszót a felhasználó semmilyen körülmények között nem jelenítheti meg a különböző adathordozókon, képernyőn, papíron stb.

Felhasználói jogosulatlan hozzáférés kísérlete esetén – a sikerességre vagy sikertelenségre való tekintet nélkül - a felhasználót felelősség terheli. Minden, az informatikai rendszerek hozzáférésével kapcsolatos visszaélési kísérletet haladéktalanul jelenteni kell az informatikusnak, aki jegyzőkönyvet vesz fel az eseményről és jelenti a jegyzőnek. ***(9. számú melléklet – Incidens bejelentő lap)***

3.2.5. ESZKÖZÖK VISSZASZOLGÁLTATÁSA

Amennyiben a dolgozó a továbbiakban nem kívánja, vagy nem jogosult használni az eszközt, vissza kell szolgáltatnia az informatikusoknak, és értesíteni kell az eszköz használatát engedélyező személyt.

Az eszközök raktárba való visszavételének lépései:

- A gépnek és tartozékainak tételes átvétele,
- Az észlelt hibák jegyzőkönyvbe vétele,
- A gépen lévő adatok törlése, vagy megfelelő helyre való mentése.

3.3. FELELŐSSÉGI KÖRÖK

A felhasználói, az üzemeltetői, rendszertámogatói és fejlesztői jogosultságokat el kell határolni.

3.3.1. FELELŐSSÉGI KÖRÖK ÖSSZEFÉRHETETLENSÉGI SZABÁLYAI

Felelősségi körök kijelöléskor az alábbi szabályokat be kell tartani:

- Szigorúan meg kell osztani a feladatokat és a felelősségeket emelt biztonságú környezetben.
- El kell különíteni egymástól a biztonsági ellenőrzést végző személyek feladatait az ellenőrzöttek körétől.
- Fejlesztői jogosultsággal rendelkező személyek nem üzemeltethetik, és nem végezhetnek adatfeldolgozást az általuk fejlesztett rendszerben.

3.4. INFORMATIKAI BIZTONSÁG OKTATÁSA

3.4.1. A FEJEZET CÉLJA

A felhasználói képzések célja, hogy a felhasználók tájékozottak legyenek az informatikai biztonsági követelményekkel kapcsolatban, és tudatában legyenek a követelmények figyelmen kívül hagyásának következményeivel és veszélyeivel. Az oktatásnak ki kell térnie az informatikai biztonsági, adatvédelmi folyamatokra, szabályozásokra és az adatfeldolgozás célszerű módszereire ezzel csökkentve a biztonsági kockázatokat.

3.4.2. MUNKATÁRSAK INFORMATIKAI BIZTONSÁGI KÉPESÍTÉSI KÖVETELMÉNYEINEK MEGHATÁROZÁSA

Az informatikai biztonsági oktatásokat a jegyző által megbízott személynek kell megszerveznie. Az oktatáson részt kell vennie a Hivatal informatikai infrastruktúrát használó alkalmazottainak. A képzésnek ki kell terjednie a biztonsági követelményekre, azok megsértésének következményeire, a kapcsolódó törvényi és hatósági szabályzásokra, a szervezeten belül használandó eljárásokra, információs folyamatokra. Tudatosítani kell az informatikai biztonsági eljárások folyamatait, a hozzáférési jogosultságokat, a szerzői stb. jogok figyelembe vételét.

Alapvető követelmény, hogy valamennyi munkatárs rendelkezzen a munkája ellátásához szükséges felkészültséggel. E követelmény teljesítése érdekében a vonatkozó jogszabályok és a munkavállalók vezetőinek igénye alapján meghatározandók a dolgozókra vonatkozó általános és speciális képesítési előírások. A munkavállalók vezetőinek igényei alapján a jegyző által megbízott személy állítsa össze a képesítési követelményeket, amely igények informatikai és biztonsági vonatkozásainál az informatikus véleményét figyelembe kell venni. A képesítési követelmények alapdokumentumai a munkaköri leírások, amelyek minden új munkakör létrehozásakor, illetve már meglévő munkakörök változásaikor szükségszerűen elkészülnek, ezért mindenkor az aktuális állapotot rögzítik.

3.4.3. INFORMATIKAI BIZTONSÁGI OKTATÁSI/KÉPZÉSI TERVEK ELKÉSZÍTÉSE

A Hivatal éves oktatási terv informatikai biztonsági oktatásokat tartalmazó részének összeállításához az oktatandó témaköröket és területeket a jegyző által megbízott személy határozza meg a tárgyévet megelőzően, figyelembe véve Hivatal oktatási tervét. Az oktatási tervet az informatikai biztonsági felelős véleményezi figyelembe véve az informatikai biztonság szempontjait.

Az informatikai biztonsági színvonal fenntartása érdekében rendszeresen biztosítani kell az informatikai biztonsági oktatást és megfelelő szintű továbbképzést:

- Az új alkalmazott felvételénél,
- Alkalmazott új munkakörbe kerülésénél
- Új alkalmazások bevezetésénél,
- Új technológia bevezetésénél.

3.4.4. INFORMATIKAI BIZTONSÁGI OKTATÁSOK, KÉPZÉSEK LEBONYOLÍTÁSA

Az informatikai biztonsági oktatás keretében kiemelt hangsúlyt kell fordítani a felhasználói tevékenységek felügyeletére és szabályozására, hiszen statisztikai adatok alapján az informatikai rendszerekben bekövetkező fennakadások, hibák legnagyobb részéért közvetve vagy közvetlenül a felhasználók a felelősek.

A képzés gyakorlati lebonyolításához a Hivatal informatikai rendszerének lehetőségei szerint kell eljárni.

3.4.5. INFORMATIKAI BIZTONSÁGI OKTATÁSOK, KÉPZÉSEK NYILVÁNTARTÁSA

A külső oktatásokon, képzéseken való részvétel igazolása, a megszerzett képesítő okirat (bizonyítvány) bemutatása a jegyző által megbízott személynek, a beiskolázott dolgozók feladata. A jegyző által megbízott személy feladata a munkatársak által elvégzett külső és belső képzések, oktatások személyre lebontott nyilvántartása.

Az alkalmazottak informatikai felkészültségét a munkaköri követelmények, a munkaköri leírások és a gyakorlati tevékenység alapján a munkavállalók vezetői évente egyszer értékelik, és az értékelés eredményét a későbbi oktatási tervben figyelembe veszik.

3.5. FELHASZNÁLÓK KÖTELESSÉGEI

3.5.1. FELÜGYELET NÉLKÜL HAGYOTT SZÁMÍTÓGÉPEK

Ha a felhasználó szünetelteti munkaállomáson végzett tevékenységét, ki kell jelentkeznie, és zárolnia kell a számítógépet. Amennyiben nem jelentkezik ki, automatikus képernyővédőt kell alkalmazni, melynek időzített aktiválása a munkaállomás kihasználatlansága esetén nem lehet több 15 percnél. A rendszernek meghatározott idő után újra kell indítania az azonosítási és a jogosultság ellenőrzési folyamatot, a felhasználó csak az újbóli bejelentkezés, illetve jelszó megadás után folytathatja a munkát.

A megnyitott alkalmazásokat, a használatot követően a felhasználónak be kell zárnia.

A felügyelet nélkül hagyott felhasználói munkaállomások védelme érdekében a munkaállomások beállításait az informatikusok végzik. A felhasználóknak tilos az informatikusok által beállított paramétereket megváltoztatni.

3.5.2. RENDSZER-FÜGGETLEN MENTÉSI ELŐÍRÁSOK FELHASZNÁLÓK SZÁMÁRA

Az alacsony, a kritikus és magas rendelkezésre állási kategóriába sorolt adatokat mindig a központi munkakönyvtárban kell tárolni.

Amennyiben nem központi mentéssel rendelkező tárterületre dolgoznak a Hivatal felhasználói (fájlszerver, alkalmazás központi adatbázisa), hanem saját munkaállomáson tárolnak, vagy dolgoznak fel adatokat, a felhasználók kötelezettek a következő szabályok betartására:

- A kritikus és magas rendelkezésre állási kategóriába sorolt adatokat mindig két különböző helyen kell tárolni (pl.: felhasználók saját munkaállomásai és központi szerver, vagy külső adathordozó).
- Az irodai alkalmazásokban be kell kapcsolni és 10 percre állítani az automatikus mentési funkciót, és ettől függetlenül öt-tízpercenként kézzel is menteni kell.
- A bizalmas és szigorúan bizalmas információkat tartalmazó adatokat titkosítással is védeni kell.

3.5.3. „TISZTA ASZTAL, TISZTA KÉPERNYŐ" POLITIKA

A következő szabályokat minden munkatársnak be kell tartania:

- Értekezletek végén a védendő, vagy kiemelten védendő adatokat tartalmazó dokumentumokat az értekezlet színhelyéről el kell távolítani.
- A Hivatal hardvereinek és szoftvereinek valamint adathordozóinak nem hivatali célból történő átadása harmadik személy részére tilos.
- Külső személyeknek csak akkor szabad a szerződéses munka kapcsán dokumentumokat átadni, ha a titoktartásról szóló megfelelő írásbeli megállapodás már létrejött.
- Védendő, vagy kiemelten védendő adatokat az *Információ védelmi szabályzatban (1. számú melléklet)* leírtak szerint kell kezelni.
- Védendő adatok faxon történő továbbításánál személyesen ellenőrizni kell mind a küldő, mind a fogadóoldalon, hogy illetéktelen személy nem férhet hozzá a dokumentációhoz.
- Ha védendő, vagy kiemelten védendő adatok faxon kerülnek továbbításra, a fax rendeltetésszerű megérkezését telefonhívással kell ellenőrizni.
- Az íróasztalon csak az adott munkafolyamattal kapcsolatos dokumentumok lehetnek, minden más dokumentumot el kell zárni.
- A nem használt adathordozókat (papír alapú és informatikai eszközök) el kell zárni.
- A számítógép „asztalán" csak a munkához szükséges alkalmazások parancsikonjai legyenek kihelyezve.
- A számítógépen csak azok az alkalmazások legyenek elindítva, illetve csak azok a dokumentumok legyen megnyitva, amelyek az adott munkafolyamat elvégzéséhez feltétlenül szükségesek.
- Amennyiben egy dokumentumra a munkafolyamat során vagy a munkafolyamat befejeztével már nincs szükség, úgy azt a központi szerverre fel kell másolni, vagy fel kell tölteni az adatkezelő alkalmazásba és a számítógépről le kell törölni.

A munkahely elhagyásánál meg kell akadályozni programok és adatok illetéktelen használatát:

- Ki kell jelentkezni a nem használt és hitelesítést igénylő alkalmazásokból.
- Be kell zárni a megnyitott dokumentumokat.
- Jelszavas képernyővédőt kell alkalmazni a 3.5.1 Felügyelet nélkül hagyott számítógépek fejezetben leírtaknak megfelelően.
- El kell távolítani és el kell zárni a hordozható adattároló eszközöket.
- Ki kell kapcsolni a számítógépet.

4. FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG

Az objektumvédelem magában foglalja:

- az épületbe, helyiségekbe, a hozzájuk kapcsolódó területekre való belépés ellenőrzését,
- az illetéktelen behatolás megakadályozását,
- az épületben, helyiségekben, a területen való mozgás figyelését, ellenőrzését,
- a műszaki létesítmények, berendezések, al- és felépítmények állapotában bekövetkező változások megfigyelését, ellenőrzését,
- valamint a megfigyelések, ellenőrzések eredményeinek elemzése-értékelése alapján történő visszacsatolást (beavatkozást, korrekciót és a beavatkozás, korrekció érdekében igénybe veendő erőforrások folyamatos biztosítását).

4.1. BIZTONSÁGI ZÓNÁK

4.1.1. A FEJEZET CÉLJA

A biztonsági zónák kialakítása magában foglalja a Hivatal informatikai védelméhez szükséges építészeti, technikai és szervezeti intézkedéseket, valamint a különálló területeken lévő különleges biztonsági követelményeket igénylő informatikai központok minden károsodással járó befolyás elleni védelmét.

4.1.2. ALAPELVEK

A Hivatal tulajdonában és kezelésében lévő informatikai eszközök üzemképességének megőrzése érdekében minden, az eszközök működését veszélyeztető fenyegetettség ellen, annak bekövetkezési valószínűsége és az esetleges kárértéke függvényében megelőző- és ellenintézkedéseket kell kialakítani. A Hivatal jelentős informatikai eszközeit fenyegető kockázati tényezők:

- Áramkimaradás,
- Túlmelegedés,
- Tűzkár,
- Lopás, szándékos károkozás,
- Vízkár,
- Természeti katasztrófa/előre nem látható katasztrófa (baleset),

- Terrorizmus/katonai akció.

A kockázati tényezők és az azokhoz rendelhető megelőző és ellenintézkedések kapcsolatát az alábbi táblázat foglalja össze:

Kockázati tényezők és lehetséges megelőző ellenintézkedések	Szünetmentes tápellátás	Környezet monitorozása	Légkondicionálás	Tartalékeszközök	Tűzvédelem	Redundáns eszközök/telephely	Betörésvédelem
Áramkimaradás	■					■	
Túlmelegedés		■	■			■	
Tűzkár		■		■	■	■	
Lopás, szándékos károkozás				■		■	■
Vízkár				■		■	
Természeti katasztrófa						■	
Terrorizmus/katonai akció						■	

A követelménycsoportok feladatai:

- **Szünetmentes tápellátás:** biztosítsa az elektromos berendezés folyamatos áramellátását és ingadozásmentes feszültségellátását.
- **Környezet felügyelete:** jelezze az informatikai rendszer biztonságos működését befolyásoló környezeti paraméterek (hőmérséklet, páratartalom, a levegő por tartalma, víz, elektrosztatikus sugárzás) megengedett szinttől való eltérését, illetve megjelenését a helyiségben.
- **Légkondicionálás:** biztosítsa a helyiség optimális hőmérsékletét.
- **Tartalékeszközök:** biztosítsa a kieső eszköz azonnali pótlását.
- **Tűzvédelem:** jelezze a helyiségben lévő tüzet.

- **Redundáns eszköz/telephely:** biztosítsa az eszköz/telephely használhatatlansága esetén az elvárt szolgáltatások megfelelő szintű ellátását.
- **Betörésvédelem:** biztosítsa az eszközök fizikai biztonságát.

A biztonsági zónákra vonatkozó előírásokat, és a belépésre jogosultak nyilvántartását rendszeresen, évente legalább egyszer felül kell vizsgálni. Szükség esetén módosítani kell a szabályzatot valamint a nyilvántartást.

4.1.3. BIZTONSÁGI ZÓNÁK KIALAKÍTÁSA

A biztonsági zónák kialakítása magában foglalja a Hivatal informatikai védelméhez szükséges építészeti, technikai és szervezeti intézkedéseket, valamint a különálló területeken lévő különleges biztonsági követelményeket igénylő informatikai központok minden károsodással járó befolyás elleni védelmét.

A Hivatal informatikai rendszereinek fizikai védelme négy (a kárértékhez igazodó) biztonsági zónára tagozódik:

1. **Alap biztonsági zóna** – a Hivatal épületeinek belső területei;
2. **Kliens számítógépek zónája** – az alap biztonsági zónákon belül kliens számítógéppel ellátott helyiségek (irodák);
3. **Emelt szintű biztonsági zóna** – a Hivatal épületeinek azon helyiségei, ahol informatikai berendezések (hálózati eszközök,) kerültek elhelyezésre (informatikus irodája, az épületekben található szerverek és adatmentő eszközök helysége);
4. **Kiemelt biztonsági zóna** – az alap biztonsági zónákon belül fokozott védelmet igénylő helyiség: a központi szerverszoba.

