Dunakeszi Polgármesteri Hivatal

Adathordozók Védelmi Szabályzata

Készítette:

Nádor RENDSZERHÁZ

Dunakeszi, 2019.

A DOKUMENTUM MÓDOSÍTÁSAINAK JEGYZÉKE

A dokumentum következő felülvizsgálatát 2020.06.30-ig el kell végezni.

V1.0	2018. 07. 10.	Első verzió	Nádor Rendszerház Kft.
Verzió	**Dátum**	**Leírás**	**Hatályba helyező utasítás száma**

TARTALOM

1 ÁLTALÁNOS RENDELKEZÉSEK

1.1 A SZABÁLYZAT CÉLJA ÉS HATÁLYA

Az Adathordozók Védelmi Szabályzatának célja, hogy meghatározza a **Dunakeszi Polgármesteri Hivatal** (továbbiakban: Hivatal) informatikai rendszerében használt adathordozók és adattárolásra alkalmas eszközök használatának és selejtezési folyamatát, továbbá az azokhoz kapcsolódó ellenőrzések megvalósítását.

1.1.1 A szabályzat karbantartása

Az Adathordozók Védelmi Szabályzatát évente felül kell vizsgálni és frissíteni kell. Felül kell vizsgálni abban az esetben is, ha az informatikai környezetben, vagy a vonatkozó jogszabályokban jelentős változás áll be.

1.2 A SZABÁLYZAT HATÁLYA

A szabályzat tárgyi hatálya kiterjed

- a Hivatal tulajdonát képező valamennyi adathordozóra, valamint az elektronikus berendezésekben lévő beépített adattárolókra, különösen, de nem kizárólag az alábbi eszközökre:
  - asztali munkaállomások, laptopok, tablet számítógépek,
  - fájl- és nyomtató szerverek, multifunkcionális nyomtatók,
  - központi infrastruktúra kiszolgálói és háttértárai,
  - eltávolítható adathordozók, kivehető és hordozható merevlemezek, CD/DVD,
  - pen-drive-ok (USB drive-ok), memóriakártyák,
  - mobil telefonok, PDA-k, digitális fényképezőgépek és egyéb adatrögzítésre alkalmas eszközökön tárolt adatokra.

A szabályzat személyi hatálya az intézményben foglalkoztatott valamennyi közszolgálati, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottaira, munkavállalóira, megbízottjaira (a továbbiakban együtt: munkatársak) egyaránt kiterjed.
A szabályzat személyi hatálya kiterjed továbbá minden személyre, aki a Hivatal informatikai vagy azzal összefüggő rendszerét, szolgáltatásait igénybe veszi, informatikai struktúráját és annak eszközeit üzemelteti vagy használja, függetlenül a Hivatalhoz kapcsolódó jogviszonyától.

2 HOZZÁFÉRÉS AZ ADATHORDOZÓKHOZ

Az eszközökbe épített adathordozókat, továbbá az elektronikus információs rendszer központi elemeinek adathordozóit, rendszer és mentési adathordozókat csak az informatikusok kezelhetik.
A személyi használatra kiadott adathordozókat, mint a laptop, pen-drive, külső merevlemez stb., csak az arra jogosult munkatársak használhatják.

2.1 Ismeretlen tulajdonos

Tilos olyan adathordozók használata, az elektronikus információs rendszerhez történő csatlakoztatása, melyek tulajdonosa nem azonosítható. (Például a Hivatal területén talált, vagy postán érkezett, nem azonosítható adathordozók használata tilos.)

2.2 Adathordozók kezelése

Az adathordozókat minden felhasználónak rendeltetésszerűen kell használnia. A Hivatal adathordozóin csak munkavégzéshez szükséges adatokat szabad tárolni.

A felhasználók saját tulajdonú informatikai eszközeiket, adathordozóikat a Hivatal informatikai hálózatához nem csatlakoztathatják.

Egyes, vagy bármely adathordozó típusok csatlakozását a Hivatal engedélyezheti, korlátozhatja, vagy tilthatja a meghatározott elektronikus információs rendszereken vagy rendszerelemeken működő biztonsági intézkedések használatával.

2.2.1 Adathordozók nyilvántartása

A Hivatal informatikai területe köteles a saját hatáskörében kezelt adathordozókról nyilvántartást vezetni.

A személyi használatra kiadott adathordozókról nyilvántartást kell vezetni, az átvétel tényét az érintett felhasználó aláírásával igazolja. A nyilvántartásért felelős a Gazdasági Osztály.

Az adathordozó nyilvántartások megfelelőségét az informatikai biztonsági felelős ellenőrizheti.

A szervezet által használt adathordozókat évente leltározni kell.

2.2.2 Adathordozók tárolása és szállítása

Az adathordozókat védeni kell, fizikailag ellenőrzött és biztonságos módon kell tárolni, mindaddig, amíg az adathordozókat jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy nem törlik.

A Hivatal üzemszerűen nem szállít adatokat, illetve adatokat tartalmazó eszközöket. Amennyiben erre szükség lenne, a szállítás során megfelelő módon gondoskodni kell az adathordozók (adatok) bizalmasságának és sértetlenségének védelméről. (Például a Kormányzati Adattrezorba történő átadás esetén).

Az esetleges adathordozó szállításokkal kapcsolatos tevékenységeket dokumentálni kell.

A személyi használatra kiadott adathordozók és eszközök mozgatását nem kell külön dokumentálni.

2.2.3 Adathordozók törlése

A meghibásodott, további felhasználásra alkalmatlan adathordozókat fizikai roncsolással kell megsemmisíteni.

Az adathordozókat selejtezés vagy az újrafelhasználásra való kibocsátás előtt helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal kell törölni.

Amennyiben az eszköz (adathordozó) a Hivatalon belül kerül újrafelhasználásra, abban az esetben elegendő a normál törlési technikák alkalmazása (formázás).

Az adathordozók törléséről, megsemmisítéséről jegyzőkönyvet kell készíteni, melyet az informatikán kell tárolni.

2.2.4 Informatikai eszközök selejtezésének különös szabályai

Az informatikai eszközök selejtezése során az egyéb szabályzatokban meghatározott eljárások szerint az eszközöket ki kell vezetni a pénzügyi és informatikai nyilvántartásokból.
Meg kell vizsgálni, hogy az eszköz adathotdozónak minősül-e, vagy tartalmaz-e beépített adathordozót. Különös figyelemmel kell eljárni a multifunkcionális fénymásoló-nyomtató jellegű eszközök esetén, melyek, típustól függően, tartalmazhatnak beépített adathordozót (merevlemezt).
A leselejtezett informatika eszközökből az adathordozókat ki kell építeni, majd az eszköztől függetlenül kell megsemmisíteni, a környezetvédelmi és hulladékkezelési előírások betartása mellett.
Amennyiben az informatikai eszköz harmadik fél részére, további használat céljából átadásra kerül, akkor a beépített adathordozót ki kell építeni, majd a 2.2.4. pont szerinti, helyreállíthatatlanságot biztosító törlési technikával kell az adatokat törölni. Csak az így törölt adathordozót szabad az eszközben visszatenni.
Nem kerülhetnek átadásra selejtezés útján sem, a számítógépeken telepített alkalmazások, szoftverek. Az OEM (harverhez kötött) licencet a számítógépet átvevő fél felhasználhatja.

2.3 Adathordozók javíttatása

Hivatali adatokat tartalmazó adathordozókat csak abban az esetben lehet külső helyszínen javíttatni, ha az adatok előzőleg szoftveres vagy hardveres úton el lettek távolítva. Minden egyéb esetben tilos az adattárolót külső helyszínen javíttatni.
Amennyiben garanciális okok miatt nem lehet az eszközből kivenni az adathordozót és azon hivatali adatok találhatók, tilos az eszközt külső helyszínen javíttatni.
Ettől eltérni csak a jegyző írásos utasítására lehet.

2.4 Adathordozók ellenőrzése

Valamennyi adathordozót ellenőrizni kell a kártékony kódok tekintetében, mielőtt azt az elektronikus információs rendszerben használnák. Az ellenőrzés történhet automatikus rendszerbeállításokkal is.

2.5 Kriptográfiai védelem

Kriptográfiai mechanizmusokat kell alkalmazni a digitális adathordozókon tárolt információk bizalmasságának és sértetlenségének a védelmére az olyan eszközök tekintetében, melyek folyamatos védett tárolása nem biztosított vagy a Hivatal területén kívülre kerülhetnek. Ennek érdekében titkosítani kell a:

- hordozható számítógépek merevlemezét,
- eltávolítható adathordozókat (pendrive, külső merevlemez)

Új beszerzés során olyan eltávolítható adathordozókat kell beszerezni a felhasználók számára, melyek a felhasználó számára megkerülhetetlen titkosítással rendelkeznek.

2.6 A KIMENETI ESZKÖZÖK HOZZÁFÉRÉS ELLENŐRZÉSE

Az elektronikus információs rendszer kimeneti eszközeihez való fizikai hozzáférést korlátozni kell annak érdekében, hogy jogosulatlan személyek ne férjenek azokhoz hozzá. Különösen a nyomtatókra és fénymásoló berendezésekre igaz, hogy a látogatói (ügyfél) forgalomtól, egyéb munkatevékenységtől elkülönített helyiségben kerüljenek elhelyezésre.

A védett elhelyezésen túl, a közös használatú eszközök esetén egyéb eljárásokkal (például biztonsági kód alkalmazásával) biztosítani kell, hogy a nyomatokhoz vagy egyéb kimenetekhez csak az arra jogosult személy férhessen hozzá.

1. SZ MELLÉKLET: INFORMATIKAI ADATHORDOZÓ ADATMEGSEMMISÍTÉSI BIZONYLAT

INFORMATIKAI ADATHORDOZÓ ADATMEGSEMMISÍTÉSI BIZONYLAT

Eszköz leírása, azonosítója:
(munkaállomás azonosító vagy az eszköz, adathordozó egyedi azonosítója, leltári vagy gyári száma): .....

(Adathordozók csoportos megsemmisítése esetén a hitelesített jegyzéket csatolni kell)

Az adattörlés célja: ☐ újrahasznosítás (Hivatalon belüli újrafelhasználás)
☐ újrahasznosítás (Hivatalon kívüli újrafelhasználás)
☐ selejtezés.

A törlési eljárás:

- ☐ formázás – csak belső újrahasznosítás esetén engedélyezett
- ☐ fizikai törlés a ..... szoftverrel
- ☐ demagnetizálás
- ☐ fizikai roncsolás ..... módon (darálás – iratmegsemmisítő, átfúrás stb.)
- ☐ adatmegsemmisítés specializált vállalkozás által.

Külső megsemmisítés esetén: *(átvételi és megsemmisítési bizonylatot csatolni kell)*

Vállalkozás megnevezése: .....

Szerződés / munkaszám: .....

Az adatmegsemmisítés időpontja: 201..év .....hó nap óra perc

Adatmegsemmisítés végrehajtója (IT felelős):

.....
aláírás

Ellenőrizte

.....
aláírás

Dunakeszi Polgármesteri Hivatal

Felhasználói Biztonsági Szabályzat

Készítette:

Nádor RENDSZERHÁZ

Dunakeszi, 2019.

Tartalom

1 Általános rendelkezések

1.1 A Felhasználói Biztonsági Szabályzat célja és területi érvényessége

A Felhasználói Biztonsági Szabályzat (a továbbiakban: Szabályzat) alapvető célja, hogy a **Dunakeszi Polgármesteri Hivatal** (továbbiakban: Hivatal) munkavállalói számára meghatározza az informatikai rendszer alkalmazásához szükséges alapvető biztonsági ismereteket és szabályokat.

Annak érdekében, hogy az érintettek felkészülhessenek a lehetséges belső és külső fenyegetések felismerésére és azok elkerülésére, meg kell ismerniük és be kell tartaniuk jelen szabályzatban foglalt védelmi intézkedéseket.

2 A Szabályzat hatálya

2.1 Személyi hatály

A Szabályzat személyi hatálya az intézményben foglalkoztatott valamennyi köztisztviselőre, fő- és részfoglalkozású munkavállalóra, illetve az informatikai eljárásban résztvevő más szervezetek dolgozóira (a továbbiakban együtt: felhasználók) egyaránt kiterjed.

2.1.1 Tárgyi hatály

A Szabályzat tárgyi hatálya kiterjed valamennyi, a Hivatal tulajdonában álló vagy általa használt elektronikus információs rendszerre, informatikai eszközökre, melyek a Hivatal kezelésében lévő adatok tárolásában, feldolgozásában, továbbításában részt vesznek.

3 Általános szabályok

3.1 Munkába állás

Munkába álláskor a munkatársak alapvető informatikai és információbiztonsági oktatásban részesülnek. A titoktartásra vonatkozóan a munka törvénykönyve (továbbiakban: Mt.) hatálya alá eső munkavállalók titoktartási nyilatkozatot írnak alá, a közszolgálati tisztviselőkről szóló törvény (a továbbiakban: Kttv.) hatálya alá eső köztisztviselők esküt tesznek.

Az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt a felhasználó köteles írásbeli nyilatkozattételre, amely nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja.

3.2 A felhasználó szerepe és felelőssége az informatikai biztonság tekintetében

A Hivatal információs vagyonát a rendszerek felhasználói kezelik, ezért az informatikai biztonsággal kapcsolatos törekvések sikerességében kritikus szerepet játszik a felhasználói tájékozottság és a kellő óvatosság, azaz az informatikai biztonságtudatosság.

A felhasználóknak tisztában kell lenniük a rájuk bízott adatok, információk bizalmas jellegével, azzal, hogy milyen fenyegetések és támadási lehetőségek veszélyeztetik ezen adatokat, információkat.

Az elektronikus információs rendszerek felhasználóinak felelőssége,

- a felhasználó által használt alkalmazói rendszerek felhasználói leírásainak ismerete és az alkalmazások használatakor azok pontos betartása;
- a Felhasználói Biztonsági Szabályzatban szereplő előírások maradéktalan betartása;

A Hivatal minden alkalmazottja köteles:

- az IBSZ-ban előírtak ellenőrzések és auditok sikeres megvalósítását elősegíteni és támogatni;
- tudomásul venni, hogy az informatikai biztonság ellenőrzése során előzetes bejelentés nélkül ellenőrizhető az informatikai biztonsághoz kapcsolódó utasítások, szabályzatok betartása.

3.3 Oktatások

Minden munkatársnak évente információbiztonsági képzésen kell részt vennie. A képzés során a felhasználók megismerik az aktuális információbiztonsági fenyegetéseket, veszélyeket, a felhasználók által gyakran elkövetett hibákat. Az oktatás felhívja a figyelmet a jogszabályi és belső szabályozási környezet változásaira is.

3.4 Fegyelmi eljárás

A Hivatal az információbiztonsági szabályok szándékos vagy gondatlan megsértése esetén, hasonlóan más szabálytalanságokhoz, a cselekmény súlyosságától függően, fegyelmi vagy büntetőjogi felelősségre vonást kezdeményez az elkövetővel szemben.

Bármilyen, az informatikai rendszerben vagy az informatikai rendszerrel végzett tevékenységgel összefüggésben a hivatalnak történő károkozás esetén a munkatárs helytállási kötelezettségét a Kttv. rendelkezései szabályozzák.

4 Általános informatikai biztonsági szabályok

A felhasználó felelőssége munkájának ellátása érdekében a hozzá rendelt informatikai eszközök eredményes, rendeltetésszerű használata, betartva a használatra vonatkozó, a Hivatal által meghatározott szabályokat.

ÁLTALÁNOS IRÁNYELV, HOGY MINDEN TILOS, AMI NINCSEN KIFEJEZETTEN MEGENGEDVE!

4.1 Hozzáférés-szabályozás

4.1.1 Hozzáférés a hivatali információs rendszerekhez, alkalmazásokhoz és megosztott könyvtárakhoz

A Hivatali információs rendszer erőforrásainak (alkalmazások, nyomtatás stb.) történő hozzáférés érdekében a felhasználók egyedi azonosítót kapnak és jelszavas bejelentkezésen keresztül juthatnak hozzá a hálózaton tárolt információkhoz. A felhasználó hozzáféréseinek meghatározása a szervezeti egység vezetőjének feladata, esetenként jegyzői jóváhagyást is igényel.

A munkatársak számára az adatok hozzáférési jogosultságának megadását, módosítását a munkahelyi vezető az adatok kezeléséért felelős vezetőtől (adatgazdától) vagy a megosztott könyvtárak tulajdonosaitól a jogosultságigénylés szabályai szerint igényli.

Jellemzően a számítógépet használó munkatársak az alábbi hozzáférésekkel, jogosultságokkal rendelkeznek, munkakörüktől függően

- hozzáférés alkalmazásokhoz;
- hozzáférés egyéb hálózati erőforrásokhoz, nyomtatás;
- HOME könyvtárak;
- megosztott könyvtárak;
- elektronikus levelezés;
- internet elérés.

4.1.1.1 Elektronikus levelezés

A Hivatal a felhasználók számára, a munkavégzéshez <vezeteknev.keresztnev>@dunakeszi.hu>, című postafiókot készít. A postafiók kizárólag hivatalos célra használható.

4.1.1.2 HOME könyvtár

A „HOME" könyvtár minden felhasználónak a saját könyvtára a hálózaton. Az elkészített dokumentumokat, kimutatásokat stb. itt kell tárolni, mert ez a terület rendszeresen mentésre kerül, az itt tárolt anyagok megőrzése biztosított.

A felhasználók számára az informatikus hozza létre a felhasználók saját könyvtárát.

Egyúttal a könyvtár elérését, az egyes kliens számítógépeken beállítja.

4.1.1.3 Megosztott könyvtárak

A „megosztott könyvtár" az adott osztály vagy szervezeti egység közösen tárolt dokumentumainak a gyűjtőhelye, a csoportmunka egyik eszköze. Ehhez a feljogosított munkatársak hozzáférnek, tudnak állományokat létrehozni, módosítani, törölni, ezért különös gondossággal kell ezeket a könyvtárakat kezelni.

A felhasználók számára az informatikus hozza létre a megosztott könyvtárakat. Egyúttal a könyvtár elérését, az egyes kliens számítógépeken beállítja.

4.2 Felelősség az eszközökért – az eszközök elfogadható használata

4.2.1 Informatikai eszközök és szoftverek

A munkatársak az informatikuson keresztül kapják meg a munkavégzésükhöz szükséges informatikai eszközöket.

A tárgyi eszköznek minősülő informatikai eszközök beszerzése és értéknövelő beruházása, továbbá szoftverek beszerzése csak az informatikus szakvéleményével, kizárólag jegyzői-engedéllyel történhet.

Az informatikai eszközök telepítését, megfelelő üzembe helyezését csak az informatikus, egyedi esetekben a szállító, forgalmazó, szervizes cég szakembere az informatikus közreműködésével végezheti el.

Szoftverek telepítését, megfelelő üzembe helyezését csak az informatikus vagy a készítő, forgalmazó cég szakembere az informatikus felügyeletével végezheti el.

Az egyes szervezeti egységek, munkatársak által használt informatikai eszközök a használó személyeknek kerülnek átadásra. Az átvevő felel az eszköz állapotáért és biztonságos használatáért. Amennyiben a személyre szóló átadás nem történik meg, a felelős az adott eszközt használó részleg vezetője.

Az asztali munkaállomás gazdája az azt használó munkatárs. Minden dolgozó a saját munkahelyén elhelyezett vagy a személyre kiadott informatikai eszközök szakszerű működtetéséért, vagyon- és állagvédelméért egyszemélyi felelős. Tilos a felhasználónak az eszközöket szétszerelnie, abból alkatrészeket eltávolítania, kicserélnie, elszállítania.

Tilos továbbá – jegyzői engedély nélkül – nem engedélyezett (nem a Hivatal tulajdonában álló) eszközöket a munkaállomásához vagy az informatikai hálózathoz csatlakoztatni

Amennyiben a felhasználó munkája során az informatikai eszköz működésében rendellenességet, hibát tapasztal, haladéktalanul jelenteni köteles az informatikus felé.

4.2.2 Információ-feldolgozó eszközök használata

Minden alkalmazottnak be kell tartania az információ-feldolgozó eszközök használatának szabályait. Ezek az alapelvek az információ-feldolgozó eszközök használatát rögzítik, miszerint meghatározzák az elektronikus levelezés és az internet használatának feltételeit, továbbá szabályozzák a mobil számítástechnikai eszközök alkalmazhatóságát a Hivatal telephelyein kívül.

A Hivatal által működtetett elektronikus információs rendszerek, az azokban tárolt adatok a Hivatal tulajdonát képezik. A Hivatal tulajdonát képezi a levelező rendszer, az abban a személyekhez rendelt e-mail címek, továbbá az internet kapcsolat is. Az eszközöknek nem a Hivatal céljaira történő (magáncélú) felhasználása tiltott.

A felhasználók munkaállomásukra, vagy központi tárolóra kizárólag a Hivatal által engedélyezett tartalmat másolhatnak fel (nem engedélyezett a magáncélú fénykép, filmek, zene stb.). Az informatikai eszközökön személyes adatnak minősülő információt magáncélból tárolni tilos.

Tilos Hivatali információkat tartalmazó levelezést magán e-mail címről folytatni.

Tilos a Hivatal elektronikus információs rendszerein és eszközeivel:

- hivatali levelező rendszert átirányítani magán e-mailre,
- nem hivatali célból rendszer-, alkalmazói- illetve játékprogramok, film- és zenei állományok valamint képfájlok letöltése, feltöltése és továbbítása,
- bármilyen, hivatali adat nem hivatali célból történő továbbítása.
- web-mail használata (Gmail, Citromail stb.),
- internetes (felhő alapú) tárhely és fájl megosztó szolgáltatások használata.

Az Önkormányzat, illetve a Hivatal nyilvános megjelenésével kapcsolatos munkaköri feladatot ellátó munkavállalók és köztisztviselők kivételével:

- nem engedélyezett a közösségi oldalak látogatása (Facebook, Twitter stb.),
- tilos továbbá a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való közzététele. A szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele tiltott a Hivatalon kívül megvalósuló internet használat során is.

A Hivatal az adatvédelem és adatbiztonság érdekében rendszeresen ellenőrzi a munkaállomásokon és központi meghajtókon tárolt tartalmakat, naplózza és rögzíti az e-mail forgalmat, ellenőrzi az e-mailek tartalmát. Naplózásra kerül az internet forgalom, beleértve a meglátogatott tartalmakat, illetve a le- és feltöltött információt.

A Hivatal az adatbiztonság érdekében korlátozhatja és monitorozhatja az internet és e-mail forgalmat.

Az informatikai terület feladata az elektronikus adatforgalom rendszeres figyelése és monitorozása.

A munkatársaknak írásban nyilatkozniuk kell arról, hogy tudomásul veszik a korlátozásokat, miszerint a Hivatal információs rendszereit csak hivatalos célra használhatják, az elektronikus információs

rendszereken végzett tevékenységek, a kimenő és bejövő elektronikus levelek biztonsági ellenőrzésre kerülnek, tudomásul veszik továbbá, hogy az internetes forgalom, a meglátogatott tartalmak rögzítésre kerülhetnek.

4.2.3 Az elektronikus levelezőrendszer használata

A felhasználók saját postafiókot kapnak a levelező rendszerben, ahonnan feladataiknak megfelelően küldhetnek és fogadhatnak levelet.

A Hivatal belső hálózatán nem hivatali célú üzenetet nem nevesített (pl. Csoport, Mindenki) felhasználóknak küldeni tilos. A tilalom betartását az informatikus ellenőrzi és indokolt esetben a jegyző részére jelentést tesz.

A munkatársak távolléte esetén, a postafiókjuk forgalma átirányításra kerül a helyettesítésüket ellátó munkatárs részére.

4.2.3.1 Az elektronikus levelezés biztonsága

Az elektronikus levelezés a papír alapú levelezéstől eltérő kockázatokkal terhelt.

Az interneten át történő levelezés sajátossága, hogy

- a levelek továbbítása, kézbesítése az interneten keresztül nem garantált,
- a továbbított levelek sértetlensége, hitelessége nem garantálható,
- internetes levelezés esetén a levél fogadása és elküldött tartalma nem bizonyítható.

Mivel az interneten át történő adattovábbítás nem védett, ezért a munkatársak nem küldhetnek bizalmas információt e-mail titkosítatlan mellékleteként!

4.2.4 A Hivatal elektronikus információs rendszereinek biztonsági monitorozása

Az informatikai terület feladata az elektronikus adatforgalom rendszeres figyelése és monitorozása, a szabályok megszegése esetén a munkahelyi vezetők értesítése.

A monitorozás alá bevont területek, egyebek mellett:

- belső vezetékes és vezeték nélküli (WiFi) hálózati forgalmak,
- interneten meglátogatott helyek, le- és feltöltött tartalmak,
- levelező rendszeren keresztül bonyolított forgalmak,
- belső nyomtatási tevékenységek, nyomtatott tartalmak, nyomtatás mennyisége.

4.3 Eszközök és szoftverek biztonságos használata

4.3.1 Fizikai biztonság

Meg kell akadályozni a berendezések elvesztését, károsodását, ellopását, a vagyontárgyak veszélyeztetését és a szervezet tevékenységének megszakítását. A berendezéseket védeni kell a fizikai és környezeti fenyegetésektől.

Az irodákban és egyéb helyiségekben elhelyezett információ-feldolgozó eszközöket védeni kell. Illetéktelenek hozzáférésének megakadályozása érdekében, a helyiségeket be kell zárni, amennyiben az oda beosztott dolgozók távoznak.

Az irodákban a számítógépeket úgy kell elhelyezni, hogy

- minimalizálják a monitorra oldalról történő rálátást
- akadályozzák meg az illetéktelen fizikai hozzáférést
- ételt, italt úgy kell tárolni, hogy az ne borulhasson a számítógépbe.

A Hivatal területéről informatikai eszközt a jegyző vagy az informatikus írásbeli engedélye nélkül kiszállítani tilos! Kivételt képeznek az egyes területek, illetve munkatársak részére átadott személyi használatú számítástechnikai eszközök.

4.4 Védelem rosszindulatú szoftverek ellen (vírusvédelem)

Összefoglaló kifejezéssel rosszindulatú kódoknak nevezzük azokat az alkalmazásokat, melyeket károkozás céljából, fejlesztettek ki, ezek a vírusok, férgek, trójaiak és egyéb, elsősorban az interneten keresztül terjedő, ártó tartalmak. Kiemelt veszélyt jelent a kártevők egy speciális formája, ezek az irodai rendszerrel terjedő makróvírusok, melyek jellemzően Microsoft Office dokumentumokhoz és táblázatokhoz kapcsolódnak

A felhasználók kötelezettségei a rosszindulatú kódok elleni védekezés során:

- ne nyissanak meg ismeretlen forrásból származó levelet,
- ne nyissanak meg gyanús csatolmányokat, mellékleteket, linkeket,
- a gyanús e-maileket olvasatlanul töröljék,
- a levelekben érkező hamis biztonsági figyelmeztetésekre ne reagáljanak, (tipikus a jelszó-megerősítést kérő oldal),
- soha ne adják meg jelszavukat e-mailes kérésekre,
- minden olyan esetben, amikor gyanús a levél, annak küldője ismeretlen, a levél megnyitása előtt forduljanak informatikus munkatárshoz.
- ne telepítsenek és ne futtassanak semmilyen szoftvert önhatalmúlag,
- ne tároljanak képeket, zenét a munkaállomáson,
- az interneten kizárólag a munkához szükséges tartalmakkal dolgozzanak,
- ne indítsanak semmilyen alkalmazást az internetről, böngészőből,
- ne csatlakoztassanak nem engedélyezett eszközöket a munkaállomásokhoz vagy laptopokhoz, mint külső adathordozók, fényképező, mobiltelefon stb.
- számítógépük biztonsági beállításait ne bírálják felül, ne állítsák át,
- a Microsoft Office állományokban ne nyissanak meg makrókat, amennyiben az állomány származása nem tisztázott.
- külső forrásból érkező adathordozókat, elektronikus leveleket felhasználás előtt vírusvédelmi szempontból ellenőrizni kell.

4.5 Eltávolítható számítógépes adathordozók kezelése

Az eltávolítható adathordozók jellegükből adódóan jelentős információbiztonsági kockázatot hordoznak.

Az eltávolítható adathordozók közé tartoznak a CD-k, DVD-k, külső merevlemezek, pendrive-ok, de ebbe a kategóriába tartoznak hozzáférhetőségük és felépítésük miatt a mobiltelefonok és fényképezőgépek memóriái is.

A Hivatal informatikai hálózatához eltávolítható adathordozót tilos jogosulatlanul hozzákapcsolni. A számítógépek USB portjai tiltásra kerülhetnek, ennek megakadályozására.

Munkavégzéshez szükséges esetben pendrive, fényképezőgép vagy egyéb adathordozó használata, egyedi munkahelyi vezető engedélyével történhet.

A hálózatra külső adathordozó (floppy, CD) lemezről, USB rendszerű adathordozóról vagy laptopról információ csak akkor kerülhet felmásolásra, ha előtte azt teljes körű vírus ellenőrzésnek vetették alá, és adatokat vírusmentesnek találták.

4.6 Általános információvédelmi megfontolások

Nem csak az elektronikus információt kell védeni!

A Hivatal alkalmazottai tartsák be, hogy

- ne hagyjanak bizalmas információt tartalmazó lapokat másológépen, faxkészülékben,
- ne folytassanak úgy bizalmas tárgyú telefonbeszélgetést, hogy azt illetéktelenek is meghallhassák,
- érzékeny információt tartalmazó üzeneteket ne hagyjanak az üzenetrögzítőkön, mert ezeket lejátszhatják jogosulatlan személyek,
- ne folytassanak bizalmas beszélgetést nyilvános helyeken, nyitott irodákban, büfében,
- amennyiben bizalmas információt tartalmazó küldeményt továbbítanak, erre használjanak belső alkalmazottat, illetve megbízható futárszolgálatot, s a küldemény csomagolása legyen megbontásra érzékeny.

4.7 „Üres asztal – tiszta képernyő" szabály

Az *üres asztal és tiszta képernyő* szabály általában az információk bizalmas voltának megőrzésére szolgál, megakadályozva azt, hogy illetéktelenek hozzáférjenek érzékeny információkhoz, legyen az papír alapon vagy elektronikus környezetben.

Olyan papírt, iratot vagy elektronikus adathordozót, amely bizalmas működési információt tartalmaz, el kell zárni, (lehetőleg páncélszekrényben vagy zárható iratszekrényben), ha nincs rá szükség, különösen, ha az irodában már nem tartózkodnak az oda beosztottak,

- a monitorokat úgy kell elhelyezni, hogy arra illetéktelenek ne láthassák a megjelenített információt,

- a felügyelet nélküli számítógépeket kijelentkezett állapotban kell hagyni vagy védeni kell egy képernyő- és billentyűzetlezáró eljárással, amelyet jelszó szabályoz,
- a beérkező és kimenő posta pontjait és a felügyelet nélkül faxgépeket védeni kell;
- meg kell előzni a fénymásolók és más másoló technikák (kamera, kamerás mobil) jogosulatlan használatát,
- az érzékeny vagy osztályozott információt tartalmazó dokumentumokat azonnal el kell távolítani a nyomtatókról, multifunkcionális másolókról,
- az íróasztalokon, különösen az ügyfelek által látogatott területen, még ideiglenesen sem maradhatnak bizalmas dokumentumok,
- érzékeny információt tartalmazó papírt, CD-t, selejt adathordozót tilos a szemétbe dobni, el kell szállítani megsemmisítésre.

4.8 A felhasználói jelszavak gondozása

A felhasználók a személyes azonosító (felhasználónév) és jelszó párossal férnek az információs rendszerek erőforrásaihoz A jelszavak általánosan használt eszközök, amelyek igazolják a használó azonosságát mielőtt hozzáférést biztosítanak egy információs rendszerhez vagy szolgáltatáshoz. *A jelszavát mindenkinek bizalmasan kell kezelnie, azt másnak át nem adhatja, nyilvánosságra kerülés esetén azonnal meg kell változtatnia.*

Általánosságban betartandók az alábbi szabályok:

- a jelszavakat biztonságosan kell tartani, nem szabad a számítógépre, papírra stb. felírni, ahol esetleg más is hozzáférhet,
- a jelszavakat haladéktalanul cserélni kell, ha esetlegesen más is megismerhette azokat,
- a jelszónak kellően biztonságosnak és bonyolultnak kell lennie (lásd később),
- nem szabad neveket, születési évszámokat és egyéb, a felhasználóhoz kötődő, vagy közismert kifejezéseket használni benne,
- a rendszerekhez kapott kezdeti jelszót első bejelentkezéskor le kell cserélni,
- a jelszavakat tilos mással megosztani, más tudomására hozni,
- ha valaki külön azonosítóval rendelkezik adminisztrátori munkájához, a jelszó ne legyen azonos a másik jelszavával.

Általában nem szabad a jelszavakat mással megosztani, más tudomására hozni.

A jelszórendszer több szintű. Az első szinten magához az informatikai rendszerhez, hálózathoz lehet hozzáférni, a munkaállomáson a Windowsba történő bejelentkezéssel, majd ezután újabb bejelentkezésekkel lehet az egyes rendszereket elérni.

A jelszavak lejárata előtt a rendszer automatikus figyelmeztető értesítést küld, majd az adott határidő lejártával a jelszóváltást ki is kényszeríti.

Az új jelszavaknak a következő követelményeknek kell megfelelniük:

- nem tartalmazhatják a felhasználói fiók nevét vagy a felhasználó teljes nevének két egymás utáni karaktert meghaladó részletét

- legalább nyolc karakter hosszúságúnak kell lenniük
- tartalmazniuk kell az alábbi elemeket:
  - ékezet nélküli nagybetűs karakterek (A-tól Z-ig)
  - ékezet nélküli kisbetűs karakterek (a-tól z-ig)
  - számjegyek (0-tól 9-ig)
- az új jelszó nem lehet azonos az előzőleg használt jelszóval

A bonyolultsági feltételeknek a jelszavak létrehozásakor vagy módosításakor kell érvényesülniük.

Ha a sikertelen bejelentkezési kísérletek száma meghaladja az előre beállított értéket (5), akkor a felhasználói azonosító letiltásra kerül. A tiltás feloldását az informatikusnál lehet kezdeményezni.

4.9 Hordozható számítástechnikai eszközök használata

A Hivatal a hatékonyabb munkavégzés érdekében lehetővé teszi hordozható számítástechnikai eszközök (laptopok, tablet PC-k, okostelefonok stb.) csatlakoztatását informatikai hálózatához. Ezek az eszközök, sajátosságaikból fakadóan, eltérő védelmi intézkedéseket igénylenek.

- Tekintettel arra, hogy a laptopoknak nincsen központi mentése, ezért az adatok mentéséért a laptop felhasználója felel.
- A laptopok teljes háttértárolóját, de legalább a tárolt bizalmas adatokat titkosítani kell. Pendrive-ra és egyéb külső adathordozóra nem kerülhetnek titkosítatlanul bizalmas adatok.
- A hordozható számítástechnikai eszközökön be kell állítani az automatikus jelszavas vagy grafikus képernyőzárat, ezért az eszköz használója felel.
- Tilos a laptopok illetve mobiltelefonok szoftverének, védelmi rendszerének feltörése, kikapcsolása, módosítása.
- Nyilvános helyen történő laptop használatnál az eszköz fizikai biztonsága mellett bizalmas adatokkal történő munka esetén ügyelni kell arra, hogy a képernyőre ráláthatnak arra nem jogosult személyek is.
- Csak fokozott óvatossággal szabad nyilvános WLAN (WiFi, hot-spot) hálózatot hivatali célokra használni, mivel az ilyen jellegű kommunikáció lehallgatható, visszafejthető.
- Az eszközöket védeni kell az ellopástól, biztonságosan, zárt táskában kell szállítani, nem szabad őrizetlenül hagyni és nem hagyhatók gépkocsi utasterében és csomagtartójában sem.
- A mobiltelefonok, táblagépek, laptopok ellopását, elvesztését kötelező azonnal jelenteni.

4.10 Incidens kezelés

4.10.1 Jelentés az informatikai biztonsági eseményekről

Az információbiztonsági eseményeket, tapasztalt rendellenességeket a lehető leggyorsabban jelenteni kell az informatikusnak. Ilyen esemény, amelyet a felhasználóknak azonnal jelenteniük kell, ha például

- szolgáltatás, a berendezés vagy az eszközök elvesztése történik,
- rendszer rendellenes működését észlelik,
- a szabályzatoknak vagy irányelveknek való nem-megfelelés válik nyilvánvalóvá,

- észlelhető a fizikai biztonsági rendelkezések megsértése,
- nem ellenőrzött rendszerbeli változásokat tapasztalnak,
- a szoftver vagy hardver hibás működése lép fel,
- hozzáférési sértések történnek.

4.11 Jelentés a biztonsági sérülékenységekről

Minden felhasználó kötelessége, hogy az informatikai rendszerekben általa észlelt rendellenességet, gyaníthatóan gyenge pontot vagy sérülékenységet jelentse az informatikusnak. Ezek a gyenge pontok támadásra, visszaélésre adnak lehetőséget, a védelmi intézkedések meghozatala szükséges.

A munkatársak csak jelentsék az észlelt problémát, de ne kíséreljék meg ellenőrizni vagy javítani a feltárt problémát, mert esetlegesen azzal is kárt okozhatnak.

A sürgős intézkedést kívánó esetekben az informatikus intézkedik.

4.12 Hibák és rendellenességek jelentése

Amennyiben a felhasználó munkája során az informatikai eszköz működésében rendellenességet, hibát tapasztal, haladéktalanul jelenteni köteles bejelentenie az informatikának. Tilos a felhasználónak megkísérelnie a hiba elhárítását.

Az informatikus segítséget nyújt a felhasználóknak, valamint hibabejelentéseket és igényeket fogad számítástechnikai, telekommunikációs és adatátviteli eszközökre, rendszerekre és jogosultságokra vonatkozóan.

A hibák és rendellenességek bejelentését az informatikus felé elektronikus úton a "Mantis" Informatikai Hibabejelentő Rendszeren keresztül kell megtenni, elérhetősége:

http://mantis/helpdesk

4.13 Szellemi tulajdonjogok védelme

A Hivatal informatikai rendszerében csak jogtiszta (tisztázott eredetű, legálisan használható) programok alkalmazhatók:

- a Hivatal számítástechnikai rendszerein nem kerülhetnek tárolásra olyan anyagok, amelyek jogvédelem alá esnek és a Hivatal nem rendelkezik a felhasználási jogokkal (filmek, zenék, könyvek stb.),
- csak akkor szabad részben, vagy teljesen könyveket, cikkeket, beszámolókat vagy más dokumentumokat másolni, ha a szerzői jogra vonatkozó előírások azt megengedik.

A szerzői és szomszédos jogok tiszteletben tartása, továbbá az információbiztonsági szabályok betartása miatt a munkavállalóknak tilos munkaállomásukra bárminemű szoftver telepítése, illetve bármilyen, nem a Hivatal tulajdonát képező állomány felmásolása (képek, zenék, filmek stb.).

4.14 Alkalmazottak által végzett fejlesztések

A Hivatal alkalmazottai által, a Hivatal eszközein, munkaköri feladatból eredően elvégzett és rendszerbe állított szoftverfejlesztések, Excel makrók, programok, batch fájlok stb. állományok a Hivatal tulajdonát képezik, ezekért a munkatársak sem munkaviszonyuk alatt, sem kilépésükkor további javadalmazást nem kapnak. Kötelesek viszont a nem kizárólag saját használatra készített fejlesztéseket dokumentálni és azok mentéséről gondoskodni, szükség esetén az informatikus bevonásával.

4.15 Az információ-feldolgozó eszközökkel való visszaélés megelőzése

A Hivatal információ-feldolgozó eszközeit kizárólag az Hivatal működésével kapcsolatos célokra szabad felhasználni, ettől eltérő, magáncélú alkalmazás az eszközök elfogadható használata értelmében csak korlátozottan engedélyezett. A berendezések jogosulatlan használata fegyelmi vétség, amely munkajogi következményeket von maga után.

A munkatársak kizárólag azokhoz a rendszerekhez férhetnek hozzá, amelyre kifejezett felhatalmazást kaptak és feladatkörükhöz tartozik. Minden más hozzáférés kezdeményezése tilos!

Tilos nem engedélyezett tartalmakat tárolni a Hivatal adathordozóin. Be kell tartani az internet és a levelező rendszerre vonatkozó előírásokat.

Legyenek tudatában a munkatársak, hogy a Hivatal informatikai rendszerein naplózás folyik, amely rögzítheti a felhasználói tevékenységeket, meglátogatott weblapokat és egyéb személyes aktivitást.