A biztonsági zónák egymáshoz való viszonya:

4.1.4. BIZTONSÁGI ZÓNÁK VÉDELME

4.1.4.1. ÁLTALÁNOS BIZTONSÁGI INTÉZKEDÉSEK, KÖVETELMÉNYEK

A jegyző feladata kezdeményezni, hogy a követelményeknek megfelelő biztonsági zónák kerüljenek kialakításra. A környezeti követelmények kialakítását, üzemeltetését és karbantartását eseti jelleggel szerződéses külső munkatárs végzi. A biztonsági zónák követelményeknek való folyamatos megfelelőségét a jegyző által megbízott személy ellenőrzi, az eltéréseket írásban rögzíti.

Amennyiben a feltételek nem kielégítőek, az érintett rendszer a hiányosságokat figyelembe véve csak korlátozottan üzemeltethető.

A munkatársakat és külső személyeket tájékoztatni kell a biztonsági zónák létezéséről és a hozzájuk kapcsolódó betartandó előírásokról. A biztonsági zónákban munkát végző felhasználó, vagy külső munkavállaló csak annyit tudhat meg a Hivatal informatikai rendszereiről és adatairól, amennyi a szerződésben meghatározott munka elvégzéséhez feltétlenül szükséges.

4.1.4.2. BELÉPTETÉS BIZTONSÁGI ZÓNÁKBA, ILLETVE AZ INFORMATIKAI BIZTONSÁGI ZÓNAHATÁROKON

A Hivatal munkatársai kötelesek jelenteni a felettes vezetőnek, ha a belépésre jogosulatlan személy tartózkodik a Hivatal területén, illetve a be és kilépés ellenőrzése nem lehetséges. A belépéshez szükséges kódokat és azonosító kulcsokat rendszeresen cserélni kell. A hitelesítő eszközök kompromittálódása, elvesztése esetén azonnal cserélni kell őket.

Kliens számítógépek biztonsági zónákba való belépés további szabályai:

- A zónába az ott dolgozó munkatársak jogosultak belépni. Jogosultsággal nem rendelkező személyek belépését az iroda munkatársa engedélyezheti, vagy informatikus kíséretében tartózkodhat ott.
- A jogosultsággal nem rendelkező személyek magatartásáért és esetleges károkozásáért a kísérő személy a felelős.
- Az irodák kulcsait csak az arra jogosultak tudják felvenni és leadni.
- A kliens számítógépek zónájába tartozó vagy attól magasabb biztonsági kategóriába sorolt helyiségeket zárva kell tartani, ha nem tartózkodik bent senki.

Emelt szintű biztonsági zónákba való belépés további szabályai:

- A zóna területén a jogosultsággal nem rendelkező személyek csak kísérő jelenlétében tartózkodhatnak. A belépést a jegyző vagy az informatikus engedélyezheti, az engedélyt elegendő szóban megadni. Az informatikai területhez tartozó kulcsokat csak az arra jogosultak tudják leadni, illetve felvenni.

Kiemelt biztonsági zónákba való belépés további szabályai:

- A zóna területén a jogosultsággal nem rendelkező személyek csak kísérő jelenlétében tartózkodhatnak. A belépést a jegyző engedélyezheti, az engedélyt elegendő szóban megadni. A jogosultsággal nem rendelkező személyek magatartásáért és esetleges károkozásáért a kísérő személy a felelős.
- Rendkívüli esemény bekövetkezésekor az informatikai területhez tartozó kulcsokat a jegyzői titkárságon, a jegyző által felhatalmazott személy veheti fel. Ezekben az esetekben a kulcsok felvételéről jegyzőkönyvet kell készíteni, mely jegyzőkönyvet az jegyzőnek el kell juttatni. Karbantartási tevékenység nem minősül rendkívüli eseménynek.

4.1.5. ALAP BIZTZONSÁGI ZÓNA

A Hivatal épületeinek külső védelme biztosítja a biztonsági zónák megfelelő, teljes és homogén elkülönítését.

A Hivatal épületének külső részét meg kell világítani.

A növényzet nem nyújthat rejtőzködési és mászási lehetőségeket a homlokzaton lévő ablakoknál és más nyílászáróknál.

A biztonsági zónák területét a létesítményekkel együtt teljeskörű és homogén rendszerrel kell biztosítani.

Az átjárók mennyiségét és nyitva tartottságát a szükséges minimumra kell korlátozni.

A zónában csak nyilvános besorolású, tájékoztató dokumentumokat szabad elhelyezni.

A zónában tilos informatikai eszközök, védendő vagy ettől magasabb biztonsági osztályba sorolt dokumentumokat tartalmazó szekrény vagy polc elhelyezése.

4.1.6. A KLIENS SZÁMÍTÓGÉPEK ZÓNÁJÁRA VONATKOZÓ KÖVETELMÉNYEK

Az általános biztonsági intézkedéseken és követelményeken felül az alábbi szabályozásoknak kell teljesülniük.

Csak a felettes vezetők, illetve az általuk kijelölt munkatársak kliens számítógépein tárolhatók védendő kategóriába sorolt adatok, dokumentumok.

A kliens számítógépeket az illetéktelen fizikai megbontás ellen védeni kell. Pl.: plombával.

A kliens számítógépeket a lehetőségekhez képest, úgy kell elhelyezni az irodában, hogy:

- a monitor képét csak a számítógépet használó munkatárs láthassa,
- az kliens számítógép fizikailag ne legyen hozzáférhető az ügyfelek részére.

4.1.7. EMELT SZINTŰ BIZTONSÁGI ZÓNÁKRA VONATKOZÓ KÖVETELMÉNYEK

A kliens biztonsági zónára vonatkozó követelményeken felül az alábbi szabályozásoknak kell teljesülniük.

Az informatikai helységek kialakítása nem javasolt alagsorban vagy ez alatti szinteken. (vízkár esetén fokozott veszélynek vannak kitéve az eszközök)

4.1.7.1. TÁPELLÁTÁSSAL KAPCSOLATOS INTÉZKEDÉSEK

Az informatikai rendszer eszközeinek üzemeltetéséhez lehetőség szerint külön elektromos hálózatot kell létrehozni. A hálózat terhelhetősége legyen nagyobb, mint amekkora terhelést a rácsatlakoztatott eszközök egyidejű használata okoz. Erre a hálózatra kizárólag csak az informatikai rendszerhez tartozó eszköz csatlakoztatható.

Az elektromos hálózat a hálózati eszközök és az eszközök menedzsmentjét, felügyeletét végző számítógépek vonatkozásában 30 perces áthidalási idejű, megszakításmentes átkapcsolással rendelkező szünetmentes tápegységgel legyen ellátva. A szünetmentes tápegységek hálózati betáplálása csak a Hivatal erre a célra kialakított elektromos hálózatáról történhet. Erre a hálózatra csak az informatikai eszközök csatlakoztatható, más elektromos fogyasztót rákapcsolni tilos.

4.1.7.2. TŰZVÉDELEMI INTÉZKEDÉSEK

A helyiségeket CO_2 tűzoltó készülékekkel kell ellátni, amelyeket a bejáratok előtt a falakon kell elhelyezni.

Minden éghető anyagot lehetőség szerint el kell távolítani a központi hálózati eszközöket tartalmazó helyiségből.

4.1.8. KIEMELT SZINTŰ BIZTONSÁGI ZÓNÁKRA VONATKOZÓ KÖVETELMÉNYEK

Az emelt szintű biztonsági zónára vonatkozó követelményeken felül az alábbi szabályozásoknak kell teljesülniük.

4.1.8.1. ÁLTALÁNOS BIZTONSÁGI INTÉZKEDÉSEK, KÖVETELMÉNYEK

Célszerű a szerverterem maximális szeparálását biztosítani és az ottani munkavégzést minimalizálni. A szerverterem feladata elsősorban a szerver gépek, hálózati eszközök biztonságos működésének biztosítása. Lehetőség szerint az informatikusok irodájában kell elvégezni mindenféle lehetséges beavatkozást a szerverek konzolon keresztüli elérése segítségével.

A szerver-helyiségekben biztosítani kell az ott elhelyezett technikai eszközök, és a kábelezés áttekinthetőségét, logikus elrendezését. Az eszközök, kábelek legyenek ellátva jól felismerhető, a rendeltetésre utaló címkével.

A helyiségeket biztonsági zárakkal, riasztórendszerrel és füstérzékelővel kell ellátni.

A szerverterem ablakai legyenek védettek betekintés ellen. A betekintés elleni védelmet függöny, vagy védőfólia segítse.

A szervereket és az archivált anyagokat tartalmazó helyiségekbe csak annak üzemeltetéséhez elengedhetetlenül szükséges közműhálózat csatlakozhat, tehát a helyiségen belül nem mehet át víz, gáz, csatorna és egyéb közművezeték, felette és a határoló falfelületeken ún. vizes blokkot tartalmazó helyiségrész ne legyen.

A belépéseket fel kell jegyezni a *Géptermi naplóba (10. számú melléklet).*

4.1.8.2. HŐMÉRSÉKLETRE, PÁRATARTALOMRA ÉS EGYÉB KÖRNYEZETI TÉNYEZŐKRE VONATKOZÓ INTÉZKEDÉSEK

A központi szerverszobát (a szünetmentes energiaellátást szolgáló berendezések helyiségét) klimatizálni kell úgy, hogy az információ-technológiai eszközök környezeti hőmérséklete működés közben 15-24 C°, tárolási hőmérséklete 0-40 C° között maradjon, a relatív páratartalom pedig ne haladja meg a 40%-ot.

A légkondicionáló berendezéseket úgy kell beállítani, hogy áramszünet után automatikusan visszakapcsoljanak.

4.1.9. BERENDEZÉSEK KARBANTARTÁSA, JAVÍTÁSA

4.1.9.1. A KARBANTARTÁS TERVEZÉSE, SZEREPLŐI

Az informatikai eszközökre vonatkozó rendszeres karbantartási munkákat a jegyző által megbízott személy tervezi és határozza meg. A számítástechnikai eszközök működtetéséhez szükséges, a környezeti infrastruktúrához kapcsolódó elemek karbantartási munkáit és azok ciklusidejét szerződéses külső munkatárs tervezi és végzi el a jegyző által megbízott személy javaslatai alapján. Rendszeresen, évente legalább egy alkalommal felül kell vizsgálni a karbantartási terveket.

A karbantartási munkák szervezésénél figyelembe kell venni a berendezések gyártóinak előírásait, ajánlásait és az üzemeltetési tapasztalatokat.

4.1.9.2. A KARBANTARTÁS ÉS JAVÍTÁS SZABÁLYAI

A műszaki üzemeltetés, karbantartás és javítás feladatait az informatikus vagy – külön eseti megbízás alapján – erre feljogosított szervezetek látják el, illetve biztosítják.

Ha az eszköz meghibásodik, károsodik, értesíteni kell az informatikust, aki megállapítja a meghibásodás okát. Nem rendeltetésszerű használatból eredő hiba esetén jegyzőkönyvet kell felvenni, és egy-egy példányát meg kell küldeni az eszköz használójának és a jegyzőnek. Ha a kár az eszköz nem rendeltetésszerű használatából következik be, kártérítési eljárás indítható.

Az informatikai rendszer egyes elemeinek karbantartását, javítását, szerelését csak olyan személyek végezhetik, akik a munkavégzésük során esetlegesen tudomásukra jutott titkos információk megőrzésére vonatkozóan titoktartási nyilatkozatot írtak alá, vagy a munkavégző személyt foglalkoztató vállalkozás – a megbízásából kiküldött személyre vonatkozóan is – titoktartási kötelezettséget vállalt.

A Hivatal informatikai berendezéseit kiszolgáló, illetve periféria típusú eszközeinek (például szünetmentes tápegységek, nyomtatók, fénymásolók, faxok) karbantartását megfelelő szakképzettséggel rendelkező személyeknek szakszerűen kell karbantartani, biztosítva ezzel a folytonos rendelkezésre állást és integritást. Csak az informatikus vagy a jegyző által megbízott, arra jogosult személy tarthatja karban és javíthatja az eszközt.

A karbantartást, vagy javítást végző szolgáltatók az emelt vagy kiemelt biztonsági zónába sorolt helyiségekben csak a munkavégzést engedélyező, a jegyző által megbízott személy felügyelete mellett tartózkodhatnak, dolgozhatnak.

Távoli karbantartás, vagy hibajavítás csak informatikus felügyelete mellett végezhető.

A hálózat-karbantartási munkákat - mentések, szoftvertelepítés, eszközszerelés és mindazon rendszermenedzseri tevékenység, amely a hálózat üzemelését jelentősen lelassítja – munkanapokon, a folyamatos munkarend zavarásának minimalizálásával vagy munkaidőn túl szabad elvégezni, a felhasználók egyidejű értesítésével, rendkívüli esetektől eltekintve.

Az informatikusok által menedzselhető rendszerbe nem integrált helyi rendszerek, illetve a hálózatba nem kapcsolt számítógépek meghibásodása esetén a felhasználók írásban jelzik az informatikusok felé a meghibásodást.

Munkaállomást javítás céljára csak abban az esetben szabad kivinni, ha nincs benne merevlemez. Kiemelten védendő besorolású adatokat tartalmazó javításra szoruló merevlemezt javításra kiadni TILOS, az ilyen merevlemezt le kell selejtezni, az 5.9.4 Selejtezés fejezetben leírt szabályok szerint. Az adathordozók szállításának feltételeit az 4.1.10 Eszközök kivitele, illetve 5.9.3 Az adathordozók használatának, szállításának feltételei, követelményei fejezet tartalmazza.

Az eszközök javítása után az informatikusnak ellenőriznie kell a javított eszköz működését, és adatbiztonsági ellenőrzést kell végezni.

4.1.9.3. DOKUMENTÁLÁSI KÖTELEZETTSÉGEK

Az eszköz javítását, karbantartását, a feladatokat elvégző személynek egyidejűleg dokumentálnia kell (munkalap). A dokumentálás során fel kell tüntetni:

- feladatot végző személy nevét,
- feladat elvégzésének okát,
- dátumát,
- feladat mibenlétét.

4.1.10. ESZKÖZÖK KIVITELE

A Hivatal tulajdonában vagy kezelésében lévő informatikai, illetve információ-kezelő eszközök kivitele a Hivatal területéről jegyző által kiállított szállítólevéllel történhet. A szállítóleveleket a jegyző által megbízott személy tárolja.

Hordozható számítógépek állandó használatára jogosult személyeket a jegyző határozza meg.

A Hivatal tulajdonát képező hordozható személyi számítógépeket a Hivatal területén kívül csak a jegyző által felhatalmazott személyek használhatják.

A tartósan a Hivatal területéről kikerülő eszközöket be kell vezetni a 2.2 Hardver- és szoftvereszközök nyilvántartása, kezelése fejezetben megjelölt módon.

4.1.11. A SZERVEREKRE VONATKOZÓ ELŐÍRÁSOK

A szervereket lehetőség szerint a kiemelt biztonsági zónákban kialakított szerverteremben kell elhelyezni.

A szerverekre vonatkozó megfelelő környezeti feltételeket 4.1.8 Kiemelt szintű biztonsági zónákra vonatkozó követelmények fejezetbe foglalt előírások szavatolják.

A szerverek esetén a javítási munkákat helyben kell elvégezni. Ha az elszállítás elkerülhetetlen, a szerverek kiszállításához - mint minden informatikai eszköz kiviteléhez - a jegyző írásos engedélye szükséges és az 4.1.10 Eszközök kivitele fejezet rendelkezéseit be kell tartani. A karbantartási feladatokat az 4.1.9 Berendezések karbantartása, javítása fejezetben leírtak szerint kell elvégezni.

A szerverterem eszközeinek beállításait (mind hardver, mind hálózati alapbeállítások) aktuálisan dokumentálni kell. A dokumentálást az informatikus végzik.

4.1.12. EGYÉB HÁLÓZATI ESZKÖZÖKRE VONATKOZÓ ELŐÍRÁSOK

Az aktív hálózati eszközöket lehetőség szerint emelt biztonsági zónákban kell elhelyezni.

4.1.13. A TELEFONKÖZPONTRA ÉS A RENDEZŐKRE VONATKOZÓ ELŐÍRÁSOK

A telefonközponthoz csak a telefonrendszer üzemeltetéséért felelős férhet hozzá.

4.1.14. FELHASZNÁLÓI SZÁMÍTÓGÉPEKRE VONATKOZÓ ELŐÍRÁSOK

Felhasználói számítógépet kizárólag csak az 4.1.6 A kliens számítógépek zónájára vonatkozó követelmények, vagy annál szigorúbb biztonsági követelményeknek megfelelő helyiségekbe lehet elhelyezni.

Az informatikusnak a beállítások jogosulatlan megváltoztatása miatt keletkezett hibák esetén jegyzőkönyvet kell felvennie a nem megfelelő használat tényéről, majd a hibát el kell hárítania. A jegyzőkönyvet a gép használójának is alá kell írnia. A jegyzőkönyv egy példányát át kell adni a felhasználó felettes vezetőjének.

Minden informatikai eszközt használó munkatárs köteles az általa használt eszköz hibájának észlelésekor tájékoztatni az informatikust. Az informatikus intézkedik a hiba elhárításáról. Meghibásodás esetén – amennyiben a hibát nem tudják elhárítani, vagy a garanciális szerződések értelmében nem háríthatják el, értesítik a javítást végző szakmailag kompetens partnert és továbbiakban az 4.1.9 Berendezések karbantartása, javítása meghatározott módon járnak el.

A felhasználó az eszközök rendeltetésszerű használatáért és működtetésért egy személyben felelős.

4.1.15. BERENDEZÉSEK KÁBELEZÉSÉNEK BIZTONSÁGA

Az informatikai kommunikációs berendezések (pl. rack-szekrény) kábelezése rendezett, strukturált kialakítású legyen. A berendezések erősáramú kábelezését fizikailag el kell választani az informatikai-kommunikációs kábelektől.

A végpontokat számmal és felirattal kell jelölni és engedély nélkül tilos a meglévő hálózati vezetékek (UTP) áthelyezése más aljzatba.

A belső hálózatot megfelelő logikai védelemmel is el kell látni. (pl: MAC cím szűrés, port védelem, 802.1x)

4.1.16. ESZKÖZÖK VÉDELME IRODÁN KÍVÜL

A hordozható számítógépeket és az ahhoz kapcsolódó számítástechnikai berendezéseket szállító személyek:

- Kötelesek a számítógépet a szállítás idejére lehetőleg minél kevésbé szem előtt lévő módon elhelyezni.
- Hordozható számítógépeket TILOS a gépjárműben őrizetlenül hagyni!
- Azokban az esetekben, amikor az eszközöket nem a Hivatal tulajdonában lévő irodában (szálloda, lakás) kell hagyni, fokozott figyelmet kell fordítani a jogosulatlan hozzáférés, az adatok esetleges módosítása, megrongálása, vagy ellopása elleni védelemnek. Ha tartozékként rendelkezésre áll biztonsági rögzítő, akkor annak használata kötelező.

- Amikor a hordozható számítógépet nem használják a pendrive-ot, mobil merevlemezes egységet a hordozható számítógépből kivéve, attól elkülönítve, biztonságos helyen szükséges.

Az eszközök kivitelére vonatkozó általános tudnivalókat az 4.1.10 Eszközök kivitele fejezet tartalmazza.

4.1.16.1. A BERENDEZÉSEK BIZTONSÁGOS TÁROLÁSA

A tartalékberendezéseket, a kritikus rendszerdokumentációk, szoftverek törzspéldányait és a biztonsági adathordozókat a munkavégzés helyétől távoli és védett helyen kell tartani.

Az érzékeny adatokat tároló és feldolgozó eszközöket úgy ajánlatos elhelyezni, hogy a használat alatti rálátás kockázatát lecsökkentsük.

A rendszer teljes életciklusa során gondoskodni kell az adott rendszerre meghatározott fizikai és környezeti biztonságról.

Biztosítani kell, hogy az informatikai rendszer kritikus elemeire maradéktalanul kiterjedjen a fizikai hozzáférés-ellenőrzés, amely így megakadályozza az illetéktelen hozzáférést a védett elemekhez.

Munkahelyről elszállított (kihelyezett) olyan eszköz, berendezés vagy tárgy (bármilyen számítógép, modem, mobiltelefon, fénymásoló, dokumentum stb.), amelyet - Hivatal felhatalmazása alapján - az irodán kívül használnak, egyenértékű biztonsági megítélés alá esik azzal, amelyet ugyanazon célra házon belül használnak, figyelembe véve azt a kockázatot, amit a Hivatal számára a házon kívül végzett tevékenység jelent.

5. A KOMMUNIKÁCIÓ ÉS ÜZEMELTETÉS IRÁNYÍTÁSA

Az informatikai rendszerek és az adatok védelmére vonatkozó előírásokat rendszeresen, de évente legalább egyszer felül kell vizsgálni.

5.1. AZ ÜZEMELTETÉSI ELJÁRÁSOK ÉS FELELŐSÉGI KÖRÖK

Az üzemeltetési feladatok meghatározása és karbantartása jegyző vagy az általa megbízott személy feladata.

Az üzemeltetési feladatokat tartalmazó szabályzatot rendszeresen, évente legalább egy alkalommal felül kell vizsgálni.

5.1.1. FELADATKÖRÖK, JOGOSULTSÁGOK, KÖTELEZETTSÉGEK ÖSSZEFÉRHETETLENSÉGE

Az informatikus, és az informatikai biztonsági felelős szerepköröket különböző személyek tölthetik be. A változások engedélyezését, beállítását, ellenőrzését nem végezheti ugyanaz a személy.

5.1.2. VÁLTOZÁSKÖVETÉS

Az üzemeltetési és változáskezelési előírásokat rendszeresen, évente legalább egy alkalommal felül kell vizsgálni.

Meg kell határozni, és le kell dokumentálni a Hivatal által használt informatikai rendszerek alapkonfigurációját. A konfiguráció és a hozzá kapcsolódó dokumentációt rendszeresen felül kell vizsgálni, és ha szükséges a módosításokat el kell végezni.

A Hivatalnál használt szoftverek frissítéseinek mindig az üzembiztosan telepíthető legfrissebb verzióját kell alkalmazni. A frissítések megjelenését követően haladéktalanul le kell tesztelni és alkalmazni kell a frissítéseket, ha üzembiztosan telepíthetők.

A szoftverek használata közben jelentkező hibát minden felhasználó köteles jelenteni az informatikusnak. A szoftver hibás működését az informatikusnak jeleznie kell a szoftver gyártója felé, és az 5.2 Rendszer tervezés és elfogadás fejezetben foglaltak szerint kell eljárnia.

Az alkalmazott operációs rendszerek frissítéseinek mindig az üzembiztosan telepíthető legfrissebb verzióját kell alkalmazni az operációs rendszer hibáiból adódó kockázatok mérséklésének érdekében. Minden az operációs rendszer működését, konfigurációját érintő változás esetén az éles rendszerrel megegyező környezetben tesztelni kell a változásokat.

Az informatikai rendszerekben, azok fejlesztése és üzemeltetése során bekövetkező változások követésére ki kell alakítani a megfelelő változás–menedzsmentet.

Az informatikai rendszer tervezése, megvalósítása és üzemeltetése során felmerült összes változást – a minőségügyi dokumentumokban meghatározott változáskövetési eljárással – dokumentálni kell.

Az informatikai rendszerek - és különösen a védelmi rendszer - összes dokumentációjára is érvényesíteni kell a változáskövetést.

Az üzemeltetési és biztonsági dokumentációkat napra készen kell tartani az üzemeltetés biztonsága és hatékony hibakezelés érdekében.

5.2. RENDSZER TERVEZÉS ÉS ELFOGADÁS

5.2.1. FEJLESZTÉSI, TESZTELÉSI ÉS ÜZEMELTETLÉSI RENDSZEREK KEZELÉSÉNEK, VÉDELMÉNEK SZABÁLYAI

A Hivatal informatikai rendszereinek teljes életciklusában biztosítani kell a rendszer által elérhető maximális védelmet. Figyelemmel kell kísérni az adatbiztonságot érintő változásokat és szükség esetén javító intézkedéseket kell tenni.

Szoftver fejlesztésekor a tervezés előtt meg kell határozni a fejlesztésben résztvevő szereplők információ biztonsági felelősségét, szerepét, feladatát.

Különbség van új szolgáltatás bevezetését célzó projekt és már létező szolgáltatáshoz kapcsolódó projekt esetében:

- Új szolgáltatás bevezetése esetében még nincs változáskezelés
- Létező szolgáltatás esetében az új módosítási igények jöhetnek az igény vagy hibalistából.

Mindkét esetben részletes rendszertervet kell készíteni, és az elkészült rendszerterv alapján biztonsági kockázatelemzést kell készíteni.

A fejlesztések során már a fejlesztés indítási fázisában el kell kezdeni összegyűjteni és kezelni a kockázatokat, és ezt folytatni kell a fejlesztés lezárásáig.

A fejlesztői és teszt tevékenységeket az éles üzemeltetői környezettől elkülönült környezetben szabad csak végezni úgy, hogy az ne veszélyeztesse az informatikai szolgáltatások működését.

A jegyzőnek kell előírni, hogy mely változás végrehajtása előtt szükséges tesztelés.

5.2.2. A BEMENŐ ADATOK ÉRVENYESSÉGÉNEK ELLENŐRZÉSE

Az adatbeviteli hibák felismerésére és korrigálására céljából ki kell dolgozni azokat az eljárásokat, amelyek biztosítják a nem megfelelő adatok visszautasítását az adatok rögzítésekkor.

5.2.3. FELDOLGOZÁS FELÜGYLETE, AZ ÜZENETEK SÉRTETLENSÉGÉNEK ELLENŐRZÉSE

Az feldolgozási folyamat csak hozzáférés-ellenőrzés mellett engedélyezett.

Az adatok feldolgozásához szükséges jogosultságokat rögzíteni kell, és a jogosultságokat rendszeresen ellenőrizni kell.

A bevitt adatok bizalmasságát, hitelességét és sértetlenségét valamint a rendelkezésre állást biztosítani kell.

Az adatfeldolgozás során biztosítani kell a sértetlenséget olyan biztonsági funkciókkal, mint pl. ellenőrző összeg képzése, digitális aláírás vagy elektronikus pecsét.

5.2.3.1. FELHASZNÁLÓI JOGOSULTSÁGOK KEZELÉSE

A hozzáférés jogosultság menedzselésénél a hozzáférés-vezérlés elvét kell alkalmazni a következő hozzáférési jogokkal:

- olvasási jog (betekintés),
- írási jog (létrehozás, módosítás),
- törlési jog,
- végrehajtási jog.

A saját fejlesztésű, illetve az éles üzemeltetés közvetlen támogatására használt idegen rendszereknek mindenképpen, az egyéb célra vásárolt (nem kritikus) rendszereknek pedig lehetőleg alkalmasnak kell lenniük a hozzáférési jogok egyedi vagy csoport szinten történő megkülönböztetésére és szabályozására.

A jogosultsági rendszereknek támogatniuk kell a jogosultságok módosítását, átadását másik személynek, törlését és időleges korlátozását. Új jogosultság kiosztását, a jogosultság törlését vagy átmeneti felfüggesztését csak erre felhatalmazott informatikus vagy adatgazda végezhesse el.

A jogosulatlan hozzáférési kísérleteket rögzíteni kell a biztonsági naplóban, amelynek értékelését rendszerenként kijelölt személyeknek, rendszerenként meghatározott időközönként el kell végezni.

5.2.4. KAPACITÁSMENEDZSELÉS

Az informatikus feladata, hogy évente felmérje a meglévő kapacitásokat és a várható kapacitás igényeket, illetve évközben nyomon kövessék az informatikai rendszerek kihasználtságát és a beszerzési időt figyelembe véve jelezze a jegyzőnek, ha kapacitásbővítésre van szükség.

A jegyző feladata, hogy az éves fejlesztési tervekbe beépítse a jogos kapacitás igényeket, valamint a váratlan kapacitás hiány esetén intézkedjen a rendelkezésre

álló kapacitások átcsoportosításáról vagy a kapacitások bővítéséhez szükséges beszerzések elindításáról.

5.2.5. RENDSZEREK BEVEZETÉSE

Üzembeállítás feltételei, új informatikai rendszerek, illetve meglévők új verziójának elfogadásának és átvételének minimális feltételei - melyek teljesülését a jegyző által megbízott személy ellenőrzi - az alábbiak:

- Átadásra kerül a telepítő készlet, forráskód, telepítő leírás, helyreállítási (roll-back) eljárás és rendszer dokumentáció egyértelmű verzióazonosítóval ellátva
- Felhasználói és üzemeltetői tesztek, beleértve a biztonsági tesztek megtörténtek
- Oktatások megtörténtek
- Kommunikáció a felhasználók felé megtörtént

Az új rendszer, vagy rendszer összetevő csak akkor vezethető be, ha az informatikai szabályzatoknak megfelel. Ha szükséges az informatikai szabályzatok frissítése, azt csak kockázatelemzés, vagy a rendszer auditálás után szabad csak elvégezni.

5.3. VÉDELEM ROSSZINDULATÚ ÉS MOBIL KÓDOK ELLEN

A fejezet célja, hogy a Hivatal egészére tekintve megfogalmazásra kerüljenek a vírusfertőzés megelőzésére, és mielőbbi detektálására, a fertőzés megszűntetésére vonatkozó szabályok és feladatok.

A vírusvédelem feladata a Hivatal informatikai rendszereinek, azaz a különböző operációs rendszerrel működő szervereknek, különféle munkaállomásoknak és hálózaton kívül üzemelő számítógépeknek a számítógép-vírusok elleni hatékony védelme. A védelemtől elvárható, hogy működjön együtt az internet böngésző alkalmazásokkal, és támogassa az elterjedt levelező klienseket is.

5.3.1. ÁLTALÁNOS VÍRUSELLENŐRZÉSI TUDNIVALÓK

A vírusvédelmi rendszerek hatékonyságának két legfontosabb összetevője:

- A védelmi szoftvernek jó minőségűnek és kellő gyakorisággal aktualizáltnak kell lennie, hogy felismerési hatékonysága maximális legyen.
- A védelmi szoftvernek minden potenciális támadási ponton aktívan üzemelnie kell.

A fenti specifikációnak megfelelően a következő védelmi rétegek kialakítása szükséges:

- A munkaállomások ellenőrzése, mivel ezek jelentik a vírusok által megcélzott elsődleges támadási felületet. A víruskereső szoftvernek minden lehetséges bejutási pontot ellenőriznie kell (CD-ROM, hálózat, e-mail, pendrive stb.).
- A rendszerben működő fájl- és alkalmazásszerverek, tűzfalak, levelező szerverek másodlagos támadási felületet jelentenek. Védelmük jelentős redundanciát visz a rendszerbe, és feltétlenül szükséges. A telepített víruskeresőnek – a munkaállomásokon futó változathoz hasonlóan – minden lehetséges bejutási pontot ellenőriznie kell (CD-ROM, hálózat, e-mail, pendrive stb.), különös tekintettel a szerverek rendeltetésszerű használata közben fellépő adatforgalomra (pl. fájlok forgalmazása, levelezés stb.).
- Az internetes levélforgalmat vizsgáló levélszemét-szűrő eszköz.