4.16 Mentések

Rendszeres mentés készül a közös használatú könyvtárakról és a felhasználók „home" könyvtárairól, de nem készül mentés az asztali számítógépek és laptopok merevlemezéről.

Az asztali munkaállomások merevlemeze nem kerül mentésre, ezért azokon az adattárolás nem engedélyezett. Az eszköz sérülése esetén az adatok helyreállítására nincsen mód. Az adatvesztésből eredő következményekért a felhasználó a felelős.

Laptopokon adatokat a felhasználó csak saját felelősségére tárolhat, mentés a felhasználó felelőssége, az eszköz sérülése esetén az adatok helyreállítására nincsen mód.

A nem hálózaton keletkezett és tárolt információkról biztonsági- vagy munkamásolatok készítése, a másolatok megfelelő és biztonságos tárolása az adatot előállító felhasználó feladata és kötelessége.

4.17 Munkaviszony megszűnése

A kilépő dolgozó köteles leadni az általa használt, a Hivatal tulajdonát képező számítástechnikai eszközöket, kulcsokat, belépőkártyákat.

A felhasználó, vagy a munkaköri vezetője a felhasználó munkaviszonyának megszűnése előtt köteles kiértesíteni a vele kapcsolatban álló belső és külső partnereket a munkaviszony megszűnéséről és a munkakört átvevő személyéről.

A kilépő elektronikus dokumentumait rendezett állapotban köteles átadni a munkakörét átvevő személynek vagy munkahelyi vezetőjének.

A kilépő dolgozó személyes mappáinak tartalma, továbbá elektronikus postafiókjának tartalma átadásra kerül a munkakörét átvevő munkatársának vagy felettesének.

Az informatikai hálózathoz, továbbá az elektronikus információs rendszerekhez való jogosultságai törlésre kerülnek.

A munkatársak titoktartási kötelezettsége nem szűnik meg a munkaviszony megszűnésével, érvényes az alkalmazás megszűnése utáni is!

A jogszabályok értelmében a Hivatal megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz. A dolgozó munkaviszonyának megszűnése esetén, a kilépése napjával postafiókja az arra kijelölt személyhez átirányításra kerül. A beérkező levelekre automatikus válaszlevél generálódik, mely értesíti a partnert postafiók megszűnéséről és a munkakört átvevő munkatárs elérhetőségéről. A postafiók tartalmát az informatikus archiválja. A kilépő dolgozó vezetője, vagy az általa megjelölt munkatárs olvasási jogot kap a kilépett postafiókjához, hogy a folyamatban lévő ügyeket szükség esetén vissza tudja keresni.

DUNAKESZI VÁROS JEGYZŐJE

Jóváhagyta:

Mellékletek

1. sz melléklet: Informatikai Felhasználói Nyilatkozat

MUNKAVÁLLALÓI FELHASZNÁLÓI NYILATKOZAT

Dunakeszi Polgármesteri Hivatal adatvédelmi és informatikai biztonsági szabályainak betartása valamennyi munkatársa számára kötelező.

A Munkavállaló Adatvédelmi Szabályzat és a Felhasználói Biztonsági Szabályzat kiemelt fontosságú pontjai:

1) A Hivatal által működtetett elektronikus információs rendszerek, az azokban tárolt adatok a Hivatal tulajdonát képezik, beleértve az elektronikus levelező rendszert, abban a személyekhez rendelt e-mail címeket, továbbá az internet kapcsolatot is. Az elektronikus levelezés (e-mail) és az internet a Hivatali tevékenységi kör keretein belül és szakmai indokkal vehető igénybe. A magánjellegű internet és e-mail használat, továbbá magáncélú személyes adatok tárolása nem engedélyezett.

2) A Hivatal célja, hogy minden esetben eleget tegyen a rá vonatkozó törvényi, jogi szabályozási és szerződéses kötelezettségeinek. A szellemi tulajdon védelme érdekében a felhasználóknak tilos a Hivatal informatika eszközein alkalmazások telepítése, jogvédett állományok tárolása vagy másolása. Tilos a Hivatal eszközein, adathordozóin magáncélú adatok tárolása. Alkalmazásokat csak az informatikus munkatársak telepíthetnek.

3) A Hivatal az adatok védelme és az informatikai rendszer biztonságos működésének biztosítása érdekében az internet és e-mail használatot, továbbá a felhasználói tevékenységeket naplózó és monitorozó eszközöket rendszeresít és használ, esetenként az elektronikus megfigyelést a kijelölt felelősök által végzett manuális vizsgálatokkal egészíti ki.

4) A Hivatal rendszeresen felülvizsgálja az asztali munkaállomások és a személyi használatra kiadott laptopok adattartalmát és biztonsági beállításait. A nem hivatalos célú adatok törlésre kerülnek.

5) Az informatikai rendszer felhasználójának felelősségi körébe tartozik a munkája során megismert, felhasznált és létrehozott számítógépes és egyéb adatok védelme, a használatában lévő berendezések és alkalmazói szoftverek üzemszerű használata.

6) Hivatali elektronikus információs rendszeréhez bármilyen külső eszközt, mint pendrive, memóriakártya, fényképezőgép, mobiltelefon stb. csatlakoztatni csak külön engedéllyel szabad.

7) A felhasználói azonosítójáért minden felhasználó személyesen felelős. A felhasználóknak a jelszavuk illetéktelenek általi megismerését minden eszközzel el kell kerülni.

8) A Hivatal munkatársaira vonatkozó előírásokat – különös tekintettel az adat- és információvédelemre – az internet használata közben is be kell tartani! Az Hivatal nyilvános megjelenésével kapcsolatos munkaköri feladatot ellátó munkatársak kivételével tilos a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való közzététele.

9) Az internetről adatállományt és egyéb alkalmazható állományt letölteni és felhasználni kizárólag Hivatali szakmai tevékenységi kör keretén belül engedélyezett.

10) A munkavállaló a munkaviszonyának megszűnésével elektronikusan kezelt állományait köteles rendezett formában átadni a munkakörét átvevő munkatárs számára.

11) A munkavállaló elektronikus levelezése („személyes postafiókja") átadásra kerül a munkakört átvevő munkatárs számára. A postafiók a kilépést követően még fogadja a beérkező üzeneteket, melyek tartalma átadásra kerül a munkakört átvevő munkatárs számára.

12) A Hivatali adatok és információk interneten át történő megadása kizárólag szakmai feladat ellátása érdekében történhet. Minden esetben meg kell győződni arról, hogy az átvevő jogosult az adatok megismerésére, valamint a szolgáltatott adatok jogszerű kezelése és védelme biztosított.

13) Az adatvédelmi és információbiztonsági szabályok megsértőivel szemben a Hivatal munkajogi és büntetőjogi felelősségre vonást kezdeményezhet.

Tudomásul veszem a Hivatalnak az elektronikus információs rendszer használatához kapcsolódó biztonsági szabályait. A Munkavállalói Adatvédelmi Szabályzatot és a Felhasználói Biztonsági Szabályzatot megismertem, a bennük foglalt kötelezettségeket megismertem és azokat saját felelősségemre betartom.

Dunakeszi, 201__ . ..... hó ..... nap

.....

felhasználó neve aláírása

(A Nyilatkozat két példányban készül. Az 1. példány a felhasználóé, a 2. példány a Munkaköri Leírás mellékletét képezi.)

Dunakeszi Polgármesteri Hivatal

Informatikai Fizikai Védelmi Szabályzat

2019.

A DOKUMENTUM MÓDOSÍTÁSAINAK JEGYZÉKE

A dokumentum következő felülvizsgálatát 2022. 06. 30-ig el kell végezni.

V1.0	.	Kiadásra javasolt verzió	Nádor Rendszerház Kft.
Verzió	**Dátum**	**Leírás**	**Hatályba helyező utasítás száma**

TARTALOM

1 ÁLTALÁNOS RENDELKEZÉSEK

1.1 A FIZIKAI VÉDELMI SZABÁLYZAT CÉLJA ÉS HATÁLYA

Az Informatikai Fizikai Védelmi Szabályzat célja, hogy meghatározza **a Dunakeszi Polgármesteri Hivatal** (továbbiakban: **Hivatal**) az elektronikus információs rendszerek szempontjából érintett létesítményekre vagy helyiségekre érvényes fizikai védelmi szabályokat, és az azokhoz kapcsolódó ellenőrzések megvalósítását.

Személyi hatálya vonatkozik valamennyi, a Hivatal létesítményeiben munkát végző személyekre, továbbá oda bármilyen célból belépő személyekre (látogatók, ügyfelek).

1.1.1 A szabályzat karbantartása

A Fizikai Védelmi szabályzatot három évente felül kell vizsgálni és frissíteni kell. Felül kell vizsgálni abban az estetben is, ha az informatikai környezetben, vagy a vonatkozó jogszabályokban jelentős változás áll be.

2 AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER ELEMEINEK ELHELYEZÉSE

Az elektronikus információs rendszer elemeit úgy kell elhelyezni, hogy a legkisebb mértékre csökkenjen a várható fizikai és környezeti veszélyekből adódó lehetséges kár és a jogosulatlan hozzáférés lehetősége.

2.1 AZ IRODAI TERÜLETEK VÉDELME

A Hivatal nem ügyfélszolgálatra szolgáló helyiségei idegenek által csak korlátozásokkal látogathatók. A munkatársakhoz érkező vendégeket belső munkatársnak kell kísérnie, illetve külsős munkavégzők csak felügyelettel végezhetik tevékenységüket.

Az őrszolgálattal nem ellátott épületekben az épületben dolgozó hivatali egység vezetője felelős a belépések felügyeletéért.

2.2 ÜGYFELEK ÁLTAL LÁTOGATHATÓ TERÜLETEK

Ügyfelek által látogatható hivatali épületek:

- Dunakeszi Polgármesteri Hivatal - 2120 Dunakeszi, Fő út 25.

Az épületben kijelölésre kerültek a nyilvánosan látogatható területek, továbbá a belépésre kijelölt időszakok.

2.2.1 Dunakeszi Polgármesteri Hivatal - 2120 Dunakeszi, Fő út 25.

Az épületben 24 órás őrszolgálat működik.

Hivatali időben a munkatársak belépését az őrszolgálat ellenőrzi. Technikai beléptetés az elektronikus beléptető rendszerrel kapuval történik, melyhez minden munkatárs proxy kártyával rendelkezik.

A Hivatal területén ügyfélfogadási időben az ügyfelek által szabadon látogatható terület a személyes ügyfélszolgálat területe. A Hivatal további területei elektronikus beléptető rendszerrel nyitható ajtókkal védettek.

2.2.1.1 Ügyfelek belépése

Személyes ügyfélszolgálat: ügyfélfogadási időben az ügyfelek által szabadon látogatható terület.
Ügyfélfogadási idő:

Hétfő	08.00-17.30
Kedd	08.00-16.00
Szerda	08.00-16.00
Csütörtök	08.00-16.00
Péntek	08.00-12.00

A Hivatal elzárt területei:

Az üvegajtókon túli területre, illetve az irodákban látogatók (ügyfélek) csak a fogadó személy (ügyintéző) kíséretében léphetnek be.

3 BELÉPÉSI JOGOSULTSÁGOK NYILVÁNTARTÁSA

3.1.1 Belépőkártyák kezelése

A Hivatal munkatársai számára belépő kártyát biztosít, amellyel a Hivatal korlátozott területeire jogosultak belépni.

Belépőkártyával láthatók el azok a személyek is, akik nem a Hivatal személyi állományába tartoznak, de rendszeres szükséges belépésük a Hivatal épületeibe.

A portaszolgálaton további belépőkártyákat kell elhelyezni, a rendszeres, hivatalos látogatók részére.

3.1.1.1 Belépőkártyák kezelése és nyilvántartása

A belépőkártyákat a Személyügyi Iroda kezeli és tartja nyilván.
Belépőkártyát kell kiadni új belépő kinevezésekor, továbbá belépőkártya elvesztése és sérülése esetén. Belépőkártya elvesztését a kártyabirtokosnak haladéktalanul jelentenie kell a Személyügyi Irodának. Az elveszett belépőkártyát azonnal le kell tiltani az elektronikus beléptető rendszerben.
A sérült belépőkártyát vissza kell vonni.
A kilépő munkatársak belépőkártyáját az utolsó munkában töltött napon vissza kell vonni. A kilépő által le nem adott kártyát le kell tiltani.
A belépőkártyák nyilvántartását évente ellenőrizni kell. Meg kell vizsgálni, hogy a kiadott belépőkártyák arra jogosult személyekhez vannak-e rendelve.

Biztosítani kell, hogy a nyilvántartás alapján visszamenőlegesen minden időpontra meg lehessen határozni a belépésre jogosultak körét. Az elektronikus és papír alapú belépési naplókat hat hónapig meg kell őrizni.

Az elektronikus beléptető rendszer működtetése során keletkezett adatokat (pl. a belépés időpontja)

a) rendszeres belépés esetén a belépésre való jogosultság megszűnésekor, de legkésőbb az adat keletkezésétől számított hat hónap elteltével,

b) alkalmi belépés esetén a távozástól számított huszonnégy óra elteltével

meg kell semmisíteni.

A belépési adatbázis adatai csak bűncselekmény vagy szabálysértés gyanújának észlelése esetén, továbbá megkeresés alapján a nyomozó hatóságnak, valamint a szabálysértés miatt eljáró hatóságnak és a szabálysértés miatt előkészítő eljárást folytató szervnek adhatók át.

3.2 KISZOLGÁLÓ INFRASTRUKTÚRA VÉDELME

Az informatikai erőforrásokat koncentráltan tartalmazó helyiségek (pl. központi gépterem, informatikai helyiségek, hálózati rendezők) számára kiemelt védelmet kell biztosítani.

3.2.1 Központi géptermek védelme

A Hivatal kiszolgáló számítógépeinek helyet adó helyiségek infrastruktúrája legyen alkalmas a folyamatos üzemű működésre és a legyen ellenálló a leggyakoribb környezeti fenyegetésekkel szemben.

3.2.1.1 Fizikai hozzáférés, belépések

A központi géptermeket a jogosulatlan hozzáféréstől mechanikai és elektronikus eszközökkel védeni kell. Az esetleges jogosulatlan belépést, betörést riasztórendszer jelezze a szerződött vagyonvédelmi társaság távfelügyeletén.

A géptermi beléptetést elektronikus beléptető rendszerrel kell kontrollálni, mely képes a hozzáférések naplózására is. A beléptető rendszer legyen alkalmas a belépők egyedi azonosítására, erre szolgáló azonosító eszközzel.
A fizikai hozzáférésekről készült naplókat rendszeresen át kell vizsgálni. A fizikai hozzáférésekről készült naplókat soron kívül át kell vizsgálni, ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak.

A létesítményekbe belépésre jogosultak listáját napra készen kell tartani. Rendszeresen felül kell vizsgálni a belépésre jogosult személyek listáját, s el kell távolítani a listáról azokat, akik a belépésre már nem jogosultak.

3.2.1.2 Áramellátó berendezések és kábelezés

Az elektronikus információs rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben védetten kell kiépíteni.

Az elsődleges áramforrás (hálózati áramellátás) kiesése esetére, továbbá a az elektromos hálózat zavarainak kiszűrése érdekében szünetmentes áramellátást kell biztosítani a kiszolgálók és az adatátviteli eszközök számára. A hosszabb áramszünetek áthidalását generátoros áramellátással kell biztosítani, melyre az átkapcsolás automatikusan történjen.

3.2.1.3 Vészkikapcsolás

Lehetőséget kell biztosítani kell gépterem vagy egyes rendszerelemek áramellátásának kikapcsolására vészhelyzetben.

A vészkikapcsoló berendezés a beosztott személyzet számára legyen biztonságosan és könnyen megközelíthető, de elhelyezése akadályozza meg a jogosulatlan vészkikapcsolást.

3.2.1.4 Tűzvédelem

A központi gépteremben független áramellátással támogatott tűzjelző berendezést kell alkalmazni, amely tűz esetén automatikusan működésbe lép, képes riasztást küldeni az épületfelügyeletnek, illetve a kijelölt informatikai ügyeleteseknek.

Az érintett helyiségekben, illetve azok bejáratánál elektromos tüzek oltására alkalmas kézi tűzoltó berendezést is el kell helyezni, melyet a tűzvédelmi szabályok szerint rendszeresen ellenőriztetni kell.

3.2.1.5 Hőmérséklet és páratartalom ellenőrzés

A központi gépteremben az erőforrások biztonságos működéséhez szükséges szinten kell tartani a hőmérsékletet és páratartalmat. Az ehhez szükséges klimatizálást olyan mértékű redundanciával kell kiépíteni, hogy egy klímaberendezés kiesése esetén a rendszer többi eleme legyen képes a működési hőmérséklet biztosítására.

Beállítandó paraméterek:

- A gépterem hőmérséklete: 16-28°C
- A gépterem páratartalma: 30-55 %

A hőmérséklet és páratartalom értékeket telemetriai eszközökkel ellenőrizni kell, eltérés esetén a rendszer küldjön riasztást e-mailben vagy SMS-ben az üzemeltetés részére.

3.2.2 Informatikai kiszolgáló helyiségek védelme

Informatikai kiszolgáló helyiségek fogalma alatt a Hivatal épületeiben elhelyezett, az épület informatikai ellátásában kulcsszerepet betöltő helyiségeket értjük. Ezek a helyiségek tartalmazhatnak tartalék vagy mentési kiszolgálókat, adatátviteli hálózati elemeket és egyéb, az elektronikus információs rendszerek működésben fontos eszközöket.

A Hivatal összeállítja, jóváhagyja, és kezeli ezekbe a helyiségekbe belépésre jogosultak listáját. helyiségekbe belépni, ott tartózkodni vagy munkát végezni csak az oda beosztott személyek felügyelete

mellett szabad. A helyiségek kulcsai, belépésre jogosító technikai eszközei (belépőkártyái) csak a belépésre jogosultak számára adhatók ki.

Az informatikai kiszolgáló helyiségekben lehetőség szerint ki kell építeni tűz és füstérzékelő berendezést, mely az épületet felügyelő biztonsági szolgálathoz közvetlenül is küld riasztást.

A helyiségben elhelyezett eszközöktől függően, biztosítani kell a megfelelő szellőzést vagy a klimatizálást.

3.2.3 Hálózati eszközök és rendezők védelme

A hivatali épületek számítástechnikai adatátviteli hálózatát, annak eszközeit az illetéktelen beavatkozástól meg kell védeni. A számítástechnikai rendező helyiségeket és rendező szekrényeket zárva kell tartani.

Az adatátviteli hálózat aktív eszközeit lehetőség szerint szünetmentes áramforrással is el kell látni.

3.2.4 Információs rendszerelemek be- és kiszállítása

Az információs rendszerelemek mozgatását, a Hivatal területére történő beszállítását vagy onnan történő kiszállítását minden esetben az informatikus munkatársaknak kell felügyelniük és a mozgatásokról nyilvántartást kell vezetniük.

Mindenki más számra tilos az informatikai eszközök szállítása vagy áthelyezése.

3.2.5 Karbantartók

Az elektronikus információs rendszerek hardver és szoftver elemeinek karbantartása során:

- nyilvántartást kell vezetni a karbantartó szervezetekről vagy személyekről;
- meg kell követelni a hozzáférési jogosultság igazolását az elektronikus információs rendszeren karbantartást végzőktől;
- a karbantartó személyeket megfelelő hozzáférési jogosultságú, műszakilag képzett belső személyek felügyelete alatt kell tartani az elektronikus információs rendszeren végzett karbantartási és diagnosztikai tevékenységük során.

A karbantartási és diagnosztikai tevékenységek megkezdése előtt az elektronikus információs rendszer minden fellelhető információtároló elemét törölni kell, a nem törölhető adathordozót el kell távolítani vagy fizikailag le kell választani a rendszertől. Ilyen lehetőség hiányában alternatív biztonsági védelmet kell kialakítani a karbantartás idejére.

3.2.6 Kimeneti információk védelme

A Hivatal területén az elektronikus információs rendszer kimeneti eszközeihez – nyomtatók, multifunkcionális nyomtatók, képernyők, fax berendezések stb. – való fizikai hozzáférést korlátozni kell annak érdekében, hogy jogosulatlan személyek ne férjenek azokhoz hozzá.

A kimeneti eszközöket – különös tekintettel a nyomtatókra – a látogatói forgalomtól, egyéb munkatevékenységtől elkülönített helyiségben kell elhelyezni.
Biztosítani kell, hogy a látogatók által hozzáférhető területeken elhelyezett nyomtatók esetén a nyomatokhoz vagy egyéb kimenetekhez csak az arra jogosult személy férhessen hozzá (pl. biztonsági kód alkalmazásával).

Dunakeszi Polgármesteri Hivatal

Hozzáférés Ellenőrzési, Azonosítási és Hitelesítési Szabályzat

Készítette:

Vádor RENDSZERHÁZ

Dunakeszi, 2019.

A DOKUMENTUM MÓDOSÍTÁSAINAK JEGYZÉKE

A dokumentum következő felülvizsgálatát 2020.06.30-ig el kell végezni.

V1.1	2019.03.05	Véglegesítés	
V1.0		Első verzió	Nádor Rendszerház Kft.
Verzió	**Dátum**	**Leírás**	**Hatályba helyező utasítás száma**

TARTALOM

1 ÁLTALÁNOS RENDELKEZÉSEK

1.1 A SZABÁLYZAT CÉLJA ÉS HATÁLYA

A Hozzáférés Ellenőrzési, Azonosítási és Hitelesítési Szabályzatának célja, hogy a **Dunakeszi Polgármesteri Hivatal** (továbbiakban: Hivatal) elektronikus információs rendszereihez rendszerek hozzáférés ellenőrzéssel, azonosítással és hitelesítéssel kapcsolatos feladatokat, felelősségeket és hatásköröket.

1.1.1 A szabályzat karbantartása

Az Azonosítási és Hitelesítési Szabályzatot évente felül kell vizsgálni és frissíteni kell. Felül kell vizsgálni abban az estetben is, ha az informatikai környezetben, vagy a vonatkozó jogszabályokban jelentős változás áll be.

1.2 A SZABÁLYZAT HATÁLYA

A szabályzat tárgyi hatálya kiterjed minden informatikai rendszerre, személyi hatálya minden felhasználóra és üzemeltetőre, a karbantartási tevékenységben résztvevő külsős szerződött partner munkatársaira, akik a karbantartási (tervezés, végrehajtás, ellenőrzés, nyomon követés stb.) tevékenységben részt vesznek.

2 AZ ELJÁRÁSREND LEÍRÁSA

A Hivatal folyamataiban nélkülözhetetlen szerepet játszanak az elektronikus információs rendszerek és az ezeken kezelt adatok. Az ezekhez történő hozzáférés csak szigorú azonosítási és hitelesítési eljárás után lehetséges, amely biztosítja, hogy a természetes személy és elektronikus azonosítója minden tranzakcióban megbízhatóan összerendelhető, így egyrészt korlátozhatóak a hozzáférések (csak a munkavégzéshez szükséges jogosultságok kerülnek kiosztásra – bizalmasság, sértetlenség, rendelkezésre állás biztosítása érdekében), másrészt utólagosan nyomon követhetők és személyhez rendelhetőek (letagadhatatlanság) a végzett tevékenységek, adatkezelések.

2.1 ÁLTALÁNOS HOZZÁFÉRÉSI SZABÁLYOK

A Hivatal elektronikus információs rendszereihez történő jogosulatlan hozzáférések és a véletlen módosítások megakadályozása érdekében minden informatikai berendezést, alkalmazási rendszert, szolgáltatást, kiszolgálókon tárolt információt megfelelő hozzáférési szabályok védenek. A védelem a felhasználók azonosításával és hitelesítésével – felhasználói név és jelszó megadásával – valósul meg.

Az ASP rendszer speciális, többfaktoros hitelesítési eljárásait a vonatkozó dokumentumok rögzítik.

A hozzáférési jogosultságok körét úgy kell kialakítani, hogy:

- a meghatározott jogosultsági körök alkalmazásával minimalizálható legyen a rosszindulatú vagy egyéb jogosulatlan hozzáférés;

- kizárólag a munkavégzés végrehajtásához szükséges jogosultsági körök legyenek meghatározva;
- az egyes területek kapcsán meghatározott jogosultsági körök összhangban legyenek az információk osztályozásával;
- legkisebb szükséges jogosultság beállításának elve: a felhasználók részére a informatikai eszközökhöz minden esetben azt a lehető legkisebb hozzáférést biztosító jogosultsági struktúrát kell kialakítani, amely a részére meghatározott tevékenységek elvégzéséhez minimálisan szükséges;
- felhasználók nem rendelkezhetnek a rendszergazdai jogosultsággal;
- a Hivatal informatikai rendszereiben bármilyen típusú rendszergazdai jogosultságot csak az kaphat, aki informatikai rendszeradminisztrációs tevékenységet végez, és ebben az esetben is alkalmazni kell a legkisebb szükséges jogosultság beállításának elvét;
- a hordozható számítógépek (laptop, tablet) felhasználói helyi rendszergazdai jogosultságot kapnak;
- a jogosultság legyen összhangban a feladat és felelősségi körök szétválasztásával;
- legyen lehetőség a jogosultságok számonkérésére, ellenőrzésére, visszavonására.

A személyügyi területnek és az adatgazdáknak évente gondoskodniuk kell annak ellenőrzéséről, hogy az alkalmazott és a rendszerben beállított hozzáférési jogosultságok összhangban vannak-e a munkaköri feladatok ellátásához szükséges jogosultságokkal.

2.2 Felhasználók azonosítása

A felhasználó azonosítónak meg kell felelni az egyediség kritériumának: különböző felhasználók számára egyazon azonosító nem adható ki, azonban egyazon fizikai személynek több azonosítója is lehet az adott hozzáféréstől függően.

A felhasználói azonosítók képzésére és új felhasználók rendszerbe történő felvitelére kizárólagosan az Informatika jogosult.

A felhasználók számára személyenként külön felhasználó azonosítókat (user ID) kell alkalmazni azért, hogy a felhasználói tevékenységek ellenőrizhetők legyenek. A hozzáférési igényt az elektronikus információs rendszerek adatgazdája hagyja jóvá.

A felhasználói jogosultság igénylés az IBSZ mellékletében közzétett igénylőlapok segítségével történik.

2.3 Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

A Hivatal informatikai rendszerében nem engedélyezettek az azonosítás és hitelesítés nélkül végzett tevékenységek.

2.4 Felhasználó fiókok kezelése

A felhasználói fiókok kezelése során a hozzáférések biztonságát az alábbi automatikus és manuális ellenőrzésekkel és beállításokkal kell támogatni:

- Ideiglenes fiókok eltávolítása: Meghatározott időtartam letelte után az elektronikus információs rendszer automatikusan eltávolítja vagy letiltja az ideiglenes vagy kényszerhelyzetben létrehozott felhasználói fiókokat vagy egyes kijelölt felhasználói fiók típusokat.
- Inaktív fiókok letiltása: Az elektronikus információs rendszer automatikusan letiltja az inaktív fiókokat három hónap letelte után.
- Automatikus naplózás: Az elektronikus információs rendszer automatikusan naplózza a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket, és értesíti ezekről a meghatározott személyeket vagy szerepköröket.
- Kiléptetés: Meghatározott időtartamú várható inaktivitás vagy egyéb előre meghatározott esetekben ki kell léptetni a felhasználót. A beállítandó maximális időtartam 15 perc.
- Szokatlan használat: figyelni kell az elektronikus információs rendszer fiókjait a szokatlan használat szempontjából, és jelenteni kell azt az alábbi személyeknek:
  - érintett szervezeti egység vezetője, aki a lehető legrövidebb időn belül megvizsgálja, hogy rendellenes tevékenységről van-e szó, és erről tájékoztatja a bejelentő rendszermérnököt.
- Letiltás: Azonnal le kell tiltani a kockázatot jelentő felhasználók fiókjait.

2.5 A HOZZÁFÉRÉS ELLENŐRZÉS SZABÁLYAI

A hozzáférés ellenőrzés általános szabályait az IBSZ 8. Hozzáférés ellenőrzés c. fejezete írja le.

2.6 INTERNET HOZZÁFÉRÉS ÉS TARTALOM SZŰRÉS

Az internet használatának szűrését az informatikai csoport áll valósítja meg a következők szerint:

- Kötelezően betartandó:
  - **Szűrt kategóriák (Filtered categories)** – Az ebbe a kategóriába eső weboldalakat elérhetetlenné kell tenni a felhasználók számára. Ebbe a kategóriába kell besorolni azon weboldalakat, amelyek sérthetik az érdekelt felek érdekeit vagy a törvényi előírásokat. (Pl.: rasszista, gyűlölködő, lázító, erőszakos stb.)
- Javasoltan betartandó:
  - **Sávszélesség igényes kategóriák (Bandwidth-consuming categories)** – Ebbe a kategóriába esnek azon weboldalak melyek jelentősen leterhelik a Hivatal sávszélességét és ezáltal kockázatot jelentenek (pl.: közösségi oldalak, online tárhelyek, online rádió / audió szolgáltatások stb.).
  - **Nyílt kategóriák (Open categories)** - Ebben a kategóriába tartoznak azon weboldalak, melyek az üzleti folyamatokhoz szükséges és nyíltak (pl.: keresők, mint a Google).

A részletes besorolási táblát lásd a 1. sz. mellékletben.

Az aktuálisan szűrt tartalmakra a rendszergazda tesz javaslatot és a jegyző jóváhagyása után állítják be azokat.

Az ASP rendszerhez csatlakozó munkaállomásokon és azok üzemeltetési környezetében csak fehérlistás internet elérés engedélyezhető. Az egyes munkaállomásokon beállítandó hozzáféréseket a munkahelyi vezető előzetes javaslata alapján a jegyző hagyja jóvá.

2.7 VEZETÉK NÉLKÜLI ÉS MOBIL ESZKÖZÖN KERESZTÜLI HOZZÁFÉRÉS

Az információs rendszerekhez a vezeték nélküli hozzáférés kizárólag szigorúan szabályozott biztonsági intézkedések mellett lehetséges. A vezeték nélküli hozzáféréssel kapcsolatosan lásd a Rendszer és kommunikáció védelmi szabályzatot.

2.8 RENDSZERADMINISZTRÁTOROK TEVÉKENYSÉGE

A rendszeradminisztrátor feladata és felelőssége:

a. rendszeradminisztrációs (üzemeltetési, adminisztrátori) tevékenységek ellátása:
   - a távoli eléréshez szükséges hardverberendezések működésének nyomon követése, hiba esetén annak kezelése, szükség szerint külső támogatás igénybevételével;
   - a távoli eléréshez szükséges szoftver elemek működésének nyomon követése, hiba esetén annak kezelése, szükség szerint külső támogatás igénybevételével;
   - felhasználói jogosultságok regisztrálása, dokumentálása, kezelése és karbantartása;
   - a bejelentkezési eljárások során alkalmazandó követelmények betartása, illetve betartatása;
   - a távoli hozzáféréssel kapcsolatos nyomonkövetési és ellenőrzési feladatok elvégzése;
   - a távoli munkavégzéshez kiadott jogosultságok felülvizsgálatának elindítása félévente.

Hatásköre:

- a felügyelete alá rendelt távoli munkavégzéshez szükséges informatikai rendszereken üzemeltetési műveletek végrehajtása;
- felügyelete alá rendelt távoli munkavégzéshez szükséges informatikai rendszereken tapasztalt szabálytalan műveletek haladéktalan jelzése az Önkormányzati Osztály vezetője felé;
- felügyelete alá rendelt távoli munkavégzéshez szükséges informatikai rendszerek tekintetében javaslattétel az üzemeltetési, biztonsági és egyéb informatikai kérdésekben. A javaslatokat az Önkormányzati Osztály vezetője felé teheti meg.

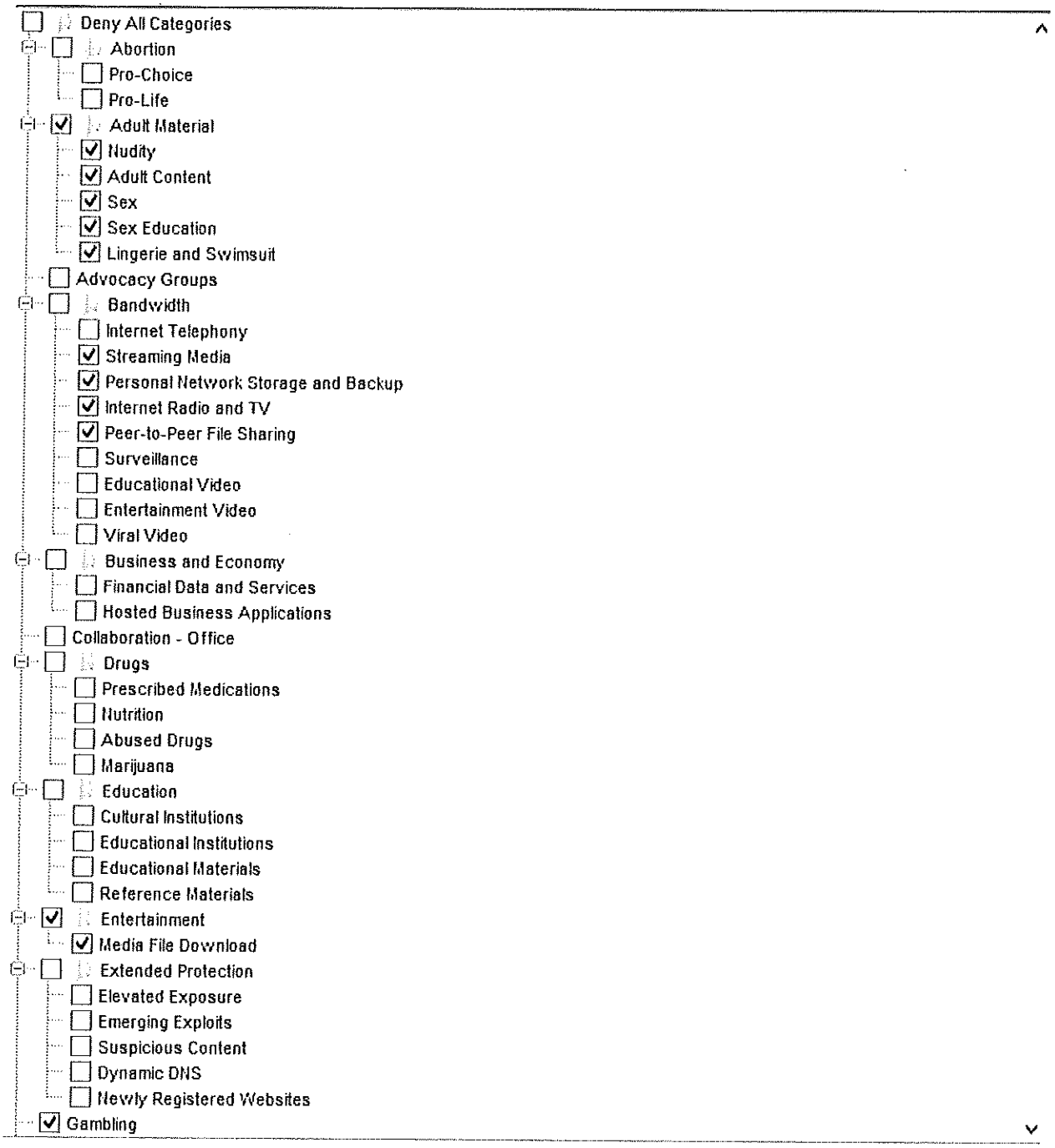
3 NYILVÁNOSAN ELÉRHETŐ TARTALOM

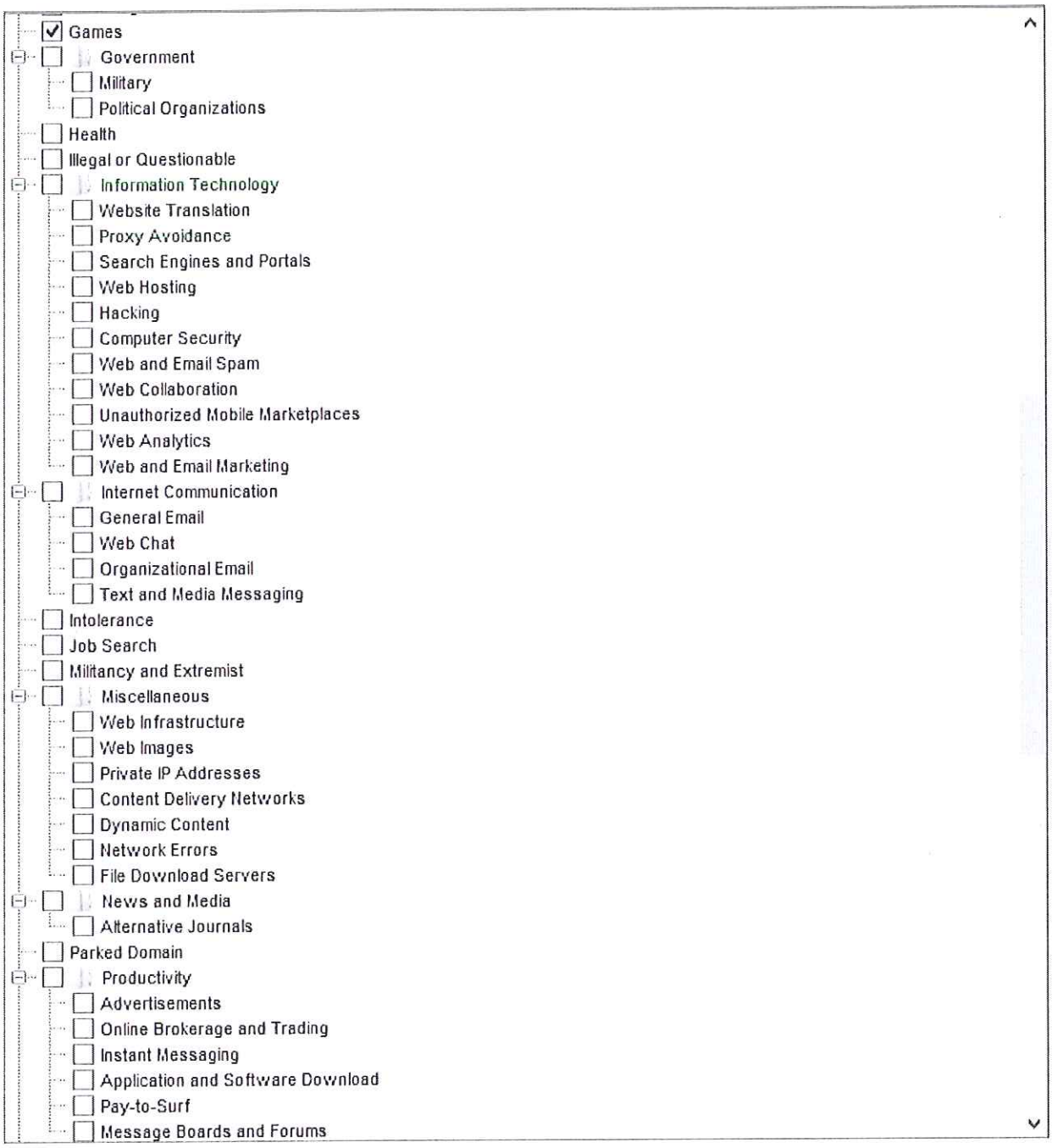
A Jegyző kijelöli azokat a személyeket, akik jogosultak a nyilvánosan hozzáférhető elektronikus információs rendszeren az érintett szervezettel kapcsolatos bármely információ közzétételére (Hivatali portál, Facebook stb.). A kijelölt személyeket képzésben kell részesíteni annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat.