A víruskereső rendszerek két alapvető működési móddal rendelkeznek: valósidejű (aktív), illetve off-line (passzív) üzemmódban dolgoznak. A hatékony védelem alapvető követelménye mindkét működési mód párhuzamos használata.

A vírusadatbázisok frissítése a rendszer hatékonyságának szempontjából kritikus fontosságú, mivel az elektronikus hálózatok korában az új vírusok megjelenése és globális elterjedése között esetenként csupán néhány óra telik el.

A vírustámadások elleni védekezés Hivatal szintű megtervezése, kialakítása valamint a vírusadatbázisok rendszeres frissítésének megszervezése, az informatikus feladata.

Biztosítani kell a Hivatal egészére kiterjedő, rendszeres és folyamatos vírusvédelmet kereskedelemben kapható, kiterjedt referenciával rendelkező szoftverekkel. A frissítésről az informatikusnak folyamatosan gondoskodnia kell.

A kialakított rendszer monitorozása és működtetése az informatikusok feladata.

5.3.2. VÍRUSVÉDELMI ELŐÍRÁSOK

A vírusvédelmi programok beállítása során – a megadott védelmi szint betartása mellett - törekedni kell a rendszerek optimális használhatóságára.

A Hivatal számítógépes hálózatához csak aktív és naprakész adatbázis frissítésekkel rendelkező vírusirtó alkalmazással ellátott számítógép csatlakoztathat.

5.3.2.1. TELEPÍTÉS

A víruskereső rendszerek konkrét telepítésének megszervezése, a telepítés automatizálása az informatikus feladata, ennek eredményeképpen minden külső adat fogadására alkalmas munkaállomáson rendszeresen frissített vírusfigyelő és törlő programnak kell működnie.

Az újonnan rendszerbe állított, illetve újratelepített számítógépeken gondoskodni kell a víruskereső rendszer telepítéséről. Megfelelően friss vírusvédelmi rendszer nélkül szervert és munkaállomást üzembe állítani tilos!

Amennyiben az alkalmazott víruskereső rendszer erre lehetőséget ad, akkor a hálózaton keresztül központosítva felügyelhető változatokat kell telepíteni. A telepítéskor gondoskodni kell róla, hogy a hálózati adminisztráció során egyértelműen megkülönböztethetők legyenek a különböző gépektől érkező adatok (üzenetek, jelentések, vírusminták, stb.).

Az informatikus feladata a központosított menedzselés, vagy előkészített telepítőkészlet hiányában telepítéskor a szükséges konfiguráció beállítása. Az informatikusnak gondoskodnia kell arról, hogy a felhasználók önhatalmúlag ne csökkenthessék a vírusvédelmi rendszer működésének hatékonyságát és be kell kapcsolnia a vírusirtó alkalmazás konfigurációs felületének jelszavas védelemét.

A központi gépeken és a tűzfalon a vírusvédelem programjait úgy kell installálni, hogy minden file-megnyitás, file-zárás, futtatható file indítása műveletet automatikusan ellenőrizzenek. Az ellenőrzés felfüggesztése tilos.

5.3.2.2. AKTÍV VÉDELEM

A vírusvédelmi rendszer fő komponense az aktív (tárrezidens, valósidejű) védelem, mely a számítógép működése során állandóan dolgozik. Feladata a felhasználói munka során igénybe vett állományok (programok, adatok, dokumentumok) közvetlen használat előtti vírusellenőrzése. Az aktív védelem kikapcsolása tilos!

Amennyiben a felhasználó a víruskereső program lefuttatása során vírust észlel, fel kell jegyeznie a fertőzött file nevét, a munkaállomása nevét, és ezeket az adatokat jelenteni kell az informatikus felé, akik gondoskodnak a vírus további terjedésének megakadályozásáról, és – amennyiben a felhasználói gépen futó program automatikusan nem törölte – a vírus szakszerű kiirtásáról.

Az aktív védelem informatikus általi bármely okból történő kikapcsolása esetén a passzív védelem kiemelt jelentőségű, ezért az informatikus feladata a vírusvédelem megoldása (akár pl. hálózati kábel kihúzása stb).

A vírusirtó aktív védelmének beállításakor engedélyezni kell, hogy a vírusirtó automatikusan küldjön riasztást az informatikus email címére, amennyiben kártevőt észlel. Az informatikusnak a beérkező riasztást meg kell vizsgálnia, és annak eredményétől függően kell eljárnia.

5.3.2.3. PASSZÍV VÉDELEM

A passzív védelem feladata a teljes állományrendszer átvizsgálása, tekintet nélkül az állományok használatára. A vizsgálatot havonta 1 alkalommal lehetőség szerint automatikusan le kell futtatni. A vizsgálat automatikus futtatásának beállítása az informatikus feladata.

A rendszerbe kívülről bekerülő fájlokat (akár USB-n beérkező, akár az Internetről letöltött adatról van szó) felhasználás előtt vírusellenőrzésnek kell alávetni. A

vírusirtót úgy kell beállítani, hogy lehetőség szerint automatikusan ellenőrizze az adathordozó illetve a fájlok tartalmát az alábbi esetekben:

- hordozható adattároló eszközök (pendrive, mobil merevlemez) csatlakoztatásakor,
- fájlok internetről történő letöltésekor,
- email megnyitásakor.

A vizsgálat automatikus futtatásának beállítása az informatikus feladata. Ha a vírusirtó nem képes automatikusan lefuttatni a víruskeresést a felsorolt események bekövetkezésekor, akkor a felhasználó feladata és felelőssége a keresés kézi indítása.

A passzív védelem futása több időt is igénybe vehet, mivel sok állomány ellenőrzését végzi. A víruskeresést megszakítani tilos.

A passzív védelem különösen fontos akkor, ha az aktív védelem valamilyen okból deaktivált. Az újbóli aktiválásig a passzív védelem használata a felhasználó feladata és felelőssége, aki köteles minden, a rendszerbe bekerülő adat (pl. USB, CD-ROM, e-mail melléklet) ellenőrzését a passzív védelmi rendszerrel azonnal, a felhasználás előtt elvégezni.

5.3.3. FRISSÍTÉSEK

A víruskereső rendszerek frissítése két vonalon zajlik: a vírusadatbázisoknak, illetve maguknak a víruskereső motoroknak a frissítése. Általánosan a vírusadatbázisok frissítése lényegesen gyakoribb.

A víruskereső programok frissítéseit (vírusinformációs adatfájlok és motorok) célszerű az Interneten keresztül elvégezni.

A víruskereső programok frissítését úgy kell beállítani, hogy az automatikusan, naponta legalább egyszer megtörténjen. Ennek technikai kidolgozása és rendszerbe állítása az informatikus feladata.

A víruskereső rendszert fejlesztő cégektől érkező figyelmeztetésekre reagálva indokolt esetben azonnali kiegészítő vírusadatbázis-frissítés szükséges.

A beszállítók számítógépein használt vírusirtók adatbázisának frissítéséről a számítógép tulajdonosának kell gondoskodnia.

5.3.4. VÍRUSFERTŐZÉS

A víruskeresők a fertőzés tényének kimutatása után a konkrét vírusok karakterisztikájától függően képesek a fertőzések eltávolítására.

Vírusfertőzés riasztás esetén a számítógépet AZONNAL ÁRAMTALANÍTANI KELL (hosszan nyomva tartva a számítógép bekapcsoló gombját). NEM HASZNÁLVA AZ OPERÁCIÓS RENDSZER LEÁLLÍTÁSI PARANCSÁT!!!

Amennyiben a fertőzés automatikusan nem távolítható el, úgy az alábbiakat kell alkalmazni:

- a fertőzött állományt törölni kell.
- Az állomány kiterjesztésének megváltoztatásával annak tartalmára a rendszer következtetni nem tud, így a vírusfertőzés megállítható, a fájl vizsgálható.
- A vírusok „karanténba" zárásával, azaz a felhasználók által nem elérhető helyre történő mozgatásával, mely könyvtárhoz csak az informatikusok férhetnek hozzá, és ők végzik el a szükség esetén a további vizsgálatokat.

5.4. BIZTONSÁGI MENTÉSI ELJÁRÁS

A fejezet célja a Hivatal informatikai rendszerében tárolt adatok mentési, visszatöltési eljárásainak, valamint a mentett, azaz sokszorosított adatok biztonságos tárolására vonatkozó szabályok meghatározása.

5.4.1. TERVEZÉSI LÉPÉSEK A HIVATAL INFORMATIKAI RENDSZEREINEK BIZTONSÁGI MENTÉSÉHEZ

Új mentési rendszer kialakításának, vagy a régi rendszer átalakításának **első lépése** a mentési rendszerterv – *Mentési utasítás (12. számú melléklet)* - meghatározása. A rendszerterv tervezésnél, mint környezeti paramétereket figyelembe kell venni, hogy milyen okokból történhet adatvesztés, és melyik informatikai biztonsági esemény milyen gyakorisággal következhet be. Az informatikus készíti el az adott rendszerre vonatkozó mentési, archiválási dokumentációt, melyet a jegyző jóváhagy. Az alábbi felsorolás sorrendje egyben bekövetkezési valószínűséget is jelent, csökkenő sorrendben.

Káresemény bekövetkezhet:

- Felhasználói hiba,
- Hardver hiba (merevlemez),
- Vírustámadás,
- Adatmentés,
- Betörés, lopás,
- Természeti csapás stb. következtében.

A rendszerterv kialakításánál az informatikai rendszer sajátosságait és alapvető követelményeit megfogalmazó alábbi alapadatokat kell figyelembe venni:

- A rendszer mentendő adatainak mennyisége,
- A rendszer mentendő adatainak növekedési üteme,

- A rendszer adatainak változási sűrűsége,
- A rendszer felhasználóinak száma,
- A hálózat átlagos és maximális sebessége,
- Az adatok tárolási környezetének bonyolultsága, a környezet újraépítésének nehézségei.
- Jogszabályi követelmények

A tervezés **második lépése** az adatok osztályozása, azaz annak meghatározása, hogy a rendszerben lévő adathalmazok milyen fontosak a szervezet számára. Ennek kialakítása az *Információ védelmi szabályzatban (1. számú melléklet)* találhatók. A mentendő adatok meghatározása után az informatikusnak kell a mentési rendszerterv alappilléreit meghatározni. A mentési alapkövetelmények a következők:

- Mentési frekvencia, – a mentések sűrűsége.
- Mentési eljárás, – központi mentés, mely a következő módszerek egyikével történhet:
    - Teljes mentés,
    - Inkrementális mentés,
    - Teljes és inkrementális mentés kombinációja.
    - Adatbázis kezelők esetében:
        - Off-line mentés,
        - On-line mentés.
- Mentő eszközök fajtája, típusa, mennyisége, elhelyezése.

Az **utolsó lépés** a mentési rendszerterv kialakításához meghatározni a mentés végrehajtását leíró következő paramétereket:

- A mentési időpontot,
- A mentések megőrzési idejét,
- A mentési eljárást a rendszeren belül,
- A mentő eszközök fajtáit.

5.4.2. MENTÉSI ELŐÍRÁSOK A BIZTONSÁGI MENTÉSÉRT FELELŐS MUNKATÁRSAK SZÁMÁRA

A mentésekért az informatikus a felelős. Meg kell határoznia a mentési terveket, a végrehajtási utasításokat, és a biztonsági előírásokat. A mentésért felelősnek kell a mentések dokumentumait ellenőriznie, és a biztonsági előírások használatát betartatni.

A rendszerekre vonatkozó *Mentési utasításban (12. számú melléklet)* definiálni kell a következőket:

- Mentendő köteteket vagy könyvtárakat,
- Az alkalmazandó média típusát, nevét,
- A rendszeres mentést indító script helyét és nevét.

A *Mentési utasítás (12. számú melléklet)* példányát zárható páncélszekrényben kell elhelyezni. A dokumentum létrehozásáért, tartalmának kialakításáért az informatikus a felelős.

Az informatikus kötelessége meggyőződni arról, hogy a mentések hiba nélkül lefutottak-e. Amennyiben a mentés során hiba történt, a hiba okát fel kell deríteni és az okot meg kell szüntetni. A hiba okának megszüntetése után, vagy ha a hibajelenségre nem található ok és feltételezhető, hogy a következő mentés hiba nélkül lezajlik, a mentést meg kell ismételni. A mentés hibás lefutása esetén a hiba kijavítása után a mentést ismételten el kell végezni.

Az adatok — alkalmazások és fájlszerverek — mentését automatikusan kell indítani *Mentési utasítás (12. számú melléklet)* meghatározottak szerint.

5.4.3. OPERÁCIÓS RENDSZEREK, AKTÍV ESZKÖZÖK BEÁLLÍTÁSAINAK RENDSZER SZINTŰ BIZTONSÁGI MENTÉSE

A Hivatal informatikai rendszerében megtalálható aktív eszközök beállításainak és firmware-nek mentésére, valamint a szerverek operációs rendszerét érintő változás esetén az operációs rendszerek mentésére rendszerszintű mentést kell készíteni, melynek felelőse az informatikus.

A munkaállomások operációs rendszerét érintő változás esetén (pl: szoftver upgrade), az operációs rendszer mentésére, ha lehetséges rendszerszintű mentést kell készíteni. A rendszerszintű mentésekből egyszerűen és gyorsan visszaállítható az adott rendszer egésze, megtakarítva az installáció nehézkes és hosszú műveletét. A rendszerszintű mentés készítését erre alkalmas szoftverrel kell elvégezni.

5.4.4. DOKUMENTÁLÁS

A mentési tevékenységről a mentőrendszer mentési naplót készít, mely tartalmazza a mentés dátumát, állapotát, és szükség esetén egyéb megjegyzéseket. A mentés során észlelt rendellenességek esetén, a hiba elhárítása után a mentést meg kell ismételni. A naplókat automatizált szoftverrel kell vizsgálni, és a naplóelemző rendszernek email értesítést kell küldenie a hibás vagy sikertelen mentésekről.

A mentési naplót a jegyző által megbízott személy ellenőrizi.

5.5. VISSZATÖLTÉSI, VISSZAÁLLÍTÁSI ELJÁRÁS

A fejezet célja a Hivatal informatikai rendszerének adathordozóin tárolt adatok visszatöltési, visszaállítási eljárásainak meghatározása.

5.5.1. ADATOK VISSZATÖLTÉSÉNEK, VISSZAÁLLÍTÁSÁNAK SZABÁLYAI

Az adatok visszatöltését az adott rendszer üzemeltetésével megbízott informatikus vagy az informatikus által megbízott külső szolgáltató végezheti el. A visszatöltést fokozott vagy kiemelt sértetlenségi kategóriába sorolt adat/alkalmazás esetén a jegyző engedélyezi.

Az egyedi felhasználók jogosultak saját munkakönyvtáraiknak adataira vonatkozó visszatöltést önállóan is kezdeményezni, az informatikusnál.

A felülírásból adódó adatvesztés megelőzése miatt, az adatok visszatöltése, visszaállítása általában nem végezhető el az adatok eredeti helyén, környezetében. Erre a célra az eredeti környezettel megegyező jogosultsági beállításokkal rendelkező ideiglenes környezetet kell létrehozni, és az adatok visszatöltését, visszaállítását ide kell végrehajtani. Az adatokat csak ezt követően szabad az eredeti helyre visszaállítani.