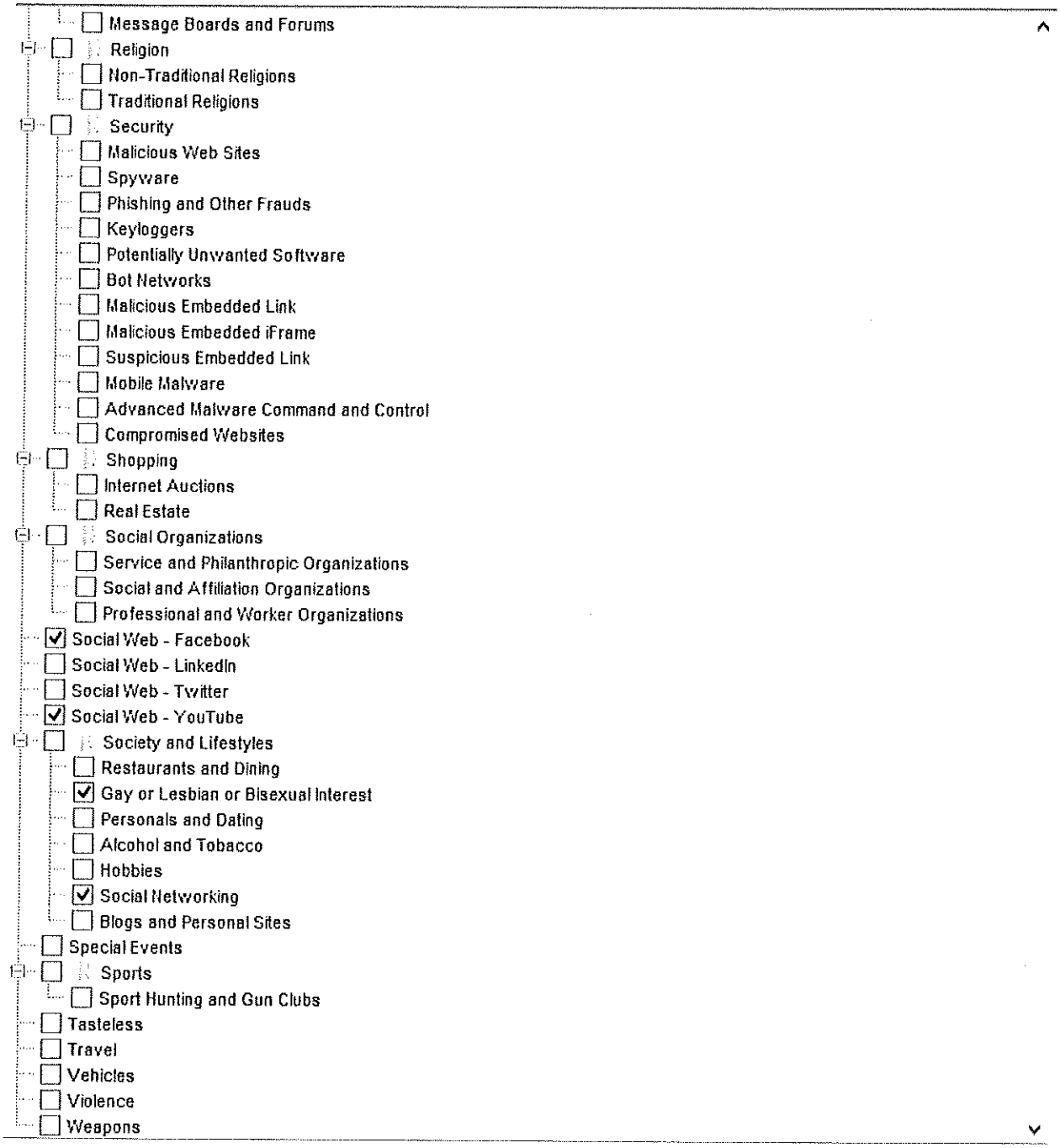
A kijelölt személyek közzététel előtt vizsgálják át a javasolt tartalmat.

Biztosítani kell, hogy éves gyakorisággal a nyilvánosan hozzáférhető elektronikus információs rendszertartalom felülvizsgálatra kerüljön a nem nyilvános információk tekintetében, és amennyiben ilyen információkat találtak, azokat haladéktalanul távolítsák el.

1. SZÁMÚ MELLÉKLET: INTERNET TARTALOMSZŰRÉSI KATEGÓRIÁK, ENGEDÉLYEK




Games
Government
Military
Political Organizations
Health
Illegal or Questionable
Information Technology
Website Translation
Proxy Avoidance
Search Engines and Portals
Web Hosting
Hacking
Computer Security
Web and Email Spam
Web Collaboration
Unauthorized Mobile Marketplaces
Web Analytics
Web and Email Marketing
Internet Communication
General Email
Web Chat
Organizational Email
Text and Media Messaging
Intolerance
Job Search
Militancy and Extremist
Miscellaneous
Web Infrastructure
Web Images
Private IP Addresses
Content Delivery Networks
Dynamic Content
Network Errors
File Download Servers
News and Media
Alternative Journals
Parked Domain
Productivity
Advertisements
Online Brokerage and Trading
Instant Messaging
Application and Software Download
Pay-to-Surf
Message Boards and Forums


Message Boards and Forums
Religion
Non-Traditional Religions
Traditional Religions
Security
Malicious Web Sites
Spyware
Phishing and Other Frauds
Keyloggers
Potentially Unwanted Software
Bot Networks
Malicious Embedded Link
Malicious Embedded iFrame
Suspicious Embedded Link
Mobile Malware
Advanced Malware Command and Control
Compromised Websites
Shopping
Internet Auctions
Real Estate
Social Organizations
Service and Philanthropic Organizations
Social and Affiliation Organizations
Professional and Worker Organizations
Social Web - Facebook
Social Web - LinkedIn
Social Web - Twitter
Social Web - YouTube
Society and Lifestyles
Restaurants and Dining
Gay or Lesbian or Bisexual Interest
Personals and Dating
Alcohol and Tobacco
Hobbies
Social Networking
Blogs and Personal Sites
Special Events
Sports
Sport Hunting and Gun Clubs
Tasteless
Travel
Vehicles
Violence
Weapons

A humán területhez kapcsolódó feladatok

a *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról* (a továbbiakban: Ibtv.) követelményeinek teljesítése kapcsán

Vonatkozó jogszabályok:

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról [a továbbiakban: Ibtv.];
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

Belépési procedúra Ibtv. követelményei:

- Új felhasználói információbiztonsági oktatása:
  - Ismertetés az alapvető biztonsági követelményekről
    - oktatási anyag: a *Hivatal informatikai működése*,
    - oktatási anyag: a *Felhasználó szabályzat*
  - Oktatás igazolása - aláírás a dolgozó részéről
  - *Felhasználói nyilatkozat*, aláírás a dolgozó részéről
- Munkatárs jogosultságainak meghatározása és beállítása (*Jogosultság Igénylő Lap vagy más megoldás)*
  - munkakörhöz szükséges informatikai jogosultságokat a felvételt kezdeményező felettes vezető határozza meg
  - a jogosultságok beállítását az Informatika, illetve az adott rendszerért felelős rendszergazda végzi
  - a beállított jogosultságokat az IT nyilvántartásba veszi (és évente a szakterülettel együtt felülvizsgálja)

Az új munkatársak felvétele során a felvételi eljárást a fentiek szerint ki kell egészíteni.

Szükséges dokumentumok:

- *A Hivatal informatikai működésének rövid ismertetője*: 1-2 oldal, rendszerek, szolgáltatások, hibabejelentések stb.
  - Készíti: informatikai terület
- *Felhasználói nyilatkozat*: a legfontosabb kötelezettségek összefoglalása (1 lap)
- *Informatikai Biztonsági Szabályzat (IBSz)*: készítése folyamatban
- *Felhasználói Szabályzat*: az IBSz kivonata, a felhasználók jogai és kötelezettségei

Személyi biztonság

3.3.2.4. Személyi biztonság
3.3.2.4.1. Az érintett szervezet:
3.3.2.4.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet;
3.3.2.4.1.2. az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja;
3.3.2.4.1.3. meghatározott gyakorisággal felülvizsgálja, és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységet a viselkedési szabályok betartását;
3.3.2.4.1.4. gondoskodik arról, hogy a 3.3.2.4.1.3. pont szerinti változás esetén a hozzáféréssel rendelkezők tekintetében a 3.3.2.4.1.2. pont szerinti eljárás megtörténjen;
3.3.2.4.1.5. meghatározza az érintett szervezeten kívüli irányban megvalósuló követelményeket.

A követelményeket az elkészülő IBSZ és a Felhasználói Szabályzat tartalmazza. A nyilatkozatot nem csak az új belépőkkel, hanem a Hivatal valamennyi munkatársával, utólagosan is alá kell íratni.

Kilépéskor előírt tevékenységek:

A munkatársak, hivatali dolgozók jogviszonyának megszűnésekor a Hivatal a *jogszabály szerint:*

- belső szabályozásban meghatározott időpontban megszünteti a hozzáférési jogosultságot az elektronikus információs rendszerhez; *(„sétálócédula" alapján, IT és a felelős rendszer(adat)gazdák igazolják)*
- megszünteti, vagy visszaveszi a személy egyéni hitelesítő eszközeit; *(IT igazolja)*
- tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről; *(a munkaviszony megszüntetéséről szóló, a kilépő által is aláírt irat része lehet)*
- visszaveszi az érintett szervezet elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt; *(IT, illetve az eszközért felelős terület igazolja)*
- megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz; *(munkahelyi vezető igénylése alapján IT beállítja, postafiók és személyes mappák átirányítása)*
- az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket *(felelős: munkahelyi vezető)*
- a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik *(felelős: munkahelyi vezető)*
- a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzi *(felelős: munkahelyi vezető, humán terület)*

A feladatok megvalósítása érdekében

- felül kell vizsgálni és szükség esetén módosítani a kilépőlap tartalmát, a kiléptetés csak a megfelelő pontok igazolása után történhet meg:
    - gondoskodni kell a jogosultságok megszüntetéséről
    - gondoskodni kell az eszközök visszavételéről
- folyamattá kell tenni és szükség szerint dokumentálni
    - a munkakör IT-hoz kapcsolódó feladatainak átadását
    - postafiók és személyes mappák átirányítását, az esetlegesen a munkaállomáson tárolt adatok lementését és átadását az illetékes szakterület részére

Fegyelmi intézkedések (IBSz tartalmazza)

Az Ibtv végrehajtási rendelete előírja a fegyelmi intézkedések meghozatalát információbiztonsági sértések esetén. Ez egyéb jogszabályokból is következik, de az Ibtv. megfelelés érdekében tételesen bekerült az erre vonatkozó hivatkozás az IBSz-be. Az új IBSz kiadása után <u>további teendő nincs</u>.

A törvényi követelmény:

> *3.1.6.7. Fegyelmi intézkedések*
> *3.1.6.7.1. Az érintett szervezet:*
> *3.1.6.7.1.1. belső eljárási rendje szerint fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben;*
> *3.1.6.7.1.2. ha az elektronikus információbiztonsági szabályokat nem az érintett szervezet személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti ezeket az eljárásokat.*

Képzési eljárásrend

A jogszabály előírja a *képzési eljárásrend* kialakítását:

> *3.1.7.2. Képzési eljárásrend*
> *3.1.7.2.1. Az érintett szervezet:*
> *3.1.7.2.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a képzési eljárásrendet, mely a képzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;*
> *3.1.7.2.1.2. a képzési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a képzési eljárásrendet.*

A képzési eljárásrend bekerülhet az IBSZ-be, vagy önálló utasításként is működhet. A képzéseket rendszeresen tervezni és dokumentálni kell.

Biztonság tudatosság képzés

A jogszabály által előírt feladatok:

3.1.7.3. Biztonság tudatosság képzés
3.1.7.3.1. Az érintett szervezet annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára:
3.1.7.3.1.1. az új felhasználók kezdeti képzésének részeként;
3.1.7.3.1.2. amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
3.1.7.3.1.3. az érintett szervezet által meghatározott gyakorisággal.

Biztonság tudatossági képzés megvalósítása: (évente, frissítő képzés, régi dolgozóknak)

- képzéseket meg kell szervezni,
- éves gyakorisággal el kell végezni,
- a képzés megtörténtét dokumentálni kell és az erről szóló dokumentumokat meg kell őrizni (jelenléti ív, e-learning igazolás stb.).

Dunakeszi Polgármesteri Hivatal

Informatikai Biztonsági Szabályzata

Készítette:

Nádor
RENDSZERHÁZ

Dunakeszi, 2019.

A DOKUMENTUM MÓDOSÍTÁSAINAK JEGYZÉKE

A dokumentum következő felülvizsgálatát 2020.06.30.-ig el kell végezni.

v1.1	2019.03.05	Véglegesített változat	
V1.0		Első verzió, Nádor Rendszerház	-
Verzió	**Dátum**	**Leírás**	**Hatályba helyező utasítás száma**

TARTALOM

1 Általános rendelkezések

1.1 Az Informatikai Biztonsági Szabályzat célja és területi érvényessége

Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa a **Dunakeszi Polgármesteri Hivatal** (továbbiakban: Hivatal) az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek eleget tegyen, biztosítsa a törvényi előírások érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az Informatikai Biztonsági Szabályzat célja továbbá:

- az Hivatal elektronikus információs rendszereinek és a rendszerekben tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása,
- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- a számítógépes feldolgozások és az eredményadatok további hasznosítása során az illetéktelen hozzáférésből és felhasználásból eredő hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az informatikai szoftver eszközökkel kapcsolatos jogbiztonság, jogtisztaság;
- a jogszabályi szinten rögzített adatvédelmi és adatbiztonsági elvárásoknak való megfelelés, különös tekintettel az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) és végrehajtási rendeleteinek előírásaira.

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

A jelen Informatikai Biztonsági Szabályzat az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

1.2 Az Informatikai Biztonsági Szabályzat hatálya

1.2.1 Személyi hatálya

Az IBSZ személyi hatálya az intézményben foglalkoztatott valamennyi közszolgálati, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottaira, munkavállalóira, megbízottjaira (a továbbiakban együtt: munkatársak) egyaránt kiterjed.

Az IBSZ személyi hatálya kiterjed továbbá minden személyre, aki a Hivatal informatikai vagy azzal összefüggő rendszerét, szolgáltatásait igénybe veszi, informatikai struktúráját és annak eszközeit üzemelteti vagy használja, függetlenül a Hivatalhoz kapcsolódó jogviszonyától.

1.2.2 Tárgyi hatálya

Az IBSZ tárgyi hatálya kiterjed

a) valamennyi (a Hivatal tulajdonában lévő, vagy általa bérelt) informatikai és telekommunikációs berendezésre, vagy a Hivatal használatában álló épületben található, leltári jelzéssel ellátott, továbbá a Hivatal megbízásából a Hivatal munkatársai számára harmadik személy által biztosított informatikai eszközre, beleértve a berendezések műszaki dokumentációját is,

b) a Hivatal eszközein működtetett rendszerprogramokra és a felhasználói programokra,

c) amennyiben a Hivatal működésére irányadó egyéb szabályzat eltérően nem rendelkezik

- az informatikai folyamatot leíró valamennyi dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési dokumentációk);
- az adathordozók tárolására és felhasználására, beleértve a feldolgozásra beérkezés és a felhasználókhoz történő eljuttatás folyamatait is, kivéve;
- az adatok felhasználására;
- a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától (bizonylatok, tablók, mágneses adathordozók, stb.) függetlenül
- minden olyan adatkezelésre és adatfeldolgozásra, amely az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (az Infotv.) szerinti személyes, különleges, közérdekű, vagy közérdekből nyilvános adatra vonatkozik, és az adatkezelés, illetve adatfeldolgozás teljesen vagy részben automatizált eszközzel történik.

1.3 Az IBSZ-hez kötődő egyéb szabályozások

Az IBSZ a jogszabályok előírásainak alkalmazásán alapul, és az információvédelemre vonatkozó jogszabályi szintű rendelkezésekkel együtt értelmezendő.

Az IBSZ-ben nem rendezett kérdésekben a fentiekben említett hatályos jogszabályok rendelkezéseit, továbbá a Hivatal egyéb belső szabályzataiban foglaltak az irányadók. Az IBSZ egyes előírásai fokozatosan kerülnek teljesítésre, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, és annak végrehajtási rendeletei alapján meghatározott ütemterv szerint. Az egyes feladatokról külön eljárásrendek készülnek.

1.4 Az Informatikai Biztonsági Szabályzat felülvizsgálata és karbantartása

Az Informatikai Biztonsági Szabályzatot a benne foglaltak pontosságának és naprakészségének fenntartása érdekében folyamatosan felül kell vizsgálni. A szabályzat felülvizsgálata három évenként esedékes, illetve felül kell vizsgálni abban az esetben is, ha az Ibtv-hez kapcsolódó cselekvési terv mérföldköveihez ilyen akció kapcsolódik.

Az alábbi esetekben a jegyző dönthet a felülvizsgálat elrendeléséről:

- ha az informatikai biztonságot illetve az Informatikai Biztonsági Szabályzat tartalmát érintő jelentős változás következett be,
- ha a jogszabályi környezetben jelentős változás következett be,
- új, lényeges kockázatok válnak ismertté
- rendkívüli esemény bekövetkezése esetében, függetlenül attól, hogy a rendkívüli esemény eredményezte vagy eredményezhette volna a Hivatal valamilyen eszközének/adatának elvesztését, megrongálódását, használhatatlanná válását vagy az információk nyilvánosságra kerülését.

A felülvizsgálatról a felülvizsgálatot végzőnek minden esetben feljegyzést kell készíteni, amelyben javaslatot kell tenni az esetleges módosításokra, vagy rögzíteni kell, hogy a szabályzat módosítása nem szükséges.

2 Szervezeti biztonság

2.1 Az informatikai biztonsággal összefüggő feladatok és felelősök

A Hivatal informatikai biztonságával összefüggő szerepkörök és feladatok kiosztása a Hivatal Szervezeti és Működési Szabályzata (SzMSz), illetve jelen szabályzat alapján kerültek meghatározásra.

Az informatikai biztonságért a Hivatal vezetője felel. A biztonság megteremtéséhez kapcsolódó feladatok azonban delegálhatók, ezért a szervezet valamennyi dolgozójának része van az informatikai biztonság megteremtésében és fenntartásában.

Az egyes szervezeti egységek a szakmai felügyeletük alá tartozó elektronikus információs rendszer adattulajdonosi, adatgazdai feladatait látják el.

Valamennyi munkatárs köteles munkakörén belül az általa hozzáférhető információ és információ feldolgozó eszköz védelmére és helyes kezelésére.

Az informatikai biztonsággal kapcsolatban a Hivatal valamennyi dolgozójára hárul felelősség, feladat.

2.1.1 Menedzsment felelősségek

Az elektronikus információs rendszerek védelmi feladatai

Az Ibtv. 11. § (1) bekezdése szerint, a Hivatal vezetőjének – a jegyzőnek – feladata és felelőssége gondoskodni az elektronikus információs rendszerek védelméről a következők szerint:

a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,

b) biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,

c) az elektronikus információs rendszer biztonsági osztálya és a szervezet biztonsági szintje alapján előírt követelményeknek megfelelően az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,

d) meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,

e) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,

f) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,

g) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,

h) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,

i) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,

j) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,

k) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,

l) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

2.1.2 Az elektronikus információs rendszer biztonságáért felelős személy

A Hivatal az Ibtv. 11. § c) szerint az elektronikus információs rendszer biztonságáért felelős személyt (IBF) nevez ki vagy bíz meg. Az IBF felel a Hivatalnál előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Feladatának ellátása során az Hivatal vezetőjének közvetlenül adhat tájékoztatást, jelentést.

Ebben a feladatkörben biztosítja az Ibtv. által előírt feladatok végrehajtását, különösen

- biztosítja a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való folyamatos összhangját,

- ellátja a szervezet elektronikus információs rendszereire vonatkozó szabályozások karbantartását, az információs rendszerek osztályba sorolásának időszakos felülvizsgálatát,
- véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,
- kapcsolatot tart a Nemzeti Elektronikus Információbiztonsági Hatósággal és a
- ellátja az előírt bejelentési kötelezettségeket,
- az elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerinti tájékoztatásokat elvégzi,
- biztosítja az Ibtv. hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenységek (fejlesztés, üzemeltetés, adatfeldolgozás stb.) esetén a törvényben meghatározott követelmények teljesülését külső felek (közreműködők) tevékenysége során.

A szervezetnél csak olyan személy végezheti az elektronikus információs rendszer biztonságáért felelős személy feladatait, aki büntetlen előéletű, rendelkezik a feladat ellátásához előírt felsőfokú végzettséggel és szakképzettséggel.

A vonatkozó szakképzettségi követelményeket és feltételeket az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet szerint kell biztosítani.

2.1.3 Informatikai munkatársak feladata és felelőssége

A Hivatal informatikai biztonságával kapcsolatos feladatokat az informatikus látja el a jegyző utasításai alapján.

A Hivatal jegyzője az informatikai biztonságot érintő fejlesztések, tervezések, beszerzések és bevezetések során kikéri az informatikus szakmai véleményét, döntése meghozatalában azt figyelembe veszi.

Az informatikus feladatai, jogai:

- rendszeresen ellenőrzik az IBSZ előírásainak betartását,
- ellenőrzik a védelmi eszközökkel való ellátottságot,
- előzetes bejelentési kötelezettség nélkül ellenőrzik az informatikai munkafolyamat bármely részét.
- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhetnek a jegyzőnél,
- javaslatot tesznek az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére,
- információvédelmi szempontból az informatikai beruházásokat véleményezik.

2.1.4 A Hivatal munkatársainak felelőssége

A munkába állás előtt a munkatársak számára információbiztonsági és adatvédelmi oktatást kell tartani, amelyben ismertetik

a) a munkakörre érvényes, informatikai biztonsággal kapcsolatos feladatokat és felelősségeket,

b) az adat és információvédelem fogalmát, továbbá azt, hogy ezek megsértése bűncselekmény,

c) a betartandó jogi és viselkedési normákat, különös tekintettel a szoftver jogok védelmére,

d) felelősséget az információ osztályozásáért és a szervezet vagyontárgyainak kezeléséért,

e) felelősséget, amely a Hivatal helyiségein kívülre és a rendes munkaórákon túlra terjed, pl. otthoni munka esetén,

f) biztonsági események jelentésének rendjét.

A kinevezésekbe/munkaszerződésekbe bele kell foglalni a titoktartási kötelezettség kiterjesztését, az alkalmazás megszűnése utáni időszakra is.

2.2 Az informatikai biztonsági felelősségek kiosztásával kapcsolatos feladatok

Az informatikai biztonsággal kapcsolatos felelősségek kiosztását a munkaköri leírásoknak kell tartalmazniuk. Az informatikai biztonság megtervezéséért, valamint a végrehajtásához szükséges intézkedések meghatározásáért a jegyző felelős, aki a döntések meghozatala előtt kikéri az elektronikus információs rendszerek biztonságáért felelős személy és az informatikus szakvéleményét is.

2.3 Feladat és felelősségi körök szétválasztása

Túl sok jogosultság és felelősségi kör egy személy kezében történő koncentrálódása lehetőséget ad a szervezet vagyontárgyainak nem jogosított vagy szándékolatlan módosítására vagy a velük való visszaélésre.

Az informatikai feldolgozás során a szerepköröket oly módon kell elhatárolni, hogy funkcionálisan szétváljon a kezdeményezés, a végrehajtás és a jóváhagyás, ne tudjon egy személy a vagyontárgyakhoz hozzáférni, azokat módosítani vagy használni, előzetes feljogosítás nélkül, vagy oly módon, hogy ne vegyék azt észre. (Az angol terminológia szerint Segregation of Duties, SOD)

Mivel a Hivatal informatikája kis létszámú szervezet, ezért nincsen lehetőség a felelősségek teljes körű szétválasztására, ezért abban az esetben, ha egy személy összeférhetetlen szerepköröket tölt be, kompenzációs kontrollokkal és gyakoribb felülvizsgálatokkal kell a kockázatokat csökkenteni.

A Hivatal törekszik az információ biztonság szempontjából összeférhetetlen feladatkörök szétválasztására, mely az alábbi módon valósul meg:

- Az informatikus csak az informatikai rendszerek biztonságos telepítési, üzemeltetési, és karbantartási feladatait végzik el. Alkalmazásfejlesztés a hivatalban nem történik. A fejlesztőktől kapott programverziókat és javításokat tesztrendszerben köteles ellenőrizni.

2.4 Az informatikai biztonság független felülvizsgálata

Annak érdekében, hogy a szervezet működése során érvényesüljenek az IBSZ-ben megfogalmazott követelmények, a hatékonyság és a gyakorlati megvalósíthatóság szavatolása céljából, szükség szerint időközönként független felülvizsgálatot kell végezni.

Ez a felülvizsgálat végezhető független szakértő vezetésével, vagy harmadik félként közreműködő, külső szervezet által, amely rendelkezik a megfelelő szakértelemmel, gyakorlattal és tapasztalattal.

3 Kockázatkezelés

A Hivatal feladata, hogy megteremtse az elektronikus információs rendszereinek biztonságát, azaz biztosítsa annak feltételeit, hogy az elektronikus információs rendszer védelme, az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

A védelem akkor arányos a kockázatokkal, ha az elektronikus információs rendszer védelmének költségei arányosak a fenyegetések által okozható károk értékével.

A károkozás jellege szerint lehet egyebek között:

a) társadalmi-politikai káros hatás, jogszabályok és egyéb szabályozások megsértése,

b) jogszabály által védett adatokkal történő visszaélés vagy azok sérülése,

c) bizalomvesztés hatóságokkal, felügyeleti szervekkel szemben,

d) különleges személyes adatok, banktitkok, üzleti titkok megsértése, szervezet, információk bizalmasságának sérülése

e) közvetlen anyagi károk (az infrastruktúrát, az elektronikus információs rendszert ért károk, és ezek rendelkezésre állásának elvesztése

f) közvetett anyagi károk (pl. helyreállítási költségek, elmaradt haszonnal arányos költségek, a környezet biztonságának veszélyeztetése, perköltségek)

A kockázatelemzések során fel kell mérni az adott vagyontárgyakat fenyegető veszélyforrásokat. Az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatokat fel kell tárni és értékelni.

Rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén kell meggyőződni arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak. A kockázatelemzés és kockázatkezelés kiegészítő szabályait eljárásrendben kell meghatározni, melyet legalább háromévente felül kell vizsgálni.

A kockázati felmérések alapján meg kell állapítani az elektronikus információs rendszerek biztonsági osztályát, azaz az elektronikus információs rendszerek védelmének elvárt erősségét.

Az Ibtv. előírja a szervezet biztonsági szintjét, amely a szervezet elérendő felkészültségi szintje az Információbiztonsági törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.

A kockázatkezelés során az eljárásrendben kell szabályozni a

- a lehetséges kockázatok felmérését;
- a kockázatok kezelésének felelősségét;
- a kockázatok kezelésének elvárt minőségét.

3.1 A kockázatfelmérés lépései

A teljes körű kockázatfelméréshez és az optimális kockázatkezeléshez az alábbi lépéseket kell végrehajtani:

- Informatikai vagyonleltár
- Fenyegetések meghatározása
- Sérülékenységek feltárása
    i. kontroll rendszer sérülékenységei
    ii. informatikai erőforrások sérülékenységei
- Káresemények meghatározása és azok ügymenetre gyakorolt hatásai
- Kockázatok meghatározása

3.2 Biztonsági kockázatok kezelése

A kockázatfelmérés eredményei alapján az azonosított kockázatok, illetve sérülékenységek vonatkozásában *Cselekvési terv* került kidolgozásra, amely mérföldkövei mentén kell a javító intézkedéseket végrehajtani.

Az Ibtv. előírja az állami és önkormányzati szervek számára, hogy végezzék el a szervezet biztonsági szintbe sorolását, továbbá az elektronikus információs rendszerek (alkalmazások) biztonsági osztályba sorolását, a bennük tárolt információ bizalmassága, sértetlensége és elérhetősége alapján. A megfelelő besorolásokat a Hivatal elvégezte és azokat a jegyző jóváhagyta, a kockázati értékelések eredménye jelen dokumentum mellékletében található.

A biztonsági osztályba sorolást az elektronikus információs rendszereket érintő változások után ismételten el kell végezni. Az osztályba sorolásnak kapcsolódnia kell az intézkedési terv mérföldköveihez.

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

A kockázatelemzés eredményét meg kell ismerniük az érintett munkatársaknak, de gondoskodni kell arról, hogy a kockázatelemzési eredmények a jogosulatlanok számára ne legyenek megismerhetők.

3.3 Biztonsági helyzet és eseményértékelés eljárási rendje

3.3.1 Jelentés az informatikai biztonsági eseményekről és gyengeségekről

Minden alkalmazottnak és a Hivatal számára szolgáltatást nyújtó szerződött felek munkatársainak ismerniük kell az információbiztonsági események kezelési eljárását, ezzel kapcsolatos saját kötelezettségeit.

3.3.2 Jelentés biztonsági eseményekről

Az információbiztonsági eseményeket haladéktalanul jelenteni kell az informatikusnak vagy a munkahelyi vezetőnek.

Biztonsági sértésre utalhat, melyet a felhasználóknak azonnal jelenteniük kell, ha

a) szolgáltatás, a berendezés vagy az eszközök elvesztése történik,

b) rendszer rendellenes működését észlelik,

c) a szabályzatoknak vagy irányelveknek való nem megfelelés válik nyilvánvalóvá,

d) észlelhető a fizikai biztonsági rendelkezések megsértése,

e) nem ellenőrzött rendszerbeli változásokat tapasztalnak,

f) a szoftver vagy hardver hibás működése lép fel,

g) hozzáférési sértések történnek.

A felhasználók tudatossági oktatásában ki kell térni arra, hogy hogyan kell válaszolniuk egy-egy felmerült incidensre, s milyen módon kell elősegíteniük a bizonyítékok gyűjtését.

3.3.3 Jelentés a biztonsági sérülékenységekről

Minden alkalmazott és a külső munkatárs kötelessége, hogy az informatikai rendszerekben és fizikai környezetben általa észlelt rendellenességet, gyaníthatóan gyenge pontot vagy sérülékenységet jelentse az informatikusnak. Ezek a gyenge pontok támadásra, visszaélésre adnak lehetőséget, a védelmi intézkedések meghozatala szükséges.

A munkatársak csak jelentsék az észlelt problémát. de ne kíséreljék meg ellenőrizni vagy javítani a feltárt problémát, mert esetlegesen azzal is kárt okozhatnak.

3.3.4 A biztonsági eseményekre és incidensekre adott válasz és fejlesztés

Az észlelt információbiztonsági eseményekre és gyengeségekre mielőbb válaszintézkedéseket kell hozni. Az események követését és a megoldási javaslatok, fejlesztések kidolgozását az informatikus végzi, beszámolnak a jegyzőnek az ezzel kapcsolatos tevékenységéről. Amennyiben az esemény komplexebb és speciális szakértelmet igényel, a megoldás kidolgozásához külső szakértőt kell igénybe venni.

Tipikusan információbiztonsági incidensek közé kell sorolni:

a) információrendszer-hibáit és a szolgáltatás megszakadását,

b) rosszindulatú kód, vírustámadás fellépését,

c) DoS támadást (szolgáltatás megtagadása),

d) a nem teljes vagy nem pontos működési adatokból eredő hibákat,

e) a bizalmasság és sértetlenség megsértését,

f) az információrendszerekkel való visszaélést.

Információbiztonsági incidensek esetén az elektronikus információs rendszerek biztonságáért felelős személy irányítja az intézkedéseket:

a) incidens megoldó team összehívása – az informatikus és az érintett szervezeti egység vezetők bevonása

b) incidens okának felderítése,

c) bizonyítékok gyűjtése,

d) incidens behatárolása és megszüntetése, helyreállítás,

e) előfordulás okának meghatározása és megszüntetése,

f) helyesbítő tevékenység az újbóli előfordulás megakadályozására,

g) tevékenységek dokumentálása,

h) adatközlés az érintettek felé,

i) jelentés a jegyző felé

3.3.5 Okulás a biztonsági eseményekből

A biztonsági események elemzése alkalmas arra, hogy a fennálló védelmi intézkedéseket hatékonyan felül lehessen vizsgálni és javítani.

A kiértékelés jelezheti az ellenőrzések és eszközök kiegészítésének szükségességét, hogy a jövőbeni előfordulások valószínűségét csökkenteni lehessen, megelőzve az anyagi és erkölcsi károkozást.

3.3.6 Bizonyítékok gyűjtése

Információbiztonsági események, visszaélések esetén, fegyelmi felelősségre vonás, polgári- vagy büntetőjogi eljárás kezdeményezése csak akkor lehetséges, amennyiben bizonyító erejű dokumentálás történik.

A dokumentálás akkor bizonyító erejű, amennyiben az hiteles és megváltoztathatatlan. Meg kell őrizni a vonatkozó naplóbejegyzéseket, adathordozókat és a papír alapú dokumentumokat is, gondoskodva a bizonyítékok megváltoztathatatlanságáról.

3.4 Vagyontárgyak kezelése

A Hivatal vagyontárgyainak megőrzése és védelme abban az esetben lehetséges, amennyiben a vagyontárgyak számba vétele megtörténik, s minden vagyontárgyhoz egyértelműen kijelölt felelős, „gazda" tartozik. A vagyontárgyakhoz azok jelentősége, üzleti értéke és biztonsági osztályozása alapján megfelelő védelmi eljárásokat kell rendelni.

3.4.1 Információs vagyonleltár

Annak érdekében, hogy a Hivatal összes vagyontárgya nyilvántartásra kerüljön, teljes körűen azonosítani kell valamennyi vagyontárgyat és azok jelentőségét (értékét). A vagyonleltár tartalmazza az összes releváns információt annak érdekében, hogy egy esetleges üzemzavar után a működést helyre lehessen állítani. Ennek megfelelően, egyebek mellett rögzíteni kell a vagyontárgy jellegét, helyét, jellemző paramétereit, üzleti funkcióját. A vagyonleltárnak nem kell megismételnie más, meglévő leltárak adatait, de azokat tartalmilag ki kell egészítenie.

A Hivatal vagyonának részét képezik egyebek mellett a következők:

a) információk – adatbázisok, szerződések és megállapodások, rendszerdokumentációk, üzemeltetési leírások, működésfolytonossági tervek, archivált információk,

b) hardver vagyontárgyak – számítógépek, adattárolók, kommunikációs- és mérőeszközök, adatátviteli hálózat, eltávolítható adathordozók stb.,

c) szoftver vagyontárgyak – vásárolt (dobozos) alkalmazás, egyedileg fejlesztett vagy fejlesztetett szoftver, rendszerszoftverek, fejlesztőeszközök és segédprogramok,

d) szolgáltatások – számítástechnikai és kommunikációs szolgáltatások, közmű jellegű szolgáltatások, mint a villamos energia, fűtés, világítás, légkondicionálás stb.,

e) munkatársak és ismereteik – az „emberi erőforrás", a szakemberek jártassága és tapasztalata,

f) egyéb nem kézzelfogható értékek, mint a Hivatal üzleti hírneve, arculata.

A vagyonleltár összeállítása előfeltétele a teljes körű kockázatkezelésnek.

3.4.2 Elektronikus információs rendszerelem leltár követelményei

Az elektronikus információs rendszer elemeiről készített leltárt meghatározott gyakorisággal felül kell vizsgálni és frissíteni.

Gondoskodni kell arról, hogy a leltár:

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

3.4.3 Eszköz-, és adatgazdák

Az információfeldolgozási eszközökhöz, mint vagyontárgyakhoz egyértelmű felelőst (eszköz vagy adatgazdát), kell rendelni. Felelőst kell rendelni:

a) az informatikai eszközökhöz, rendszerekhez és alapszoftverekhez,

b) szakmai és ügyviteli alkalmazásokhoz és azok adataihoz.

A vagyontárgyak gazdája felelős:

a) az információ-feldolgozó eszköz megfelelő kockázati osztályozásáért,

b) a vagyontárgyhoz kapcsolódó hozzáférések szabályozásáért,

c) a vagyontárgy osztályozás és hozzáférések éves átvizsgálásáért.

Az eszközök gazdája az eszköz napi üzemeltetésével kapcsolatos feladatokat delegálhatja, például az informatikai üzemeltetésre vagy az informatikai alkalmazásgazdákra, de a működtetési és hozzáférési feltételek meghatározásának felelőssége továbbra is az övé marad.

Az adatgazda annak a szervezeti egységnek a vezetője, ahová belső szabályozás az adat kezelését rendeli, illetve ahol az adat keletkezik. A szakmai alkalmazások tulajdonosa a szakterületi adatgazda, szakmailag felelős az adott számítógépes alkalmazás működtetéséért, törzsadatainak gondozásáért, az adatok karbantartásáért, a rendszer adatainak felhasználásáért, és a felmerülő igények alapján a rendszer szakmai továbbfejlesztéséért (általában az adott terület vezetője).

A központi informatika eszközök és alapszoftverek gazdája az informatikai terület.

3.4.4 Információs vagyon osztályozása

Az információkat értékük szerint biztonsági osztályokba kell sorolni, és meg kell határozni az osztályokhoz tartozó biztonsági követelmények szintjét is.

3.4.4.1 Osztályozási irányelvek

Az információkat a szervezet szempontjából vett értékük és érzékenységük szerint osztályba kell sorolni. Az információtétel (dokumentum, adatfeljegyzés) osztályba sorolása és az osztályba sorolás szabályos időközönkénti felülvizsgálata az információ szerzőjének vagy megnevezett tulajdonosának feladata.

Jelen szabályzat hatálya kizárólag az elektronikus információs rendszerek vagyonelemeire, valamint az azok tárolását, kezelését, feldolgozását szolgáló szoftver- és hardver vagyonelemekre terjed ki.

3.4.4.2 Információs vagyonelemek besorolása és kezelése

A Hivatal elektronikus információs rendszereit az Ibtv. szerint biztonsági osztályok valamelyikébe be kell sorolni a törvény végrehajtási utasítása szerint. Az osztályba sorolásokat jelen szabályzat melléklete tartalmazza.

Az Ibtv. végrehajtási rendelete értelmében a Hivatal az elektronikus információs rendszereiről nyilvántartást vezet és azt folyamatosan aktualizálja.

A nyilvántartás minden rendszerre nézve tartalmazza:

- annak alapfeladatait;
- a rendszerek által biztosítandó szolgáltatásokat;
- az érintett rendszerekhez tartozó licenc számot (ha azok az érintett szervezet kezelésében vannak);
- a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait (adatgazdákat);
- a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

4 Személyi és környezeti biztonság

A Hivatalon belül meg kell tervezni és egyeztetni az elektronikus információs rendszer biztonságát érintő tevékenységeket, hogy csökkenteni lehessen azok hatását (belső egyeztetés). Ki kell jelölni a biztonsági szerepköröket, mind a szakmai, mind az informatikai területen. Meg kell határozni a felhasználók felelősségét.

4.1 A felhasználókra biztonsági előírások

A Hivatal által nyilvántartott és kezelt adatok jellemzően a személyes adatok, magántitok, üzleti titok, adótitok, közérdekű adatok, Hivatali ügymeneti adatok körébe sorolhatók. Az informatikai rendszerekhez megfelelő jogosultsággal rendelkező felhasználók ezen adatok birtokába juthatnak, azokat módosítani tudják.

A cél olyan biztonsági rendszer kidolgozása, mely meghatározza a munkakörökhöz és szerepkörökhöz tartozó hozzáférési jogosultságokat, biztonsági elvárásokat, kizárva az illetéktelen adathozzáférés és jogosulatlan adatmódosítás lehetőségét.

4.2 Munkakörök, szerepkörök, valamint azok biztonsága

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed az érintett szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki az érintett szervezet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet.

Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem az érintett szervezet tagja, a jelen fejezet szerinti elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás, megkötés során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

Valamennyi munkakörhöz, illetve feladathoz hozzá kell rendelni annak biztonsági szempontú besorolását, és a kapcsolódó feladatokat és felelősségeket a munkaköri leírásokba kell foglalni.

Rendszeresen (legalább három évente) felül kell vizsgálni és frissíteni a munkakörök és feladatok biztonsági szempontú besorolását.

4.2.1 A foglalkoztatás biztonsági feltételei

A titoktartásra vonatkozóan a munka törvénykönyve (továbbiakban: Mt.) hatálya alá eső munkavállalók titoktartási nyilatkozatot írnak alá, a közszolgálati tisztviselőkről szóló törvény (a továbbiakban: Kttv.) hatálya alá eső köztisztviselők esküt tesznek. Ezen túl az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt a Hivatal írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja. A nyilatkozatot az alkalmazott személyzeti anyagához kell csatolni.

A Hivatallal informatikai és ügymeneti rendszerével kapcsolatba kerülő szolgáltatási szerződéssel rendelkező vállalkozók valamint jogi személyiségek által aláírt nyilatkozatokat a szerződésekhez kell csatolni.

A Hivatal informatikai rendszeréhez, a rendszerben tárolt adatokhoz kizárólag az Informatikai Biztonsági Szabályzat oktatásában részesült személyek férhetnek hozzá. Az oktatás meglétének hiányában informatikai hozzáférési jogosultság nem adható ki.

Az elektronikus információs rendszerhez való hozzáférési jogosultság megadása előtt ellenőrizni kell, hogy az adott munkatárs a munkakörhöz szükséges feltételeknek megfelel-e. Az adott munkakör betöltésének időtartama alatt a feltételeknek folyamatosan teljesülniük kell.