Speciális szoftverek segítik a különféle mentési, visszatöltési, visszaállítási eljárások használatát. Ezek a szoftverek általában operációs rendszer és adatbázis, valamint mentőeszköz függők. Kiválasztásukat a mentési rendszerterv részeként kell elvégezni.

Az adatmentés megfelelő működésének ellenőrzése érdekében, rendszeresen, évente legalább egy alakalommal adatvisszaállítási próbát kell végezni, és jegyzőkönyvet kell felvenni a tesztelésről. Az adatvisszaállítási próba elvégzése az informatikus feladata. A teszt adatok visszaállítását egy ideiglenes környezetbe kell elvégezni, és ellenőrizni kell az visszaállított adatok használhatóságát. A teszt befejezése után törölni kell a tesztkörnyezetet.

5.5.2. VISSZATÖLTÉSHEZ, VISSZAÁLLÍTÁSHOZ SZÜKSÉGES PARAMÉTEREK KIJELÖLÉSE

A visszatöltéshez, visszaállításhoz, a feladatot végrehajtó informatikusnak az alábbi feltételeket kell vizsgálnia:

- A visszatöltendő, visszaállítandó adatok körét,
- A visszatöltendő, visszaállítandó adatok verzióját, forrását,
- A visszatöltés, visszaállítás helyét,
- A visszatöltés, visszaállítás időzítését.

A visszatöltendő, visszaállítandó adatokat és a visszatöltés, visszaállítás forrását azonosítani kell, ezzel egyértelműen meghatározzuk, hogy mikori adatok kerülnek visszatöltésre.

5.5.3. DOKUMENTÁLÁS

A mentések, archiválások felbontását, illetve felhasználását, valamint a visszatöltéshez, visszaállításhoz kapcsolódó paramétereket és a visszatöltés, visszaállítás végrehajtását minden esetben a feladatot végző informatikusnak a ***Géptermi naplóban (10. számú melléklet)*** kell dokumentálnia.

5.6. ARCHIVÁLÁSI ELJÁRÁS

A fejezet célja a Hivatal informatikai rendszerében tárolt adatok archiválási eljárásainak, az archivált adatok biztonságos kezelésének meghatározása. Az archiválás rendszerfüggetlen mentés, amelynek célja a rendszer archiváláskori adatállományának hosszú távú megőrzése.

5.6.1. AZ ARCHIVÁLÓ RENDSZER KIALAKÍTÁSA

Az archiváló rendszer kialakításánál figyelembe kell venni a következő tényezőket:

- Mekkora adatmennyiség kerül archiválásra, milyen időközönként,
- Milyen az archiválandó adatok növekedésének üteme,
- Mennyi ideig kell megőrizni az adatokat,
- Mennyi a maximális visszakeresési idő,
- Milyen formátumban érdemes az adatokat tárolni.

5.6.2. AZ ARCHIVÁLÓ RENDSZER MŰKÖDTETÉSE

Az archiválás az informatikus feladata. Az archiválást minden kritikus rendszerre, alkalmazásra meghatározott időközönként, de legalább évente egyszer, illetve rendszer változtatások esetén el kell végezni.

Kerülni kell azon adathordozók használatát, amely fokozottan érzékenyek a külső környezeti hatásokra (mágnes és optikai lemezek), vagy érzékenyek a csatlakozáskori elektromos impulzusokra (flash memória alapú adattárolók). Archiváláshoz ajánlott adathordozók, technológiai megoldások: merevlemez, szalagos egység, NAS, storage, stb.

A rendszerekre vonatkozó archiválási frekvencia meghatározása a jegyző feladata.

5.6.3. AZ ARCHÍV ANYAGOK TÁROLÁSÁNAK FELTÉTELEI

A tárolásra vonatkozó, az 5.9 Adathordozók kezelése fejezetben meghatározott biztonsági előírásokat, és a gyártó által előírt tárolási körülmények biztosítását (mágneses tér, hőmérséklet és páratartalom), be kell tartani.

Ha az archivált anyagok fájlmegosztáson tárolódnak, akkor az éles rendszerektől és a napi mentéstől független tárhelyre kerüljenek. (Pl külön NAS vagy storage eszköz)

Az archiválásra használt adathordozók tárolását és az archívumokat tartalmazó könyvtárak jogosultságait úgy kell kialakítani, hogy azokhoz kizárólag az informatikus férjen hozzá.

5.6.4. DOKUMENTÁLÁS

Minden archiválási folyamatot — a mentések dokumentálására előírt módon — rögzíteni kell a folyamatot végző informatikusnak az ***Archiválási naplóban (11. számú melléklet)***.

Az archiválási médiumok érthető, világos jelölését a mentésekre vonatkozó előírások betartásával kell megvalósítani.

Ha az archivált anyagok fájlmegosztáson tárolódnak, úgy az információkat célszerű a fájl nevében (archiválás ideje, archivált rendszer neve), vagy a fájl adatlapján feltüntetni.

5.7. HÁLÓZATBIZTONSÁGI ELJÁRÁS

A fejezet célja, hogy az informatikai rendszerek által használt hálózati szolgáltatásokhoz való hozzáférések szabályai rögzítésre kerüljenek, valamint meghatározásra kerüljenek a hálózati szolgáltatások által elérhető egyéb funkciók, az Internet, intranet és az elektronikus levelezőrendszer tekintetében.

5.7.1. BIZTONSÁGI ELŐÍRÁSOK A HÁLÓZATI TERVEZÉS ÉS MŰKÖDTETÉS SORÁN

A kommunikációs rendszerek tervezésénél a topológia kiválasztásával is támogatni kell a funkcionalitást, a működőképességet és az elvárt rendelkezésre állást.

Védett rendszerekről, valamint azok védett zónába eső szegmenseiről a külvilág felé kapcsolat nem létesíthető, ha az nem védett hálózati útvonalon keresztül valósul meg.

Az adat-hálózatok védelme számos hálózat-biztonsági eszközzel és rendszertechnikai megoldással (izolált hálózat, üzenettovábbító szerverek alkalmazása, tűzfalak, távoli elérés tiltása, titkosítás stb.) valósítható meg. A biztonsági eszközök szakszerű

alkalmazásával el kell kerülni, hogy a védelem csak az operációs rendszerek és az alkalmazások biztonsági eszközeire háruljon.

A védett rendszer minden érintett elemének (adó- és fogadógépek, útvonalválasztók stb.) meg kell akadályoznia a kommunikációs csatornához történő illetéktelen logikai hozzáférést.

A hálózatra csatlakoztatott számítógépeket és más hálózati erőforrásokat védett helyiségekben kell elhelyezni.

Megelőző és szükséghelyzeti intézkedéseket kell hozni a hálózat egyes komponenseinek kiesése esetére.

A hálózati csatlakozások számát a lehető legkevesebbre kell korlátozni.

A jelszavak védett formában, rejtjelezve kerüljenek továbbításra a hálózatokon.

Az adatátviteli hálózatok rendelkezésre állásának követelményét az érintett szolgáltatás szerint kell meghatározni, és ezt a szabályzatokban, utasításokban, szerződésekben stb. rögzíteni kell.

A hálózati aktív eszközöket jelszóval kell védeni, a jelszót — amelyet csak informatikus ismer, — zárt borítékban informatikusok által kezelt zárható szekrényben kell elhelyezni.

Az aktív eszközök beállításait menteni kell az 5.4.3 Operációs rendszerek, aktív eszközök beállításainak rendszer szintű biztonsági mentése fejezetben meghatározott módon.

A Hivatal területén külső (nem a Hivatal által felügyelt) wireless (vezeték nélküli hálózati) eszközhöz csatlakozni tilos.

Idegen tulajdonú hordozható számítógépek csatlakoztatása a Hivatal belső hálózatához csak a jegyző írásos engedélyével történhet.

5.7.1.1. INTERNET ELÉRÉSSEL KAPCSOLATOS SZABÁLYOK, BIZTONSÁGI ELŐÍRÁSOK

A Hivatal belső hálózatát tűzfallal kell leválasztani az Internettől. Valamint csak egy központi Internet kapcsolat engedélyezett a hálózaton. Több Internet kapcsolat egyidejű létesítése TILTOTT a Hivatal hálózatán és a Hivatal eszközein.

Az internetes forgalmat célszerű (a különböző internetes szolgáltatásokra, protokollokra lebontottan) skálázható dedikált célhardveren (tűzfal) keresztül bonyolítani, ezáltal az Internet elérés hálózati forgalma jelentősen csökkenthető, valamint elvégezhető az internetes oldalak tartalom alapú kategorizálása, szűrése. További lehetőség dinamikus IP szűrés segítségével csak a szükséges portokat engedélyezni „és a portok nyitottsága csak az aktív folyamatok idejére" elvén alapuló korlátozásokkal csökkenteni a külső támadások rizikóját.

Az internetes elérést a felhasználói alkalmazások logikai hozzáférésének megfelelő módon kell kezelni.

Az Internet forgalmat az informatikusoknak naplózniuk kell, de a naplók kizárólag az informatikai biztonsági incidensek okainak és felelőseinek meghatározására használhatók fel.

A Hivatal fenntartja a jogot, hogy az erőforrások védelme és a jogszabályi megfelelés érdekében hozzáférhetetlenné tegye egyes Web helyek látogatását és bizonyos állomány típusok letöltését.

Az internetes szolgáltatásokra vonatkozó vírusvédelmi előírásokat az 5.3.2 Vírusvédelmi előírások fejezet tartalmazza.

5.7.1.2. AZ INTERNETTEL KAPCSOLATOS SZABÁLYOK, BIZTONSÁGI ELŐÍRÁSOK

A Hivatal saját informatikai hálózatára csatlakoztatott informatikai berendezések, eszközök vírusvédelméről és annak folyamatos karbantartásáról az 5.3.2 Vírusvédelmi előírások fejezetben leírtak szerint az informatikus gondoskodik.

A Hivatal internet csatlakozása hivatali felhasználásra rendelt, magánjellegű felhasználása kerülendő. A felhasználó az Internet indokolatlan használatával nem terhelheti a Hivatal informatikai alapszolgáltatásokat nyújtó rendszerét.

Tilos olyan tevékenységet folytatni, amelynek célja vagy előrelátható következménye a Hivatal hálózatának vagy szoftverintegritásának bármelyfokú és természetű megsértése.

Az internet elérését biztosító szoftverek beállításait tilos a munkaállomásokon megváltoztatni, erre csak az informatikus jogosult.

Az internet munkahelyi használata során nem engedélyezett:

- Futtatható programok illegális letöltése,
- A programok védelmi rendszerét megkerülő alkalmazások letöltése, használata (kulcsgenerátorok, programtörések, exploitok)
- Jogdíjas termékek illegális letöltése, másolása, tárolása, továbbítása és telepítése,

Tilos önhatalmúlag tesztelni a biztonsági mechanizmusokat, működésüket.

Tilos tudatosan kihasználni az esetleges előforduló szoftver hibákat, védelmi hiányosságokat.

Az Internet munkahelyi használatára vonatkozó előírások megsértéséből eredő károkért a károkozó kártérítési felelősséggel tartozik.

5.7.2. A HIVATAL INTERNETES HONLAPJA

A Hivatal a széleskörű tájékoztatás, gyorsabb információszolgáltatás, valamint tevékenységének bemutatása érdekében honlapot üzemeltet.

5.7.2.1. A HONLAP MŰKÖDTETÉSÉNEK SZEMPONTJAI

Működtetésekor az alábbi szempontokat kell figyelembe venni:

- Tükrözze a Hivatal céljait,
- Folyamatosan karbantartott, friss információkat tartalmazzon,
- Az információk áttekinthetőek és kereshetőek legyenek,
- Az anyagok és szolgáltatások folyamatosan elérhetőek legyenek,
- A tárolt információ és a szolgáltatások védve legyenek külső és belső támadások ellen.

A Hivatal honlapját kommunikációs tevékenysége részének kell tekinteni, hiszen tartalma és szolgáltatásai befolyásolják a Hivatalról kialakuló belső és külső képet.

5.7.2.2. BIZTONSÁGI FELADATOK, FELELŐSSÉGEK

Nem publikálható szerzői jogi oltalom alá tartozó anyag, kivéve, ha a szerző írásos engedélyt adott.

A személyiségi jogok védelmében nem publikálható az emberi erőforrásokkal kapcsolatos bármilyen nem nyilvános információ, személyes adat (pl. otthoni lakcím, telefonszám stb.).

Tilos az Interneten publikálni a Hivatal informatikai rendszerére vonatkozó bármilyen információt, amennyiben a törvényi előírás nem rendelkezik másképp.

A Hivatal weboldalára csak engedélyezett tartalom tölthető fel. A weboldal tartalmát csak a jegyző által arra feljogosított személy módosíthatja.

Rendszeresen felül kell vizsgálni valamennyi publikusan elérhető informatikai rendszer tartalmát, és a nem nyilvános információkat el kell távolítani.

A Hivatal weboldalának kialakításakor figyelembe kell venni a biztonsági szempontokat. A weboldal adminisztrátori felületéhez hozzáférni csak felhasználónévvel és jelszóval történő hitelesítés után lehet. Célszerű a weboldal védelmét kiegészíteni tanúsítvánnyal. Amennyiben szükséges a weboldal szerkesztéshez különböző jogosultsági szinteket kell kialakítani.

A weboldal mappastruktúrájának jogosultság beállításait a weboldal élesítése előtt ellenőrizni kell, és csak a weboldal megfelelő működéséhez szükséges jogosultságokat szabad beállítani. A működéshez szükségtelen könyvtárakat le kell törölni.

A weboldal biztonságos működéséről rendszeresen, legalább kétévente meg kell győződni, technikai felülvizsgálat keretében.

5.7.3. AZ ELEKTRONIKUS LEVELEZÉS ELŐÍRÁSAI

Az elektronikus levelezés a Hivatal informatikai szolgáltatása, mely lehetővé teszi, hogy a hálózat egy felhasználója egy másik felhasználó számára elektronikus levelet, üzenetet küldjön.

A belső munkatárs az általa használt munkaállomásáról a Hivatal levelezőrendszerének megfelelő levelezőklienssel kapcsolódik az email kiszolgálón lévő postaládájához, ezen keresztül küldhet leveleket, illetve olvashatja el a beérkező üzeneteket.

A Hivatal dolgozóinak a Hivatalnál szabványosított és az informatikus által telepített levelező szoftvert kell használnia.

A Hivatal informatikai rendszere és adatai védelmében a leveleket vírus ellenőrzésnek kell alávetni. Minden kimenő és bejövő levélen szűrés történik, melynek során ellenőrzésre kerül, hogy a levél nem tartalmaz-e vírust. A részleteket az 5.3.2 Vírusvédelmi előírások fejezet tartalmazza.

5.7.3.1. A FELHASZNÁLÓ ELEKTRONIKUS LEVELEZÉSRE VONATKOZÓ JOGAI ÉS KÖTELEZETTSÉGEI

Az elektronikus levelezésben is érvényesek az egyének közötti társalgás és levélírás alapvető illemszabályai. Az elektronikus levelezésben be kell tartani a levelezési konvenciókat.

A felhasználók elektronikus levelezéssel kapcsolatos jogai, kötelezettségei illetve a használattal kapcsolatos szabályok megegyeznek az 5.7.1.2 Az Internettel kapcsolatos szabályok, biztonsági előírások fejezetben foglaltakkal, ezen felül az elektronikus levelezőrendszer felhasználóira a következő további szabályok vonatkoznak:

- A levelező rendszer hivatali felhasználásra rendelt.
- A levél nem tartalmazhat olyan adatot, amely ***Információ védelmi szabályzat (1. számú melléklet)*** Adatok osztályozása szerint kiemelten védendő besorolást kapott.
- A csatolt fájloknak vírusmentesnek kell lennie.
- A levelek és csatolt mellékletek együttes maximális mérete 20 MB lehet.
- A küldő, vagy fogadó mezőben a Hivatal alkalmazásában álló munkavállaló címének kell szerepelnie, vagyis tiltott az ún. "relay".
- Tilos a magáncélú levelek Hivatali emailcímre történő továbbítása.
- A címzett mezőben maximum 5 címzett szerepelhet.
- Az elektronikus postaládát minden felhasználónak lehetőség szerint naponta legalább egyszer meg kell néznie.

- Az elektronikus levél fejlécében található tárgy mezőt minden esetben kötelező kitölteni.

Az elektronikus levélhez csatolt mellékleteket Hivatal standard szoftverekkel kell előállítani, hogy a címzett is el tudja olvasni azokat. Ha ez valamely okból nem tartható be, akkor a mellékletet tartalmazó levélben ezt jelezni kell, illetve a küldése előtt meg kell egyezni a címzettel a szoftvert, verziót és formátumot illetően.

Nagyméretű (20 MB-nál nagyobb) állományt a Hivatalnál standard tömörítő (.zip) program segítségével tömörített formában kell elküldeni. Ha a mellékletek tömörített mérete meghaladja a maximálisan küldhető méretet, akkor több levélben kell a küldést elvégezni.

Amennyiben a nagyméretű fájlok megküldésére a levelező rendszer nem alkalmas úgy a Hivatalnál az erre a célra alkalmazott szolgáltatást (ftp, sftp, hivatali kapu, e-papír) kell igénybe venni.

A levelező rendszerben található adatok hitelességét egyéni felhasználónévvel és jelszóval kell védeni.

A következő kiterjesztésű állományok elektronikus úton, mellékletként történő továbbítása nem engedélyezett a Hivatal informatikai rendszerében: bas, bat, cmd, com, cpe, inf, msp, msg, mst, reg, scr, vbs, exe stb. Az informatikusok a felsorolt állományok küldését megakadályozó technikai jellegű intézkedéseket hajthatnak végre, illetve módosíthatják a kiterjesztések listáját.

5.8. ADATOK KEZELÉSE, TÁROLÁSA

A fájlmegosztásokat úgy kell kialakítani, hogy azok tartalmához csak a jogosultsággal rendelkező felhasználók férjenek hozzá, jogosultságaiknak megfelelően. A Hivatal munkatársai az általuk kezelt fájlokat a munkafolyamat befejezése után kötelesek a Hivatal alkalmazásaiba, vagy központi fájl tárolóeszközére feltölteni. A Hivatal kliens eszközein (számítógép, laptop) fájlokat, adatokat tárolni csak adatgazdai vagy jegyzői engedély esetén szabad.

Az adatok kezelése során be kell tartani a Hivatal ***Adatvédelmi Szabályzatába*** és ***Iratkezelési Szabályzatába*** foglalt előírásokat.

A hivatal informatikai eszközein csak a munkavégzéshez szükséges adatokat szabad tárolni. A Hivatal informatikai eszközein TILOS tárolni:

- magán dokumentumokat,
- nem a munkavégzéshez szükséges képeket, filmeket,
- illegálisan letöltött jogvédett fájlokat, tartalmakat (multimédiás tartalom, szoftver, dokumentum),
- szoftverek védelmi rendszerének, integritásának megsértését előidéző alkalmazásokat (crack programok, kulcsgenerátorok)

- illegális licence kulcsok
- nem a munkavégzéshez szükséges program telepítőkészletek.

Az informatikus köteles a Hivatal központi fájltároló eszközeit rendszeresen havonta 1 alkalommal átnézni, és nem engedélyezett tartalom esetén eljárni az alábbiak szerint:

- megállapítani a tiltott tartalom feltöltőjének tulajdonosát
- jegyzőkönyvet felvenni az incidensről
- törölni a nem engedélyezett tartalmat.

A jegyzőkönyvet az érintett felhasználónak és az informatikusnak is alá kell írnia és el kell juttatni a jegyzőhöz.

Amennyiben nem állapítható meg a nem engedélyezett tartalom feltöltőjének tulajdonosa, úgy a jegyzőkönyvet csak az informatikusnak kell aláírnia, és el kell juttatnia a jegyzőhöz.

A felhasználók számítógépein az ellenőrzéseket évente legalább 1 alkalommal el kell végezni. Ha a számítógépen nem engedélyezett tartalom található, ugyanúgy kell eljárni, mint a központi fájltároló eszköz eseténben.

5.9. ADATHORDOZÓK KEZELÉSE

Jelen fejezet alapján kerülnek rögzítésre az informatikai adathordozók használatba vételével, tárolásával, használatból kikerülésével, illetve selejtezésével kapcsolatos biztonsági követelmények.

Az adathordozók kezelésének szabályait rendszeresen, de évente legalább egy alkalommal felül kell vizsgálni.

5.9.1. HASZNÁLATBA VÉTEL, JELÖLÉS

A kiemelten védendő adathordozót használatba vétel előtt fel kell címkézni és egyedi azonosítóval kell ellátni.

Nyilvántartást kell vezetni a munkatársaknak kiadott adathordozók típusáról, és adatairól.

5.9.2. TÁROLÁS

A tároláshoz szükséges káros hatások (túl magas hőmérséklet, por, nedvesség, páratartalom, elektromágneses behatások) elleni védelmet biztosító tárolóeszköz használata. A tároláskor figyelembe kell venni az adattároló eszköz gyártói által specifikált környezetet, amely mellett az eszköz a leghosszabb ideig képes az adatokat megőrizni.

A tartalék vagy ideiglenesen nem használt adathordozók tárolóhelye csak az informatikusok számára legyen hozzáférhető.

5.9.3. AZ ADATHORDOZÓK HASZNÁLATÁNAK, SZÁLLÍTÁSÁNAK FELTÉTELEI, KÖVETELMÉNYEI

Idegen, talált pendrive-ot a Hivatal tulajdonában levő számítógépre csatlakoztatni TILOS! Az utcán talált mások által szándékosan elhagyott pendrive-ok vírust tartalmazhatnak.

Ezen rendelkezések az adatok és az adatokat fizikailag tároló adathordozók kezelésére vonatkoznak.

Az adathordozók biztonsági tárolása és szállítása érdekében az alábbi szempontokat kell figyelembe venni:

- Az adathordozókat óvni kell a fizikai sérülésektől.
- Az adathordozók állapotát rendszeresen ellenőrizni kell. A saját használatra kiadott adathordozó eszközök állapotának ellenőrzése a felhasználók feladata. Azt az adathordozót, melyet fizikai károsodás ért, vagy a megengedett hibahatárt elérte, selejtezni kell.
- A védendő adatokat tartalmazó adathordozót felszabadítani (visszaminősíteni) csak a megfelelő törlési eljárással történt törlés után szabad. A felszabadított adathordozót a továbbiakban is csak az a szervezeti egység használhatja, amelynél a visszaminősítés előtt is használatban volt.
- A kiemelten védendő adatokat tartalmazó adathordozót visszaminősíteni tilos.
- Az védendő és kiemelten védendő adatokat tartalmazó adathordozók szállításakor a rendelkezésre álló valamennyi védelmi intézkedést (pl. széf, zár, riasztó, őrzött parkoló) kötelező alkalmazni.
- Szállítási céllal történő mozgatás esetén a nem nyilvános adatot tartalmazó adathordozón lévő adattartalmat másolni szigorúan tilos!
- Védendő és kiemelten védendő adatot az adathordozón csak titkosítva szabad tárolni.

A Hivatal számítógépeihez csak a Hivatal által biztosított adathordozókat szabad csatlakoztatni. Az adathordozók csatlakoztathatóságát a jegyző utasítására az informatikus korlátozhatja hardver vagy szoftver eszközzel.

5.9.4. SELEJTEZÉS

Adathordozót akkor kell selejtezni, ha:

- Fizikailag sérült,

- Gyári, gyártási hibából következően felhasználásra alkalmatlan,
- Az adathordozó tároló kapacitása, az elhasználódás miatt, a műszakilag még megengedhető érték alá csökken (75%),
- Véglegesen elhasználódott.

A felhasználók feladata a használhatatlanná vált adathordozókat visszaszolgáltatni az informatikusnak. A leselejtezésre váró adathordozókat (CD, DVD, pendrive stb.) az informatikus egy közös helyen gyűjti, és egyszerre selejtezi le, illetve semmisíti meg.

Az adathordozók selejtezését és megsemmisítését ellenőrzött eljárás keretében kell elvégezni. A selejtezési eljárást az informatikus végzi. Az eljárás során biztosítani kell az adathordozón tárolt adatok biztonságos törlését (fizikai törléssel, biztonságos formattálással). Ha a tárolt adatok biztonságosan nem törölhetők, akkor az adathordozót úgy kell megsemmisíteni, hogy további felhasználásra már alkalmatlan legyen, azaz fizikai roncsolással kell használhatatlanná tenni.

Az eljárás lebonyolításáról Megsemmisítési jegyzőkönyvet kell felvenni, mely tartalmazza a selejtezéssel, megsemmisítéssel kapcsolatos minden fontos körülményt, tevékenységet. A Megsemmisítési jegyzőkönyvet az eljárás lebonyolításával megbízott személy készíti el.

Ha külső vállalkozó kapja az adathordozók megsemmisítésének feladatát, a vállalkozótól valamennyi megsemmisítési eljárás megtörténtéről Megsemmisítési jegyzőkönyvet kell kérni.

5.9.5. A HIVATAL HATÁSKÖRÉBŐL KIKERÜLŐ ADATHORDOZÓK

A nem nyilvános adatot tartalmazó hordozható adathordozók (mobil merevlemez, pendrive) adataihoz az informatikusnak felhasználót kell nevesítenie, akik felelősek az adott adathordozó adatainak biztonságáért az informatikus előírásai alapján.

5.10. RENDSZEREK FELÜGYELETE

A rendszerek naplózására vonatkozó szabályozást rendszeresen, évente legalább egyszer felül kell vizsgálni.

Az informatikai eszközök monitoring és naplózó rendszerének alkalmasnak kell lennie egy esetleges hacker támadás jelzésére, a megadott figyelési paraméterek szerint.

Az informatikai rendszerek által biztosított naplóadatokból meg kell tudni állapítani a rendszer jogosulatlan használatát.

Az informatikai rendszerek biztonsági és használati naplózásának beállítását egyeztetni kell azon szervezeti egységekkel, melyek az elkészült naplók feldolgozását, riportolását végzik, vagy munkájuk során bármilyen formában feldolgozzák a naplók tartalmát.

A Hivatal informatikai eszközeinek állapotát folyamatosan monitorozni kell. Az esetleges hibákról a felügyeleti rendszernek riasztást kell küldenie, legalább a kritikus fontosságú eszközök esetében.

5.10.1. RENDSZER ESEMÉNYEK NAPLÓZÁSA

Az informatikai rendszereknek automatikusan tárolnia kell a folyamatokhoz tartozó meghatározott biztonsági adatokat (a szükséges mértékben) a hatékony biztonságkezelés érdekében.

A naplóadatok tárolására megfelelő méretű, és felülírástól védett munkaterületet kell biztosítani a háttértároló rendszeren.

A nyomkövetési naplóbejegyzéseket áttekinthető szerkezetben kell tárolni, és adott esetben rendelkezésre kell bocsátani a feljogosítottak számára.

Az informatikai biztonsági felelős köteles megvizsgálni, az informatikai rendszerek naplózásának megfelelőségét.

5.10.1.1. NAPLÓZÁS HATÁLYA

Az informatikai rendszerekben történt konfiguráció-módosítást, beállítások megváltoztatását, valamint rendszerelemek üzembeállítását, illetve üzemből történő kivonását rögzíteni kell.

A naplófájlnak tartalmaznia kell legalább a következőket:

- a felhasználó azonosítóját,
- a be- és kijelentkezés dátumát és időpontját,
- a sikeres és a sikertelen rendszer-hozzáférési kísérletekről készült feljegyzéseket (rekordokat),
- a sikeres és a sikertelen adathozzáférési és más erőforrás-elérési kísérletekről készült feljegyzéseket (rekordokat)
- amennyiben az információ releváns, az alábbi információkat is tartalmazzák a naplóbejegyzések:
    - a munkaállomás azonosítója
    - szoftverek konfigurációjában végzett változások
    - tűzfalon zajló változások, távoli bejelentkezések monitorozása
    - hardver hibák naplóbejegyzései

5.10.1.2. NAPLÓK VÉDELME

A naplóeszközöket a jogosulatlan hozzáférés ellen védeni kell.

A nyomkövetési napló adatait védeni kell az illetéktelen megismerés, (véletlen vagy szándékos) módosítás és megsemmisítés ellen a biztonsági fokozatnak megfelelően.

A naplóállományokat - amennyiben az eszköz/szoftver erre alkalmas - minimum 30 napig meg kell őrizni. A biztonsági napló állományok és minden kapcsolódó dokumentum (riportok, jelentések) titokköri besorolása megegyezik az adott rendszer által kezelt adatok besorolási szintjével.

5.10.1.3. ADMINISZTRÁTORI ÉS KEZELŐI NAPLÓK

A rendszeradminisztrátori és rendszerkezelői tevékenységeket naplózni és a naplókat rendszeresen ellenőrizni szükséges.

5.10.1.4. HIBÁK NAPLÓZÁSA

A felhasználók és rendszerprogramok által jelentett hibákat naplózni és elemezni kell, ezek alapján meg kell tenni a megfelelő intézkedéseket.

5.10.1.5. NAPLÓK ELEMZÉSE, RIASZTÁS

Az informatikus felelőssége és feladata, hogy a naplóállományok rendszeresen átvizsgálásra kerüljenek. Az elemző szoftvert úgy kell konfigurálni, hogy automatikusan riasztást küldjön, ha a biztonság megsértésére vagy az eszköz nem megfelelő működésére utaló naplóbejegyzést észlel.

5.10.2. RENDSZERÓRÁK SZINKORNIZÁLÁSA

A számítógépek rendszeróráit pontos és egységes értékre kell beállítani így szavatolható az eseménynaplók pontossága, amelyek adott esetben vizsgálatokhoz is szükségesek lehetnek.

Ahol a szerver vagy hálózati eszköz valós, hálózati időszolgáltatást tud nyújtani a rendszer számára, akkor azt ajánlatos egy nemzetközi órajelszolgáltatóhoz szinkronizálni és a helyi informatikai eszközöket ehhez a központi hálózati időszolgáltatáshoz konfigurálni.

A számítógép pontos dátumának és órajelének beállítására olyan eljárást kell alkalmazni, amely az időeltérést ellenőrzi és kijavítja.

6. HOZZÁFÉRÉS ELLENŐRZÉS

Rendszeresen, évente legalább egy alkalommal felül kell vizsgálni a hozzáférések védelmére vonatkozó szabályozást.

A Hivatal információs rendszereiben kezelt adatokhoz és működtető programokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal - amelynek megvalósítása különböző (pl. felhasználói név és jelszó) – lehet hozzáférni.

6.1. FELHASZNÁLÓ AZONOSÍTÓK HASZNÁLATA, MŰKÖDÉSE

A hitelesítési és azonosítási szabályokat rendszeresen, évente legalább egy alkalommal felül kell vizsgálni.

A hardver és szoftver eszközök alapértelmezett hitelesítési adatait meg kell változtatni, a Hivatal hozzáférésekre vonatkozó szabályainak megfelelően.

A Hivatal által üzemeltetett informatikai rendszerhez történő távoli hozzáférés során a felhasználók hitelesítésére, csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványok alkalmazhatók.