4.2.2 Titoktartásra vonatkozó egyéb szabályok

A Hivatal alkalmazottja, volt alkalmazottja, akinek feladataival összefüggésben bizalmas információ jut a tudomására, köteles azt megőrizni.

A Hivatallal fennálló jogviszony megszűnését követően a megismert bizalmas információt határidőhöz nem kötötten köteles továbbra is megőrizni.

4.2.3 Eljárás áthelyezések, átirányítások és kirendelések esetén

Munkatársak állandó vagy ideiglenes áthelyezése esetén ellenőrizni kell, hogy a betölteni kívánt új munkakörnek biztonsági szempontból megfelel-e.

Az újonnan használni kívánt elektronikus információs rendszerhez engedélyezni kell számára a logikai és fizikai hozzáférést, a korábbi, már nem szükséges hozzáférési engedélyeket módosítani kell vagy vissza kell vonni.

A jogviszony változásáról értesíteni kell a munkakörrel szakmai kapcsolatban lévő belső és külső, meghatározott szerepköröket betöltő, feladatokat ellátó személyeket.

4.2.4 Eljárás a jogviszony megszüntetése esetén

Egy munkatárs kilépése esetén gondoskodni kell arról, hogy az elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátása továbbra is biztosított legyen, ezt a munkaköri feladatok és a papír alapú, továbbá az elektronikus dokumentumok átadás-átvételi folyamata biztosítja. A kilépő munkatárs munkahelyi vezetője jelöli ki az átvevő személyét.

Meg kell előzni azt, hogy a jogviszonyt megszüntető munkatárs esetlegesen az elektronikus információs rendszert, illetve abban tárolt adatokat bármilyen formában jogosulatlanul törölje, módosítsa vagy másolatot készítsen azokról, vagy más módon megsérthesse az elektronikus információbiztonsági szabályokat. Tájékoztatni kell kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről.

A kilépés során, a jogviszony megszűnését megelőzően gondoskodni kell a kilépő:

- elektronikus információs rendszerekhez történő hozzáférési jogosultságainak megszüntetéséről,
- egyéni hitelesítő eszközeinek visszavételéről vagy megszüntetéséről,
- a Hivatal tulajdonában álló informatikai eszközök visszavételéről,

A Hivatal megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz, beleértve a kilépő elektronikus levelezését és tárolt dokumentumait.

Szükség esetén a Hivatal tájékoztatja a jogviszony megszűnéséről a kilépő munkatárssal munkakapcsolatban lévő belső és külső munkatársakat.

4.2.5 Általános biztonsági elvárások

A Hivatalon belül minden munkakört és feladatot biztonsági szempontból be kell sorolni, mely besorolást rendszeresen felül kell vizsgálni és frissíteni.

A munkavégzéshez csak az elengedhetetlenül szükséges és elégséges jogosultságokat szabad biztosítani. A Hivatal adataihoz való hozzáféréseknek minden esetben – a jogszabályokkal összhangban – célhoz kötöttnek kell lennie. Egyedi felhasználói azonosító alkalmazása kötelező. A Hivatal alkalmazásaihoz való hozzáférésre csak a felhasználó azonosítását és hitelesítését követően kerülhet sor.

Felügyelet nélkül hagyott munkaállomás esetén az illetéktelen hozzáférés megakadályozásáról a felhasználónak kell gondoskodnia (kijelentkezés, munkaállomás zárolás, kikapcsolás).

4.3 Harmadik fél hozzáférési kockázatának kezelése

Harmadik fél általi (külsős) hozzáférésnek minősül a Hivatallal szerződéses jogviszonyba kerülő vállalkozó vagy vállalkozás, az eljárásokba bevont külsős szakértők továbbá minden más személy által a Hivatal informatikai rendszeréhez és adataihoz történő hozzáférés.

A Hivatal informatikai rendszereihez és eszközeihez történő külsős hozzáférés csak hatályos szerződés szerint történhet.

4.3.1 A hozzáférés informatikai biztonságának szerződéses követelményei

Bármely megbízási vagy vállalkozási szerződés megkötésekor a szerződésben szerepeltetni kell az alapvető adat- és információvédelmi rendelkezéseket. Ennek érdekében az informatikai tárgyú szerződések tervezetét véleményezés céljából az Információbiztonsági Felelősnek és az informatikusnak meg kell küldeni. A szerződésekben minimálisan az alábbi elvárásoknak kell teljesülnie:

- előzetesen meg kell határozni a rendelkezésre bocsátandó szolgáltatások körét,
- egyértelműen és teljes körűen meg kell határozni a szerződéses tevékenységeket, szolgáltatási határokat és kompetenciákat,
- meg kell követelni, hogy a külső szervezet határozza meg a Hivatallal kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is,
- meg kell követelni, hogy a szerződő fél feleljen meg a Hivatal által meghatározott személybiztonsági követelményeknek, továbbá ezeket dokumentálja,
- elő kell írni, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az érintett szervezet elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az érintett szervezetnek,
- meg kell határozni a szerződő felek kölcsönös kötelezettségeit,
- a Hivatal informatikai rendszereihez és eszközeihez történő külsős hozzáférésre irányuló bármely szerződés kizárólag olyan féllel köthető, aki az Informatikai Biztonsági Szabályzatban foglaltakat magára nézve kötelezőnek fogadja el
- rögzíteni kell, hogy a Hivatal jogosult a rendelkezésre álló bármely eszközzel ellenőrizni, hogy a munkavégzés során sérült-e a Hivatal információbiztonsága, továbbá azt, hogy az előzőekben meghatározott személybiztonsági követelmények fennállnak,
- rögzíteni kell a biztonsági eseményekről és a biztonság megsértéséről szóló ellenőrzések, jelentések mechanizmusát, valamint a kivizsgálás során követendő eljárásokat,
- rögzíteni kell, hogy a szerződéses partner a szerződésben foglalt, valamint a teljesítés során tudomására jutott információkat bizalmasan, üzleti titokként kezeli, harmadik félnek, (jogszabályi előírás vagy a másik fél írásbeli hozzájárulása kivételével) nem adja át,
- a szerződéses partner, vagy annak foglalkoztatottai vagy alvállalkozói által megismert adatok minden esetben bizalmas információnak minősülnek. Az adatokat kötelesek a megfelelő biztonsággal kezelni, tárolni, megőrizni, azt – a szerződésszerű teljesítés kivételével – semmilyen formában nem használhatják fel, harmadik félnek nem adhatják át,

- a szerződéses partner köteles a Hivatal adatvédelemmel és adatbiztonsággal kapcsolatos teendőit és felelősségét megismerni, és erről foglalkoztatottait vagy alvállalkozóit tájékoztatni,
- amennyiben a szerződéses partner, vagy foglalkoztatottai vagy alvállalkozói az adatvédelemmel kapcsolatos szabályokat megszegik, úgy a Hivatal a szerződésben meghatározott szankciókat érvényesítheti.

4.4 Informatikai biztonság veszélyeztetése

A Hivatal fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben.

Informatikai biztonsági szabályok megsértésének minősül különösen:

- titoktartási kötelezettség megsértése,
- a jogosultsági rendszer megsértése,
- károkozók, rosszindulatú kódok bejuttatása az informatikai rendszerbe,
- adatok jogosulatlan kezelése, másolása, továbbítása,
- az informatikai infrastruktúra helytelen kezelése.

Amennyiben az elektronikus információbiztonsági szabályokat nem a Hivatal személyi állományába tartozó személy sérti meg, akkor érvényesíteni kell a vonatkozó szerződésben meghatározott következményeket és meg kell tenni a szükséges jogi lépéseket.

4.5 Elektronikus információs rendszerek és szolgáltatások beszerzése

Az IBSZ előírásait az írott szerződésben meg kell jeleníteni minden olyan esetben, amikor a Hivatal külső szolgáltatóval, szállítóval az Ibtv. hatálya eső tárgyban szerződést köt.

Új rendszer fejlesztésével, létező rendszerek továbbfejlesztésével, az új rendszerek, verziók bevezetésével és szükséges dokumentációival kapcsolatosan teljesíteni kell a biztonsági elvárásokat. A rendszerfejlesztés, rendszerbevezetés pályázatának, szerződésének mellékleteként csatolni kell biztonsági követelményeket, a benne foglaltakat a szállítóktól meg kell követelni.

Külső elektronikus információs rendszerek szolgáltatásaihoz kapcsolódódó szerződés követelményeit ki kell egészíteni az előírt védelmi intézkedésekkel, olyan mélységben, hogy a szerződés tartalmi megfelelőségét annak megkötése előtt meg lehessen ítélni.

Külső és belső ellenőrzési eszközökkel ellenőrizni kell, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

A beruházás, vagy költségvetési tervezés részeként az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat és biztonsági követelményeket meg kell határozni és a szükséges feltételeket biztosítani kell.

A beruházási és költségvetési tervezési dokumentumokban az elektronikus információs rendszerek biztonságát érintő költségsorokat fel kell tüntetni és elkülönítetten kell kezelni.

Valamennyi rendszer vagy rendszerelem, hardver és szoftver beszerzése során meg kell határozni és szerződéses követelményként elő kell írni:

- a funkcionális biztonsági követelményeket;
- az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak dokumentálását;
- a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint);
- a biztonsággal kapcsolatos dokumentációs követelményeket;
- a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;
- az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat;
- az elfogadási kritériumokat.

A beszerzés, vagy a beszerzett eszköz beillesztéséből adódó lehetséges kockázatokat fel kell mérni és az integráció során a hivatali elektronikus információs rendszer védelméről és a kockázatok minimalizálásáról gondoskodni kell.

4.5.1 A rendszerek fejlesztési életciklusa

A rendszer fejlesztések során a rendszer valamennyi életciklusában értékelni és érvényesíteni kell a biztonsági követelményeket. Meg kell határozni a rendszerhez kapcsolódó információbiztonsági szerepköröket és felelősségeket.

A rendszer életciklus szakaszokat a következők szerint kell meghatározni:

- követelmény meghatározás;
- fejlesztés vagy beszerzés;
- megvalósítás vagy értékelés;
- üzemeltetés és fenntartás;
- kivonás (archiválás, megsemmisítés).

4.6 Dokumentációkhoz kapcsolódó védelmi intézkedések

Az elektronikus információs rendszerek beszerzése és fejlesztése során meg kell követelni a rendszer adminisztrátori és fejlesztői dokumentációjának az elkészítését, melyeknek tartalmazniuk kell rendszer biztonsági vonatkozásait, a biztonságos konfigurálását, telepítését és üzemeltetését, a biztonsági funkciók hatékony alkalmazását és fenntartását, ismert sérülékenységeket, továbbá a felhasználó által elérhető biztonsági funkciókat és a felhasználó kötelezettségeit a biztonság fenntartásához.

Minden nyilvántartott szoftverhez nyilván kell tartani a szoftver dokumentációját, ami magába foglalja legalább az alábbiakat:

a) felépítésének, funkcióinak és adatkapcsolatainak felső szintű leírását, valamint alapvető jellemzőit (mérete, nyelve, működési környezet, készítőjét), leírását;

b) felhasználói és üzemeltetői kézikönyveket, különösképpen a felhasználói jogosultság rendszer leírását, továbbá a felhasználó kötelezettségeit a biztonság fenntartásához;

c) a rendszer telepítőkészletét, telepítési segédleteit, biztonságos konfigurálási funkciókat;

d) a tesztelést igazoló, valamint az üzemeltetésre átvétel jegyzőkönyveit;

e) az üzemi, konfigurációs és biztonsági beállítások leírását;

f) a rendszert üzemeltetésével, támogatásával kapcsolatos partneri megállapodásokat (pl.: licencek, support szerződések, elérhetőségek)

g) a rendszer biztonsági vonatkozásait, az ismert sérülékenységeket, biztonsági funkciók hatékony alkalmazását és fenntartását.

A felsorolt dokumentumok őrzése az informatikus feladata. A rendszerleírási és rendszerprogram dokumentációinak első példányát az informatikus által hozzáférhető informatikai könyvtárban kell tárolni elektronikus formában. A leírások és dokumentációk másodpéldányát papíron (és lehetőség szerint elektronikus formában is) tűzbiztos lemezszekrényben, kell tárolni. A dokumentációkat minden esetben úgy kell elhelyezni, hogy azok a tárolás közben ne sérüljenek vagy károsodjanak.

Gondoskodni kell arról, hogy az információs rendszerre vonatkozó – különösen az adminisztrátori és fejlesztői – dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható.

Gondoskodni kell a dokumentációknak az érintett szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről.

4.6.1 Rendszerdokumentációk

A rendszerleírások és rendszerprogram dokumentációinak frissítését minden olyan esetben, amikor a rendszeren változtatás (rendszerkonfiguráció változtatás, javítás, verzióváltás stb.) történik, az üzembe állítás (üzemeltetésre átadás) előtt frissíteni kell. A dokumentációk naprakészségért az informatikus a felelős. A rendszerleírásokról és rendszerprogram dokumentációkról nyilvántartást kell vezetni, a verziószámoknak és a telepítés időpontjainak a feltüntetésével. A nyilvántartásnak biztosítania kell, hogy legalább 1 évre visszamenőleg meghatározható legyen minden, az egyes rendszerekkel kapcsolatos változás ideje, oka, mibenléte. A nyilvántartás vezetése és annak folyamatos aktualizálása az informatikus feladata.

4.6.2 Felhasználói dokumentációk

A felhasználói dokumentációk folyamatos rendelkezésre állása megköveteli, hogy a dokumentumokat gyorsan és egyszerűen el lehessen érni. A felhasználói dokumentációkat elektronikusan, a Hivatal belső hálózatán, hozzáférés-ellenőrzéssel védetten kell tárolni.

4.7 Karbantartások

A Hivatal a rendszer karbantartások és az azokhoz kapcsolódó ellenőrzések elvégzése érdekében rendszer-karbantartási eljárásokat alakít ki. Az informatikus karbantartási tevékenységekről nyilvántartást vezet. A karbantartások tervezése és végrehajtása során:

- a gyártói vagy a forgalmazó specifikációknak megfelelően, továbbá a szervezeti igények szerint a karbantartásokat és javításokat ütemezetten hajtja végre;
- dokumentálja és felülvizsgálja a karbantartásokról és javításokról készült feljegyzéseket;
- jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;
- külső karbantartó személyzet esetén minden esetben ellenőrizni kell karbantartást végzők, szervezetek vagy személyek jogosultságát a munka elvégzésére;
- az informatikus jóváhagyása szükséges az elektronikus információs rendszer vagy a rendszerelemek Hivatal létesítményeiből történő kiszállításhoz vagy eszközök beszállításához;
- a Hivatal területére bevitt, onnan kivitt információs rendszerelemekről nyilvántartást kell vezetni;
- gondoskodni kell arról, hogy az elszállítás előtt minden adat és információ – mentést követően – a berendezésről törlésre kerüljön;
- a javítási tevékenységek után ellenőrizni kell, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek kell alávetni azokat;
- a meghatározott, karbantartással kapcsolatos információkat a karbantartási nyilvántartáshoz kell csatolni;
- a diagnosztikai és teszt programokat tartalmazó adathordozókat ellenőrizni kell a kártékony kódok tekintetében, mielőtt azt az elektronikus információs rendszerben használnák;
- karbantartási támogatást kell beszerezni azon elektronikus információs rendszerelemekhez, melyek kezelése saját erőforrásból nem megoldható.

A karbantartási terveket és eljárásokat évente felül kell vizsgálni és szükség szerint aktualizálni.

A karbantartások részletes szabályait rendszer karbantartási eljárásrendben (szabályzatban) kell szabályozni.

5 Fizikai biztonság

A fizikai hozzáférések felügyelete, beléptetés bekezdésben meghatározott követelmények az adott létesítmény bárki által szabadon látogatható, vagy igénybe vehető területeire nem vonatkoznak.

Ezeket a területeket a jegyző a fizikai védelmi utasításban határozza meg.

5.1 Beléptetés

A Hivatal ellenőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt fizikai hozzáféréseket annak érdekében, hogy észlelje a fizikai biztonsági eseményeket és reagáljon arra.

A Hivatal és a hozzátartozó intézmények esetében a be- és kilépést az intézményvezető felelős döntése alapján kell szabályozni. A beléptetés szabályok alkalmazása során figyelemmel kell lenni a más jogszabályban meghatározott tűz-, és személyvédelmi, valamint a személyes adatok kezelésére vonatkozó rendelkezésekre is.

Össze kell állítani és napra készen kell tartani a Hivatal területére, különösen az elektronikus információs rendszer egy vagy több elemét tartalmazó helyiségekbe (szerverszoba, informatikai helyiségek) belépésre jogosultak listáját. A belépésre jogosultak körét a jegyző hagyja jóvá.

A belépésre jogosult személyek listáját rendszeresen, legalább évente felül kell vizsgálni, a listáról el kell távolítani azokat, akiknek a belépése nem indokolt.

A Hivatal a belépési jogosultságot igazoló dokumentumokat (intelligens kártyák) bocsát ki a belépéshez a belépni szándékozó részére. A belépési jogosultság megszűnése esetén gondoskodni kell a belépési jogosultságot igazoló dokumentum visszavonásáról vagy érvénytelenítéséről.

5.2 A fizikai belépés ellenőrzése

A Hivatal a látogatói belépéseket csak a meghatározott be-, és kilépési pontokon teszi lehetővé, ahol az egyéni belépési engedélyek ellenőrzésre kerülnek.

A látogatói belépéseket naplózni kell, a látogatók kíséréséről és tevékenységük figyelemmel kíséréséről gondoskodni kell. A belépésre jogosultak által elérhető helyiségeket felügyelet alatt kell tartani. A látogatói naplókat havi rendszerességgel ellenőrizni kell.

A látogatói belépésekről szóló információkat az adatvédelmi jogszabályoknak megfelelő ideig meg kel őrizni.

A hivatali helyiségek kulcsait, vagy egyéb, fizikai belépést biztosító eszközeit nyilván kell tartani, azok használatát ellenőrizni kell. A kulcsok, vagy a fizikai belépést biztosító eszközök esetleges elvesztése esetén gondoskodni kell a zárak, illetve kódok azonnali cseréjéről is. A belépést biztosító eszközök meglétét legalább évente ellenőrizni kell (leltár).

A kulcsokat és kódokat rendszeresen cserélni kell.

Valamennyi dolgozó kötelessége, hogy az észlelt, esetlegesen jogosulatlan fizikai hozzáféréseket vagy hozzáférési kísérleteket haladéktalanul jelezze munkahelyi vezetője felé, aki megteszi a szükséges intézkedéseket.

5.3 Biztonsági területek

A Hivatal objektumait biztonsági szempontból kategóriákba kell sorolni és meg kell határozni a különböző kategóriába tartozó területek minimális biztonsági követelményeit. A szerverszobát kiemelt biztonságú helyiségnek kell minősíteni.

5.4 Biztonsági előírások

A kiemelt biztonságú helyiségekben oda nem beosztott személyek csak az illetékes területi vezető engedélyével, kísérettel tartózkodhatnak.

A Hivatal szerverszobájában csak az informatikus jelenlétében és felügyeletében lehet tartózkodni és munkát végezni.

A Hivatal irodáiban ügyfelek felügyelet nélkül nem tartózkodhatnak, és nem közlekedhetnek.

5.5 Az infrastruktúrához kapcsolódó védelmi intézkedések

Az információ, mint erőforrás napjainkra a korszerű, versenyképes és folyamatos tervezési és fejlesztési tevékenység alapvető feltételévé vált. Ennek következtében a Hivatalnál alkalmazott informatikai rendszerek rendeltetésszerű, biztonságos működése a Hivatal egészének alapvető érdeke.

A Hivatal informatikai rendszerében csak a munkavégzéssel kapcsolatos feladatok láthatók el, melyek során különös figyelmet kell fordítani az informatikai rendszerek működőképességének fenntartására.

A Hivatal informatikai rendszereiben, vagy hagyományos adathordozókon tárolt adatokkal kapcsolatba kerülő, azok biztonságát akár közvetetten is érintő hardver, szoftver eszközök, objektumok beszerzésére, kialakítására vagy átalakítására irányuló beszerzések, beruházások, felújítások indításához az elektronikus információs rendszerek biztonságáért felelős személy és az informatikus előzetes szakmai véleményezése szükséges.

5.5.1 Számítógépek védelmi előírásai

A számítógép csatlakozóit (kivéve a 230V-os hálózati csatlakozót, amit csak a számítógép kikapcsolt állapotában szabad kihúzni vagy csatlakoztatni) csak az informatikus csatlakoztathatja, kivéve értelemszerűen a mobil számítógépeket.

Az észlelt áramszünetet az informatikus számára minden esetben jelenteni kell. Áramszünet után, ha a számítógép rendellenes működést mutat, szintén értesíteni kell az informatikust.

A számítógépet a napi munka befejezését követően ki kell kapcsolni.

Minden számítástechnikai berendezést óvni kell a mechanikai behatásoktól és a szennyeződésektől.

A számítástechnikai berendezések közelében nem megengedett mágnest tartani, erős elektromágneses mezőt gerjesztő készüléket használni, egyúttal figyelemmel kell lenni a tűz- és munkavédelmi szabályzat előírásaira is.

Számítástechnikai berendezések közelében nedves, vizes tárgyakat, eszközöket (virág, szökőkút stb.) tartani és üzemeltetni nem szabad.

Az informatikai eszközök fizikai mozgatását csak az informatikus végezheti, az erre vonatkozó igényt az informatikusnak minden esetben be kell jelenteni.

5.5.2 Szervertároló helyiség védelmi előírásai

Az informatikai kritikus eszközöket tartalmazó helyiségeket (szerverszoba, informatikai technikai helyiségek, kommunikációs rendezők stb.) zárva kell tartani és csak arra feljogosított személyek férhetnek hozzá.

A szervertároló helyiséget megfelelő kézi tűzoltó berendezéssel kell ellátni, melyek időszakos ellenőrzését a tűzvédelmi szabályok szerint el kell végeztetni.

A szerverszoba technikai feltételeinek az alábbi biztonsági elvárásokat kell teljesíteniük:

- A szerverszobába kizárólag kiszolgáló funkciót ellátó berendezések és az azok üzemeltetéséhez szükséges kiegészítő eszközök telepíthetők.
- A szerverszobát független áramellátással támogatott tűz- és füstérzékelő rendszerrel kell felszerelni, mely a felügyeletet ellátó BOD- Reflex Kft részére, illetve a gondoknak küldi a riasztást.
- A szerverszobában csak a számítástechnikai eszközök folyamatos működtetéséhez szükséges eszközök tárolhatók, telepíthetők és üzemeltethetők. A leselejtezett számítástechnikai eszközöket és a hozzájuk tartozó berendezéseket el kell távolítani.
- Tűzveszélyes anyag, papír, irat a szerver szobában nem tárolható.
- A szerverszobát a szerverek működéséhez szükséges ideális hőmérséklet és páratartalom állandó szinten tartása érdekében klímaberendezéssel kell ellátni.
- Az elektronikus információs rendszert, különösen a szerverszobát védeni kell a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzárószelepek hozzáférhetőek és működőképesek, valamint a kulcsszemélyek számára ismertek legyenek.

5.5.3 Informatikai eszközök áramellátása

Az áramellátást biztosító kábelezést az informatikai kábelektől elkülönülten, attól megfelelő távolságban elhelyezve, lehetőség szerint föld alatt vagy falon belül kell vezetni.

Biztosítani kell a számítógéptermek folyamatos energia ellátását, valamint az alkalmazott számítástechnikai eszközök hálózati tranziensek elleni védelmét. A Hivatal szerverszobájának kiszolgálóit szünetmentes tápegységhez kell csatlakoztatni, amelyek áthidalási ideje elegendő áramszünet esetén a kiszolgálók biztonságos leállításához.

5.5.4 Adatátviteli/telefon kábelezés kialakítása

A hálózati kábelezést védeni kell a jogosulatlan lehallgatástól vagy károsodástól. A megvalósításnál külön védőcsöveket kell alkalmazni, az erősáramú kábelezéstől elkülönítve kell vezetni. A nyomvonal tervezésekor a közterületeken való vezetést lehetőség szerint el kell kerülni.

A kábelek csatlakozó pontjait (patch panelek) zárt rendezőszekrényben kell elhelyezni, mely csak az informatikus vagy a jegyző által megbízott személy felügyelete mellett nyitható.

A kábelszekrényben a csatlakozópontokról a kábeleket rendezett módon kell elvezetni, a használaton kívüli kábeleket el kell távolítani.

Az irodákban található, tartósan használaton kívüli végpontok kirendezését meg kell szüntetni. A rendezőszekrények oldaláról évente, (lehetőleg műszeresen) kell ellenőrizni, hogy az összes kirendezett végponton van-e számítógép és a használaton kívüli végpontokat fel kell számolni. Ügyfélfogadásra használt területen nyílt, élő végpont nem lehet.

6 Az üzemeltetés biztonsága

6.1 Konfigurációkezelés szabályok

Az elektronikus információs rendszerek kontrollált fenntartása érdekében ki kell dolgozni a konfigurációkezelésre vonatkozó szabályzatot, amely konfigurációkezelést és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

6.2 Legszűkebb funkcionalitás

Az elektronikus információs rendszert úgy kell konfigurálni, hogy az csak a szükséges szolgáltatásokat nyújtsa. Meg kell határozni a tiltott, vagy korlátozott, nem szükséges funkciókat, portokat, protokollokat, szolgáltatásokat, szoftvereket.

6.3 Duplikálás elleni védelem

Rendszeresen ellenőrizni kell, hogy az elektronikus információs rendszer hatókörén belüli elemek nincsenek-e felvéve más elektronikus információs rendszerek leltárában.

6.4 Szervertároló helyiség üzemeltetési biztonsága

A Hivatal informatikai rendszereinek biztonságos üzemeltetésének és ellenőrzésének feltételeit a fizikai védelmet szabályozó eljárásrendben kell szabályozni.

A szabályzatnak legalább az alábbi főbb területekre kell kitérnie:

- az üzemeltetéshez kapcsolódó főbb feladat- és felelősségi körök, kapcsolódó eljárás- és dokumentációs rend,
- az üzemeltetés során használt adathordozók kezelése, dokumentálása,
- az üzemeltetéssel összefüggő karbantartások kezelése, dokumentálása,
- az üzemzavarok és más incidensek kezelése, dokumentálása,
- a számítógépteremben elhelyezhető eszközök és azok használatának rendje, dokumentálása,
- tűz és vagyonvédelmi intézkedések.

6.5 Munkaállomások üzemeltetésének biztonsága

A Hivatal munkaállomásainak üzemeltetéséért az informatikus a felelős, akinek a számítástechnikai eszközökről nyilvántartással kell rendelkeznie.

A munkaállomások és egyéb informatikai beleértve egyéb irodatechnikai eszközök elhelyezésének vonatkozásában minimum az alábbiaknak kell megfelelni:

- Az eszköz beüzemelésének egyik alapfeltétele, hogy engedélyezett megrendeléshez köthető legyen, valamint konzisztens legyen a meglévő infrastruktúra elemekkel.
- Az eszköz beüzemelése a hozzá tartozó üzembe helyezési leírások alapján azok betartásával végezhető el, amennyiben szükséges, a beüzemelést felügyelő vezető elrendelheti az eszköz szeparált tesztkörnyezetben való együttműködési teszt lefolytatását.

A munkaállomások üzemeltetésével kapcsolatos, az IBSZ által nem szabályozott kérdéseket az IBSZ-hez kapcsolódó egyéb üzemeltetési szabályozás tartalmazza.

6.5.1 Munkaállomások általános biztonsági követelményei

- A felhasználóknak a munkaállomások BIOS-át módosítani, valamint a hardverkonfigurációt bármilyen módon megváltoztatni nem szabad.
- A BIOS adminisztrátori jelszót megváltoztatni tilos.
- A munkaállomást és tartozékait csak a kezelési útmutatóban foglalt előírásoknak megfelelően, rendeltetésszerűen szabad használni.
- A munkaállomást és tartozékait csak kikapcsolt és áramtalanított állapotban szabad tisztítani az erre vonatkozó előírások betartásával.
- A munkaállomásokat – ahol rendelkezésre áll – szünetmentes áramforrással biztosított erősáramú hálózati aljzatba szükséges csatlakoztatni.
- A munkaállomások fizikai szétszerelése esetén a merevlemez/egység az informatikus az adatok bizalmasságának megőrzését figyelembe véve kötelesek biztonságos helyen tárolni.
- Szervizbe szállított munkaállomásból el kell távolítani a merevlemezt.
- A Hivatal hálózatához kapcsolódó munkaállomások operációs rendszerét csak az informatikus által kidolgozott és az elektronikus információs rendszerek biztonságáért felelős személy által jóváhagyott eljárásokkal (hálózati telepítés, lemezkép) lehet telepíteni. Ezen lépéseket az IBSZ-hez kapcsolódó egyéb üzemeltetési szabályozás tartalmazza.

6.5.2 Hálózati nyomtatók használatának biztonsági követelményei

A multifunkcionális illetve egyéb hálózati nyomtatók használata során, továbbá az egyéb kimeneti eszközök kezelésekor az alábbi biztonsági előírásokat kell betartani:

- Folyosón illetve egyéb közös helyiségben a nyomtató berendezést kizárólag ügyfelektől elzárt területen szabad telepíteni, vagy csak felhasználói azonosítás (jelszó, kártya) után használhatók a nyomtatási, másolási funkciók.
- A nyomtatónál kinyomtatott dokumentum nem maradhat. Ezeket a nyomtatás után a felhasználónak el kell vinnie.
- A fénymásolók és multifunkcionális eszközök szervizelését csak felügyelet mellett végezheti a titoktartási nyilatkozattal és karbantartási szerződéssel rendelkező vállalkozás és annak alkalmazottja.
- A berendezés elszállításakor a benne lévő merevlemezre is az adathordozókra vonatkozó előírások az érvényesek.

- A Hivatal nyomtatóin csak a Hivatal ügymenetével kapcsolatos dokumentációk nyomtathatók. A szabály megsértése esetén a Hivatal a szabálysértővel szemben eljárást kezdeményezhet.

6.5.3 Rendelkezésre állással kapcsolatos intézkedések

Az informatikai biztonságot vagy a folyamatos rendelkezésre állást érintő fenyegetettségről, vagy bekövetkezett eseményről az alkalmazottaknak az informatikust haladéktalanul értesíteniük kell, akik helyszíni vagy az általuk biztonságosnak ítélt távmenedzsment megoldásokkal elvégzi az üzemeltetési feladatokat. Amennyiben az esemény nem a napi gyakorlat keretében elhárítható, szokásos tevékenységek körébe tartozik, akkor az informatikus értesíti az elektronikus információs rendszerek biztonságáért felelős személyt.

6.6 Kriptográfia

A kriptográfia (titkosítás) az adatok valamely matematikai algoritmus szerinti megváltoztatása abból a célból, hogy csak a jogosultak ismerhessék meg annak tartalmát. A kriptográfia valamely adat sértetlenségének és hitelességének a bizonyítására is szolgál.

Amennyiben ilyen alkalmazásra kerül, a Hivatal kommunikációs folyamataiban (levelezés, https kapcsolatok, távoli elérés) és kiemelt rendszereinél használt tanúsítványokat, titkosító kulcsokat bizalmasan kell kezelni. Az ezekről készített biztonsági másolatokat páncélszekrényben kell tárolni. Ezekhez csak az informatikus vagy a jegyző által felhatalmazott személy férhet hozzá.

A kiemelt rendszerek (banki, közigazgatási rendszerek) eléréshez szükséges azonosítókat csak a munkafolyamattal megbízott alkalmazottak ismerhetik. Minden, hozzáféréssel rendelkező munkatársnak egyedi azonosítót kell biztosítani.

A titkosítási feladatokra használható kulcsok jellemzőit, kezelését és a kapcsolatos feladatok elvégzésének felelőseit az IBSZ-hez kapcsolódó egyéb üzemeltetési szabályozás tartalmazza.

6.7 Együttműködésen alapuló számítástechnikai eszközök:

Az elektronikus információs rendszernek meg kell gátolnia az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha az engedélyezve van. A távoli aktivitásról az eszköz nyújtson közvetlen kijelzést azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

6.8 A folyamatok elkülönítése

Az elektronikus információs rendszerben elkülönített végrehajtási tartományt kell fenntartani minden végrehajtó folyamat számára.

Ez a megfelelő kiszolgáló operációs rendszerek használatával elérhető.

7 Adathordozók kezelése és biztonsága

Az adathordozók sérülésének, a rajtuk tárolt adatok illetéktelen kezekbe jutásának, illetve az üzemszerű tevékenységek megszakadásának megelőzése céljából az adathordozókat rendszeresen ellenőrizni, és fizikailag védeni kell.

A tárolóeszköz adattartalmának véletlen megváltoztatását, amennyiben úgy lett kialakítva, a tárolóeszközön kialakított fizikai írásvédelmi eszközzel kell megakadályozni.

Adatok, programok a mentéseken és biztonsági másolatokon kívül csak szükséges és elégséges számú példányban tárolhatók.

Az adathordozókat a rajtuk lévő adatok érzékenységének megfelelően, védeni kell, használaton kívül el kell zárni.

Adathordozó (adat) a Hivatal területéről csak a jegyző engedélyével kerülhet ki, ez vonatkozik az adathordozókon történő kivitelre, vagy az egyéb, elektronikus úton történő továbbításra, mint az internetes vagy a mobiltelefonos adattovábbítás.

A központi infrastruktúrán (kiszolgálók, csoportkönyvtárak, fájl szerverek stb.) kívül például felhasználói munkaállomásokon, laptopokon csak olyan adatot szabad tárolni, melyek sérülése, elvesztése vagy illetéktelenek kezébe történő kerülése nem okozhat a Hivatal számára kárt vagy bizalomvesztést. Az itt tárolt adatok nem kerülnek központi mentésre, ezért a mentési igényt minden esetben az informatikus felé kell jelezni.

A személyi használatra kiadott laptopokon bizalmas információt csak titkosítva szabad tárolni.

7.1.1 Adathordozók kezelése

Az adathordozók kezelését minden esetben a rajtuk tárolt információ érzékenysége szerint kell végezni.

Az adathordozók nyilvántartásának minimálisan a következő adatokat kell tartalmaznia:

- a kötet azonosítója,
- a létrehozás dátuma,
- a megőrzés dátuma,
- a tárgy megjelölése,
- a felhasználás illetékességének adatai,
- felülírás dátuma vagy rendszeressége.

A hivatalos munkavégzés során szükséges felhasználáson kívül számítógépes adathordozót, vagy elektronikus eszközt (pl.: digitális fényképezőgép, MP3 lejátszó, USB kulcs (pendrive), bluetooth illetve Wi-Fi eszközök, stb.) a Hivatal éles üzemű informatikai rendszereihez csatlakoztatni tilos. A hivatalos munkavégzéshez kizárólag a Hivatal által biztosított adathordozók és eszközök használhatók.

7.1.2 Adathordozók tárolása

Az adatállományok és az üzemszerűen használt programok biztonsági mentéseit tartalmazó adathordozókat a gyártói ajánlásokat figyelembe véve lehetőség szerint tűzbiztos páncélszekrényben kell

tárolni. Abban az esetben, ha ez nem megoldható, az adathordozók tárolására a szerverszobán kívüli műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

Az adatállományok biztonsági mentéseit az informatikus helyezhetik el, illetve távolíthatják el a páncélszekrényből.

7.1.3 Adathordozók szállítása

Adathordozót a Hivatal objektumaiból kivinni csak az érintett szervezeti egység vezetőjének írásos engedélyével az adathordozó informatikus általi átvizsgálása után lehet.

Külső cég által javításra, cserére adathordozó csak a rajta lévő adatok olvashatatlanná tételét követően adható át. Amennyiben ez nem megvalósítható, a jegyző jóváhagyásával az adathordozó átadható.

7.1.4 Adathordozók megőrzése

Az adathordozók megőrzési idejét a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló többször módosított 1995. évi LXVI. törvényben foglaltak, továbbá a Hivatal hatályos irattári rendjében foglaltak alapján az adatkezelő határozza meg.

7.1.5 Adathordozók nyilvántartása

Az adathordozók leltározását a leltározási eljárásoknak és szabályoknak megfelelően kell elvégezni.

7.1.6 Adathordozók selejtezése és megsemmisítése

Azt az adathordozót, amelyet javíthatatlan fizikai károsodás ért, vagy a megengedett hibajelzést túllépte, le kell selejtezni, majd a selejtezést követően meg kell semmisíteni. A megsemmisítést az informatikus végezheti el, vagy erre szakosodott, adatmegsemmisítéssel foglalkozó vállalkozást kell megbízni a feladattal.

Az adathordozók selejtezése előtt az adathordozón tárolt adatokat olvashatatlanná kell tenni:

- fizikai törléssel (WIPE-olás),
- demagnetizálással, vagy
- fizikai roncsolással.

A fizikai törlés során az adathordozó teljes felületét több ciklusban véletlenszerű adatokkal kell felülírni. A fizikai törlés pontos technikai megvalósítását az informatikus végzi el.

Demagnetizálásra akkor kerülhet sor, ha az adathordozón tárolt adatok fizikai törlése valamilyen okból nem végezhető el. Adathordozók demagnetizálását kizárólag az informatikus végezheti.

Olyan adathordozó esetében, amelyen adattárolás történt, de annak sem fizikai törlése, sem demagnetizálása nem valósítható meg, az adathordozó olvasását fizikai roncsolással kell megakadályozni.

Az adathordozók megsemmisítéséről jegyzőkönyvet kell felvenni, melynek tartalmaznia kell:

- a megsemmisített adathordozók egyedi azonosítóját,
- a megsemmisítés időpontját,
- a megsemmisítés módját,

A papír alapú adathordozók megsemmisítésénél olyan technológiát kell alkalmazni, amelynek következtében a papíron lévő információ visszaállítása az információ értékét jelentősen meghaladó ráfordítással lehetséges. Törekedni kell iratmegsemmisítő, vagy ipari zúzógép használatára.

Az adathordozókat azok megsemmisítéséig illetéktelen hozzáférésekkel szemben védeni kell.

7.2 Szoftverekkel kapcsolatos biztonsági intézkedések

A Hivatal ügymeneteivel kapcsolatos feladatokhoz az érintett szervezeti egységekkel együttműködve az informatikus határozza meg a feladatcsoportok ellátásához szükséges minimális és elégséges szoftverkövetelményeket, melyek jegyzői jóváhagyás után lépnek életbe.

Az alkalmazandó szoftverek listáját az informatikus évente vagy az új vagy új platformon üzemelő alkalmazások bevezetése esetén felülvizsgálja.

Az új operációs rendszerek, valamint az új alkalmazói szoftverek előzetes alkalmazhatósági, biztonsági kompatibilitási teszteknek kell alávetni, mely elvégzése az informatikus feladata.

A Hivatal számítógépein kizárólag csak a Hivatal által megvásárolt, vagy licenc szerződés alapján használt jogtiszta szoftver, illetve az informatikai csoport által telepített egyéb jogtiszta (Freeware, open source) alkalmazások használata megengedett.

A szoftverek installációs adathordozóit, illetve a róluk készült biztonsági mentéseket, valamint a hozzájuk tartozó licenc dokumentumokat zárt helyen kell tárolni. Azokhoz csak az informatikus és a jegyző által meghatalmazott személyek férhetnek hozzá.

7.3 Hálózat biztonságával kapcsolatos intézkedések

A Hivatal az elektronikus információs rendszerének kapcsolódását más elektronikus információs rendszerekhez jegyzői jóváhagyáshoz köti.

Az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát minden esetben dokumentálni kell.

Belső elektronikus információs rendszerek összekapcsolását előzetes jegyzői jóváhagyás után az informatikus engedélyezheti és állítja be.

A hálózat biztonságát szavatoló intézkedések célja a Hivatal hálózati infrastruktúrájának, a hálózati szerverek és munkaállomásokon tárolt adatainak sértetlenségének és bizalmasságának, valamint a hivatali ügymenetek zavartalan végzésének biztosítása.

A belső hálózaton rosszindulatú tevékenység vagy rendellenes működés észlelése esetén korlátozni kell annak hatását, akár a megtámadott eszköz kiiktatása vagy a kapcsolat megszakítása árán is. Az ilyen eseményekről haladéktalanul tájékoztatni kell az elektronikus információs rendszerek biztonságáért felelős személyt is.

Külső hálózatból csak időszakosan engedélyezett és az informatikus által biztonságosnak ítélt, támogatott és felügyelt kapcsolaton keresztül kapcsolódhatnak a támogatási szerződéssel rendelkező vállalkozások. Az informatikus visszaélés, rosszindulatú kód küldése, vagy a Hivatali napi munkafolyamatait veszélyeztető cselekedetek észlelése esetében a kapcsolatot haladéktalanul megszakíthatja és ezt az elektronikus információs rendszerek biztonságáért felelős személy felé jelezni kötelesek.