A számítógépes felhasználói azonosítók létrehozásának célja, hogy lehetővé tegye az adatok és az erőforrások használatát a felhasználó számára, úgy, hogy az a munkaköri feladatainak ellátásához szükséges mértékű legyen.

A rendszerek jogosultsági szintjeinek kialakítása érdekében a lehetséges tevékenységek, és munkakörök figyelembevételével felhasználói csoportokat kell definiálni és egy-egy felhasználói azonosító meghatározásakor a csoportba vagy csoportokba sorolást el kell végezni.

Minden egyes megosztott informatikai erőforráshoz (könyvtárak, adatbázisok, nyomtatók) hozzáférés típusonként (írás, olvasás, törlés, végrehajtás) egy-egy csoportot kell létrehoznia, a csoportoknak a szükséges engedélyt meg kell adnia, majd ezekhez kell a felhasználókat hozzárendelni.

A Hivatalhoz nem tartozó személyek számára felhasználói azonosítót kizárólag a jegyző írásos engedélyével szabad létrehozni.

A felhasználói azonosítók kezelésre vonatkozó általános előírások:

- A rendszer lehetőség szerint a felhasználót kényszerítse a felhasználói azonosító első használatakor a (informatikus által neki kijelölt) jelszavának megváltoztatására. Ennek minden olyan esetben is be kell következnie, amikor az informatikus egy ideiglenes jelszót rendel a felhasználói azonosítóhoz.

- A felhasználói azonosító tulajdonosa felelős a felhasználói azonosítója nevében végzett valamennyi tevékenységért, a szervezet által birtokolt adatok és erőforrások védelméért, etikus módon történő használatáért.
- A felhasználói azonosítókat rendszeresen ellenőrizni kell. Minden hosszabb ideig nem használt felhasználói azonosítót le kell tiltania úgy, hogy a felhasználói azonosító tulajdonosának az informatikushoz kelljen fordulnia a felhasználói azonosító újbóli aktivizálása érdekében.
- A felhasználói azonosítókkal kapcsolatos minden incidenst (téves bejelentkezés vagy elöregedés miatti kitiltás, a jelszónak nem a tulajdonos által történő megváltoztatása stb.) jegyzőkönyvezni kell, és a jegyzőnek írásban jelenteni.

6.1.1. FELHASZNÁLÓI HOZZÁFÉRÉSEK ELLENŐRZÉSE

6.1.1.1. JELSZÓMENEDZSMENT

A Hivatal kritikus rendszereiben használatos jelszavak tárolása és átvitele a hálózatokon (LAN és WAN) csak titkosítottan történhet, ezzel csökkentve a kockázatát, hogy a hálózati forgalom megfigyelésével valaki más felhasználó jelszavát megtudhassa, és más felhasználó nevében bejelentkezve jogosulatlan tevékenységeket végezzen.

A Hivatal informatikai rendszereihez való illetéktelen logikai hozzáférés megakadályozására jelszavas védelmet kell alkalmazni.

A Hivatal számítógépes hálózatába, illetve az alkalmazásokba bejelentkezési jogosultsággal rendelkező felhasználó köteles a bejelentkező nevéhez tartozó jelszó megőrzésére. A saját bejelentkező névhez tartozó jelszót mások által is elérhető módon feljegyezni nem szabad.

Azon informatikai rendszerek esetén, melyek rendelkeznek a megfelelő technikai feltételekkel, a hitelesítéshez használt **felhasználói** hozzáféréshez rendelt jelszavaknak az alábbi kritériumoknak kell megfelelni:

- A felhasználói jelszavak minimális hossza 8 karakter.
- A felhasználói jelszavak maximum egy évig lehetnek érvényesek.
- Az utolsó 3 jelszót nem lehet újra használni.
- A felhasználóknak meg kell változtatniuk a jelszavukat, amikor első alkalommal használják felhasználói azonosítójukat.
- Jelszavakra vonatkozó ajánlások:
    - Ne tartalmazzon bármilyen nyelvű szót szótári alakban.
    - Ne egyezzen meg a felhasználó nevével, felhasználói azonosítójával, egyik telefonszámával sem, engedélyének számával, személyi számával vagy dolgozói kódjával, valamint a felhasználóhoz kötődő bármely karaktersorozattal (pl. születési dátum, lakcím).

- Ne egyezzen meg személynévvel.
- Ne egyezzen meg irodalmi, színházi, televíziós, közéleti személyek nevével és egyéb közismert szavakkal, kifejezésekkel.
- Ne tartalmazzon azonos, vagy ismert logika szerint egymást követő karaktereket (pl. 11111, aaaaa, qwert, asdfg, gegegeg).
- Ne utaljon a felhasználóra, munkakörére, munkahelyére.

- Mind a sikeres, mind a sikertelen belépési és kilépési kísérleteket naplózni kell.
- Ha egy felhasználói azonosító 60 napig inaktív, akkor azt az informatikus jogosult letiltani.
- Egy letiltott felhasználói azonosító ismételt felhasználása nem lehetséges a letiltást követő 60 napig.

A fenti követelményekről minden felhasználót tájékoztatni kell munkájának megkezdése előtt.

A hitelesítésre szolgáló eszközt (pl. token) minden esetben le kell cserélni, amikor az érintett fiók megváltozik.

6.1.1.2. FELHASZNÁLÓK BEJELENTKEZÉSE

A Hivatal számítógépes hálózatába bejelentkezni csak a rendszerben definiált bejelentkező név és a hozzátartozó jelszó ismeretében lehet.

A több felhasználós informatikai rendszerek elérésénél a felhasználók megkülönböztetésére, illetve a bizalmasság és a sértetlenség megőrzésére bejelentkezési eljárásokat kell definiálni.

A bejelentkezési eljárások meghatározásánál az alábbi biztonsági követelményeket kell figyelembe venni:

- Egyéni felhasználói azonosítók használata, amely felhasználóhoz köthető és az ő műveleteiért felelős.
- Ellenőrizni kell, hogy a felhasználónak van-e engedélye az informatikai rendszer, vagy alkalmazás használatára.
- A felhasználó a hozzáférési jogairól kapjon értesítést.
- Listát kell készíteni az alkalmazásokat használó regisztrált személyekről.
- Rendszeresen ellenőrizni kell, és el kell távolítani a felesleges felhasználói azonosítókat.
- Biztosítani kell, hogy a feleslegessé vált felhasználói azonosítók ne kerüljenek ismét felhasználásra.

- Az operációs rendszerhez, illetve az alkalmazói rendszerekhez való hozzáférés esetén, ahol lehet, az utolsó sikeresen bejelentkezett felhasználói azonosítónak rejtve kell maradnia.

6.1.1.3. HOZZÁFÉRÉSI JOGOSULTSÁGOK NYILVÁNTARTÁSA

A jogosultságokat a központilag kell nyilvántartani, névre szólóan kell meghatározni és beállítani.

A hozzáférési jogokat, azok szükségességét rendszeresen évente és minden egyes releváns változást követően felül kell vizsgálni.

A felhasználói jogosultságok létrehozásának, módosításának, törlésének szabályait, eljárásait a Hozzáférési rendszer követelményei fejezet tartalmazza.

A munkatársak által használt hitelesítő eszközökről nyilvántartást kell vezetni. (token, hardverkulcs). Az eszközök kompromittálódása, elvesztése, sérülése esetén a hozzárendelt jogosultságokat meg kell szüntetni, és cserélni kell az eszközt.

6.1.1.4. JOGOSULTSÁGOK KEZELÉSE

A rendszerhez és szolgáltatáshoz történő hozzáférési jogot csak szabályszerű nyilvántartásba vételi eljárást követően lehet megadni.

Az egyéni azonosítóknak egyértelműnek kell lenniük azért, hogy a személyekhez és tevékenységekhez a megfelelő felelősségeket hozzá lehessen rendelni.

Ellenőrizni kell, hogy a kiadott hozzáférési jogosultság szintje alkalmas-e a kívánt feladatra.

Gondoskodni kell a felesleges egyéni azonosítók időről időre történő ellenőrzéséről és eltávolításáról.

Gondoskodni kell arról, hogy a személyek az egyéni azonosítókat ne adják át másnak.

A kiemelt jogosultságok kiosztását és használatát (amely lehetővé teszi a rendszer vezérlésébe történő beavatkozást) korlátozni és ellenőrizni kell.

6.1.2. FELHASZNÁLÓI FELELŐSSÉGEK

A Hivatal informatikai rendszereinek elérésére használható hozzáférés szintjei:

1. **Névre szóló felhasználói hozzáférés** keretében a felhasználó külön, saját névre szóló, más által nem használt, kizárólag a munkája ellátása miatt elengedhetetlen jogosítványokkal rendelkezik az informatikai és telekommunikációs rendszerekhez és azok erőforrásaihoz, a szervezeti folyamatok ellátásához kapcsolódó feladatok elvégzéséhez.

2. **Névre szóló rendszergazdai hozzáférés** esetén, a rendszergazdai jogosítványt a rendszergazda a saját nevére szóló, kizárólagosan általa használt, megfelelő rendszergazdai jogkörrel felruházott felhasználói azonosító segítségével lehet használni. A beépített (root, administrator, stb.) rendszergazdai hozzáférés csak abban az esetben tekinthető ilyennek, ha azt kizárólag egy személy használja.

6.2. HÁLÓZATI SZOLGÁLTATÁSOK BIZTONSÁGA

6.2.1. TÁVOLI HOZZÁFÉRÉS A HIVATAL HÁLÓZATÁHOZ

A Hivatal informatikai erőforrásai valamint a tárolt adatok, a Hivatal irodáján kívülről nem érhetőek el.

A szükséges hozzáféréseket az informatikus állítja be, a jegyző engedélye alapján.

A távoli hozzáféréseket rendszeresen, évente legalább 1 alkalommal felül kell vizsgálni.

6.3. SZOFTVEREK KEZELÉSÉNEK SZABÁLYAI

6.3.1. OPERÁCIÓS RENDSZER SZINTŰ HOZZÁFÉRÉS ELLENŐRZÉS

Az informatikai infrastruktúrában olyan operációs rendszereket kell alkalmazni, amely a biztonságpolitikát legalább a következő területeken támogatja:

- Account-politika, amely meghatározza a felhasználó által karbantartott jelszavakkal kapcsolatos követelményeket,
- Felhasználói jog politika, amely meghatározza, hogy a felhasználókat (felhasználói csoportokat) milyen jogok illethetik meg és
- Audit-politika, amely meghatározza azt, hogy milyen informatikai eseményekről készüljön napló.

Központilag kell ellátni legalább az alábbi biztonság-kezelési funkciókat:

- Az operációs rendszerek adminisztrációja,
- Az rendszerprogramok központi installálása és konfigurálása,
- Valamennyi log-fájl archiválása,
- Jogosultságmenedzsment stb.

6.3.2. SZOFTVEREK HASZNÁLATA

A Hivatal informatikai rendszereit és szoftvereit csak a Hivatal munkatársai használhatják. A szoftvereket – egyéb engedélyezés hiányában – csak olyan személy használhatja, aki az adott szoftver használatát illetően képzésben részesült, illetve a használat módjáról kellő ismeretekkel és jártassággal rendelkezik. Ennek hiányában a szoftver csak olyan személy felügyelete mellett használható, aki rendelkezik ezekkel a feltételekkel és a szoftver rendeltetésszerű használatát illetően felelősséget vállal a felügyelete alatt dolgozó munkatárs munkájáért.

A szoftver használata során a felhasználó a szoftverek rendszer beállításait (kiszolgáló adatok, adatbázis információk, licence adatok, könyvtár útvonalak, stb.) nem módosíthatja, a szoftvereket nem törölheti és azokról másolat nem készíthet. Ettől eltérni csak a jegyző engedélyével lehet.

A telepített szoftverekre előírt felhasználási előírásokat megsértő munkatárs munkajogi, polgári jogi és büntetőjogi felelősséggel tartozik.

A felhasználók jogosultságainak beállítását rendszeresen, évente legalább egy alkalommal ellenőrizni kell.

6.3.3. ALKALMAZÁS SZINTŰ HOZZÁFÉRÉS ELLENŐRZÉS

Az információs rendszer logikai védelme az egyes funkcionális rendszerelemek (hardver, szoftver kommunikációs elemek stb.) által biztosított funkciókkal, tulajdonságokkal, képességekkel, továbbá az alkalmazott eljárásokkal, módszerekkel és/vagy biztonsági eszközökkel, algoritmusokkal, megoldásokkal, de - legfőképpen - ezek összhangjával biztosítható.

Az információs rendszer logikai védelmével kapcsolatban az alábbi követelményeket kell alkalmazni:

- Olyan architektúrát kell kialakítani, amely külön kezeli, illetve valósítja meg a kommunikációs, authentikációs és authorizációs, valamint az alkalmazás rétegeket.
- Biztosítani kell, hogy a központi rendszer egyetlen eleme sem legyen kihagyható vagy megkerülhető a rendszer felhasználói számára.

6.4. MOBIL ESZKÖZÖK HASZNÁLATA ÉS TÁVMUNKA

A Hivatal hálózatához kapcsolódásra képes eszközökhöz (pl. notebook) kapcsolódó általános szabályok:

- külön biztonsági oktatásban kell részesülnie annak, aki ilyen eszközt fog használni, mielőtt az eszközt használatba veszi,

- a beépített merevlemezes egységen a kiemelten védendő adatokat kódolva kell tárolni,
- a mobil eszközt csak a munkatárs használhatja, aki az eszközt munkavégzésre megkapta,
- a mobil eszközt csak Hivatali munkavégzésre lehet használni,
- a 3.5.1 Felügyelet nélkül hagyott számítógépek fejezetben meghatározottak szerint kötelező az időzár (time-out) beállítása,
- a Hivatal irodáján kívül használt mobil eszközök védelmét 4.1.16 Eszközök védelme irodán kívül fejezetben meghatározottak szerint kell biztosítani,
- a mobil eszközökön található adatok mentéséről a 3.5.2 Rendszer-független mentési előírások felhasználók számára fejezet szerint kell eljárni,
- a mobil eszközökön tűzfal és vírusvédelmi szoftvernek kell működnie, a 5.3.2 Vírusvédelmi előírások fejezetben foglaltaknak megfelelően.

Az eszköz elvesztése, eltulajdonítása esetén a 6.4.1 Mi a teendő, ha az eszközt eltulajdonították fejezetben foglaltak szerint kell eljárni.

Távoli munkavégzés csak biztonságos kapcsolatokon keresztül történhet, a 6.2.1 Távoli hozzáférés a Hivatal hálózatához fejezet szerint.

6.4.1. MI A TEENDŐ, HA AZ ESZKÖZT ELTULAJDONÍTOTTÁK

Az eszköz használójának:

- Írásban jelenteni kell a számítógép eltulajdonításának tényét az informatikusnak, és a jegyzőnek.
- Értesíteni kell a rendőrséget, és a rendőrségi jegyzőkönyvet el kell juttatni a jegyzőnek.
- Értesíteni kell a szálloda vezetését, ha a számítógépet a szállodai szobából, vagy a szálloda ingatlanján álló kocsiból lopták el.

Valamennyi rendőrségi és biztosítói jegyzőkönyvet, jelentést meg kell őrizni, és a jegyzőnek át kell adni.

6.4.1.1. A HORDOZHATÓ ESZKÖZÖK HASZNÁLATBA VÉTELE

A jogosult személyek a gépet tartozékokkal és szoftverekkel együtt veszik át az informatikusoktól, visszaszolgáltatási kötelezettséggel.

Átadáskor az informatikus a működőképes hordozható számítógép mellett a tartozéklistában felsorolt kiegészítőket, a munkavégzéshez szükséges, a szoftverjegyzékben szereplő telepített szoftverekkel együtt adja át.

6.5. ELTÉRÉS AZ ÁLTALÁNOS KÖVETELMÉNYEKTŐL

Az IBSZ-ben általános jelleggel meghatározott biztonsági követelmények teljesítésétől az informatikus felmentést kérhet, ha az alábbi feltételek egyidejűleg fennállnak:

- a követelmények teljesítését a Hivatal rendelkezésére álló hardver és szoftver technológia nem teszi lehetővé, és
- felmérte a munkafolyamatban fennálló azon kockázatokat, amelyek a biztonsági kontrollok elhagyásából fakadnak, és
- a biztonsági kontrollok kialakításának költsége nem áll arányban a biztonsági kontrollok elhagyásából fakadó kockázatokkal.

Az eltérést a biztonsági követelményektől a jegyző engedélyezheti.

7. INFORMÁCIÓBIZTONSÁGI INCIDENSEK KEZELÉSE

7.1. INCIDENSEK JELENTÉSE, VÉDELMI GYENGESÉGEK VIZSGÁLATA

Az információk kiszivárgásának megelőzése érdekében a Hivatal rendszeres kockázatelemzést alkalmaz, így azonosítja a biztonsági réseket. A kockázatnak megfelelő arányú védelmi intézkedéseket vezet be.

A Hivatal informatikusa felügyeli a rendszerek működését és használatát, és amennyiben az információk kiszivárogtatásának gyanúja felmerül, azt jelenti a jegyzőnek.

A rendszer sebezhetőségének azonosítása, kezelése és ellenőrzése érdekében rendszeresen felül kell vizsgálni a beállításokat, illetve a működést.

Az észlelt információvédelmi eseményeket, és a feltételezett gyengeségeket írásban, az *Incidens bejelentő lapon (9. számú melléklet)* bizalmasan kell bejelenteni az jegyzőnek.

7.1.1. RENDKÍVÜLI ESEMÉNY BEJELENTÉSE

A bejelentőlap kitöltésekor az esemény vagy a felfedezett sérülékenység ismertetésénél a következőkre kell kitérni:

- Az esemény bekövetkezésének időpontja, ha ismert
- Az esemény észlelésének időpontja és módja
- A szabálysértés, hibás működés vagy szokatlan jelenség leírása, mi történt, hogyan történt
- A képernyőn megjelenő üzenetek leírása
- Az észlelt jelenség folyamatosan fennáll-e
- Az informatikai rendszer mely erőforrásait érintette az esemény, ha ismert (szerverek, munkaállomások, hálózati eszközök, alkalmazások, adatok)
- Az esemény észlelése után történt-e beavatkozás (pl. program újraindítása, számítógép újraindítása)

Feltételezett információvédelmi gyengeség bejelentésekor előfordulhat, hogy az adott gyengeség által jelentett kockázat a jegyző előtt ismert, és azt tudatosan felvállalta. Ebben az esetben a jegyző tájékoztatja a bejelentőt.

7.2. INCIDENSEK KEZELÉSE

Az információvédelmi események nyilvántartását a jegyző, illetve az általa megbízott személy vezeti. A nyilvántartásba két forrásból kerülhetnek adatok:

– az *Incidens bejelentő lap (9. számú melléklet)* alapján, vagy

– az üzemeltetési, biztonsági riportok átvizsgálásának eredményeképpen.

A jegyző értékeli a feltárt (bejelentett) információvédelmet érintő eseményt és ennek alapján dönt az incidens kezelésének módjáról.

Az esemény lezárásakor meg kell állapítani az eseményre fordított költségeket is (nagyságrendileg, ha nem fix költség).

A jegyzőnek ellenőriznie kell, hogy történt-e intézkedés a bejelentett eseményekkel kapcsolatban.

7.2.1. INCIDENS VIZSGÁLATA, FELELŐSSÉGEK ÉS ELJÁRÁSOK MEGHATÁROZÁSA

Rendkívüli esemény bekövetkezése esetén a rendkívüli esemény jelentése után az jegyző felelőssége a további intézkedések megfogalmazása.

Amennyiben felmerül a gyanú, hogy kihágás történt, akkor nyomozást kell folytatni. Az adatbiztonsági kihágásokkal kapcsolatos nyomozás közben különös figyelemmel kell eljárni. A nyomozást bizalmasan kell kezelni, tájékoztatást adni kizárólag a jegyző által meghatározott személyeknek szabad. A nyomozás során tisztázni kell, hogy hibáztatható-e valaki a megtörténtek miatt, és ha igen, akkor szükséges-e fegyelmi lépéseket tenni az ügyben.

A nyomozati szakaszban szükséges lehet az üzemeltetési, biztonsági naplókban található adatok és egyéb bizonyítékok begyűjtése ahhoz, hogy:

- Fel lehessen használni a szerződésszegés vagy a szabályzat megszegésének bizonyítékaként;
- Fel lehessen használni a hardver és / vagy szoftverszállítókkal folytatandó, kártérítésre vonatkozó tárgyalásokon;
- A számítógép nem rendeltetésszerű használatával vagy adatok védelmével kapcsolatos esetleges bírósági tárgyalás folyamán bizonyítékként lehessen felhasználni.

A begyűjtött bizonyítékokat oly módon kell megőrizni, hogy azokat egy esetleges bírósági tárgyalás során hitelesnek fogadják el, azaz a bizonyítékok manipulációjának gyanúja ne merülhessen fel.

Ennek érdekében az adatbiztonsági kihágásokhoz kapcsolódó nyomozás lefolytatásáról és az azt lezáró határozathozatal eseményeiről az informatikusnak jegyzőkönyvet kell vezetnie.

Az incidens jegyzőkönyvét és valamennyi azt alátámasztó dokumentációt végső áttekintés után iktatni kell. Az adatbiztonsági kihágás jegyzőkönyveit a törvény szerint meghatározott ideig szükséges tárolni és megőrizni.

A jegyző intézkedik az eseménnyel és a keletkezett károk elhárításával kapcsolatban.

Első lépésként az esemény kivizsgálását kell elvégezni. Lehetőség szerint meg kell állapítani, hogy pontosan mi történt, és milyen javító intézkedések lehetségesek.

Ezt követően, ha nem lehetséges a helyes működés azonnali visszaállítása, akkor átmeneti javító (vagy a hibát megkerülő) intézkedést kell hozni a működés vagy szolgáltatás részleges helyreállítása érdekében.

A végleges javító intézkedés elvégzésével helyre kell állítani a helyes működést.

Az incidens lezárása után az informatikus tájékoztatja az incidenst bejelentő munkatársat az incidens lezárásáról és annak eredményéről. A tájékoztatásnak az a célja, hogy a bejelentő pozitív visszacsatolást kapjon arról, hogy a bejelentésének volt értelme, azzal érdemben foglalkoztak, és a továbbiakban is számítanak az információ-védelmet erősítő bejelentéseire. A tájékoztatás részletességénél figyelembe kell venni a végrehajtott intézkedések bizalmasságát.

7.2.2. JAVÍTÓ FEJLESZTÉSEK KEZELÉSE

Az ideiglenes vagy végleges javítás megtörténte után, a gazdaságossági szempontok figyelembevételével helyesbítő tevékenységet kell végezni az esemény újbóli előfordulásának megakadályozására. Ennek során

- meg kell állapítani az eseményt kiváltó okot,
- meg kell határozni a helyesbítő intézkedést,
- be kell vezetni a helyesbítő intézkedést,
- meg kell határozni a helyesbítő intézkedés hatásosságának ellenőrzési módszerét,
- egy későbbi időpontban ellenőrizni kell, hogy a helyesbítő intézkedés hatásos volt-e, azaz beváltotta-e a hozzáfűzött reményeket, vagyis tényleg nem fordult-e elő az esemény ismétlődése a helyesbítő intézkedés bevezetése óta.

A Hivatal által elvégzett intézkedést (átmeneti és végleges javító, valamint a helyesbítő intézkedést) dokumentálni kell, melyet a jegyzőnek át kell adni megőrzésre. Ugyanazzal az eseménnyel kapcsolatos folytatólagos intézkedéseket egy űrlapon kell vezetni.

A jegyzőkönyvek elzártan történő tárolása a jegyző feladata.

A jegyző az információvédelmi oktatások tematikájának kialakításakor figyelembe veszi az információvédelmi események nyilvántartásában szereplő tételeket.

8. MŰKÖDÉS FOLYTONOSSÁG BIZTOSÍTÁSA

A Hivatalnak rendelkeznie kell a működés folytonosság fenntartásához és javításához szükséges eljárási és működtetési dokumentációkkal.

A működésfolytonossági tervek elkészítését, illetve módosítását követően tesztelni kell a dokumentumokban foglaltakat. A jegyző által megbízott személy tervezi meg, koordinálja és dokumentálja a teszteket.

A működésfolytonossági tervek felülvizsgálata akkor szükséges, ha a kockázatok, az üzleti követelmények vagy az informatikai rendszerek változnak. Az informatikai biztonsági felelős évente megvizsgálja, és dokumentálja, hogy történtek-e olyan változások, amelyek a működésfolytonossági tervek módosítását és újratesztelését szükségessé teszik.

9. KÖVETELMÉNYEKNEK VALÓ MEGFELELÉS

9.1. JOGI KÖVETELMÉNYEK

9.1.1. JOGSZABÁLYOK

A számítástechnikai eszköz felhasználásával elkövetett illegális cselekményt (számítógépes visszaélést) az követ el, aki:

- jogosulatlanul (hozzáférési engedély nélkül) használja az számítástechnikai erőforrásokat,
- szabotálja a számítógép használatát,
- kárt okoz a számítógépes adatokban és (vagy) a programokban, például megváltoztatja vagy törli az adatokat vagy programokat,
- jogosulatlanul megismeri (lehallgatja) az adatokat, számítógéppel kémkedik,
- hamisít (számítógép segítségével),
- csal (számítógép segítségével),
- jogellenesen másolja a védett számítógépes programokat
- számítástechnikai rendszer védelmét biztosító technikai intézkedést kijátszik

A Büntető törvénykönyvben meghatározottak szerint bűncselekményt követ el az adatokkal kapcsolatban, aki:

- jogosulatlanul megismeri a magántitkot
- megsérti a magántitkot
- megsérti a levéltitkot
- szerzői jogot sért
- számítógépes rendszer és adatok ellen bűncselekményt követ el
- jogosulatlanul végez adatkezelést
- visszaél a különleges személyes adatokkal
- gazdasági titoksértést követ el

9.1.2. SZOFTVEREK JOGTISZTASÁGA

A Hivatal tulajdonában és használatában lévő számítógépekre csak jogilag tiszta szoftvert telepíthető és az adathordozókon kizárólag jogilag tiszta szoftver tárolható.

A Hivatal informatikai rendszereiben csak központilag telepített vagy engedélyezett és felügyelt szoftverek használhatók.

A Hivatal által birtokolt és használt szoftverek telepítő készleteit, telepítő kódjait tilos kivinni, átadni, másolni vagy mások részére hozzáférhetővé tenni, kivéve, ha erről a Hivatallal kötött szerződések másként rendelkeznek.

A Hivatal tulajdonában és használatában lévő számítógépek csak Hivatal által engedélyezett és nyilvántartott szoftvereket tartalmazhatják.

A szoftverek frissítése esetén a jogilag tisztán birtokolt szoftverek gyártói által biztosított javító készleteket kell használni.

Próbaverzióval rendelkező szoftver licencek használatát kerülni kell.

Az ingyenesen használható és próba licencek esetében a gyártó licencszerződésében meghatározottak szerint kell eljárni.

9.1.3. ADATVÉDELMI INTÉZKEDÉSEK

A fontosabb dokumentációk másolásáról és biztonságos tárolásáról gondoskodni kell.

A védett, vagy kiemelten védett adatok továbbításáról (az átadás tényéről, időpontjáról, az átadott adatok köréről) a Hivatal adatgazdáinak nyilvántartást kell vezetnie.

A rendszerről készült dokumentációkat bizalmasan kell kezelni. A készített dokumentumokat az informatikus őrzi.

Az installált rendszerszoftverek és az egyedinek tekinthető, a nem reprodukálható alkalmazói szoftverek referencia-másolatait biztonságosan kell tárolni.

Az auditok során készített jegyzőkönyveket, elemzéseket bizalmasan kell kezelni. A készített dokumentumokat a jegyző megbízottja őrzi.

9.1.4. TITKOSÍTÁSI ELŐÍRÁSOK

Az informatikusnak nyilvántartást kell vezetnie a felhasználóknak átadott titkosításhoz használt kulcsokról, visszavonáskor gondoskodnia kell a kulcsok megsemmisítéséről. Biztosítani kell a titkosításhoz használt kulcsok biztonságos előállítását, tárolását.

Az adatok titkosításához csak megbízható rejtjelező algoritmust alkalmazó eszközöket szabad használni.

A bizalmasság és integritás védelmében alkalmazott rejtjelkulcsok (a szimmetrikus algoritmusok kulcsai) továbbítása az információs rendszerben (pl. a védett kulcsok időszakos cseréje miatt) csak védett csatornán keresztül történhet.

A Hivatal számítógépein egységes titkosító szoftver megoldást kell használni.

A titkosításhoz használt kulcsokat védeni kell, nem szabad harmadik személynek kiadni.

9.2. INFORMATIKAI RENDSZER FELÜLVIZSGÁLATA

9.2.1. FELÜLVIZSGÁLATI ELŐÍRÁSOK

A Hivatal alkalmazásainak auditálása az érintett szervezeti egységek vezetőivel egyeztetve folytatható úgy, hogy az ne veszélyeztesse azoknak a biztonságát.

Az informatikai rendszerek biztonsági állapotáról a külső auditor által elvégzett biztonsági ellenőrzésekkel és értékelésekkel kell meggyőződni.

A megfelelő feltételeket, például személyeket, infrastruktúrát, eszközöket, hatásköröket stb. biztosítani kell a rendszeres biztonsági ellenőrzésekhez

A biztonsági előírások számon kérhetőségét a munkatársak kiválasztásával, a feladatok, hatáskörök, jogosultságok és felelősségek kiosztásával, a munkatársak biztonsági kiképzésével és ellenőrzési mechanizmusok életbe léptetésével kell megalapozni.

A szakszerűséget, tárgyilagosságot és függetlenséget biztosítani kell a biztonsági ellenőrzéseknél a résztvevők - külső cégek és (vagy) belső személyek - kiválasztásával.

A minőségügyi vizsgálatok eredményeit elemezni kell abból a szempontból, hogy az informatikai szolgáltatásokra tett megállapítások visszavezethetők-e informatikabiztonsági hiányosságokra. Az elemzést dokumentálni kell.

Az ellenőrzések során feltárt hiányosságokat értékelni kell, majd a biztonsági kockázatok csökkentésére vonatkozóan intézkedéseket kell bevezetni.

10. FÜGGELÉK

10.1. MELLÉKLETEK

1. számú melléklet – Információ védelmi szabályzat
2. számú melléklet – Selejtezési Szabályzat
3. számú melléklet –Jogosultság kiosztási nyilvántartás
4. számú melléklet – Besorolási ív
5. számú melléklet - Alkalmazotti nyilatkozat
6. számú melléklet – Adat besorolási kérelem
7. számú melléklet – Munkahelyi környezet létrehozása/megszüntetése
8. számú melléklet – Felhasználói jogosultság igénylő lap
9. számú melléklet – Incidens bejelentő lap
10. számú melléklet - Géptermi napló
11. számú melléklet - Archiválási napló
12. számú melléklet - Mentési utasítás