Notebookok esetében meg kell akadályozni, hogy az eszköz egyszerre csatlakozzon a Hivatal belső hálózatához és egy, nem a Hivatal által felügyelt WiFi hálózathoz.

A megosztott könyvtárakhoz jelszófüggő jogokat kell rendelni.

Hálózati alkalmazások használata után be kell zárni a már nem használt programot.

A Hivatal Informatikai rendszerének bármely elemén kizárólag csak az arra felhatalmazott informatikus végezhet rendszergazdai jogosultsághoz kötött módosításokat Az operációs rendszerek hálózati és biztonsági beállításainak megváltoztatására, hálózati végpont menedzselésére (átépítés, áthelyezés bővítés, átkötés, megszüntetés, kábelezés bárminemű módosítása) kizárólag az informatikus jogosult. A központi rendszereken végzett bármilyen olyan beállítás, amihez rendszergazdai jogosultság szükséges, csak a Hivatal területén végezhető.

Megtörtént, vagy folyamatban levő biztonsági incidens észlelésekor a felhasználó haladéktalanul köteles értesíteni az informatikai területet. A felhasználó nem kísérelheti meg a támadó felderítését, nem tehet ellenlépéseket, kivéve, ha az informatikus erre kifejezett utasítást ad.

7.3.1 Behatolás védelmi szabályok és tűzfalak:

A Hivatal a rendszereit tűzfallal vagy azzal egyenértékű tűzfal jellegű berendezéssel (továbbiakban: tűzfal) kell védeni annak megakadályozására, hogy kívülről illetéktelen személy a rendszerbe behatolhasson.

A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban kell elhelyezni, elkülönítve a belső szervezeti hálózattól.

A Hivatal hálózatáról szigorúan tilos bármilyen, a tűzfalat megkerülő kapcsolatot létesíteni nyilvános hálózatokkal (pl.: internetet modemen keresztül használni, külső WiFi hálózathoz csatlakozni).

Nem nyilvános hálózatokat csak ellenőrzött kapcsolaton keresztül szabad használni.

Az alkalmazott tűzfalon változtatást csak az arra feljogosított személy végezhet.

A Hivatal Hozzáférés ellenőrzési szabályzatban határozza meg a külső elektronikus információs rendszerekhez való kapcsolódások szabályait, amelynek eredménye lehet az összes kapcsolat engedélyezése vagy tiltása, meghatározott kapcsolatok engedélyezése, meghatározott kapcsolatok tiltása.

7.3.2 Infokommunikációs szolgáltatások

Az Hivatal - a Nemzeti Távközlési Gerinchálózatra csatlakozó elektronikus információs rendszerek kivételével - tartalék infokommunikációs szolgáltatásokat létesít, erre vonatkozóan olyan

megállapodásokat köt, amelyek lehetővé teszik az elektronikus információs rendszer alapfunkciói, vagy meghatározott műveletek számára azok meghatározott időtartamon belüli újrakezdését, amennyiben az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszínen.

Szolgáltatások prioritása:

Amennyiben az elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására szerződés keretében kerül sor, az tartalmazza a szolgáltatás-prioritási rendelkezéseket, a Hivatal rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban.

7.3.3 Vezeték nélküli hozzáférés

A Hivatal a mobil eszközökkel rendelkező felhasználói számára, egyedi engedélyezési eljárás után, vezeték nélküli (WiFi) hozzáférési lehetőséget biztosíthat elektronikus információs rendszereihez.

A Hivatal vezeték nélküli (WiFi) hálózatok titkosítását az eszköz által támogatott lehetséges legnagyobb kulcshosszúsággal és legmagasabb biztonsági szintű megoldással kell konfigurálni (pl.: AES128, AES256, WPA vagy WPA2). WEP titkosítás a Hivatalban nem alkalmazható. A Hivatalon belül kialakított WiFi hálózat nem kapcsolódhat közvetlenül a Hivatal belső hálózatához.

A vezeték nélküli hálózat létesítése és üzemeltetése során az alábbi feltételeknek kell teljesülniük:

a) a vezeték nélküli hozzáférést titkosítással és a felhasználók, vagy eszközök hitelesítésével kell védeni;

b) a vezeték nélküli hálózat konfigurálását a rendszergazdák csak közvetlen jogosultság birtokában, a védett hálózaton kialakított vezetékes kapcsolaton keresztül végezhetik;

c) a vezeték nélküli hálózat üzemeltetése során megfelelő karakterisztikájú és teljesítményszintű antennák, vagy egyéb technikákat alkalmazásával gondoskodni kell arról, hogy a szervezet fizikai határain kívülről a jelek észlelésének a valószínűsége minimális legyen.

7.4 Információcsere

A lakossággal, a kapcsolódó társszervekkel és közigazgatási egységekkel, a vállalkozásokkal folytatott hivatali kommunikáció során biztosítani kell annak a törvényi előírások által meghatározott adatvédelmi és titoktartási intézkedések betartását. A Hivatali kommunikáció során az egyes csatornákon továbbított információk megvédésére eljárási rendet és szabályozást kell meghatározni.

7.4.1 Elektronikus levelezés biztonsága

A Hivatal az ügymenet támogatásához elektronikus levelezési szolgáltatást alkalmaz. Az elektronikus levelezés magáncélú használata tilos. A Hivatal az e-mail forgalmat naplózza, továbbá automatikus és manuális módon ellenőrizheti.

Az email szerver világhálón keresztüli elérése csak biztonságos (HTTPS) kapcsolaton keresztül történhet.

A Hivatal belső hálózatán nem hivatali célú üzenetet nem nevesített (pl. Csoport, Mindenki) felhasználóknak küldeni tilos. A tilalom betartását az informatikus ellenőrzi és indokolt esetben a jegyző részére jelentést tesz.

7.4.2 Internet használat biztonsága

A felhasználók Internet elérési jogosultságát az egyéb rendszerekhez történő hozzáférési jogosultsághoz hasonlóan külön engedélyezni kell. A Hivatal munkaállomásai csak az informatika által felügyelt tűzfalon keresztül kapcsolódhatnak az internetre. A nem naprakész vírus definíciós adatbázissal rendelkező munkaállomás Internet elérését az adatbázis frissítéséig fel kell függeszteni.

A Hivatal az internet használatot rendszeresen ellenőrzi, az elérhető tartalmakat korlátozza, az interneten végzett tevékenységeket naplózza.

A Hivatal tiltja:

- az internet magáncélú felhasználását,
- az interneten megvalósuló egyes tevékenységeket (pl.: chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták, stb.),
- a közösségi oldalak használatát, magánpostafiók (webmail) elérését, és más, a szervezettől idegen tevékenységet.

A kormányzati ASP rendszerhez kapcsolódó hálózati szegmensen csak az úgynevezett fehérlistás internet elérés engedélyezhető.

A Hivatali munkatársaknak az internet használat során az alábbi szabályokat kell betartaniuk:

- Az internetet a felhasználók munkaköri leírásaikban meghatározott feladataik elvégzéséhez használhatják, betartva az ide vonatkozó szabályokat, utasításokat. Ezen szolgáltatás minden magán és egyéb célú használat során esetlegesen bekövetkezett károkért a felhasználó teljes felelősséggel tartozik.
- Tilos a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele. A tilalmat megsértőkkel szemben munkajogi és büntetőjogi felelősségre vonást kezdeményez a Hivatal.
- Tilos a szoftverek letöltésével a szoftver tulajdonosa által szabott jogi feltételeket megszegni.
- Tilos a felhasználóknak a Web-böngészők biztonsági beállításait (cookie-k, a JavaScriptek, JVM-ek, ActiveX környezetek, plug-in-ek, jelszó megjegyzés tiltás használatát) megváltoztatni.
- Az internetről letöltött fájlokat csak vírusellenőrzés után szabad megnyitni.
- Tilos a felhasználónak az iternet használata során jogellenes tevékenységet megvalósítani.
- Az Internet használat monitorozását, az elérhető tartalmak kontrollálását az informatikus végzik el az IBSZ-hez kapcsolódó egyéb üzemeltetési szabályozásban foglaltak alapján.

7.4.3 Telefon és telefax használat biztonsága

Telefon és fax készülékek használata során figyelembe kell venni, hogy az átviteli közeg bizalmassága nem biztosított, bizalmas vagy titkos információt így továbbítani nem szabad.

Figyelembe kell venni, hogy a telefax üzenetek, az e-mailhez hasonlóan, egyéb hitelesítés nélkül jogilag nem bizonyító erejűek, elküldésük és fogadásuk nem bizonyítható egyértelműen.

7.4.4 Az információ csere egyéb fajtái

A Hivatal objektumaiban a Hivatal számítástechnikai hálózatához csatlakozó, nem a Hivatal tulajdonát és az informatikus által karbantartott számítógépet vagy egyéb informatikai rendszerelemet üzemeltetni kizárólag az informatikus előzetes vizsgálata és szakvéleménye alapján jegyzői jóváhagyással lehet. Az informatikus által lefolytatott vizsgálatnak ki kell terjednie a számítógép/notebook operációs rendszerének, vírusvédelmi rendszerének naprakész állapotára.

7.5 Kártékony szoftverek elleni védelem

A kártékony szoftverek támadásaival szemben a szoftver eszközök és információk sértetlenségének megőrzését szavatoló eljárásokat és a megelőző intézkedéseket kell bevezetni. A kiépített védelmi rendszernek az alábbi feltételeket kell teljesítenie:

- az elektronikus információs rendszer be- és kilépési pontjain a kártékony kódokat fel kell deríteni és meg kell semmisíteni azokat,
- frissíteni kell a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg;

A védelmi eszközöket úgy kell konfigurálni, hogy védelmi rendszer:

- rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren, és hajtsa végre a külső forrásokból származó fájlok valós idejű ellenőrzését a végpontokon, a hálózati belépési, vagy kilépési pontokon, a biztonsági szabályzatnak megfelelően, amikor a fájlokat letöltik, megnyitják, vagy elindítják,
- a kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt és riassza a rendszeradminisztrátort,
- ellenőrizze a téves riasztásokat a kártékony kód észlelése és megsemmisítése során.

7.6 Mentés és archiválás

A Hivatal elektronikus információs rendszereiről, informatikai rendszerében lévő fájl szerveren tárolt adatokról, a levelezési postafiókokról, a szerverekről, a naplóállományokról az adatok érzékenységének, helyreállítási idejének és elvárt helyreállítási pontjainak figyelembe vételével időszakonként mentést kell készíteni, illetve az adatokat az ügymenet elvárásai szerint archiválni kell.

A mentés alapvetően az incidensek utáni helyreállítást szolgálja.

A Hivatal működésével kapcsolatos adatokat, dokumentumokat részben törvényi előírások, részben szerződési, szabályozási vagy üzleti követelmények miatt esetenként hosszabb időre meg kell őrizni, ezt a folyamatot nevezzük archiválásnak.

Az elektronikus információs rendszerek biztonsági mentésének során:

- meg kell határozni minden elektronikus információs rendszerre vonatkozóan a mentések szükséges gyakoriságát, a mentendő adatok körét.
- A mentésekre vonatkozó igényeket összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal a szakmai területekkel egyeztetve kell kialakítani.
- meghatározott gyakorisággal menteni kell az elektronikus információs rendszerben tárolt rendszerszintű információkat és rendszerdokumentációkat, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;
- meg kell védeni a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen.

A mentéseket/archív adathordozókat az adatforrástól (szerverteremtől) fizikailag elkülönítve, biztonságosan kell tárolni, lehetőleg más épületben, de legalább másik tűzszakaszban.

Rendszeresen tesztelni kell a mentések visszaállíthatóságát, az ügymenet folytonossági tervekkel is összhangban, s a tesztelések eredményét dokumentálni kell.

A munkaállomások, laptopok helyi merevlemezén adatot tárolni nem szabad, mert nem kerül mentésre.

A mentési eljárásba bevont adathordozókat nyilván kell tartani és amennyiben ez értelmezhető, akkor tárolt adatok osztályba sorolásával megegyező jelzéssel (nyilvános, kiemelt, magas) címkékkel kell ellátni. A nyilvántartásnak tartalmaznia kell a mentés valamennyi lényeges egyéb technikai paraméterét is (mentési ideje, teljes vagy inkrementális mentés stb.).

Külön szabályzatban kell dokumentálni a rendszerekhez kapcsolódó részletes mentési és archiválási előírásokat.

8 Hozzáférés ellenőrzés biztonsága

8.1 Hozzáférés ellenőrzés általános követelményei

A Hivatal informatikai rendszerében a hozzáférési megoldások kidolgozása és felügyelete az informatikus feladata. Az általa javasolt intézkedések és megoldások jegyzői jóváhagyás után vezethetők be. A részletes hozzáférés szabályozást azonosítási és hitelesítési eljárásrendben kell rögzíteni.

8.2 Hozzáférés menedzselés

A felhasználói azonosítók és jelszavak kiadását és a hozzáférési jogosultságok beállítását a felhasználó felettesének írásos jogosultságigénylése alapján az informatikus végzi el.

A felhasználó Hivataltól történő távozásakor a hozzáférési jogosultságokat vissza kell vonni.

A felhasználók részére kiosztott hozzáférési jogosultságokat évente vagy a Szervezeti és Működési Szabályzat módosításakor az informatikusnak a szervezeti egységek vezetőivel történő egyeztetés után ellenőriznie kell. Az időközben feleslegessé vált hozzáférési jogosultságokat vissza kell vonni.

8.3 Jelszavak biztonsági követelményei

A Hivatal informatikai rendszerei esetében 3 jelszócsoportot különböztetünk meg:

- felhasználói jelszavak,
- adminisztrátori és technikai azonosítókhoz tartozó jelszavak,
- alkalmazásokhoz tartozó jelszavak.

A Hivatal informatikai rendszereibe bejelentkezési azonosítóval rendelkező felhasználó számára kötelező a bejelentkező azonosítóhoz tartozó jelszó bizalmas megőrzése. Az informatikai rendszerekben a jelszavak továbbítása és tárolása csak titkosítottan történhet.

A felhasználói jelszavakkal szembeni biztonsági követelmények:

- a jelszavakat bizalmasan, magánjellegűként kell kezelni, jelszót telefonon, email-en, weboldalon keresztül megadni tilos,
- az utoljára használt öt, adminisztrátori jelszó esetén tizenkét jelszót tárolja el és akadályozza meg azok újbóli felhasználását,
- a képernyőn a jelszavakat még bevitelkor se jelenítse meg olvasható formában,
- a jelszóállományokat az alkalmazási rendszer adataitól függetlenül, titkosított formában tárolja és erre a célra egyirányú titkosító algoritmust alkalmazzon,
- a jelszó legyen legalább nyolc karakter hosszúságú,
- a jelszó nem tartalmazhat könnyen kitalálható, ismétlődő karaktersorozatot, valamint nem utalhat a felhasználó személyére, nevére, becézett formájára,
- ahol ezt az operációs rendszer támogatja, meghatározott számú sikertelen bejelentkezés után az operációs rendszernek le kell tiltania a felhasználó fiókját,
- A jelszót haladéktalanul meg kell változtatni, ha az illetéktelen személy tudomására jutott, vagy juthatott. A változtatást felhasználó kérésére az informatikus végzi el.
- A használt jelszavakat rendszeres időközönként, de legalább évente meg kell változtatni.

Az adminisztrátori és technikai azonosítókhoz tartozó jelszavakat az informatikus állítja be. A jelszavaknak legalább tíz karakter hosszúságúnak kell lenniük és a komplexitás tekintetében a felhasználói jelszavak esetében megfogalmazott szabályokat kell betartani.

A technikai azonosítók közé tartoznak az aktív hálózati eszközök menedzsment felületére történő belépési azonosítók, szolgáltatások futtatását biztosító azonosítókhoz tartozó jelszavak, valamint a WiFi hálózat eléréséhez szükséges azonosító adatok is.

Az adminisztrátori és technikai azonosítókhoz tartozó jelszavakat az informatikusnak és a szakmai alkalmazásokért felelős munkatársaknak jegyzői páncélszekrényben elhelyezett lezárt borítékban és saját nyilvántartásukban naprakészen kell tárolniuk. A saját nyilvántartásukat mások által hozzáférhetetlen helyen, lehetőség szerint titkosítva kell tárolniuk. A páncélszekrényben elhelyezett jelszavakat zárt az azonosító feltüntetésével megcímzett borítékban kell elhelyezni, melyet csak az informatikus és a jegyző által felhatalmazott személy nyithatja fel. A borítékok felnyitásáról és a jelszavak módosításáról nyilvántartást kell vezetni az alábbi adatokkal:

- a felnyitást és módosítást végző személy neve,
- a felnyitás és módosítás oka,
- a felnyitás és módosítás dátuma.

Az alkalmazásoknál használt jelszavakra esetében törekedni kell a felhasználói jelszavak esetében meghatározott komplexitási beállítások érvényesítésére.

8.4 Felhasználó felelősségi köre

Az informatikai rendszer felhasználójának felelősségi körébe tartozik a munkája során megismert, felhasznált és létrehozott számítógépes és egyéb adatok védelme a használatában lévő berendezések és alkalmazói szoftverek üzemszerű használata.

A jelszóhasználatra vonatkozó szabályok, előírások betartásáért minden felhasználó személyesen felelős. A felhasználóknak a jelszó illetéktelenek általi megismerését minden eszközzel el kell kerülni.

Amennyiben a felhasználó a munkaállomást felügyelet nélkül hagyja, köteles azt zárolni, készenléti állapotba helyezni vagy jelszavas képernyőkímélő használatával az illetéktelen hozzáférést meggátolni. Amennyiben ezt a munkaállomáson futó operációs rendszer nem teszi lehetővé, vagy a munkaállomást több személy is használhatja, úgy minden felhasználónak, munkája végeztével, minden futó programból ki kell jelentkeznie.

Az azonosítóval történő bejelentkezéstől a kijelentkezésig az adott munkaállomás illetéktelen hozzáférés elleni védettségéért, a bejelentkezett munkaállomáson végzett minden tranzakcióért a bejelentkezett azonosítóval rendelkező a felelős. A felelősség abban az esetben is fennáll, ha megállapítható, hogy a jelen szabályzat szerinti előírások be nem tartásából eredően a tranzakciókat ténylegesen harmadik – illetéktelen – személy hajtotta végre.

A munkaállomásokon adatot tárolni nem szabad, az adatokat központilag létrehozott és rendszeresen mentett, szerveren lévő könyvtárakba kell menteni.

8.5 Hozzáférés ellenőrzés az operációs rendszereken

A munkaállomásra történő bejelentkezési eljárása során a felhasználónak felhasználói azonosító adatot és jelszót kell megadnia. A hitelesítő adatokat az informatikus adja ki és saját nyilvántartásában kezeli azokat.

A biztonságos bejelentkezési folyamattal szemben támasztott követelmények:

- a munkaállomásra utolsóként bejelentkező felhasználó azonosítójának elrejtése új bejelentkezéskor,
- bejelentkezési eljárás alatt a munkaállomás nem adhat olyan hibaüzenetet, amely a jogosulatlan felhasználót segíthetné,
- a megengedett bejelentkezési kísérletek maximális száma 5 lehet, ezután a felhasználói azonosító inaktív állapotba kell tenni,
- a sikertelen bejelentkezéseket naplózni kell.

Az operációs rendszer informatikus által beállított – a rendszer üzemszerű működéséhez hozzátartozó - tulajdonságait (beállítások, paraméterek, megjelenés, képernyőkímélő, registry, stb.) megváltoztatni tilos. Az operációs rendszer egyéb beállításait az informatikus által kiosztott jogosultságoknak megfelelően a felhasználók állítják be.

A Hivatal szervezeti egységei által használt számítógépeken bármilyen szoftvert - így operációs rendszert is - telepíteni kizárólag az informatikus jogosult.

A legtöbb szerver számítógéprendszer rendelkezik olyan segédprogramokkal, melyek képesek a rendszer- és alkalmazásvezérlések hatástalanítására. Ezek használatát a Hivatal informatikai rendszereiben korlátozni, és szigorúan ellenőrizni kell, az alábbiak betartásával:

- a rendszer segédprogramjaihoz hitelesítő eljárást kell alkalmazni,
- a rendszer segédprogramjait külön kell választani az alkalmazási szoftvertől,
- a rendszer segédprogramjainak használatára feljogosítottak körét a szükséges és elégséges felhasználók legszűkebb csoportjára kell korlátozni,
- a rendszer segédprogramok használatát teljes körűen naplózni kell,
- a rendszer segédprogramok használatára jogosultak körét és a feljogosítási szinteket dokumentálni kell,
- a Hivatal informatikai rendszerében használt operációs rendszerek valamennyi olyan segédprogramját el kell távolítani, amelyek használata az adott környezetben a feladatellátáshoz - beleértve az informatikai rendszer üzemeltetését is – szükségtelen. Ezen programok körének meghatározása az informatikus feladata.

8.6 Kritériumok az alkalmazás hozzáférésekhez

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.

Minden felhasználónak jelszóval kell védenie hozzáféréseit. Ezeket a jelszavakat illetéktelen személyektől gondosan védeni kell.

Az alkalmazásokkal szembeni biztonsági elvárásokat be kell tartani a következők szerint:

- ellenőrizzék a felhasználói hozzáférést,
- kerüljék el más, olyan rendszerek biztonsági veszélyeztetését, amelyekkel az adott rendszer osztozik valamely informatikai erőforrás használatában,
- legyenek képesek személyi és csoportszintű hozzáférés kezelésére,
- az alkalmazói rendszerek menüszerkezetének funkcióihoz való hozzáférését folyamatosan ellenőrizni kell.

A Hivatal informatikai környezetében alkalmazott rendszerek felhasználói és üzemeltetői kizárólag a munkavégzéshez elengedhetetlenül szükséges és elégséges mértékben rendelkezhetnek hozzáféréssel mind az informatikai funkciókhoz, mind az alkalmazási rendszer funkcióihoz, szolgáltatásaihoz. Ezen elvárások biztosítása érdekében:

- A felhasználói dokumentumok szerkesztésével biztosítani kell, hogy minden felhasználó a dokumentációnak kizárólag ahhoz a részéhez férjen hozzá, amely funkciókhoz jogosultsággal rendelkezik,
- a felhasználók hozzáférési jogainak szabályozását valamennyi alkalmazásrendszer esetében az alkalmazás megrendelő, felügyelő szervezeti egységnek részletesen ki kell dolgozni (írás, olvasás, törlés és végrehajtás joga kit és milyen mértékben illet meg),
- az információs eszközökön továbbítható, védett információt kezelő alkalmazási rendszerek kimenetei csak annyi információt tartalmazhatnak, amennyi az adott kimeneten minimálisan elégséges, és csakis az arra illetékes terminálokra nyomtatókra és helyszínekre legyenek továbbítva.

Az okmányiroda rendszerek esetében a kártyás belépéshez használt azonosító eszközöket (kártyákat) és a hozzájuk tartozó PIN kódokat biztonságosan, egymástól elkülönítve kell tárolni.

9 Naplózás és elszámoltathatóság

9.1 Monitorozás

Az elektronikus információs rendszerek figyelemmel kísérésének eszköze az eseménynaplók adatainak gyűjtése és feldolgozása. Be kell vezetni a felhasználói tevékenységekre és a technikai eseményekre vonatkozó naplózást is.

A naplógyűjtést és feldolgozást oly mértékben automatizálni kell, hogy a kritikus események nyomán riasztás keletkezzen és a rendszeradminisztrátorok haladéktalanul tudjanak intézkedni.

9.2 Naplózási eljárásrend

Létre kell hozni az Informatikai területen a naplózás részletszabályait tartalmazó *naplózási eljárásrendet*, amelyben a naplózás és a hozzá tartozó ellenőrzések megvalósulását segíti.

9.2.1 A rendszer használat monitorozása

Az informatikai infrastruktúra működésének és felhasználásának ellenőrzésére felügyeleti eszközöket kell alkalmazni, amelyek probléma esetén meghatározott módon riasztást adnak az illetékes rendszergazda számára. A megfigyelendő paramétereket és riasztási értékeket kockázatértékelés alapján kell meghatározni, meg kell határozni a naplózható és naplózandó eseményeket, s erre fel kell készíteni az elektronikus információs rendszert.

A megfigyelések terjedjenek ki technikai paraméterek ellenőrzésére, továbbá az eszközökhöz és szolgáltatásokhoz történő hozzáférésre is.

Az alábbi események naplózását feltétlenül be kell állítani, amennyiben az alkalmazás ezt lehetővé teszi:

a. a felhasználók tevékenysége,
b. az adatállományok (adatbázisok) módosítása az alkalmazói rendszerekben,
c. lekérdezések és jogosulatlan lekérdezési kísérletek,
d. az üzemeltetők operációs rendszerbe történő be-és kijelentkezése,
e. az üzemeltetők tevékenysége az operációs rendszerben,
f. a hozzáférési jogosultságok módosítása,
g. operációs rendszer események, esetleges hibák,
h. hálózati menedzsment riasztások,
i. konfigurációs beállítások módosítása,
j. jogosulatlan hozzáférési kísérletek, az egyes rendszerek detektálási képességein belül.

A naplózható események fedjék le az alkalmazások működését és az alapinfrastruktúrát oly mélységben, hogy megfelelőek legyenek a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

A naplóbejegyzésekben legyen elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

9.2.2 Napló információk védelme

A naplóinformációk keletkezésük után is szükségesek lehetnek az üzemeltetési vagy információbiztonsági incidensek utólagos kiértékelése céljából, továbbá illegális beavatkozások esetén azok bizonyítására is felhasználhatók.

A naplóinformációkat a naplókezelő eszközöket meg kell védeni az jogosulatlan hozzáféréstől és az utólagos megváltoztatástól vagy törléstől. Meg kell oldani, hogy a rendszeradminisztrátorok ne tudják utólagosan módosítani a naplóbejegyzéseket, és ezzel a saját tevékenységükre vonatkozó információkat megmásítani.

A naplóbejegyzéseket napi gyakorisággal ellenőrizni és elemezni kell a nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából. Rendellenes jelenség esetén azt jelenteni kell az illetékes vezetőknek.

Amennyiben jogszabály egyes esetekben másképp nem rendelkezik, a naplóállományokat legalább egy évig meg kell őrizni.

9.3 Naplógenerálás és ellenőrzés

A naplózó funkcionalitásnak biztosítania kell naplóbejegyzés generálását az előre meghatározott, naplózható eseményekre. A naplózott eseményeket az arra feljogosított rendszeradminisztrátorok állíthatják be.

A normálistól eltérő működési jellemzők megállapítása az üzemeltető feladata.

Az egyes naplók tartalmának ellenőrzését, kiértékelését előre meghatározott ütemtervnek megfelelően kell végezni, a feljegyzésre kerülő események mennyisége alapján megállapított gyakorisággal. Az ellenőrzéseket az adott rendszerek üzemeltetői végzik. Az ellenőrzések elvégzését dokumentálni kell. Az ellenőrzés végrehajtását az informatikus háromhavonta felülvizsgálja. A felülvizsgálat tényét, és az esetleges megállapításokat jegyzőkönyvben kell rögzíteni.

9.3.1 Naplózási hibák kezelése

Az elektronikus információs rendszerek naplózó funkciójának alkalmasnak kell lennie arra, hogy az informatikai alkalmazás és infrastruktúra naplózási hibája esetén riasztást küldjön az illetékes rendszergazdának, s ezzel párhuzamosan végrehajtsa azokat a tevékenységeket, amelyeket a rendszer biztonságának fenntartása érdekében el kell végezni (például rendszer leállítás, régi naplóbejegyzések felülírása, naplózás leállítása)

9.3.2 Időszinkronizálás

A Hivatal információ-feldolgozó rendszerének óráit egymással, illetve egy hiteles külső időforrással szinkronizálni kell.

A rendszeres szinkronizálás azért szükséges, mert a berendezések belső órái eltolódnak, továbbá más módon nem biztosítható azok együttes működése.

Ez szükséges lehet üzemeltetési események kivizsgálásánál, vagy bizonyítékként jogi vagy fegyelmi esetekben. A nem szinkronizált bejegyzések akadályozhatják ezeket a kivizsgálásokat és árthatnak az ilyen bizonyíték hitelességének.

A szervezeten belül ki kell jelölni egy pontos idő szervert, vagy szervereket, amelyekhez a többi berendezés szinkronizál. Az idő-szerver a pontos időt lehetőség szerint valamelyik hitelesített külső NTP szerverről kérje le.

9.3.3 Mobil számítástechnika és telekommunikáció

Mobil számítástechnikai és kommunikációs berendezések használata során, mint pl. notebook, tablet, mobiltelefon vagy pendrive, különleges gondot kell fordítani arra, hogy működési információ ne legyen veszélyeztetve. Tekintettel kell arra lenni, hogy a laptopoknak nincsen központi mentése, ezért az adatok mentéséért a laptop felhasználója felel.

A mobil telefonokon és táblagépeken be kell állítani az automatikus jelszavas vagy grafikus képernyőzárat, ezért az eszköz használója felel. Tilos megváltoztatni vagy hatástalanítani a mobil készülék védelmi rendszerét, tűzfalat, vírusvédelmet kikapcsolni vagy az operációs rendszer védelmi beállításait átállítani.

Engedélyezni kell a biztonsági frissítések automatikus telepítését.

Nyilvános helyen történő laptop használatnál az eszköz fizikai biztonsága mellett bizalmas adatokkal történő munka esetén ügyelni kell arra, hogy a képernyőre ráláthatnak arra nem jogosult személyek is.

Nyilvános WiFi (hot-spot) használata esetén tudatában kell lenni annak, hogy az eszközzel végzett kommunikáció lehallgatható, visszafejthető.

A mobil eszközök biztonságáról, adat és vagyonvédelmi szempontjairól a felhasználók számára tartott biztonsági tudatossági oktatás keretében külön hangsúly kell fektetni arra, hogy a telefonon keresztül bizalmas adatokhoz férhetnek hozzá.

A Hivatal tulajdonát képező mobil eszközökön a felhasználók nem engedélyezett tartalmú adatot (illegális szoftvereket, filmeket, zenéket) nem tárolhatnak. A rendelkezés megszegéséből bekövetkező jogvédelmi károk megtérítéséért a felhasználó a felelős.

Az eszközöket védeni kell az ellopástól, biztonságosan, zárt táskában kell szállítani, nem szabad őrizetlenül hagyni és nem hagyhatók gépkocsi csomagtartójában sem.

A mobil eszközökön bizalmas adatok csak titkosítva tárolhatók. A laptopoknak nincsen automatikus mentése, az adatok megőrzéséről és mentéséről a felhasználónak kell gondoskodnia.

Okostelefon, tablet eszköz használata esetén a felhasználó köteles a levelek szinkronizálásból eredő biztonsági kockázatok csökkentését az érzékeny levelek illetéktelen hozzáférésekkel szembeni megvédésével vagy a levél törlésével biztosítani.

A Hivatal tulajdonát képező eltávolítható adathordozókra (CD/DVD, memóriakártyák, pendrive-ok), az információbiztonsági intézkedések betartásával szabad adatokat másolni. Magántulajdonú adathordozók használata tilos.

9.4 Távoli elérés

A Hivatal informatika rendszerének távoli elérése csak az információbiztonsági eljárások és a hálózat biztonsági előírások figyelembe vételével, egyedi engedély alapján lehetséges.

Az elérések során kriptográfiai eszközökkel meg kell akadályozni a kommunikáció lehallgatását.

A Hivatal informatikai rendszeréhez történő hozzáférést a rendszertámogatást végző vállalkozások távoli kapcsolatát az informatikus felügyeli. A támogatást végző külső munkatársakat egyedileg kell azonosítani.

9.5 Alkalmazói rendszerek biztonsága

A Hivatal informatikai rendszerében csak a törvényi előírások által engedélyezett alkalmazások telepíthetők.

A Hivatal által fejlesztett vagy fejlesztetett alkalmazásokra vonatkozó biztonsági előírásokat az IBSZ-hez kapcsolódó egyéb üzemeltetési szabályozás tartalmazza.

10 Változáskezelés

Az információ-feldolgozó eszközök és rendszerek változtatásait szigorú változtatáskezelési eljárás alá kell vonni. A változáskezelés célja, hogy az informatikai üzemeltetés napra készen követni tudja a konfigurációk változásait, ismerje a pillanatnyi állapotát, hiba felmerülése esetén pedig annak oka könnyebben kideríthető legyen.

Változásnak minősül az informatikai környezetben minden hardver és szoftver átalakítás, bővítés, konfigurálás, beállítások megváltoztatása. Változásként kell kezelni a telekommunikációs és hálózati eszközök bárminemű módosítását is.

Változások jóváhagyására döntési fórumot kell kialakítani, melyben az esetlegesen érintett szakmai területeknek is képviseltetniük kell magukat.

Egy változást akkor lehet bevezetni, ha megtörténik:

a) a lehetséges *hatások felmérése*, beleértve a változtatások biztonsági hatásait,

b) megtörténik a megfelelő szintű *jóváhagyás* a javasolt változtatásokra,

c) a tervezett változtatás sikeresen *tesztelve lett*,

d) elkészültek *visszalépési eljárások*, (backup eljárások), arra az esetre, amennyiben a változás előre nem látott körülmények miatt sikertelen lenne,

e) megtörténik a változtatások részletes *közlése* minden érdekelt személlyel.

A változásokkal kapcsolatos tennivalók:

a) a változtatást csak feljogosított felhasználók végezhetik,

b) az érintett infrastruktúra elemek (hardver, szoftver, adatbázis stb.) azonosítása, amelyet a módosítás érint,

c) hivatalos jóváhagyás a feladatokra,

d) dokumentációk frissítése,

e) régi verziók archiválása,

f) változás részletes dokumentálása,

g) aktualizálni kell az üzemeltetési dokumentációt

h) biztosítani kell a bevezetés tervezett végrehajtását és az üzemeltetés zavartalanságát.

i) a változásokat az ügymenet folytonossági tervekben át kell vezetni.

A változásokat a visszakereshetőség érdekében dokumentálni kell, mely dokumentumnak része kell, hogy legyen a teljes változási dokumentáció, a hatásfelmérés, a teszteredmények, a visszalépési eljárások és a jóváhagyási dokumentumok.

Az adminisztrációs terhek csökkentése és az operatív működés támogatása érdekében meg kell határozni azon kisebb hatású változások körét, amelyeket előzetes engedélyezés nélkül is végre lehet hajtani, ezeket nevezzük „kisebb sztenderd változásoknak". Ilyenek lehetnek például egyes hálózati vagy tűzfal beállítások.

11 A folyamatos rendelkezésre állás (ügymenet folytonosság) és a helyreállítás tervezése

A Hivatali informatikai infrastruktúráját úgy kell kialakítani, hogy az biztosítsa a folyamatos ügymenet kezelést. Az informatikai rendszereket rendelkezésre állásuk, a rajtuk tárolt adatok kiesési és visszaállítási idejük figyelembe vételével kell priorizálni.

A szerverek és munkaállomások tekintetében gondoskodni kell a szerverek és munkaállomások zavartalan áramellátásáról, a feszültség ingadozások kivédéséről valamint biztosítani kell az eszközök áramszünet bekövetkezésekor történő biztonságos leállításukat, ezzel is csökkentve az adatvesztés kockázatát.

Az ügymenet folytonosság érdekében biztosítani kell, hogy:

a) Az informatikus meghatározott gyakorisággal mentést végezzen az elektronikus információs rendszerben tárolt felhasználószintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;

   i. meg kell határozni minden elektronikus információs rendszerre vonatkozóan a mentések szükséges gyakoriságát, a mentendő adatok körét.

   ii. a mentésekre vonatkozó igényeket összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal (RPO, RTO) a szakmai területekkel egyeztetve kell kialakítani.

b) Az informatikus meghatározott gyakorisággal mentse az elektronikus információs rendszerek dokumentációját, köztük a biztonságra vonatkozókat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;

c) védjék meg a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen.

d) A legfontosabb adatokról az informatikus a szakmai igények szerinti gyakorisággal és részletezettséggel végezzen archiválást.

e) A mentési és archiválási adathordozókat azonosító sorszámmal lássák el és azokról vezessenek nyilvántartást.

f) Az archiválásokat és mentéseket tartalmazó adathordozókon jól láthatóan és azonosíthatóan fel kell tüntetni az adathordozó azonosítóját. A mentések és archiválások típusát és idejét az eszközöktől függő módon, manuálisan vagy elektronikusan nyilván kell tartani.

g) Az archiválásokat és mentéseket tartalmazó adathordozókat a hálózati meghajtóktól és szerverektől elkülönített épületben, zárt helyiségben vagy szekrényben kell őrizni.

h) Rendszeresen ellenőrizni kell a mentések és archiválások helyreállíthatóságát, tesztelni kell a mentett információkat, az adathordozók megbízhatóságának és az információ sértetlenségének garantálása érdekében.

A szerverek és a hálózati eszközök rendelkezésre állását és katasztrófa helyzetben lefolytatandó eljárásokat, kiesési időhatárokat, a rendszerek biztonságos és folyamatos működését lehetővé tevő, rendszerenkénti hideg és meleg tartalékokat az *ügymenet folytonosságot szabályozó tervek* tartalmazzák.

Az ügymenet-folytonossági terv kidolgozása során az alábbi szempontokat kell figyelembe venni:

a) elektronikus információs rendszer vagy a működtetési környezet változásainak, az, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálni kell az üzletmenet-folytonossági tervet;

b) tájékoztatni kell az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket;

c) gondoskodni kell arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható;

d) meg kell határozni az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;

e) rendelkezni kell a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről;

f) ki kell jelölni a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket;

g) fenn kell tartani a Hivatal által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is;

h) ki kell dolgozni a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket;

i) meg kell határozni az alapfunkciók újrakezdésének időpontját az üzletmenet-folytonossági terv aktiválását követőn.

A folyamatos működésre felkészítő képzést kell tartani a felhasználóknak, szerepkörüknek és felelősségüknek megfelelően, szerepkörbe vagy felelősségbe kerülésüket követő meghatározott időn belül, továbbá éves gyakorisággal, vagy amikor az elektronikus információs rendszer változásai ezt szükségessé teszik.

11.1 Helyreállítások

A mentésekből helyreállítást abban az esetben kell elvégezni, ha az éles üzemi adatállomány megsérült. Felhasználói véletlen adattörlés esetén az adatok helyreállítása kizárólag az illetékes adatgazda írásos igénye alapján végezhető.

12 MEGFELELŐSÉG

12.1 Megfelelés a jogi követelményeknek

A Hivatal célja, hogy minden esetben eleget tegyen a rá vonatkozó törvényi, jogi szabályozási és szerződéses kötelezettségeinek.

12.1.1 A szellemi tulajdonjogok

A szellemi tulajdonjogok védelmével kapcsolatos feladatok a számítástechnikai rendszerekben használt programok, alkalmazások jogszerű használatával kapcsolatos kötelezettségekben, továbbá a Hivatal informatika eszközein tárolt, esetlegesen jogvédett állományok helyes kezelésében testesülnek meg. Általános esetben ez a védelem vonatkozik mindenféle szerzői joggal védett termék, könyv, dokumentáció, zene és egyéb műalkotás védelmére is.

Alapvető feladatok és tudnivalók a szellemi tulajdonjogok védelmével kapcsolatban:

a) a Hivatal informatikai rendszerében csak jogtiszta (tisztázott eredetű, legálisan használt) programok használhatók,

b) szoftvereket csak legális forrásból, dokumentált módon szabad beszerezni, a beszerzést igazoló dokumentumokat meg kell őrizni,

c) a nem kereskedelmi, nyílt forráskódú szoftverek esetében figyelembe kell venni a szoftverhez kapcsolódó felhasználási szabályozást,

d) a telepített szoftverekről nyilvántartást kell vezetni és a felhasználást időszakonként ellenőrizni (erre megfelelnek a számítástechnikai eszközökkel készített leltárak),

e) biztosítani kell, hogy a felhasználói licencszerződésnek (End User Agreement) megfelelően történjen a szoftverek használata, továbbá teljesüljenek a szoftver használatára előírt korlátozások, processzor típus, felhasználószám stb. tekintetében,

f) biztosítani kell, hogy a szoftverek telepítő lemezei és dokumentációja csak az engedélyezett feltételek mellett kerüljön felhasználásra, (a szoftverek archiválási célú lemásolása nem minősül a szerzői jog megsértésének),

g) a Hivatal megbízásából kifejlesztett szoftverek felhasználási feltételeit és tulajdonjogát a fejlesztési szerződésben tisztázni kell,

h) biztosítani kell, hogy a Hivatal számítástechnikai rendszerein ne kerüljenek tárolásra olyan anyagok, amelyek jogvédelem alá esnek és a Hivatal nem rendelkezik a felhasználási jogokkal (filmek, zenék, könyvek stb.),

i) csak akkor szabad részben, vagy teljesen könyveket, cikkeket, beszámolókat vagy más dokumentumokat másolni, ha a szerzői jog megengedi.

A szerzői és szomszédos jogok tiszteletben tartása, továbbá az információbiztonsági szabályok betartása miatt a munkavállalóknak tilos munkaállomásukra bárminemű szoftver telepítése, illetve bármilyen, nem a Hivatal tulajdonát képező állomány felmásolása (képek, zenék, filmek stb.). Ennek az előírásnak a megsértése az információbiztonsági előírások durva megszegése, amelyért a dolgozónak vállalnia kell a munkajogi és büntetőjogi (kártérítési) felelősségeket.

12.1.2 A szervezeti feljegyzések védelme

A Hivatal működésével kapcsolatos adatokat, dokumentumokat részben törvényi előírások, részben szerződési, szabályozási vagy ügyviteli követelmények miatt meg kell őrizni (archiválás)

A megőrzendő anyagok lehetnek elektronikus vagy papír alapú anyagok, adatbázisok, listák, tranzakciós naplók, audit naplók, szerződések. Az adathordozó lehet papír, mikrofilm vagy különféle elektronikus adathordozó. Amennyiben titkosított anyag kerül megőrzésre, gondoskodni kell arról, hogy a hozzá tartozó kriptográfiai kulcs is megőrzésre kerüljön.

Meg kell határozni a feljegyzések és információk megőrzésére, tárolására, kezelésére és selejtezésére vonatkozó irányelveket:

a) a megőrzésre kerülő információk körét, a megőrzés időtartamát az adatgazda határozza meg a jogi és működési követelményekkel összhangban,

b) biztosítani kell a tárol információt az elvesztés, megsemmisülés és a hamisítás ellen,

c) gondoskodni kell a tárolt információ megőrzéséről a megőrzési időszak alatt

   a. biztosítani kell az adathordozó épségét és olvashatóságát, a gyártói előírásokkal összhangban

   b. technológiaváltás esetén is gondoskodni kell a visszaolvashatóságról, az adatok átírásával,

   c. biztosítani kell az adatok elvárt időn belüli és megfelelő formátumú kinyerhetőségét,

12.1.3 Adatvédelem és a személyes információ védelme

Az érintettek információs önrendelkezésével kapcsolatos jogainak biztosítása és érvényesítése a személyes információk vonatkozó jogszabályok szerinti kezelése alapján biztosított.

12.1.4 Felhő alapú adattárolás és fájl megosztó szolgáltatások

A Hivatal informatikai rendszerén kívüli, internetes felhő alapú adattárolás, továbbá fájl megosztó szolgáltatások használata általában tilos. Hazai felhő alapú tárhely csak megbízható szolgáltatótól vehető igénybe, egyedi jegyzői engedély alapján.

Külföldi tárhely-szolgáltatás igénybe vétele csak a jegyző jóváhagyásával, az Elektronikus Információbiztonsági Hatóság (NEIH) előzetes engedélye alapján történhet.

13 Információbiztonsági tudatosság és képzés

Annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést kell nyújtani az elektronikus információs rendszer felhasználói számára. Az informatikai biztonság tudatosítására irányuló tevékenység és képzés az érintett szervezet összes közszolgálati, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekintetében kötelező.

Informatikai és információbiztonsági képzéseket kell tartani:

- új belépők részére, munkába álláskor, az elektronikus információs rendszerhez való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően;
- munkakör változása esetén;
- amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
- éves rendszerességgel, információbiztonsági frissítő jelleggel.

A képzések megtörténtét és az ellenőrző teszt eredményeit dokumentálni kell.

A képzés alkalmazkodjon a munkatárs által betöltött szerepkörhöz, feladatokhoz, illetve a használt elektronikus információs rendszerekhez.

A biztonságtudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzéseken a képzésen résztvevőkkel a képzés megtörténtét el kell ismertetni és ezt a dokumentumot meg kell őrizni.

A képzések részleteit, azok dokumentálási követelményeit *eljárásrendben* kell szabályozni.

1 sz. Melléklet: Informatikai Képzési Eljárásrend

1.1 Az Informatikai Képzési Eljárásrend célja és területi érvényessége

Az Informatikai Képzési Eljárásrend (a továbbiakban: Eljárásrend) alapvető célja, hogy a Dunakeszi Polgármesteri Hivatal felhasználói számára meghatározza az informatikai rendszer alkalmazásához szükséges biztonsági képzések kialakításának és lefolytatásának rendjét.

Annak érdekében, hogy az érintettek felkészülhessenek a lehetséges belső és külső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést kell nyújtani az elektronikus információs rendszer felhasználói számára.

A rendszeres képzések célja, hogy a felhasználók rendszeres tájékoztatást kapjanak az elektronikus információs rendszerek használata során fellépő biztonsági veszélyekről, fenyegetettségekről.

A képzéseknek ki kell terjedniük a Hivatal által használt elektronikus információs rendszerekre, azok szakmai vonatkozásaira és a fennálló jogszabályi követelményekre is.

1.2 Az Eljárásrend felülvizsgálata

Jelen eljárásrendet a Hivatal működésikörnyezetének jelentős változása esetén, illetve legalább háromévenként felül kell vizsgálni.

1.3 Az Informatikai Képzési Eljárásrend hatálya

1.3.1 Személyi hatály

Az Eljárásrend személyi hatálya kiterjed a Hivatal összes közszolgálati, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottaira, munkavállalóira, megbízottjaira (a továbbiakban: felhasználók).

A Hivatal informatikai rendszeréhez, a rendszerben tárolt adatokhoz kizárólag az Informatikai Képzési Eljárásrendben meghatározott oktatásában részesült személyek férhetnek hozzá. Az oktatás meglétének hiányában informatikai hozzáférési jogosultság nem adható ki.

1.4 Az Eljárásrendhez kötődő dokumentumok

- munkaköri leírások
- oktatásokon felvett jelenléti ívek

1.5 Képzések megtervezése

1.5.1 Új belépők képzése

A Hivatalhoz belépő, új felhasználók részére informatikai bevezető és tájékoztató alapképzést kell tartani. A képzés igazodjék a belépő által betöltött munkakörhöz.

A kezdeti informatikai képzés terjedjen ki az alapvető felhasználói ismeretek átadására, a Hivatalban kialakított jogosultsági rendre, annak igénylési folyamatára, az informatikai kiszolgáló infrastruktúra helyes használatára.

Az információbiztonsági oktatásnak a munkakör igényei szerint

a) alkalmazkodnia kell az alkalmazott által betöltött feladatkörhöz,

b) tartalmaznia kell az ismert fenyegetésekre történő felkészülést,

c) ismertetnie kell az információbiztonság belső szervezetét

d) ismertetnie kell az információbiztonsági fenyegetések felismerésének módját és a szükséges intézkedéseket, eszkalációt.

1.5.2 Képzés munkakör változásakor

A felhasználók számára az új munkakör (szerepkör) átvételét megelőzően kiegészítő képzést kell tartani, az új munkakör informatikai sajátosságainak (rendszereinek) és információbiztonsági követelményeinek ismertetésével.

1.5.3 Rendszeres információbiztonsági frissítő képzés

Évente legalább egy alkalommal, valamennyi felhasználóra kiterjedően információbiztonság tudatossági frissítő képzést kell tartani, amelyen minden, számítógépet használó munkatársnak részt kell vennie. Az éves frissítő képzések során

a) ellenőrizni és frissíteni kell az alapvető információbiztonsági tudatossággal kapcsolatos ismereteket;

b) tájékoztatni kell a munkatársakat az újabb fenyegetésekről és az azok elleni védekezésről;

c) ismertetni kell az információ-feldolgozó eszközök helyes használatára vonatkozó tudnivalókat és változásokat;

d) tájékoztatást kell adni a szoftverjogi követelmények alapjairól;

e) frissíteni kell az információbiztonsági incidensek kezelésével kapcsolatos tudnivalókat.

A képzések megtörténtét dokumentálni kell.

A képzés alkalmazkodjon a munkatársak által betöltött szerepkörhöz, használt rendszerekhez. A képzés formája lehet csoportos vagy egyéni képzés és számonkérés, de történhet elektronikus (e-learning) formában is.

1.5.4 Rendkívüli képzések, változás esetén

Az elektronikus információs rendszerek, illetve a biztonsági környezet változása esetén rendkívüli tájékoztatást kell tartani, a változásokban érintett munkatársak számára.

1.5.5 Az informatikai és informatikai biztonságtudatossági képzések nyilvántartása és dokumentálása

A képzések megszervezéséért és dokumentálásáért a személyügyi ügyintéző felelős. A képzések megtörténtét nyilván kell tartani, az erről szóló dokumentumokat az érintett munkatársak személyi anyagában is fel kell tüntetni.

1.6 Az Informatikai Képzési Eljárásrend melléklete: Jegyzőkönyv az informatikai biztonsági oktatásról

Jegyzőkönyv informatikai biztonsági oktatásról		
Az informatikai biztonsági képzés tárgya: A képzés időpontja: A képzést megtartotta:		
A képzésen részt vettek:		
Név		Aláírás
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12,		
13.		
14.		
15.		

2 .sz. Melléklet: A Hivatal szervezeti biztonsági szintje és elektronikus információs rendszereinek osztályba sorolása

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.), továbbá a kapcsolódó, a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 41/2015. (VII. 15) BM rendelet értelmében a Hivatal

a) **szervezeti biztonsági szintje a 4. szintben került megállapításra.**

b) Az elektronikus információs **rendszereinek biztonsági osztálya**, továbbá a rendszerekhez rendelt adatgazdák személye az alábbi táblázat szerint került megállapításra:

Alkalmazás azonosítója	Osztály	Funkció/ alapfeladatok	Adatgazda / Felügyeletet gyakorló
DOK	2	Archiv pénzügyi rendszer	
EDTR	1	Egységes döntéstámogatás	dr. Németh Samu
Exchange 2013	2	Levelezés	Szabó László
Védett fájlmegosztások	2	Védett fájlmegosztások	Szabó László
FMQserver	1	nyomtató rendszer (follow me kártyás azonosítás)	Szabó László
Gordiusz	2	Pénzügyi rendszer	Pálné Kovács Mária
Govcenter	1	Telephely nyilvántartás, internetes kliens	Slisszné Kárpáti Rózsa
Govsys	2	Integrált Iratkezelő rendszer	Laczkó Szilvia
Intepsystem	2	Munkaidő nyilvántartó és beléptető rendszer	Szabó László
ITR3	1	Térképészeti rendszer	Passa Gábor
KataWin	1	Ingatlan nyilvántartó rendszer	Pálné Kovács Mária
Mikrovoks	2	Jegyzőkönyvező, szavazatszámláló, és konferencia rendszer	dr. Németh Samu
Onkado	2	Adóügyi rendszer	dr. Szarvas Alíz
WINIKSZ	2	Integrált közszolgálati szoftvercsomag	dr. Németh Samu

Indoklás a szervezeti biztonsági szint meghatározásához

A 41/2015. (VII. 15) BM rendelet 2. melléklete írja elő az elektronikus információs rendszerrel rendelkező szervezetek, vagy szervezeti egységek biztonsági szintbe sorolásának követelményeit. A besorolás szempontja a szervezet által használt elektronikus információs rendszerek adattartalma, illetve a rendszer típusa, miszerint jogszabály által kijelölt szolgáltató biztosítja-e az alkalmazást, vagy a szervezet szakfeladatait támogató rendszert alkalmaz-e. Döntő kritérium, hogy a szervezet a rendszert maga üzemelteti-e.

A követelmények alapján a **Hivatal a 4. biztonsági szintbe tartozik**, mivel a szervezet jogszabály alapján kijelölt szolgáltatókon kívül szakfeladatait támogató elektronikus információs rendszert használ, és azt üzemelteti is.

Indoklás az elektronikus információs rendszerek biztonsági osztályba sorolásához

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) hatálya alá tartozó elektronikus információs rendszerrel rendelkező szervezet az elektronikus információs rendszereit a 41/2015. (VII. 15) BM rendelet 1. mellékletében felsorolt szempontok szerint sorolja biztonsági osztályba. A rendszereket a bizalmassággal, sértetlenséggel és rendelkezésre állással kapcsolatos kockázatok elemzése alapján kell az 5 szintű besorolási rendszerben elhelyezni. A biztonsági osztályok megállapítása a rendelet kritériumrendszere alapján készült.

A besorolásokat a jegyző, mint a szervezet vezetője jóváhagyta.

Cselekvési terv

Az elektronikus információs rendszerére vonatkozó elért biztonsági osztály meghatározásánál, továbbá az elért szervezeti biztonsági osztály esetében megállapított hiányosságok felszámolására *Cselekvési terv* (intézkedési terv) készült. A Cselekvési tervben dokumentálásra kerültek a megállapított hiányosságok, ezek javítására határidők, mérföldkövek kerültek meghatározásra.

Dunakeszi Polgármesteri Hivatal

IT Konfigurációkezelési Szabályzat

2019.

A DOKUMENTUM MÓDOSÍTÁSAINAK JEGYZÉKE

A dokumentum következő felülvizsgálatát 2022.06.30-ig el kell végezni.

Verzió	Dátum	Leírás	Hatályba helyező utasítás száma
V1.0	.	Első verzió	Nádor Rendszerház Kft.

TARTALOM

1 ÁLTALÁNOS RENDELKEZÉSEK

1.1 A KONFIGURÁCIÓKEZELÉSI SZABÁLYZAT CÉLJA ÉS HATÁLYA

A Konfigurációkezelési Szabályzat célja, hogy meghatározza a **Dunakeszi Polgármesteri Hivatal** (továbbiakban: Hivatal) informatikai rendszerében a biztonságos és hatékony működéshez használt hardver és szoftver konfigurációk kialakításának és kezelésének szabályait.

1.1.1 A szabályzat karbantartása

A konfigurációkezelési szabályzatot három évente felül kell vizsgálni és frissíteni kell. Felül kell vizsgálni abban az estetben is, ha az informatikai környezetben, vagy a vonatkozó jogszabályokban jelentős változás áll be.

1.2 A SZABÁLYZAT HATÁLYA

A szabályzat tárgyi hatálya kiterjed minden informatikai rendszere, felhasználóra és üzemeltetőre.

A szabályzat személyi hatálya az intézményben foglalkoztatott valamennyi közszolgálati, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottaira, munkavállalóira, megbízottjaira (a továbbiakban együtt: munkatársak) egyaránt kiterjed.
A szabályzat személyi hatálya kiterjed továbbá minden személyre, aki a Hivatal informatikai vagy azzal összefüggő rendszerét, szolgáltatásait igénybe veszi, informatikai struktúráját és annak eszközeit üzemelteti vagy használja, függetlenül a Hivatalhoz kapcsolódó jogviszonyától.

2 AZ ELJÁRÁSREND LEÍRÁSA

2.1 ALAPKONFIGURÁCIÓ

A Hivatal az elektronikus információs rendszereihez egy-egy alapkonfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges elemeit. Az alapkonfigurációkat olyan módon kell meghatározni, hogy minden működési folyamatban a nyilvántartás alapján beazonosítható legyen, hogy a működéshez milyen konfiguráció biztosítása szükséges. Ezen alapkonfigurációs leírásokat dokumentált formában biztonságos helyen kell tárolni és megőrizni. Az alapkonfigurációs leírások elkészítéséért és aktualizálásáért az informatikus a felelős.

A dokumentációnak minimálisan a következő elemeket kell magában foglalnia:

a) Hardver elemek;

b) Szoftverek;

c) Telepítőkészletek;

d) Egyes szoftverkomponensek alapkonfigurációi.

Minden, az alapkonfigurációkban meghatározott szoftver telepítő készletéről biztonsági mentéssel kell rendelkezni. Virtualizált rendszerek esetében célszerűen teljes alkalmazás image kerüljön mentésre.
A tárolt alapkonfigurációkat évente át kell tekinteni, az alapkonfiguráció el kell elvégezni.

2.1.1 Korábbi konfigurációk megőrzése

Változatlan állapotban meg kell őrizni az elektronikus információs rendszer alapkonfigurációját és annak korábbi verzióit, hogy szükség esetén lehetővé váljon az erre való visszatérés.

2.2 A KONFIGURÁCIÓVÁLTOZÁSOK FELÜGYELETE (VÁLTOZÁSKEZELÉS)

A változáskezeléssel kapcsolatosan az Informatikai Biztonsági Szabályzat 10. fejezetének előírásait kell alkalmazni.

2.3 KONFIGURÁCIÓS BEÁLLÍTÁSOK

A Hivatal meghatározza a elektronikus információs rendszerei működési követelményeinek még megfelelő, de biztonsági szempontból a lehető leginkább korlátozott módon - a "szükséges minimum" elv alapján - az elektronikus információs rendszerben használt információtechnológiai termékekre kötelező konfigurációs beállítást, és ezt ellenőrzési listaként dokumentálja;

- elvégzi a konfigurációs beállításokat az elektronikus információs rendszer valamennyi elemében;
- a meghatározott elemek konfigurációs beállításaiban azonosít, dokumentál és jóváhagy minden eltérést;
- figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait.

A konfigurációs beállítások felügyeletéért felelős az informatikus.

Az informatikai berendezések konfigurációs beállításait óvni kell a jogosulatlan, véletlen vagy rosszindulatú módosításoktól, ezeket minden esetben megfelelő szintű jogosultsághoz, felhasználó azonosításhoz kell kötni. A gyártói név/jelszó azonosítókat („default jelszavak") minden esetben meg kell változtatni. Ahol lehetséges, tiltani kell, illetve szoftveresen felügyelni kell a felhasználói alkalmazás telepítési kísérleteket.

A felhasználók nem rendelkezhetnek rendszergazdai jogosultságokkal.

2.4 LEGSZŰKEBB FUNKCIONALITÁS

Az informatikai rendszer komponenseit „a szükséges, minimális jogok elve alapján" úgy kell konfigurálni, hogy csak azok a szolgáltatások, portok, protokollok legyenek engedélyezve, melyek a rendszer biztonságos működéséhez szükségesek.

Az engedélyezett és tiltott, vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek listáját a rendszerdokumentációban kell rögzíteni.

A legszűkebb funkcionalitás elvének gyakorlati megvalósítását a konfigurációs beállítások ellenőrzése során is vizsgálni kell a szolgáltatás menedzsereknek. Az ellenőrzés eszközei lehetnek a következő módszerek:

- telepített szoftver modulok lekérdezése,
- véletlenszerű mintavételes ellenőrzés egy adott konfiguráció esetén,
- engedélyezett portok listájának összevetése a lekérdezésekkel; stb.

2.5 ELEKTRONIKUS INFORMÁCIÓS RENDSZERELEM LELTÁR

Az informatikai rendszer valamennyi hardver/szoftver eleméről nyilvántartást kell vezetni. A nyilvántartásnak tartalmaznia kell a kiszolgálók, a munkaállomások, a hálózati és egyéb informatikai eszközök pontos és naprakész hardver és szoftver konfigurációját, az elhelyezkedésüket, a működő alkalmazások egyedi beállításait és az értük felelős személy (támogató) nevét, továbbá a vonatkozó rendszerdokumentációt.

A leltár folyamatos vezetéséért és aktualizálásáért az informatikus a felelős.

2.6 A SZOFTVERHASZNÁLAT KORLÁTOZÁSAI

Az informatikai rendszer működtetése során kizárólag jogtiszta, a megfelelő licence-el rendelkező szoftvereket lehet használni. Szabad (nyílt forráskódú) szoftverek vagy egyedi fejlesztésű cél alkalmazások használatbavételéről általános esetben az informatikus javaslatát figyelembe véve, a jegyző dönt. Ezen szoftvereket használatba vétel előtt biztonságos körülmények között tesztelni kell, különös tekintettel adatszivárgások megelőzésére vagy jogosulatlan adatkezelési, rendszer módosítási tevékenység felfedésére. Szoftverek telepítését csak az informatikus, vagy felügyelete mellett külső szakértők végezhetik.

Az alkalmazott szoftverekről a vonatkozó jogszabályoknak is megfelelő leltárt kell vezetni. A felhasznált szoftverek esetében a hivatalnak rendelkeznie kell a felhasználási jogokkal (jogtisztaság).

2.7 A FELHASZNÁLÓ ÁLTAL TELEPÍTETT SZOFTVEREK

A felhasználók munkaállomásukról csak az előre telepített helyi vagy engedélyezett hálózati alkalmazásokat, erőforrásokat érhetik el. Ezen beállítások megváltoztatása a felhasználók számára tilos.

Tilos a felhasználók számára bármilyen alkalmazás internetről történő telepítése vagy futtatása. Tilos standalone vagy portable (telepítés nélkül használható) alkalmazások engedély nélküli használata.

DUNAKESZI VÁROS JEGYZŐJE

Jóváhagyta:

Dunakeszi Polgármesteri Hivatal

Naplózási Szabályzat

Készítette:

Vádor RENDSZERHÁZ

Dunakeszi, 2019.

A DOKUMENTUM MÓDOSÍTÁSAINAK JEGYZÉKE

A dokumentum következő felülvizsgálatát 2019.06.30-ig el kell végezni.

V1.0		Első verzió	Nádor Rendszerház Kft.
Verzió	**Dátum**	**Leírás**	**Hatályba helyező utasítás száma**

TARTALOM

1 ÁLTALÁNOS RENDELKEZÉSEK

1.1 A SZABÁLYZAT CÉLJA ÉS HATÁLYA

A Naplózási Szabályzat célja, hogy meghatározza a **Dunakeszi Polgármesteri Hivatal** (továbbiakban: Hivatal) informatikai rendszerében alkalmazott naplózás folyamatát, továbbá az azokhoz kapcsolódó ellenőrzések megvalósítását.

1.1.1 A szabályzat karbantartása

A Naplózási Szabályzatot évente felül kell vizsgálni és frissíteni kell. Felül kell vizsgálni abban az esetben is, ha az informatikai környezetben, vagy a vonatkozó jogszabályokban jelentős változás áll be.

1.2 A SZABÁLYZAT HATÁLYA

A szabályzat hatálya kiterjed a Hivatal elektronikus információs rendszereire, függetlenül attól, hogy a rendszer saját üzemeltetésű vagy a Hivatal részére szolgáltatásként nyújtja harmadik fél.

2 NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

2.1 NAPLÓZHATÓ ESEMÉNYEK MEGHATÁROZÁSA ÉS BEÁLLÍTÁSA

A naplózást úgy kell kialakítani, hogy minden rendszer legalább a következő eseményeket tudja naplózni:

a) a felhasználók adminisztrációs tevékenysége:
   i. bejelentkezés;
   ii. kijelentkezés;
   iii. jelszómódosítás.
b) az adatállományok (adatbázisok) módosítása az éles alkalmazási rendszerekben;
c) a rendszergazdák a rendszer bármely rétegébe (éles/teszt/fejlesztői) történő be-és kijelentkezése;
d) a rendszergazdák tevékenysége (éles/teszt/fejlesztői) a rendszer bármely rétegében;
e) a felhasználói jogosultságok módosítása;
f) rendszer események, esetleges hibák;
g) konfigurációs beállítások módosítása (operációs rendszer szintű változások);
h) naplózási paraméterek megváltoztatását.

2.2 NAPLÓBEJEGYZÉSEK SZÜKSÉGES TARTALMA

Az információs rendszerek naplóbejegyzéseit úgy kell kialakítani, hogy azok gyűjtsenek be elegendő információt arra vonatkozóan, hogy

- milyen események történtek,
- mi volt az események oka,
- és mi volt ezen események kimenetele, következménye.

A naplóbejegyzéseknek minimálisan a következőket kell tartalmazniuk:

a) a rendszerelem azonosítóját,

b) az adatazonosítót (fájl / rekord / mező),

c) az esemény ismertetését / a funkcióazonosítót,

d) a felhasználó azonosítóját,

e) az esemény időpontját,

f) az esemény elemzéséhez szükséges adattartalmakat, vagy az arra vonatkozó hivatkozásokat, illetve annak végrehajtási státuszát.

A naplóbejegyzések szükséges minimális tartalmáról az érintett hivatali szakterületeknek egyeztetniük kell.

2.3 Naplóvizsgálat és jelentéskészítés

Az üzemeltetésért felelős személyeknek, beszállító partnereknek a felelősségük alá tartozó rendszerek naplóállományait ellenőrizni kell hibák, rendellenességek után, s szükség esetén javító intézkedéseket tennie a felettes vezető tájékoztatása mellett.

Az informatikus feladata és kötelessége a rendszerek monitorozása és az üzemeltetési naplók felülvizsgálata. Az alkalmazások naplóinak felülvizsgálatáért az adatgazda felelős.

Az információs rendszerek eseménynaplóit és biztonsági naplóit a napi üzemeltetési feladatok során át kell vizsgálni annak céljából, hogy abban vannak-e nem megfelelő vagy szokatlan működésre utaló jelek.

A hibabejegyzéseket és a szokatlan működésre utaló jeleket biztonsági eseményként kell kezelni, majd a biztonsági eseménykezelési eljárásrend szerint kell kezelni.

2.4 Időbélyegek

Az információs rendszerek valamennyi naplóbejegyzését időbélyeggel kell ellátni, melyhez a rendszerórát kell alapul venni.

Az információs rendszereket úgy kell kialakítani, hogy a hálózati időszinkron protokoll (NTP) segítségével szinkronizálják a rendszerórákat az egyezményes koordinált világidőhöz. Az idők megfelelő szintű szinkronizálódása érdekében a kiszolgálókon a „Europe/Budapest" időzónát kell beállítani, az időbélyegek operációs rendszer szinten CET, azaz közép-európai idő szerint rögzítenek.

2.5 A naplóinformációk védelme jogosulatlan módosítás ellen

Az elektronikus információs rendszerben keletkező naplóinformációt és a napló kezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben védeni kell.

2.6 A NAPLÓBEJEGYZÉSEK MEGŐRZÉSE

A naplóinformációkat az alkalmazások és rendszerek egyéb információival együtt be kell vonni a mentések rendszerébe. A mentéseket összhangban a napló tárkapacitással úgy kell kialakítani, hogy a naplóbejegyzések ne vesszenek el.

A naplóinformációkat a biztonsági események utólagos kivizsgálása érdekében meg kell őrizni.

A megőrzési idő megegyezik az adott rendszerre, alkalmazásra vonatkozó jogszabályi-számviteli megőrzési idővel, de legalább három hónapos megőrzési időt kell biztosítani. A technikai információk naplóit egy hónapig kell megőrizni.

2.7 NAPLÓGENERÁLÁS

Az elektronikus információs rendszereket fel kell készíteni a következő naplózásra vonatkozó követelményekre:

a) biztosítania kell a naplóbejegyzések előállítási lehetőségét a 2.1. pontban meghatározott naplózható eseményekre

b) lehetővé kell tenni a hivatali szakmai vezetőknek (adatgazdáknak), hogy kiválasszák, hogy mely naplózható események legyenek naplózva az információs rendszer egyes elemeire,

c) naplóbejegyzéseket kell tudnia előállítani a 2.1. pontban meghatározottak szerinti eseményekre a 2.2. pontban meghatározott tartalommal.

Jóváhagyta:

DUNAKESZI VÁROS JEGYZŐJE

3 MELLÉKLET – RÖGZÍTETT RENDSZER NAPLÓK

Megnevezés	Hely	Intervallum
Windows Kliens Logok	Helyben tárolva	30 nap
Windows Server Logok	Helyben tárolva	30 nap
SQL Logok	Helyben tárolva	30 nap
Hálózati eszközök (Switch)	Központilag tárolva (swconf srv)	30 nap
Tűzfal	Az eszközön	30 nap
Antivírus alkalmazás		30 nap
Alkalmazás Logok	-	
SQL ki-bejelentkezések	Helyben tárolva	30 nap
Jelszó módosítások	-	
Rendszergazdai tevékenységek	Kiszolgálókon külön az eseménykezelőben	30 nap

Dunakeszi Polgármesteri Hivatal

Rendszer és Információsértetlenségi Szabályzata

2019.

A DOKUMENTUM MÓDOSÍTÁSAINAK JEGYZÉKE

A dokumentum következő felülvizsgálatát 2022.06.30-ig el kell végezni.

V1.0	.	Első verzió	Nádor Rendszerház Kft.
Verzió	**Dátum**	**Leírás**	**Hatályba helyező utasítás száma**

TARTALOM

1 Általános rendelkezések

1.1 A Rendszer és Információsértetlenségi Szabályzat célja és hatálya

A Rendszer és Információsértetlenségi Szabályzat célja, hogy meghatározza a **Dunakeszi Polgármesteri Hivatal** (továbbiakban: Hivatal) elektronikus információs rendszereiben alkalmazott rendszer és Információsértetlenségi eljárásokat, szabályokat, az ezzel kapcsolatos feladatokat, felelősségeket és hatásköröket. A szabályzat meghatározza:

- a hibajavítások (patch management) folyamatát;
- a kártékony, rosszindulatú és mobil kódok elleni védekezés feladatait;
- az elektronikus információs rendszer felügyeleti feladatait;
- a biztonsági riasztások és tájékoztatások rendszerét;
- és a kimeneti információk kezelésének és megőrzésének általános szabályait.

1.1.1 A szabályzat karbantartása

A Rendszer és Információsértetlenségi Szabályzatot három évente felül kell vizsgálni és frissíteni kell. Felül kell vizsgálni abban az estetben is, ha az informatikai környezetben, vagy a vonatkozó jogszabályokban jelentős változás áll be.

1.2 A szabályzat hatálya

A szabályzat tárgyi hatálya kiterjed minden informatikai rendszerre, személyi hatálya minden munkatársra vonatkozik, akik az informatikai rendszer üzemeltetésében részt vesznek, a leírt folyamatokban közreműködnek. A rendszer felhasználói felé is elvárás az üzemeltetési előírások, korlátozások, elfogadható és nem elfogadható tevékenység ismerete.

2 Az eljárásrend leírása

2.1 Frissítések és hibajavítások (patch management)

A Hivatal elektronikus információs rendszerei sérülékenységeinek csökkentése érdekében szükséges az ismertté vált sérülékenységek mielőbbi javítása. A sérülékenységekről szóló információk és a javítások (patchek) megjelenése az alábbi információforrások segítségével ismerhető meg:

- gyártók által közzétett biztonsági frissítések, fejlesztések;
- Kormányzati Eseménykezelő (GovCERT) által kibocsátott biztonsági riasztások;
- biztonsági portálokon megjelenő leírások, figyelmeztetések;
- a Hivatal működése során ismertté vált hibák, incidensek;
- az elektronikus információs rendszer felügyelete során keletkező információk.

A rendszeresen megjelenő frissítések figyelése és telepítése az informatikai üzemeltetés feladata és felelőssége, míg a GovCERT riasztásait az IBF (elektronikus információs rendszerek biztonságáért felelős személy) továbbítja az informatikus számára.

A hibajavítás folyamatába külső alvállalkozókat is be kell vonni, amennyiben külső üzemeltetésben lévő rendszereket érint az alkalmazás frissítése, hibajavítása.

A hibajavítások alkalmazása során minden esetben előzetes tesztelést kell végezni a következők szerint:

- hibajavítás ellenőrzése teszt környezetben
- hibajavítás ellenőrzése szűk, meghatározott felhasználói körben (ha több üzemelő rendszert érint a javítás)
- hibajavítás terítése ütemezve, minden rendszerre, éles üzemben

A hibajavítások megfelelő működésének ellenőrzéséért az informatikus a felelős. A tesztelésbe alkalmazás oldali felhasználókat is be kell vonni (alkalmazások hibajavítások kapcsán).

A Microsoft termékek biztonsági frissítéseinek telepítésére a munkaállásokat úgy kell konfigurálni, mely biztosítja a frissítések ütemezését, a munkaállomások és a kiszolgálók újraindításának kikényszerítését, a telepítési műveletek naplózását.

Gondoskodni kell a segédprogramok (pl.: böngészők, Java, PDF kezelő eszközök, tömörítők stb.) napra készségének biztosításáról.

A közzétett javítások telepítését a javítás megjelenése után a lehető leggyorsabban le kell folytatni, figyelembe véve a gyártói, szakértői, hatósági ajánlásokat.

2.2 VÉDEKEZÉS VÍRUSOK, ROSSZINDULATÚ ÉS MOBIL KÓDOK ELLEN

A védekezés célja a Hivatal informatikai rendszerének kártékony programok elleni védelmének biztosítása. A védelem kialakítása során jelentkező biztonsági előírások két szinten jelentkeznek (felhasználói és rendszergazdai szinten).

A Hivatal több féle, a rosszindulatú kódok, vírusok és egyéb nemkívánatos mobil kódok (pl.: cookie) ellen védekezési, figyelemmel kísérési és reagálási módszereket alkalmaz. A védelmi rendszer minimális elemei:

- kizárólag jogtiszta szoftverek használata, ellenőrizhető forrásból
- tűzfalas védekezés (internet kijáratokon kívül a notebook-okon kötelezőként beállítandó),
- internetre és levelezésre kiterjedő tartalomszűrés,
- kéretlen levél (spam) elleni védelem,
- vírusvédelmi rendszer.

Az informatikai rendszerek biztonságos üzemeltetéséhez az informatikus feladata gondoskodni a vírusvédelmi rendszer kialakításáról és működtetéséről. Valamennyi számítógépre telepíteni kell a Hivatalban rendszeresített vírusvédelmi rendszert és azt folyamatosan működtetni kell.

A vírusvédelmet napra készen kell tartani az vírus adatbázis frissítések automatikus letöltésével, továbbá védelmi programok szükség szerinti frissítésével.

2.3 Aktív és passzív védelem

A vírusvédelmi rendszer fő komponense az aktív, memóriarezidens módon működő, valósidejű védelem, mely a számítógépek működése során állandóan dolgozik. Feladata a felhasználói munka során igénybe vett állományok (programok, adatok, dokumentumok) közvetlenül a használat előtti vírusellenőrzése.

A munkaállomások és kiszolgálók vírusvédelmét úgy kell beállítani, hogy legalább hetente egyszer megtörténjen az automatikus és kikényszerített vírus ellenőrzés futtatása. A tesztek eredményét ellenőrizhető napló állományokba kell rögzíteni.

A rendszerbe kívülről bekerülő adatokat (pendrive, CD/DVD stb., illetve az internetről letöltött adatok) felhasználás előtt vírusellenőrzésnek kell alávetni. A külső adathordozók csatlakoztatása esetén a vírusvédelmet automatikusan le kell futtatni.

2.4 Elektronikus levelezés vírusvédelme

Az elektronikus levelezés a vírusok továbbításának leggyorsabb és leggyakoribb módja, ezért erre külön figyelmet kell fordítani.

Ha a levél vagy a csatolt állomány fertőzött, arról a víruskereső szoftver értesíti a felhasználót és a rendszeradminisztrátort. Ha az aktív védelem nem képes a fertőzés eltávolítására, akkor a víruskereső rendszer a fertőzött állományt karanténba helyezi.

Az elektronikus levélben ok nélkül, váratlanul vagy a levél szövege alapján nem indokoltan érkezett állomány, idegen nyelvű szöveg, esetleg helytelen magyarsággal fogalmazott levél lehetséges vírushordozó, ezért a levél és csatolmányai megnyitása tilos, haladéktalanul értesíteni kell az informatikai csoportot.

2.5 Az elektronikus információs rendszer felügyelete

Az informatikus feladata és felelőssége, hogy biztosítsa az elektronikus információs rendszer felügyeletér, hogy észleljék a kibertámadásokat, vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárják a jogosulatlan lokális, hálózati és távoli kapcsolatokat. Lehetséges kibertámadásra utal az indokolatlanul megnövekedett hálózati forgalom, a határvédelmi eszközökre érkező kérések számának megugrása (túlterheléses támadás), port-scanek stb.

Azonosítani kell az elektronikus információs rendszer jogosulatlan használatát, illetve az erre irányuló kísérleteket, melyek jelei például a megnövekedett számú, sikertelen bejelentkezési kísérletek, felhasználói fiókok szokatlan aktivitása, felhasználói szoftver telepítési kísérletek, a védelmi rendszer (vírusvédelem, helyi tűzfal) kiiktatása vagy annak kísérlete stb.

Felügyeleti eszközöket kell alkalmazni a meghatározott alapvető információk gyűjtésére, és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére. A felügyeleti eszközökből nyert információkat védeni kell a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

Meg kell erősíteni az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jeleket észlelnek.

Az adatgazda felelőssége, hogy az egyes elektronikus információs rendszerek felügyeleti információi meghatározott gyakorisággal átvizsgálásra kerüljenek.

2.6 A KIMENETI INFORMÁCIÓ KEZELÉSE ÉS MEGŐRZÉSE

A kimeneti információk (pl.: papír alapú nyomtatványok, alkalmazások által generált elektronikus üzenetek, rendszer naplók stb.) kezelésével és szétosztásával kapcsolatban a jogszabályok, hatósági és belső előírások, valamint az iratkezelés szabályzata a követendő.

a) gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről;

b) gondoskodni kell arról, hogy a kimeneti információhoz történő fizikai és logikai hozzáférés csak az arra jogosított személyekre korlátozódjon;

c) biztosítani kell, hogy a megőrzendő információk tárolása biztosítsa az információ helyreállíthatóságát az előírt időtartamon belül.

Jóváhagyta:

DUNAKESZI VÁROS JEGYZŐJE

Dunakeszi Polgármesteri Hivatal

Rendszer- és Kommunikáció védelmi Szabályzat

2019.

A DOKUMENTUM MÓDOSÍTÁSAINAK JEGYZÉKE

A dokumentum következő felülvizsgálatát 2020.06.30-ig el kell végezni.

V1.1	2019.03.05	Véglegesített változat	
V1.0	.	Első verzió	Nádor Rendszerház Kft.
Verzió	**Dátum**	**Leírás**	**Hatályba helyező utasítás száma**

TARTALOM

1 ÁLTALÁNOS RENDELKEZÉSEK

1.1 A RENDSZER- ÉS KOMMUNIKÁCIÓ VÉDELMI SZABÁLYZAT CÉLJA ÉS HATÁLYA

A Rendszer- és Kommunikáció Védelmi Szabályzat célja, hogy meghatározza a **Dunakeszi Polgármesteri Hivatal** (továbbiakban: Hivatal) elektronikus információs rendszereinek egyes védelmi szabályait, a feladathoz tartozó felelősségeket és hatásköröket.

1.1.1 A szabályzat karbantartása

A Rendszer- és Kommunikáció Védelmi Szabályzatot kétévente felül kell vizsgálni és frissíteni kell. Felül kell vizsgálni abban az esetben is, ha az informatikai környezetben, vagy a vonatkozó jogszabályokban jelentős változás áll be.

1.2 A SZABÁLYZAT HATÁLYA

A szabályzat tárgyi hatálya kiterjed minden informatikai rendszerre, személyi hatálya minden munkatársra vonatkozik, akik az informatikai rendszer üzemeltetésében részt vesznek, a leírt folyamatokban közreműködnek.

2 A SZABÁLYOZÁS LEÍRÁSA

2.1 AZ INTERNET BIZTONSÁGOS HASZNÁLATÁNAK SZABÁLYOZÁSA

Az internetet a felhasználók a munkaköri leírásukban meghatározott feladataik elvégzéséhez, mint szolgáltatást használhatják, betartva az ide vonatkozó szabályokat, utasításokat. Ezen szolgáltatás minden magán és egyéb célú használata során esetlegesen bekövetkezett károkért a felhasználó felelősséggel tartozik.

Az internet használatának feltételeit a Felhasználói Biztonsági Szabályzat határozza meg.

Az interneten elérhető tartalmak és szolgálatások beállítási iránymutatását a Hozzáférés ellenőrzési, azonosítási és hitelesítési szabályzat tartalmazza.

A Hivatal asztali munkaállomásainak felhasználói kizárólag a helyi hálózaton keresztül csatlakozhatnak az Internethez. Bármely egyéb módon történő internet elérés létesítése az azt kialakító munkavállaló felelősségre vonását eredményezi. Tilos továbbá a felhasználóknak a web-böngészők biztonsági beállításait megváltoztatniuk.

A vezetékes és vezeték nélküli hálózati csatlakozási lehetőséggel is rendelkező eszközök (jellemzően: laptopok) felhasználóinak tilos eszközüket egyidejűleg a Hivatal vezetékes hálózatához és bármely vezeték nélküli hálózathoz egyidejűleg csatlakoztatni.

Az informatikai rendszer biztonsága érdekében az internet felhasználók által meglátogatott oldalak naplózásra kerülnek. A naplókat az adatvédelmi előírásoknak megfelelően kell kezelni.

2.2 AZ ELEKTRONIKUS LEVELEZÉS BIZTONSÁGOS HASZNÁLATÁNAK SZABÁLYOZÁSA

A felhasználók elektronikus levelezésének szabályairól a Felhasználói Biztonsági Szabályzat rendelkezik.

A munkavégzés célját szolgáló elektronikus címről küldött és arra érkező üzenetet és mellékleteit a munkáltató jogosult megtekinteni, mivel az a munkavégzéssel összefüggésben bizalmas információkat tartalmazhat (a munka törvénykönyvéről szóló 2012. évi I. tv. 11.§ (1) bekezdése alapján). Az elektronikus üzenetekben foglalt információk nem rendeltetésszerű felhasználása, teljes vagy részleges terjesztése vagy közlése tilos a munkáltató kifejezett hozzájárulása hiányában.

Az informatikai rendszer működőképességét veszélyeztető fenyegetés (vírus-fertőzés, levélbombák, egyéb külső támadás stb.) esetén az informatikai csoport a levelezés rendszer vagy postafiók használatát felfüggesztheti, azt átvizsgálhatja és szükség esetén újra konfigurálhatja. A postafiók átvizsgálása során esetlegesen megismert személyes adatok vonatkozásában az átvizsgálást végző munkatársat titoktartási kötelezettség terheli. Az intézkedésekről a jegyző, vagy az általa megbízott vezető tájékoztatja az érintett felhasználót és a munkáltatói jogokat gyakorló vezetőjét.

2.3 A HATÁROK VÉDELME

A Hivatal elektronikus információs rendszerén felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt. A külső határ védelme úgynevezett tűzfalakkal valósul meg.

A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban kell elhelyezni, elkülönítve a belső szervezeti hálózattól (DMZ).

Csak a Hivatal biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül engedélyezett a külső hálózatokhoz vagy külső elektronikus információs rendszerekhez történő kapcsolódás. A külső kapcsolatok kialakítása során követendő szabályok:

- korlátozni kell az elektronikus információs rendszer külső hálózati kapcsolatainak a számát.
- felügyelt interfészt működtet minden külső infokommunikációs szolgáltatáshoz;
- minden felügyelt interfészhez forgalomáramlási szabályokat alakít ki;
- védeni kell az összes interfésznél az átvitelre kerülő információk bizalmasságát és sértetlenségét;

2.4 A FOLYAMATOK ELKÜLÖNÍTÉSE

Az elektronikus információs rendszer elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára. Ezt az alkalmazott operációs rendszerek biztosítják.

Jóváhagyta:

DUNAKESZI VÁROS JEGYZŐJE

Dunakeszi Polgármesteri Hivatal

Rendszer Karbantartási Szabályzat

2019.

A DOKUMENTUM MÓDOSÍTÁSAINAK JEGYZÉKE

A dokumentum következő felülvizsgálatát 2022.06.30-ig el kell végezni.

V1.0		Első verzió	Nádor Rendszerház Kft.
Verzió	**Dátum**	**Leírás**	**Hatályba helyező utasítás száma**

TARTALOM

1 ÁLTALÁNOS RENDELKEZÉSEK

1.1 A KONFIGURÁCIÓKEZELÉSI SZABÁLYZAT CÉLJA ÉS HATÁLYA

A Rendszer Karbantartási Szabályzat célja, hogy meghatározza a **Dunakeszi Polgármesteri Hivatal** (továbbiakban: Hivatal) informatikai rendszerének karbantartásával kapcsolatos feladatokat, felelősségeket és hatásköröket.

1.1.1 A szabályzat karbantartása

A konfigurációkezelési szabályzatot három évente felül kell vizsgálni és frissíteni kell. Felül kell vizsgálni abban az estetben is, ha az informatikai környezetben, vagy a vonatkozó jogszabályokban jelentős változás áll be.

1.2 A SZABÁLYZAT HATÁLYA

A szabályzat tárgyi hatálya kiterjed minden informatikai rendszerre, személyi hatálya minden felhasználóra és üzemeltetőre, a karbantartási tevékenységben résztvevő külsős szerződött partner munkatársaira, akik a karbantartási (tervezés, végrehajtás, ellenőrzés, nyomon követés stb.) tevékenységben részt vesznek.

2 AZ ELJÁRÁSREND LEÍRÁSA

A Hivatal jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban. Az informatikus feladata és felelőssége, hogy tervezetten és rendszeresen történjen meg az informatikai eszközök és rendszerek karbantartása a gyártók és fejlesztők ajánlásai alapján.
Az információs rendszereknél a következőkben részletezett karbantartási eljárásrendet kell kialakítani.

2.1 KARBANTARTÁSOK TERVEZÉSE, ÜTEMEZÉSE ÉS KOMMUNIKÁCIÓJA

Az informatikus a felelős az elektronikus információs rendszerek hardver és szoftver komponenseinek karbantartásáért, azok ütemezett végrehajtásáért illetve végrehajtatásáért.
A végrehajtandó karbantartásokról előzetesen tervet kell készíteni, amelyben dokumentálni kell pontosan a feladatot és a kapcsolódó felelős, végrehajtó szerepköröket is.
A tervet jóvá kell hagynia a jegyző által megbízott vezetőnek.
A karbantartások végrehajtásához kapcsolódó leállások lehetséges időpontjai miatt a terveket egyeztetni kell a jegyzővel is.
A karbantartás tervezését úgy kell megtervezni, hogy az informatika, vagy a szállító az adott időablakon belül tudja végrehajtani a karbantartást/frissítést, ennek érdekében az időablak pontos paramétereit előre meg kell határozni. Az időablak minimális paraméterei a következők:

- Érintett hivatali folyamatok
- Tervezett leállás időpontja, óra perc megadásával

- Várható leállás ideje,
- Érintett rendszerek.

2.2 INFORMATIKAI ESZKÖZÖK JAVÍTÁSA ÉS KARBANTARTÁSA

Az elektronikus információs rendszer hardver elemeinek karbantartását és javítását a hivatali helyiségekben kell elvégezni, illetve elvégezetetni. A külső támogatók által végzett javítási-karbantartási tevékenységet a helyi informatikusnak felügyelnie kell.
Amennyiben a javítás vagy karbantartás a helyszínen nem lehetséges, az informatikus felelőssége, hogy az elszállítás előtt minden adat és információ - mentést követően – törlésre kerüljön a berendezésről.
Az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a hivatali épületből dokumentálni kell.

2.3 A KARBANTARTÁS ELLENŐRZÉSE

Az elvégzett karbantartás után az eszköz fajtájától függően funkcionális és biztonsági teszteket kell végezni, melynek eredményét rögzíteni kell a karbantartási nyilvántartásban. Sikertelen teszt esetén az eszköz nem helyezhető újra éles üzembe.

2.4 TÁVOLI KARBANTARTÁS

A Hivatal jóváhagyja, nyomon követi és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket.
A távoli karbantartási és diagnosztikai eszközök használata csak abban az esetben engedélyezhető, át, ha az összhangban áll az informatikai biztonsági szabályzat 9.4 Távoli elérés fejezetének előírásaival, továbbá a szállító által elvégzett tevékenység olyan szinten naplózásra kerül, hogy a napló alkalmas legyen a tevékenység utólagos ellenőrzésére is.
A távoli karbantartásokhoz egyedileg kell engedélyezni és megnyitni a munkaszakaszokat, melyek csak az adott, engedélyezett tevékenység elvégzésének idejére lehetenek megnyitva. A távoli karbantartás befejeződésekor a munkaszakaszt és a hálózati kapcsolatokat le kell zárni.

Jóváhagyta: DUNAKESZI VÁROS JEGYZŐJE

Dunakeszi Polgármesteri Hivatal

Rendszerbiztonsági Terve

Bizalmas információ, nem tehető közzé!

Készítette:

Nádor
RENDSZERHÁZ

Dunakeszi, 2019.

A DOKUMENTUM MÓDOSÍTÁSAINAK JEGYZÉKE

A dokumentum következő felülvizsgálatát 2020.06.30.-ig el kell végezni.

V1.0	2019.03.18	Első verzió, Nádor Rendszerház	Első verzió
Verzió	**Dátum**	**Leírás**	**Hatályba helyező utasítás száma**

TARTALOM

1 Általános rendelkezések

1.1 A Szabályzat célja és területi érvényessége

A **Dunakeszi Polgármesteri Hivatal** (a továbbiakban Hivatal) Rendszerbiztonsági Tervének (a továbbiakban: Szabályzat) alapvető célja, hogy megfogalmazza, és dokumentálja, és a munka- és feladatkörük miatt érintettek számára ismertesse az elektronikus információs rendszerek biztonságtervezési eljárási folyamatait, valamint biztosítsa annak ellenőrzését.

A Szabályzat leírja a megvalósított biztonsági feladatokat, összhangban a Hivatal szervezeti szintű architektúrájával, meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait, biztonságkritikus elemeit és alapfunkcióit.

1.2 A Szabályzat hatálya

A Szabályzat tárgyi és személyi hatálya az Informatikai Biztonsági Szabályzatban (IBSZ) meghatározottak szerinti. Jelen szabályzat az információbiztonsági szabályzatok része.

1.3 A Szabályzat felülvizsgálata és frissítése

Jelen Szabályzatot az informatikai biztonsági tervekkel párhuzamosan rendszeresen felül kell vizsgálni és szükség szerint frissíteni kell. A felülvizsgálatot évente legalább egyszer, tervezetten végre kell hajtani.

Frissíteni kell a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén, illetve minden esetben el kell végezni soron kívül, ha az üzemeltetési környezetben, szervezetekben, eljárásrendekben jelentős változás következett be.

1.4 A Szabályzat kezelése

A rendszerbiztonsági tervet csak a Hivatal a meghatározott vezetői és munkatársai ismerhetik meg.

A megismerésre jogosult kör:

- a Hivatal információbiztonsági koordinációs feladatot ellátó munkatársai és vezetői;
- a támogató szolgáltató munkatársai és vezetői, akik a Hivatal rendszereinek üzemeltetését végzik.

A hivatali és informatikai munkatársak a rendszerbiztonsági terv kidolgozása során elvégzik a szükséges belső egyeztetéseket.

A felsorolt munkakörökben dolgozók jogosultak és kötelezettek a Szabályzat változásait is megismerni.

A rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

2 Az elektronikus információs rendszer hatóköre, alapfeladatai

A Hivatalban működtetett elektronikus információs rendszer az önkormányzat működésével, továbbá a jogszabályokon alapuló feladatvégzési és ellátási kötelezettségi tevékenységének informatikai támogatását szolgálja.

2.1 Az elektronikus információs rendszer biztonsági osztálya

A Hivatal által alkalmazott elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztály besorolását, az egyes rendszerek funkcióit az Informatikai Biztonsági Szabályzat (IBSZ) tartalmazza.

2.2 Biztonsági követelmények értékelése

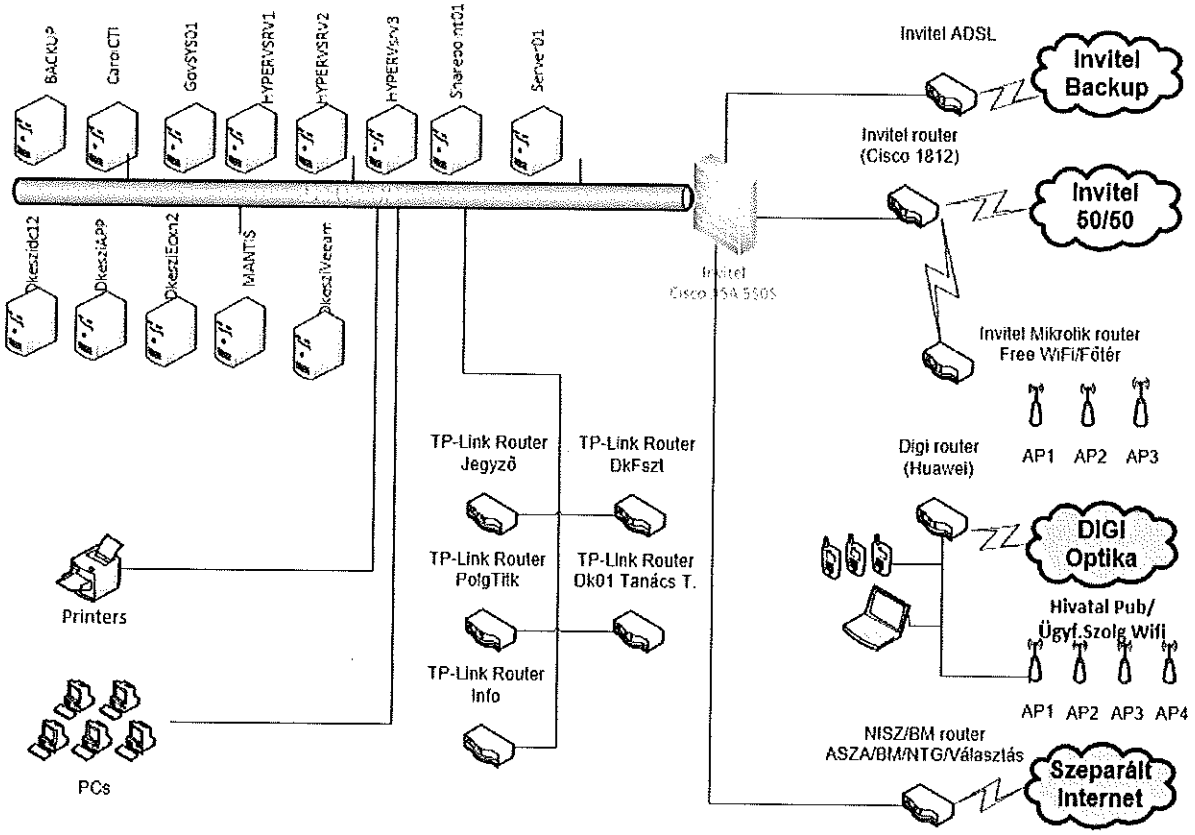
A jogszabálynak megfelelő üzemeltetési környezet megfelelési értékelése, a szervezet biztonsági szintjének megállapítása, továbbá az elektronikus információs rendszerek osztályba sorolása a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) által kibocsátott értékelő táblák alapján történik.

3 Az elektronikus információs rendszer biztonságkritikus elemei

Az elektronikus információs rendszer főbb elemeit az alábbi pontok ismertetik. A rendszer architektúra megismerését a mellékelt logikai ábra, továbbá a hardver és szoftver környezet leírása támogatja.

3.1 Logikai ábra

A rendszer logikai felépítését a"H:\IT\Muszaki_dokumentacio\" helyen található PMH informatika összefüggési rajz .pdf nevű állomány tartalmazza. - H: [\\dkeszidc12\Hivatal]



3.2 Hardver és szoftver környezet

A hardver környezet leírását a "H:\IT\Muszaki_dokumentacio" mappa alatt található leírások tartalmazzák.

Jellemző elemei a

- rendszerkomponensek
- hálózat, hálózati szolgáltatások
- levelezési szolgáltatás
- tűzfal
- mentések

- Szerver termek beépítési séma
- Hálózati kapcsolati ábrák

- Vezeték nélküli hálózatok

3.3 Adatátviteli hálózat

Az informatikai hálózat felépítését a "H:\IT\Muszaki_dokumentacio\" helyen található Szerverek_halozat.xls nevű állomány tartalmazza.

Internet kapcsolat: INVITEL Zrt. - Internet szolgáltatás, Mail relay szolgáltatás, Tűzfal, Router kezelés, mail.dunakeszi.hu|Alapértelmezett átjáró: 192.168.2.1|DNS1:192.168.2.9

Az adatátviteli hálózat fontosabb paramétereit a "H:\IT\Muszaki_dokumentacio\" hálózati könyvtárban található Informatikai_rendszer_dokumentacio_v2.0.docx nevű állomány részletezi.

4 Az elektronikus információs rendszer védelmi intézkedései

A védelmi intézkedések eszközei:

Tűzfal: 1db. Cisco ASA 5505 Invitel tulajdon

Vírusvédelem: ESET Endpoint Antivirus Business Edition 7.0.577.0 Minden munkaállomáson, központi menedzsmenttel.

4.1 Külső rendszerkapcsolatok

A külső rendszerkapcsolatok, azok tulajdonságai:

- ASP - Önkormányzati ASP
- Gordius - Pénzügyi rendszer
- IPL - Integrál Portál-alapú lekérdező rendszer (BM)
- ÉTDR - Építés hatósági rendszer
- Intermap - Térinformatika
- WinIKSZ - Szociális rendszer

4.2 Információbiztonsági architektúra leírás

Az elektronikus információs rendszer bizalmasságának, sértetlenségének és rendelkezésre állásának védelmét szolgáló, megvalósításra került követelményeket és megközelítést a paramétereit a "H:\IT\Muszaki_dokumentacio\" hálózati könyvtárban található Informatikai_rendszer_dokumentacio_v2.0.docx nevű állomány részletezi.

Egyéb vonatkozó szabályozások:

- Azonosítási és hitelesítési eljárásrend (a 41/2015. (VII. 15.) BM rendelet 3. melléklet 3.3.9.1. pontja szerint),

- Hozzáférés ellenőrzési eljárásrend (a 41/2015. (VII. 15.) BM rendelet 3. melléklet 3.3.10.1. pontja szerint),
- Naplózási eljárásrend (a 41/2015. (VII. 15.) BM rendelet 3. melléklet 3.3.12.1. pontja szerint),
- Rendszer- és kommunikációvédelmi eljárásrend (a 41/2015. (VII. 15.) BM rendelet 3. melléklet 3.3.13.1. pontja szerint).

4.2.1 *Informatikai tárgyú szerződések nyilvántartása*

Az informatikai szolgáltatásokat az alábbiakban felsorolt szervezetek nyújtanak közvetlenül vagy közvetve a Hivatal számára.

Szolgáltatás megnevezése	Szolgáltató, szerződött partner	Szolgáltatás részletes leírása
Informatikai hibák, szerver-kliens software/hardware	Nádor Rendszerház Kft.	2. level server Outsourcing
Nyomtatók hiba bejelentése	Delfin Rendszerház Kft.	Központi nyomtatás
Carol	CAROL-CTI Kft.	Call Center
EDTR	Globomax Zrt.	Elektronikus döntés támogató rendszer
Gordius	Korend Rendszerház Kft.	Pénzügyi rendszer
Govsys	Professzionál Zrt.	Integrált ügyiratkezelő rendszer
Ügyfélhívó rendszer	MULTIMEX Kft.	Ügyfélhívó rendszer
Intep	INTEP Elektronikai Fejlesztő és Gyártó Kft.	Beléptető rendszer
ASP	Magyar Államkincstár	ASP Központ
ÖnkAdó	Kommunáldata KFT. Magyar Államkincstár	Adó

DUNAKESZI VÁROS JEGYZŐJE

Jóváhagyta:

Dunakeszi Polgármesteri Hivatal

Ügymenet Folytonossági Szabályzata

Készítette:

Vádor RENDSZERHÁZ

Dunakeszi, 2019.

A DOKUMENTUM MÓDOSÍTÁSAINAK JEGYZÉKE

A dokumentum következő felülvizsgálatát 2020.06.30.-ig el kell végezni.

Verzió	Dátum	Leírás	Hatályba helyező utasítás száma
V1.0		Első verzió, Nádor Rendszerház	

TARTALOM

1 Általános rendelkezések

1.1 A Szabályzat célja és területi érvényessége

A **Dunakeszi Polgármesteri Hivatal** (a továbbiakban Hivatal) Ügymenet Folytonossági Tervének (a továbbiakban: Szabályzat) alapvető célja, hogy megfogalmazza és dokumentálja az informatikai szolgáltatások teljes vagy részleges kiesése esetén követendő ügymenetet, illetve megállapítsa az informatikai szolgáltatásokkal szembeni szolgáltatási szint elvárásokat, az elvárt helyreállítási célokat és a maximálisan elfogadható adatvesztés mértékét.

1.2 A Szabályzat hatálya

A Szabályzat tárgyi és személyi hatálya az Informatikai Biztonsági Szabályzatban (IBSZ) meghatározottak szerinti. Jelen szabályzat az információbiztonsági szabályzatok része.

1.3 A dokumentum felülvizsgálata

Jelen Szabályzatot a katasztrófa helyreállítási tervekkel párhuzamosan rendszeresen felül kell vizsgálni és szükség szerint frissíteni kell. A felülvizsgálatot évente legalább egyszer, tervezetten végre kell hajtani, illetve minden esetben el kell végezni soron kívül, ha az üzemeltetési környezetben, szervezetekben, eljárásrendekben jelentős változás következett be.

1.4 A szabályzatban alkalmazott fogalmak

A szabályzatban alkalmazott fogalmak magyarázatát a *Helyreállítási Szabályzat Informatikai katasztrófa esetére* dokumentum tartalmazza (Katasztrófa Helyreállítási Terv).

1.5 Az ügymenet folytonossági tervek oktatása

A folyamatban érintett munkatársakat évente oktatásban kell részesíteni.

2 Ügymenet folytonossági megfontolások

Gondosan megtervezett és megvalósított megelőző intézkedések esetén is lehetséges, hogy olyan meghibásodások, emberi tévedések és/vagy természeti katasztrófák történnek, amelyek a biztonsági rendszerek és szolgáltatások kiesését okozzák. A helyreállítási intézkedések megtervezéséhez szükséges kiinduló adatok meghatározása a szakmai terület elvárásai alapján a Kockázati Jelentésben került összefoglalásra.

2.1 MTO

Az egyes működési területekre, meghatározásra kerültek a maximálisan elfogadható kiesési idők, (MTO, Maximum Tolerable Outage), melyek időtartamig az adott szolgáltatás nélkülözhető. Ezek az időtartamok tekintendők a katasztrófa helyzet utáni visszaállítás cél-értékének, az úgynevezett sebezhetőségi ablaknak.

Azok az események, melyek hatása az adott eszközre vonatkozó sebezhetőségi ablakon belül helyreállíthatók, nem tekinthetők katasztrófa helyzetnek.

A katasztrófa helyreállítási tervezés során az a cél, hogy legalább az adott funkció visszaállítási ideje a sebezhetőségi ablakon belül maradjon. A biztonsági architektúra több elemének sérülése esetén nem kerül meghatározásra a szakmai prioritások alapján a visszaállítási sorrend, mivel a sorrendet a technikai lehetőségek határozzák meg. Az informatikai alap infrastruktúra nagyobb arányú sérülése esetén a visszaállítás, illetve helyreállítás során informatikai szempontból meg kell állapítani a helyreállítási tevékenységek sorrendjét, melyek az architektúra tulajdonságaiból következnek, például a hálózati működés helyreállítása előbb történik, mint a tartományvezérlők helyreállítása.)

A Hivatal követelményei szerint:

- Elfogadható kiesési idő:
  - kritikus rendszereknél: 24 óra,
  - egyéb kategóriák: egy hét,
  - maximum: egy hónapon belül valamennyi funkciónak működnie kell.
- Az események szakmai hatás szerinti kategorizálása:
  - szakmailag kritikus hiba,
  - szakmailag nem kritikus hiba.
- A kritikus hibák következményeik szerint az alábbi kategóriákba kerültek:
  - indifferens,
  - kisebb hiba,
  - súlyos hiba,
  - katasztrofális hiba,

2.2 RPO

RPO (Recovery Point Objective):„Visszaállítási időpont cél" Az RPO adja meg azt a maximálisan elfogadható időtartamot, amelyre vonatkozó adatvesztés el tud fogadni az szakmai felhasználó kiterjedt meghibásodások, katasztrófák esetén. Például egy 24 órás RPO érték azt jelenti, hogy az adatbázis megsemmisülését követő visszaállítás után az utolsó (a katasztrófát megelőző) 24 órában rögzített adatok elvesztek, csak az azt megelőzően rögzített adatok állíthatók vissza.

2.3 RTO

RTO (Recovery Time Objective): „Visszaállítási időtartam cél". Az RTO az az időtartam, amely egy adott IT rendszer visszaállítását biztosítani kell annak kiesését követően. A RTO-t közvetlenül az IT rendszerekre határozzuk meg, míg a hasonló tartalmú sérülékenységi ablakot az elsődleges informatikai szolgáltatok kapcsán értelmezzük.

A továbbiakban rendszerenként meghatározásra kerülnek az RTO és RPO értékek, melyekkel összhangban kell lenniük az informatikai mentési szolgáltatásoknak és helyreállítási terveknek.

2.4 Informatikai szolgáltatások kiesése

Az informatikai szolgáltatások teljes vagy részleges kiesése a Hivatal működésére hátrányos hatást gyakorol.

2.4.1 Informatikai szolgáltatások teljes kiesése

Az informatikai szolgáltatások teljes kiesése esetén valamennyi, az informatika által biztosított központi és helyi szolgáltatás megszűnik, szélsőséges esetben a lokális számítógép használat és helyi nyomtatás lehetősége is (például egy általános vírus fertőzés esetén).

Az ügymenet folytatása a számítástechnikai szolgáltatások nélkül, kizárólag papír alapon lehetséges.

2.4.2 Informatikai szolgáltatások részleges kiesése

Az informatikai szolgáltatások részleges kiesése esetén egyes alkalmazások, szolgáltatások nem elérhetők, de bizonyos alapfunkciók rendelkezésre állhatnak, például az internet használat vagy a helyi, hálózatos nyomtatás lehetősége, illetve egyes munkaállomások használata lehetséges.

2.4.3 Külső (központi) informatikai szolgáltatások kiesése

Speciális eset az állami szolgáltatások (ASP) szolgáltatás zavara, amely adódhat külső rendszer hibából vagy az adatátviteli szolgáltatás üzemképtelensége miatt.

3 Ügymenet folytonossági tervek

Az alábbiakban kerülnek ismertetésre az egyes alkalmazások teljes vagy részleges kiesése esetén követendő eljárások.

Az intézkedések felelősei, illetve az intézkedések aktiválása a *Helyreállítási Szabályzat Informatikai katasztrófa esetére* című dokumentumban leírtak szerintiek.

A Hivatal működését érintő, alábbi rendszerekben kerültek megállapításra az ügymenet folytonosság tervei és követelményei:

- Informatikai alaprendszerek
    - informatikai belső hálózati funkciók, bejelentkezés, nyomtatás, fájl szerver, home és csoport könyvtárak
    - elektronikus levelezés
    - internet használat
- Belső üzemeltetésű informatikai rendszerek
    - iktató
    - pénzügyi rendszer
    - stb.
- Külső üzemeltetésű informatikai rendszerek (ASP rendszerek)
    - anyakönyvi rendszer
    - stb.

ALKALMAZÁS / SZOLGÁLTATÁS	Informatikai belső hálózati funkciók, bejelentkezés, nyomtatás, fájl szerver, home és csoport könyvtárak
RTO – visszaállítási idő cél	**RPO – maximálisan elfogadható adatvesztés**
1 nap – kiemelt felhasználók számára 3 nap – teljes Hivatal ügyintézői állomány részére	1 nap
A probléma észlelése: A hálózatra nem lehet bejelentkezni. A felsorolt szolgáltatások nem elérhetők.	
Ügymenet folytatása az informatikai támogatás teljes hiánya esetén: A felsorolt szolgáltatások elérhetetlensége esetén a funkciók kézi megoldásokkal nem helyettesíthetők.	
Ügymenet folytatása részleges informatikai szolgáltatás rendelkezésre állása esetén:	
A szükséges minimális informatikai szolgáltatás:	Legalább a helyi nyomtatást meg kell oldani, kiemelt felhasználók számára a fájl szerveren tárolt adatokat elérhetővé kell tenni, 1 napon belül.
A korlátozott funkcionalitás mellett gondoskodni kell a készült anyagok visszaszinkronizálásáról, a teljes visszaállás után.	

ALKALMAZÁS / SZOLGÁLTATÁS	Iktatás
RTO – visszaállítási idő cél	**RPO – maximálisan elfogadható adatvesztés**
1 hét	1 nap

A probléma észlelése:

Az iktató rendszer nem működik, sem adatot felvinni, sem lekérdezni nem lehet.

Ügymenet folytatása az informatikai támogatás teljes hiánya esetén:

Az ügyfélfogadás korlátozottan folytatható.

A benyújtott beadványokat kézi úton kell iktatni, ideiglenes iktatószámot kell adni. A nyilvántartást egy hitelesített, sorszámozott lapokkal ellátott füzetben kell vezetni.

A rendszer helyreállítása után a beadványokat fel kell vinni a gépi nyilvántartásba. Az ideiglenes kézi nyilvántartás és a végleges iktatószámok közötti megfeleltetést el kell végezni és erről külön nyilvántartást kell vezetni.

Ügymenet folytatása részleges informatikai szolgáltatás rendelkezésre állása esetén:

A szükséges minimális informatikai szolgáltatás:	Csak lekérdezés az iktatóból.

Részleges működés az adatbázis hibája esetén, csak lekérdezést tesz lehetővé.

A beadványok fogadása az előző pontban leírtak szerint történik.

Az esetlegesen felmerülő ügyféltájékoztatás a gépi lekérdezésből biztosítható.

ALKALMAZÁS / SZOLGÁLTATÁS	Pénzügyi rendszer
RTO – visszaállítási idő cél	**RPO – maximálisan elfogadható adatvesztés**
1 nap / 1 hét / 1 hónap	1 nap
A probléma észlelése: A pénzügyi rendszer nem működik.	
Ügymenet folytatása az informatikai támogatás teljes hiánya esetén: A pénzügyi-számviteli feladatok nem folytathatók informatikai támogatás nélkül.	
Ügymenet folytatása részleges informatikai szolgáltatás rendelkezésre állása esetén:	
A szükséges minimális informatikai szolgáltatás:	

ALKALMAZÁS / SZOLGÁLTATÁS	
RTO – visszaállítási idő cél	**RPO – maximálisan elfogadható adatvesztés**
1 nap / 1 hét / 1 hónap	1 nap
A probléma észlelése:	
Ügymenet folytatása az informatikai támogatás teljes hiánya esetén:	
Ügymenet folytatása részleges informatikai szolgáltatás rendelkezésre állása esetén:	
A szükséges minimális informatikai szolgáltatás:	

ALKALMAZÁS / SZOLGÁLTATÁS	
RTO – visszaállítási idő cél	**RPO – maximálisan elfogadható adatvesztés**
1 nap / 1 hét / 1 hónap	1 nap
A probléma észlelése:	
Ügymenet folytatása az informatikai támogatás teljes hiánya esetén:	
Ügymenet folytatása részleges informatikai szolgáltatás rendelkezésre állása esetén:	
A szükséges minimális informatikai szolgáltatás:	

Jóváhagyta:

Dunakeszi Polgármesteri Hivatal
Helyreállítási Szabályzat
Informatikai katasztrófa esetére

Értesítési listák

Vádor
RENDSZERHÁZ

2019.

Tartalomjegyzék

Bevezetés

Ez a kézikönyv a Dunakeszi Polgármesteri Hivatal informatikai helyreállítási szabályzatának része.

A katasztrófa hatású események következményeinek felszámolásához kulcsfontosságú, hogy a szükséges intézkedések gyorsan, koordináltan kerüljenek végrehajtásra. A hatékonyság elengedhetetlen eleme, hogy mindig rendelkezésre álljon a helyreállításban közreműködők, az érintett felek aktuális elérhetősége, hogy a beavatkozások haladéktalanul elkezdődhessenek.

Katasztrófahelyzetre, vagy katasztrófa közeli helyzetre utaló események észlelése során az *Aktiválási Kézikönyv*ben foglaltak szerint kell eljárni.

Amint a *Helyreállítási Team Vezető* értesül a kialakult helyzetről, és döntés született a katasztrófa elhárítási tervek aktiválásáról, értesíti a felelős vezetőket, illetve az üzemeltetés illetékes munkatársait az eseményről, illetve a teendőkről.

A jelen dokumentumban foglalt értesítési listák arra szolgálnak, hogy a katasztrófa elhárítási lépések során mind a Katasztrófa Helyreállítási Team operatív vezetése, mind az helyreállításban részt vevő műszaki személyzet, ismerje a katasztrófa elhárításban részt vevő belső és külső közreműködők elérhetőségét.

Katasztrófa elhárítás értesítési listák

Értesítési listák karbantartása

Az értesítési listákat napra készen kell tartani, a változásokat haladéktalanul át kell vezetni.

Az aktuális lista elérhető a katasztrófa helyreállítási dokumentumok tárolási helyein (lásd: Katasztrófa Helyreállítási Szabályzat):

- A jegyzőnél, a jegyzői iroda zárt iratszekrényében,
- Informatikus irodájában,

A lista napra kész állapotáért felel: a Helyreállítási Team vezetője

Belső vészhelyzeti értesítési lista

HELYREÁLLÍTÁSI SZEREPKÖR	FELELŐS
Helyreállítási Team vezetője	Jegyző
Helyreállítási Team informatikai vezetője	Informatikus
Helyreállítás hivatali operatív vezetője	Aljegyző, a helyreállítás vezetésére kijelölt hivatali felső vezető
Rendszerek szakmai felelősei	Helyreállítás vezetésére kijelölt szakmai vezető(k)
Informatikus támogatók	Helyreállítás szakmai végrehajtói, rendszertámogatás

Elsődleges felelős:

- **dr. Molnár György - Jegyző**
  telefonszáma: 06-27-542-800 /106 m.
  mobilszáma: 06/20-398-12-21
  email címe: Molnar.Gy@dunakeszi.hu

Másodlagos felelősök:

- **dr. Szarvas Aliz - Aljegyző**
  telefonszáma: 06-27-542-800 /174 m.
  mobilszáma: 06/70-699-48-73
  email címe: Szarvas.Aliz@dunakeszi.hu

- **Szabó László - Informatikus**
  telefonszáma: 06-27-542-800 /243 m.
  mobilszáma: 06/70-699-49-72
  email címe: Szabo.Laszlo@dunakeszi.hu

Szállítók értesítési listája

A kritikus rendszerek, szolgáltatások támogató partnerei a következők:

Informatikai hibák, szerver-kliens software/hardware
Nádor Rendszerház Kft. H-1152 Budapest, Telek utca 7-9. www.nador.hu
Tel.: +36 1 470-5000/158, Fax: +36 1 470-5011
Hibabejelentés: nrticket@nador.hu

Oravecz Szabolcs - Üzemeltetési vezető
E-mail: oravecz.szabolcs@nador.hu
Mobil: 06203124427

Kiss Imre - Rendszermérnök
Mobil: +36 20 974 0137
E-mail: kiss.imre@nador.hu

IT eszközök-beszerzések:
Biener Bálint - Értékesítési tanácsadó
Mobil: + 36 20 547-3533
E-mail: biener.balint@nador.hu

Internet hiba bejelentés:
Invitech Megoldások Zrt. +36 80 88 00 88 help@invitech.hu www.invitech.hu

Borbély Olivér – Key Account Manager
Mobil: +36 20 256 7329
E-mail: BorbelyO@invitech.hu

Nyomtatók hiba bejelentése, toner rendelés:
Kádár Sándorné
Delfin Rendszerház Kft. H-1116 Budapest, Fehérvári út 130. www.delfinrendszerhaz.hu
Tel: +36 1 464-7480
Mobil. +36 20-320-2701
E-mail: edit@delfinrendszerhaz.hu

Arany Csaba - értékesítési igazgató
Mobil: +36 20 22 55 600
arany.csaba@delfinrendszerhaz.hu

CAROL-CTI Kft. - H-1143 Budapest, Gizella út 51-57.
Windisch József
Mobile: +36 30 415 9017
E-mail: jozsef.windisch@carolcc.com
Informatikus: Agócs Albert albert.agocs@carolcc.com

DRS - Hangrögzítés
Pályi Attila 06 30 933 17 12
A fejlesztő cég: DSR Group Kft.
Gonda András 1117 Bp. Prielle Kornélia utca 19/g
Telefon: 06 30 944 58 87

Email: andras.gonda@dsr.hu

EDTR Elektronikus döntés támogató rendszer
Globomax Zrt.
Telefon: Oládi Péter +36/30 2569737
Magyar Zoltán +36/30 644 2090
Huszti Benjámin +36/30-581-3991 email: huszti.benjamin@globomax.hu

Gordius Pénzügyi rendszer
Korend Rendszerház Kft. 2800 Tatabánya, Mártírok útja 12.
Telefon és fax: +36 34/302-480, +36 34/309-021

Kozma László – ügyvezető e-mail: kozma.laszlo@korend.hu mobil: +36 30/927-03-29
Varga Pál - vezető menedzser e-mail: varga.pal@korend.hu mobil: +36 20/220-34-19
Magyar Henrik - önkormányzati szaktanácsadó e-mail: magyar.henrik@korend.hu mobil: +36 20/455-77-50
Kozma Gábor – programozó e-mail: kozma.gabor@korend.hu mobil: +36 20/323-99-79
Bräutigam Géza - informatikai szakmenedzser e-mail: geza@korend.hu mobil: +36 20/499-92-63

Govsys - Integrált ügyiratkezelő rendszer
Professzionál Zrt. -_1117 Budapest, Sopron út 19.
Kapcsolat: govsyshiba@professzional.hu
Telefon: Mihalics Gábor : +36/30 4050926
Kapcsolat tartó: Deák Tímea 06-30-9-49-34-19

Ügyfélhívó rendszer
MULTIMEX Kft. - Cím: 1037 Budapest, Jablonka út 118/a.
Tel: +36 1 203 05 07 Fax: +36 1 481 40 04
Dmitrasinovity Tamás - szoftverspecialista, designer
Email: dtamas@multimex.hu Web: www.multimex.hu

ASZA-s gépek
M&S informatikai Zrt.
Sinkó Zsolt - Szervíztechnikus
HelpDesk: 06-1-237-1-237
Mobil: 06-30-703-2-932
Email: sinko.zsolt@mands.hu

Intep - Beléptető rendszer
INTEP Elektronikai Fejlesztő és Gyártó Kft.
Kecskés Gábor - Projekt vezető
Mobil: +36-30-2515-947
Tel: +36-1-278-0500
Mail : gabor@intep.hu support@intep.hu
www.intep.hu www.intepsystem.hu

ASP Központ
Magyar Államkincstár
1138 Budapest, Váci út 135-139. C. épület.
Telefon: +36-1-327-5840
E-mail: asp@allamkincstar.gov.hu

ÖnkAdó
Németh Ferenc - államháztartási referens
Magyar Államkincstár Budapesti és Pest Megyei Igazgatóság
Államháztartási Iroda - II. Államháztartási Osztály
1138 Budapest, Váci út 135-139. Telefon: 06-1-429-5312 Fax: +36-1-429-5361
E-mail: nemethferenc@allamkincstar.gov.hu

DUNAKESZI JEGYZŐSÉG

Jóváhagyta:

Dunakeszi Polgármesteri Hivatal

Helyreállítási Szabályzat
Informatikai katasztrófa esetére

Aktiválási kézikönyv

Nádor
RENDSZERHÁZ

2019.

Tartalomjegyzék

Bevezetés

Ez a kézikönyv a Dunakeszi Polgármesteri Hivatal informatikai helyreállítási szabályzatának része.

A katasztrófa hatású események következményeinek felszámolásához kulcsfontosságú, hogy a szükséges intézkedések gyorsan, koordináltan kerüljenek végrehajtásra. A nem tervezett, szakszerűtlen intézkedés az esemény súlyosságát fokozhatja, további funkció, illetve adatvesztéshez vezethet, továbbá a helyreállítás ideje megnövekedhet.

Lényeges az is, hogy a helyreállítás során tisztázottak legyenek a döntési hatáskörök, az utasítási hierarchia. Az események fellépése esetén a részt vevőknek ismerniük kell a rendellenesség bejelentésének lehetőségeit, a megoldáshoz vezető eszkalációs lépéseket.

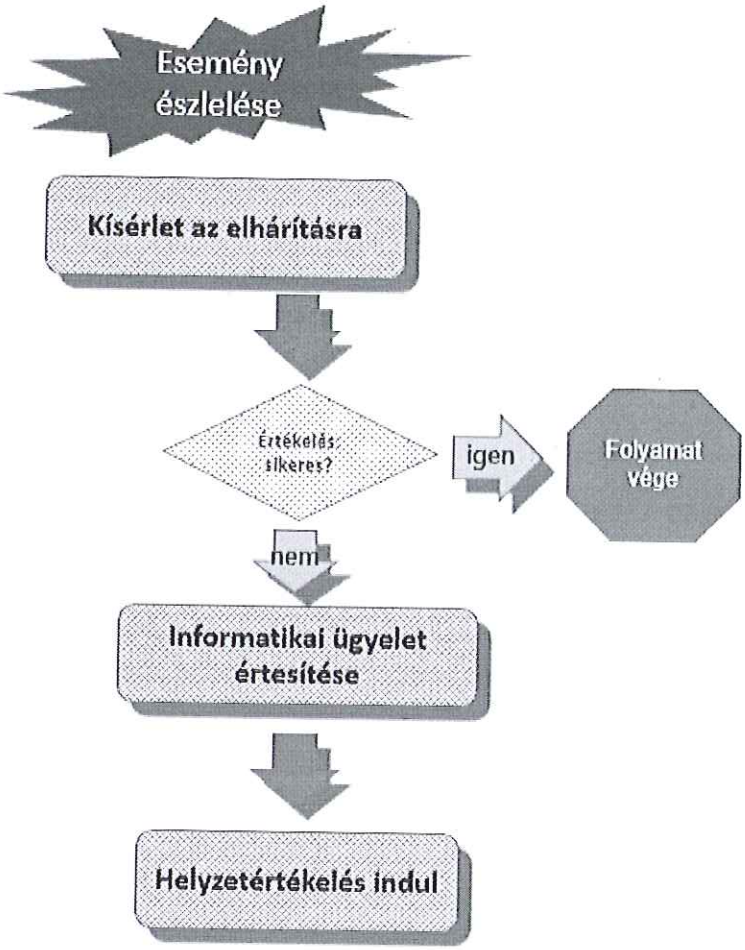
Jelen dokumentumban meghatározásra kerülnek az egyes események bekövetkezésének észlelésekor és a megoldás során követendő lépések:

- esemény észlelése és jelentése
- hibakeresés lépései
- eszkaláció
- katasztrófa helyzet kihirdetése

Események észlelése és jelentése

Az informatikai rendszer rendellenességeit a rendszer felhasználói és üzemeltetői észlelik.

Problémák felhasználói észlelése



Első körben a felhasználó megkísérli saját hatáskörben az elhárítást, például ellenőrzi a problémás eszköz hálózati és elektromos csatlakozásait, újraindítja az eszközt stb.

Amennyiben a próbálkozás nem vezet eredményre, abban az esetben az bejelenti az informatikus felé. A felhasználó részéről történő észlelés még nem jelenti feltétlenül azt, hogy informatikai értelemben katasztrófa helyzet lenne, erről a felelősöknek kell döntést hozniuk.

Problémák észlelése az informatikai üzemeltetés részéről

Amennyiben az ügyeletes informatikus detektálja a hibát, mely a hibajelenséget mutató eszköz, vagy szolgáltatás, illetve az elhárítás várható ideje miatt a katasztrófa kategóriába esik, akkor értesíti az informatikai vezetőt, illetve elérhetetlensége esetén kijelölt helyettesét.

Eszkalációs rend

ESZKALÁCIÓS REND		
Személy	Kinek eszkalál?	Tevékenység
Felhasználó	Informatikai ügyeletes	Észlelt probléma jelentése
informatikus	Hivatali felelősök felé, szükség esetén	Észlelt probléma értékelése, döntés a katasztrófa helyreállítási intézkedések beindítására

A működésfolytonosság biztosítása katasztrófa helyzet esetén

Az informatikai üzemeltetési eseményeket, amennyiben lehetséges, az incidenskezelés folyamatában kell kezelni és feldolgozni. A Katasztrófa Helyreállítási Szabályzat a súlyos, működésfolytonossági incidens bekövetkezése után a károk felmérését, és a normál működési szintre való hatékony visszaállást szabályozó intézkedések együttese.

Az incidenskezelés folyamata az alábbiak szerint történik:

1) Az incidenst kiváltó hiba azonosítása
    a. helyi hardver eszköz;
    b. helyi szoftver eszköz;
    c. helyi hálózat;
    d. külső informatikai szolgáltatás;
    e. telekommunikációs szolgáltatás;
    f. külső hálózat, internetelérés;
2) Helyettesítő cselekvési tervek, folyamatok bevezetése.

A kialakult helyzet értékelése

A legfontosabb tényezők, amelyek katasztrófahelyzetre, vagy katasztrófa közeli helyzetre utalhatnak:

a) természeti katasztrófa (tűz, vízbetörés stb.) vagy támadás következtében megrongálódott a szerverterem vagy az informatikai infrastruktúra kritikus elemei;

b) megrongálódtak az adatátviteli rendszer elemei;

c) támogató infrastruktúra kiesése lépett fel (elektromos áramellátás szünetel vagy szünetelt, klimatizálás megszűnt stb.);

d) informatikai eszközök súlyos egyéb sérülése, hacker támadás vagy vírusbetörés, továbbá minden olyan egyéb esemény, amely az informatikai szolgáltatások leállását okozhatja.

Döntés a katasztrófa helyzet kihirdetéséről

Amint az informatikus értesül a kialakult helyzetről, mérlegelnie kell az esemény súlyát, és döntenie kell arról, hogy az esemény kezelése megoldható-e normál üzemeltetési feladatként.

Amennyiben a hibajavítás folyamata nem biztosítja a működés helyreállítását, akkor a Helyreállítási Team döntést hoz:

1. a helyettesítő cselekvési tervről és a
2. Katasztrófa Helyreállítási Szabályzat aktiválásáról.

A katasztrófa helyzet helyreállítása során az egyes eseményeket a Katasztrófa Helyreállítási Szabályzatban foglaltak szerint kell kezelni.

Kommunikációs és adminisztrációs terv:

Belső kommunikáció

A munkatársak tájékoztatásáról a Helyreállítási Team dönt, és a tájékoztatást a belső kommunikációs előírásoknak megfelelően hajtják végre. A vészhelyzeti helyreállítás során szükséges lehet a kommunikáció a szerződött partnerekkel és ügyfelekkel is.

Az operatív feladatokat végző személyeket az aktuális értesítési listákon keresztül lehet elérni. *(Értesítési lista.docx)*

Külső kommunikáció

A katasztrófa helyreállítási tevékenységgel kapcsolatos külső kommunikációt kizárólag a Hivatal vezetése által felhatalmazott személyek folytathatnak. Ez a kommunikáció kiterjed a

- ügyfelek közvetlen tájékoztatására (hirdetmény, weblap stb.),
- érintett hatóságok előírt tájékoztatására,
- média tájékoztatására.

A munkatársaknak tilos felhatalmazás nélkül szervezeten kívüli személyeknek az felmerült eseményről tájékoztatást adniuk.

Az informatikai incidensről a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) felé a jogszabályban előírt tájékoztatást és kapcsolattartást az elektronikus információs rendszerek biztonságáért felelős személy végzi.

A helyreállítás adminisztrációja

A helyreállítási tevékenység végrehajtási lépéseit, a meghozott intézkedéseket dokumentálni kell. A dokumentálás azért elengedhetetlen, mert csak ezen a módon lehet később rekonstruálni a tevékenységeket és bizonyítani az adatok teljességét, egy esetleges felülvizsgálat során.

Az eseményeket rögzíteni kell:

- *Az informatikai üzemeltetés* által irányított tevékenységek esetén az informatikai üzemeltetési feljegyzésekben;

A helyreállítás és dokumentálás során, amennyiben az események emberi mulasztás vagy szándékos beavatkozás miatt következtek be, gondoskodni kell a bizonyítékok megőrzéséről is.

DUNAKESZI VÁROS JEGYZŐJE

Jóváhagyta:

Dunakeszi Polgármesteri Hivatal

Informatikai Kockázatelemzési Szabályzata

Kockázatelemzési és kockázatkezelési eljárásrend

Készítette:

Nádor RENDSZERHÁZ

Dunakeszi, 2019.

TARTALOM

0. A SZABÁLYZAT KAPCSOLÓDÁSA AZ HIVATAL ELŐÍRÁSAIHOZ

A **Dunakeszi Polgármesteri Hivatal** (a továbbiakban: Hivatal) jelen dokumentumban szabályozza az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban Ibtv.), továbbá annak végrehajtási rendeletében, a 41/2015. (VII. 15.) BM rendelet által előírt, kockázatkezelési szabályozásokat, nevezetten a rendelet alábbi pontjait:

3.1.2. KOCKÁZATELEMZÉS
3.1.2.1. Kockázatelemzési és kockázatkezelési eljárásrend
3.1.2.3. Kockázatelemzés

Jelen szabályzat kiegészíti az államháztartásról szóló 2011. évi CXCV. törvény 69. §-a szerinti, Dunakeszi Polgármesteri Hivatal Jegyzőjének _____ számú Szabályzatát a Kockázatkezelési Eljárásrendről.

A kockázatkezelés stratégiája

Az átfogó informatikai biztonsági kockázatelemzéseket legalább három évenként végre kell hajtani, illetve el kell végezni akkor is, amikor változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát. Ettől függetlenül eleget kell tenni a Kockázatkezelési Eljárásrendről c. szabályzatban foglalt felülvizsgálati kötelezettségeknek is.

A kockázatok csökkentésére, illetve megszüntetésére a vizsgálat során elkészülő értékelések alapján az informatikus tesz javaslatot. Az informatikus felelőssége, hogy a kockázatelemzés eredményét beépítse az informatikai fejlesztési tervekbe és azokat elfogadásra a jegyző elé terjessze. A nem informatikai kockázatok kezeléséért felelős személyeket a jegyző jelöli ki. A kockázatok elfogadásáról, vagy a mérséklésükhöz szükséges intézkedések meghozataláról a Jegyző dönt.

A kockázatkezelő intézkedéseknek a kockázatokat az elfogadható szintre, vagy az alá kell csökkenteniük.

Az Ibtv. által előírt (4-es) szervezeti biztonsági szint eléréséig az Ibtv. fejlesztési mérföldköveihez kapcsolódóan, a kockázatelemzést meg kell ismételni. Az ilyen módon feltárt kockázatok kezelését a Cselekvési tervbe be kell építeni.

Jelen kockázatelemzési és kockázatkezelési szabályozást legalább háromévente felül kell vizsgálni, illetve felül kell vizsgálni az informatikai működési környezet jelentős változása esetén is. A kockázatelemzés eredményei bizalmas belső dokumentumként kezelendők, azokat csak a végrehajtásban érintettek ismerhetik meg.

1 BEVEZETŐ

1.1 Előzmények

Az Ibtv. célja az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint az ezeket alkotó rendszerelemek sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelme, ezáltal a kibertér védelméhez kapcsolódó jogszabályi keretek biztosítása.
Az Ibtv. által meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről a törvény végrehajtási rendlelete, a 41/2015. (VII. 15.) BM rendelet ad részletes végrehajtási utasítást.

1.2 Törvényi hivatkozások és definíciók

Az általános információbiztonsági fogalmak nem képezik részét a jelen szabályzatnak, mivel azok meghatározása a Hivatal Információbiztonsági Szabályzatában (IBSZ) is elérhető, így jelen fogalommagyarázat kizárólag a kockázatelemzésre, kockázatfelmérésre vonatkozó fogalmakra terjed ki.

a) *adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;*
b) *auditálás: előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;*
c) *bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;*
d) *fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;*
e) *fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;*
f) *kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;*
g) *kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;*
h) *kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;*

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

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

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

Az Ibtv. 7. § (1) bekezdésének előírása szerint, annak érdekében, hogy a törvény hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás kockázata szempontjából.
Az Ibtv. 9. § (1) bekezdés rendelkezése értelmében a kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a Hivatal elektronikus információs rendszerek védelmére való felkészültsége alapján meg kell állapítani a jogszabályban meghatározott szempontok szerinti a Hivatal szervezeti biztonsági szintjét.
A besorolások alkalmával, a megállapított kockázatok alapján – 1-től 5-ig számozott fokozatot kell alkalmazni.

A elektronikus információs rendszerek osztályba sorolása során meg kell állapítani a lehetséges káreseményeket, súlyosságuk szerint:

- társadalmi-politikai káros hatások, károk,
- jogsértésből, kötelezettség elmulasztásából fakadó káros hatásokat, károk,
- nemzeti adatvagyon sérülései,
- jogszabályok és egyéb szabályozások megsértése,
- jogszabály által védett adatokkal történő visszaélés vagy azok sérülése,
- közérdekűség követelményének sérülése,
- személyiséghez fűződő jogok megsértése,
- bizalomvesztés hatóságokkal, felügyeleti szervekkel szemben,
- az ország jogrendjének sérülése, vagy ennek lehetővé tétele,
- személyeket, csoportokat érintő károk, káros hatások (pl. különleges személyes adatok, banktitkok, üzleti titkok megsértése, szervezet, személyek vagy csoportok jó hírének károsodása,
- személyi sérülések, vagy haláleset bekövetkeztének veszélye,
- közvetlen anyagi károk (az infrastruktúrát, az elektronikus információs rendszert ért károk, és ezek rendelkezésre állásának elvesztése miatti pénzügyi veszteség, adatok sértetlenségének, rendelkezésre állásának elvesztése miatti költségek, dologi kár),
- közvetett anyagi károk (pl. helyreállítási költségek, elmaradt haszonnal arányos költségek, a környezet biztonságának veszélyeztetése, perköltségek).

1.3 Hatósági kockázatelemzési segédletek

A hivatal szervezeti biztonsági szintjének megállapításához, továbbá elektronikus információs rendszereinek osztályba sorolásához a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) a jogszabályon alapuló kockázatelemzési segédleteit kell alkalmazni, melyek a

- NEIH-SZVI űrlap a *szervezeti biztonsági szint* megállapításához, és az
- NEIH-OVI űrlap az *elektronikus információs rendszerek osztályba sorolásához*.

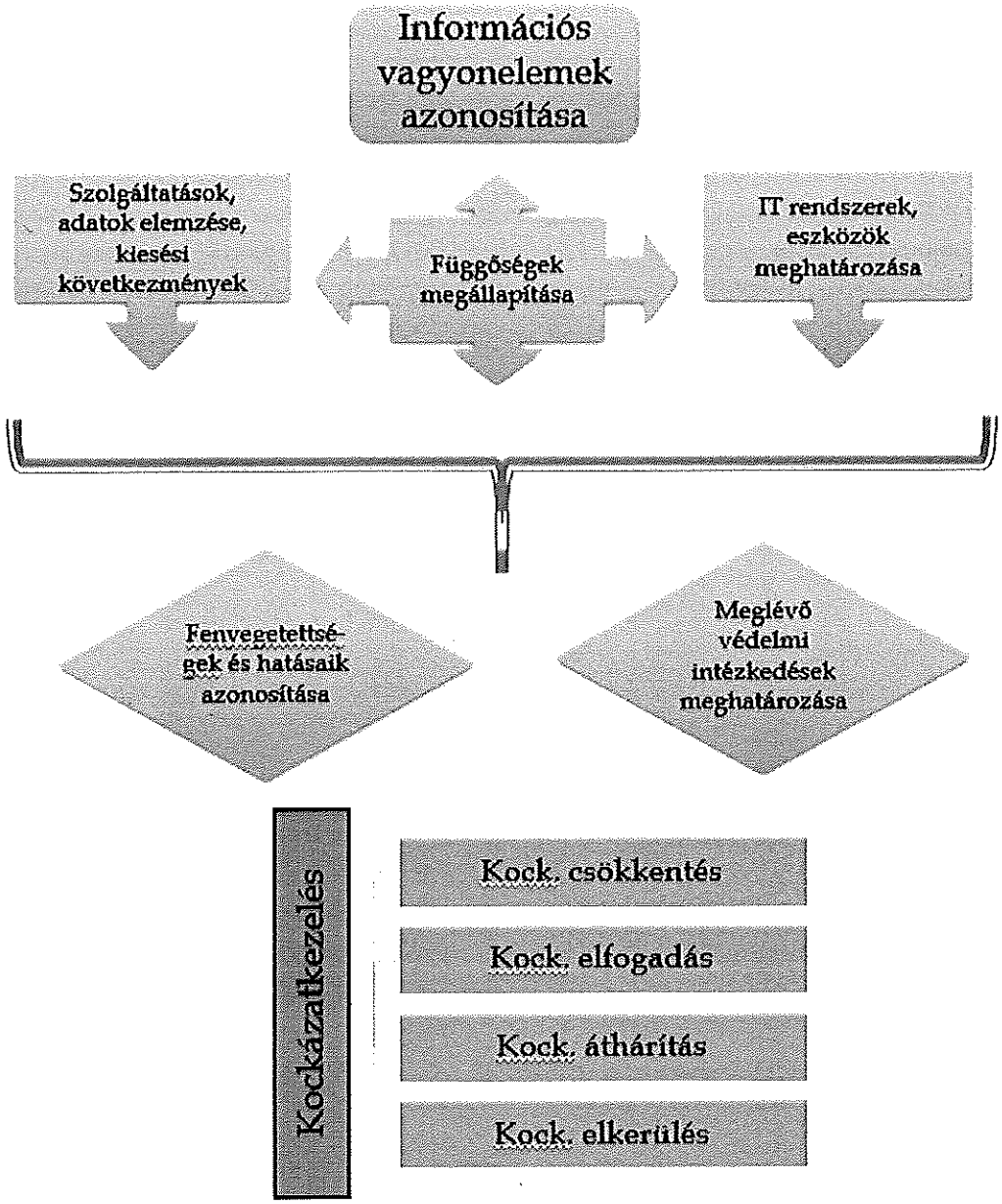
1.3.1 A biztonsági kockázatelemzés végrehajtása

Az 1.3 pontban meghatározott kockázatelemzési segédletek kitöltésével meg kell határozni az elvárt és valós (elért) szervezeti biztonsági szintet és ugyanígy meg kell állapítani az elektronikus információs rendszerek elvárt és valós biztonsági osztályát.
A besorolásokat a jegyző hagyja jóvá és a kockázatelemzések eredményét, a biztonsági szint és osztályba sorolás formájában az Informatikai Biztonsági Szabályzatban rögzíteni kell.
A kockázatelemzés részleteit jogosulatlanok számára nem szabad hozzáférhetővé tenni.

2 A kockázatelemzési vizsgálat kiegészítése

A kockázatfelmérés módszertana az ISO/IEC 15408 (Az informatikai biztonságértékelés közös szempontjai) nemzetközi szabvány, és a jó gyakorlat módszerén alapul. A hatósági kockázatelemzési értékelés kiegészíthető a Hivatal szolgáltatásainak és információs vagyonelemeinek függőségi vizsgálatával és a specifikus fenyegetettségek és kockázatok meghatározásával.
A kockázat tágabb értelemben véve azoknak az eseményeknek az összességét jelenti, amelyek bekövetkezése hatással lehet a Hivatal működésére. A kockázat megnehezíti, hátráltatja vagy legrosszabb esetben meg is akadályozhatja bizonyos funkciók ellátását, illetve célok teljesülését.
Erre a kihívásra a Hivatal kockázatkezelési eljárása ad választ oly módon, hogy elősegítse a célok, feladatok teljesülését és ezzel egy időben minimálisra csökkentse az ezt veszélyeztető tényezők bekövetkeztének esélyét, lehetséges hatását. Ezt kockázatkezeléssel érheti el a szervezet, amely tartalmazza a kockázati tényezők meghatározását, azok hatásainak felmérését, megbecsülését és a kockázati tényezőkre történő reagálást.

A kockázatelemzés folyamata:



A kockázati értékelés időszaki felülvizsgálata eredményeképpen 3. pont szerint meg kell határozni a szükséges kockázatcsökkentő intézkedéseket, illetve a kockázatkezelési folyamat után is fennálló maradvány kockázatokat. (Mivel a kockázatokat nem lehet teljes mértékben megszüntetni, ezért mindig valamilyen szinten számolni kell velük, ez a maradvány kockázat.)
A kockázatok kezelési módjai:

- ✓ Kockázatelkerülés
- ✓ Kockázatcsökkentés
  - o kármegelőző intézkedések
  - o kárcsökkentő intézkedések
- ✓ Kockázat áthárítása
  - o biztosítás jelleg, nem feltétlenül alkalmazható önkormányzat számára

- ✓ Kockázat elfogadás
  - o a nem túl jelentős kockázatok esetén

2.1.1 Kockázatértékelés kategóriái

A fenyegetés súlyossága, bekövetkezési valószínűségével arányosan eredményezhet működési zavart, de ezeket a kockázatokat kezelni kell. Az alábbi mátrix szerint kell az azonosított kockázatokat és kockázatkezelő intézkedéseket értékelni.

Kockázati besorolások

Magas	3	**1**	**2**	**3**
Közepes	2	**1**	**2**	**2**
Alacsony	1	**1**	**1**	**1**
Valószínűség		1	2	3
Hatás		Alacsony	Közepes	Magas

A kockázati besorolás három-szintű:
1.: alacsony kockázat
2.: közepes kockázat
3.: magas kockázat

A kockázati tényezők bekövetkezésének valószínűsége:
1.: alacsony valószínűség
2.: közepes valószínűség
3.: magas valószínűség

Azon kockázati tényezők, melyek valószínűségének és hatásának szorzata 1-3 közé esik, elfogadható kockázatúnak minősülnek. E feletti értékek esetében a kockázatot kezelni kell. A kockázatelemzések eredményét jelen szabályzat 1.3 fejezetében rögzített hatósági kockázatelemzési segédletekben, továbbá az 1. sz. mellékletben megadott táblázatban kell rögzíteni.

A kockázati tűréshatár feletti tartományba eső kockázatokat mindenképpen kezelni kell.

Az informatikai kockázatelemzések eredményét jelen szabályzat 1.3 fejezetében rögzített hatósági kockázatelemzési segédletekben, továbbá az 1. sz. mellékletben megadott táblázatban kell rögzíteni.

3 A kockázatok kezelése

A feltárt, informatikai rendszert érintő kockázatok kezelésének kidolgozásáért a feladatok végrehajtásáért az informatikus és a folyamatgazdák (szervezeti egységek vezetői) a felelősek.
A kockázatcsökkentő intézkedéseket a Cselekvési tervben kell rögzíteni.
A kockázatokat olyan mértékben kell csökkenteni, hogy a maradvány kockázat feleljen meg a jogszabályokban előírt szabályozásoknak, illetve a jegyző által jóváhagyott szintnek.

4 Cselekvési (intézkedési) terv készítése

Amennyiben a kockázatelemzési vizsgálat az előírt szervezeti szinthez, vagy az elektronikus információs rendszerek osztályaihoz kapcsolódó követelményekhez képest hiányosságokat tárt fel, ezek felszámolására a jogszabályok szerint cselekvési tervet kell kidolgozni, mely meghatározza a hiányosságok megszüntetésének lépéseit, mérföldköveit. A jogszabály szerint lehetőség van a hiányosságok fokozatos megszüntetésére. A cselekvési terv kidolgoztatásáért a jegyző, a kidolgozásért az informatikus felelős.
A Cselekvési tervet a 41/2015. (VII. 15) BM rendelet

3.1. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK
3.1.1. SZERVEZETI SZINTŰ ALAPFELADATOK
3.1.1.3. Az intézkedési terv és mérföldkövei

továbbá a

3.3.2. TERVEZÉS
3.3.2.3. Cselekvési terv

pontjainak előírásai szerint kell összeállítani.
A cselekvési tervet évente felül kell vizsgálni, az aktuális állapotot rögzíteni, az esetlegesen szükséges módosításokat át kell vezetni és a jegyzőnek kell jóváhagynia.

Jóváhagyta:

1. sz. melléklet

Dunakeszi IT Kockázatelemzés tábla.xlsx segédtábla

Sorsz.	Kontroll típus	Követelmény	Fenyegetés	Valószínűség	Hatás	Besorolás	Elfogadott/intézkedés szükséges	Kezelt/Maradvány kockázat?
1	Szervezeti szinten elvárt intézkedések, szabályzatok	Jogszabályi megfelelés, szabályozási terület, adminisztratív intézkedések	Jogszabályi nem-megfelelés hatósági ellenőrzés esetén	2	2	Közepes	A Hivatal rendelkezik az Ibtv. Megfelelés kezelésére Cselekvési tervvel.	A megfelelés érdekében a belső folyamatok felgyorsításra kerülnek
2		Jogszabályi megfelelés, fizikai védelmi intézkedések	Jogszabályi nem-megfelelés hatósági ellenőrzés esetén	2	3	Közepes	A Hivatal rendelkezik az Ibtv. Megfelelés kezelésére Cselekvési tervvel.	A megfelelés érdekében a belső folyamatok felgyorsításra kerülnek
3		Jogszabályi megfelelés, logikai védelmi intézkedések	Jogszabályi nem-megfelelés hatósági ellenőrzés esetén	2	2	Közepes	A Hivatal rendelkezik az Ibtv. Megfelelés kezelésére Cselekvési tervvel.	A megfelelés érdekében a belső folyamatok felgyorsításra kerülnek
4		IT kockázatok felmérése és kezelése	Nem kezelt kockázatok	3	3	Magas	Folyamatos és időszakos kockázati értékelések	Kezelt, rendszeres tevékenység
5								
6								
7	Emberi erőforrás kockázata	Informatikusok korlátos kapacitása	Nem elegendő az informatikai kiszolgáló munkatársak kapacitása	2	2	Közepes	Szükség esetén külső támogatás bevonása	Folyamatos felügyeletet igényel
8		Speciális ismereteket igénylő feladatok	Nem áll rendelkezésre belső erőforrás	3	3	Magas	Szükség esetén külső támogatás bevonása	Informatikusok jelzése alapján
9		Munkavállalók hozzáférési jogosultsággal	A szükségesnél több jogosultság, hozzáférés	1	3	Alacsony	Rendszer beállítások, külső adathordozó használat felülvizsgálata	Folyamatban
10								
11								
12								
13	Fizikai környezet biztonsága	Tűz és füstjelző	Hibás készülék esetén nem érkezik riasztás	1	3	Alacsony	Felülvizsgálat szükséges	Felülvizsgálat szükséges
14		Informatikai helyiségek belépési nyilvántartása	Jogosulatlan belépés	3	3	Magas	Nyilvántartás kialkítása szükséges	Kezelt, csak az IT munkatársak léphetnek be
15		Informatikai helyiségek fizikai védelme	Illetéktelenek hozzáférése	2	2	Közepes	Fizikai védelmi intézkedések felülvizsgálata	Folyamatban
16		Irodai helyiségek és munkaállomások védelme	Ügyfélszolgálat során potenciális információszivárgás	2	3	Közepes	Felül kell vizsgálni az irodai és ügyfélfogadási környezet kialakítását	Felülvizsgálat szükséges
17								
18								
19	A Elektronikus információs rendszerrel kapcsolatos dokumentumok, eljárásrendek	Központi ASP rendszerek dokumentációs hiányosságai, biztonsági besorolások és követelmények hiánya	A Hivatal nem tud időben felkészülni a követelményeknek való megfelelésre.	2	2	Közepes	Nem hivatali hatáskör	Nem hivatali felelősség
20								
21								
22								
23								
24								
25	A Elektronikus információs rendszer informatikai környezete	Kiszolgálók	Kapacitás problémák	1	4	Közepes	Folymatos monitoring	Kezelt
26		Háttértárak	Kapacitás problémák	1	4	Közepes	Folyamatos monitoring	kezelt
27		Mentések	Mentések sérülése fizikai vagy logikai behatás esetén	3	3	Magas	Mentések és adattárolás felülvizsgálata	kezelt
28		Határvédelmi rendszerek	Tűzfal nem megfelelősége, frissítés elmaradása	2	2	Közepes	Folyamatos személyi (rendszer adminisztrátori) felügyelet, ellenőrzés szükséges.	Felülvizsgálandó
29		Vírusvédelmi rendszer	Vírusvédelem frissítésének elmaradása vagy a vírusvédelem nem megfelelősége	2	2	Közepes	Folyamatos személyi (rendszer adminisztrátori) felügyelet, ellenőrzés szükséges.	Kezelt
30								

Alkalmazás azonosítója	Osztály	Funkció/ alapfeladatok	Rendszer szolgáltatások	Licencszám (ha értelmezhető)	Adatgazda / Felügyeletet gyakorló	Szállító, fejlesztő, karbantartó elérhetősége
DOK	2	Archív pénzügyi rendszer	Archív pénzügyi rendszer	N/A		MÁK
EDTR	1	Egységes döntéstámogatás	Egységes döntéstámogatás	N/A	Szabó László	Globomax Rt.
Exchange 2013	2	Levelezés	Levelezési rendszer	95	Szabó László	
Védett fájlmegosztások	2	Védett fájlmegosztások	Védett fájlmegosztások	N/A	Szabó László	
FMQserver	1	nyomtató rendszer (follow me kártyás azonosítás)	nyomtató rendszer (follow me kártyás azonosítás)	N/A	Szabó László	Delfin rendszerház Kft.
Gordiusz	2	Pénzügyi rendszer	Pénzügyi rendszer	N/A	Szabó László, Pállné Kovács Mária	Korend Kft.
Govcenter	1	Telephely nyilvántartás, internetes kliens	Telephely nyilvántartás, internetes kliens	N/A	Slisszné Kárpáti Rózsa	
Govsys	2	Integrált iratkezelő rendszer	Integrált iratkezelő rendszer	N/A	Szabó László	Professzinál Zrt.
Intepsystem	2	Munkaidő nyilvántartó és beléptető rendszer	Munkaidő nyilvántartó és belépttető rendszer	N/A	Szabó László	Intep Kft.
ITR3	1	Térképészeti rendszer	Térképeszeti rendszer	N/A	Passa Gábor, Szabó László	DigiCart Kft.
KataWin	1	Ingatlan nyilvántartó rendszer	Ingatlan nyilvántartó rendszer	N/A	Szabó László, Pállné Kovács Mária	E-szoftverfejlesztő Kft.
Mikrovoks	2	Jegyzőkönyvező, szavazatszámláló, és konferencia rendszer	Jegyzőkönyvező, szavazatszámláló, és konferencia rendszer	N/A	Szabó László	Globomax Rt.
Onkado	2	Adóügyi rendszer	Adóügyi rendszer	N/A	Szabó László, Lukács Adrienn	Magyar Államkincstár
WINIKSZ	2	Integrált közszolgálati szoftvercsomag	Integrált közszolgálati szoftvercsomag	N/A	Jakabnet Kft.,Szabó László	Jakabnet Kft.

Dunakeszi Polgármesteri Hivatal

Helyreállítási Szabályzat
Informatikai katasztrófa esetére

Nádor
RENDSZERHÁZ

2019.

A DOKUMENTUM MÓDOSÍTÁSAINAK JEGYZÉKE

A dokumentum következő felülvizsgálatát 2020. 06.30.-ig el kell végezni.

1	1.1	2019.03. 05	szerepkör módosítás, véglegesítés		
1	1	.			
Kiadás	**Verzió**	**Dátum**	**A megelőző dokumentum száma**	**Dokumentum azonosító (ikt. sz.)**	**Hatályba helyező utasítás száma**

TARTALOMJEGYZÉK

1 Általános rendelkezések

1.1 A Helyreállítási Szabályzat célja

A Katasztrófa Helyreállítási Szabályzat (angol teminológiával Disaster Recovery Plan, DRP) célja, hogy a **Dunakeszi Polgármesteri Hivatal** (a továbbiakban: Hivatal) az elvárásoknak megfelelve, magas színvonalon biztosítsa elektronikus információs rendszerének folytonos működését, működési szempontból meghatározó jelentőségű funkciók kiesése – úgynevezett informatikai katasztrófa helyzet – esetén pedig a funkcionalitás mielőbbi helyreállítását és az ügymenet mielőbbi folytatását.

1.2 Személyi hatálya

A Szabályzat személyi hatálya az intézményben foglalkoztatott valamennyi alkalmazottra, fő- és részfoglalkozású munkavállalóra, illetve az informatikai eljárásban résztvevő más szervezetek dolgozóira (a továbbiakban együtt: munkatársak) egyaránt kiterjed.

A Helyreállítási Szabályzat személyi hatálya kiterjed továbbá minden személyre, aki az Hivatal informatikai vagy azzal összefüggő rendszerét, szolgáltatásait igénybe veszi, informatikai struktúráját és annak eszközeit üzemelteti vagy használja, függetlenül az Hivatalhoz kapcsolódó jogviszonyától.

1.3 Tárgyi hatály

Kiterjed az Hivatal működése szempontjából kiemelt fontosságú informatikai rendszereire, amelyek tárolják, kezelik, feldolgozzák, felügyelik, ellenőrzik és/vagy továbbítják az Hivatal kezelésében/tulajdonában álló adatokat, információkat.

2 A Szabályzat leírása

A Helyreállítási Szabályzat az esetlegesen bekövetkező informatikai katasztrófa helyzetet követő feladatokat határozza meg, azaz pontosan a katasztrófa utáni *helyreállítás* tervezéséről van szó. Meghatározza ugyanakkor a normál működési rend során elvégzendő felkészülési feladatokat, a helyreállítás személyi és tárgyi feltételeinek biztosítását.

Definíció szerint a katasztrófa Helyreállítási Szabályzat súlyos incidens bekövetkezése után a károk felmérését, és a normál működési szintre való hatékony visszaállást szabályozó intézkedések együttese.

Ez a Szabályzat azokat a felmérési, tervezési, ellenőrzési és javítási feladatokat fogalmazza meg, melyek biztosítják, hogy egy esetleges katasztrófa helyzetet követően a normál működés mielőbb helyreálljon.

A szabályzat segítségével, katasztrófa helyzet bekövetkezése esetén az Hivatal

- képes a károk bekövetkezése utáni a gyors és koordinált reagálásra,
- képes a működésben bekövetkező kiesését és ennek hatásait a minimálisra csökkenteni,
- képes az informatikai szolgáltatások mielőbbi helyreállítására

A szabályzat a következő részekből épül fel:

- A Helyreállítási Szabályzat hatóköre
- Szerepek és felelősségek
- Kockázati felmérés
- A katasztrófa kezelés fázisai
  - felkészülési fázis
  - válasz fázis
  - visszaállási fázis
  - helyreállítási fázis
- Releváns erőforrások helyreállítási terve
  - központi erőforrások helyreállítása
  - hivatali épületek erőforrásainak helyreállítása
- A Szabályzat karbantartása
  - a szabályzat előírásainak tesztelése
  - a szabályzat oktatása

2.1 A szabályzatban alkalmazott fogalmak

A szabályzatban alkalmazott fogalmak magyarázatát az alábbiakban adjuk meg.

a) *alternatív megoldás*: a zavar áthidalását célzó (egyik) lehetőség;

b) biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

c) *egyszerű informatikai incidens*: egyedi, kis jelentőségű meghibásodások. Az informatikai rendszer működése lényegében folyamatos. Tipikus esetek: elfelejtett jelszó, felhasználói gép meghibásodása.

d) *elsődleges informatikai szolgáltatások*: azok az informatikai szolgáltatások, amelyekkel az szakmai felhasználók közvetlenül találkoznak.

e) *helyreállítás*: a biztonsági rendszerek teljes funkcionalitású, eredeti állapotba történő hozása;

f) *incidens, esemény*: egymás szinonimájaként használt kifejezések, amely alatt az információbiztonság (bizalmasság, sértetlenség és rendelkezésre állás) sérülését értjük. Általánosan használt kifejezések, amelyek a legkisebb jelentőségű eseménytől (pl. jelszó elfelejtése) a katasztrófa helyzetig terjed.

g) *informatikai katasztrófa:* informatikai katasztrófák esetén az informatikai szolgáltatások jelentős része nem elérhető. Helyreállítás nem lehetséges a sebezhetőségi ablakon belül. Tipikus esetek: tűz, természeti katasztrófa, rendszer elleni vírus vagy hacker támadás.

h) *informatikai üzemzavar*: egy-két szerver vagy hálózati aktív eszköz meghibásodása. Az informatikai szolgáltatások egy része nem elérhető.

i) *káresemény*: a káresemény az információbiztonság (bizalmasság, sértetlenség és rendelkezésre állás) sérülése. Az esemény, incidens kifejezések szinonimája azokban az esetekben, amikor az esemény valóban információbiztonsági kárral jár.

j) *Katasztrófa Helyreállítási Team:* több működési terület szakmai képviselőiből, továbbá informatikai támogató szervezetekből álló munkacsoport, amely a fellépő katasztrófa helyzetek megoldásban döntési jogkörrel rendelkezik;

k) *katasztrófa*: Az szakmai folyamatok, és/vagy az azokat kiszolgáló háttérrendszerek folyamatos és zavarmentes működését veszélyeztető, átmenetileg, vagy végleg lehetetlenné tevő rendkívüli esemény. Katasztrófaforrások lehetnek pl.: informatikai rendszerelemek hibái, egyéb kiszolgáló infrastruktúra hibái és/vagy hiányosságai, természeti katasztrófák és egyéb külső tényezők, külső, vagy belső rosszakaratú károkozás, belső nem rosszakaratú károkozás, stb.;

l) *MTO (Maximum Tolerable Outage)*: „Maximális elfogadható kiesés" Az MTO az a maximális időtartam, ameddig az Hivatal feladatainak akadályoztatása informatikai katasztrófa helyzet esetén még éppen elviselhető. Az MTO időtartamánál nem hosszabb szolgáltatás kiesés legfeljebb magas vagy nagyon magas szakmai hatást (veszteséget) okozhat, de nem okozhat katasztrofális veszteséget.

m) *RPO (Recovery Point Objective)*:„Visszaállítási időpont cél" Az RPO adja meg azt a maximálisan elfogadható időtartamot, amelyre vonatkozó adatvesztés el tud fogadni az szakmai felhasználó kiterjedt meghibásodások, katasztrófák esetén. Például egy 24 órás RPO érték azt jelenti, hogy az adatbázis megsemmisülését követő visszaállítás után az utolsó (a katasztrófát megelőző) 24 órában rögzített adatok elvesztek, csak az azt megelőzően rögzített adatok állíthatók vissza.

n) *RTO (Recovery Time Objective)*: „Visszaállítási időtartam cél". Az RTO az az időtartam, amely egy adott IT rendszer visszaállítását biztosítani kell annak kiesését követően. A RTO-t közvetlenül az IT rendszerekre határozzuk meg, míg a hasonló tartalmú sérülékenységi ablakot az elsődleges informatikai szolgáltatok kapcsán értelmezzük.

o) *sebezhetőségi ablak:* A sebezhetőségi ablak az a maximális időtartam, ameddig az Hivatal feladatainak ellátása lényegében fenntartható egyes informatikai erőforrások kiesése esetén. A sebezhetőségi ablak időtartamánál nem hosszabb szolgáltatás kiesés legfeljebb alacsony szakmai hatást (veszteséget) okozhat.

p) *UPS (Uninterruptible Power Supply)*: szünetmentes tápellátást biztosító tápegység, amely az elektromos hálózat (230V) kimaradása esetén egy adott ideig képes a rákapcsolt eszközök tápellátását biztosítani.

q) *visszaállítás:* azon lépések sorozata, amelyek által legalább minimális funkcionalitással újra működőképessé

2.2 A Szabályzat hatálya alá nem tartozó feladatok

A Helyreállítási Szabályzat csak az elektronikus információs rendszerek támogató rendszereire terjed ki, nem foglalkozik az emberek mentésével, illetve más (nem informatikai biztonsági szolgáltatást nyújtó) vagyontárgyak kezelésével kapcsolatos katasztrófa helyzetek esetén. Ezeket a területeket más

eljárásrendek, utasítások fedik le, amelyekkel összhangban kell alkalmazni jelen Szabályzatot és a kapcsolódó dokumentumokat.

A Szabályzat hatóköréből kivont informatikai események:

- az informatikai üzemzavar esetei, amelyek a *sebezhetőségi ablakon* belül megoldhatók,
- azok a tervezett leállások, karbantartási időszakok, amelyek akár a sebezhetőségi ablakot meghaladó szolgáltatás kiesést okoznak.

3 Szerepek és felelősségek

A katasztrófa utáni helyreállítás folyamatának szervezett és begyakorlott végrehajtása érdekében felelősségi köröket, feladatokat kell meghatározni, és ezekhez a funkciókhoz személyeket kell rendelni, állandó vagy ideiglenes jelleggel.

Az esetleges informatikai jellegű katasztrófa elhárítás tevékenysége lényegében a rendszerek üzemeltetésével, karbantartásával, telepítésével azonos szakmai kompetenciákat kíván, ezért a vészhelyzeti helyreállításban, az esemény jellegétől függően kell a központi rendszerek üzemeltetőit bevonni.

3.1 Helyreállítási team

Működésfolytonosságot érintő incidens bekövetkezése esetén a helyettesítő szolgáltatások beindítását, a helyreállítási folyamat működtetését az informatikai irodavezető koordinálja.

Az informatikai irodavezető feladata az ügymenet folytonossági tervek, és ezen belül a katasztrófa utáni helyreállítási tervek működésének figyelemmel kísérése, valamint szükség esetén változtatások kezdeményezése. Az informatikai irodavezető saját hatáskörében kijelöli a helyreállítási tevékenység folyamatos felügyeletét, működtetését biztosító munkatársakat.

A helyreállítás tervezésének és végrehajtásának a Hivatal szakmai céljait kell szolgálni, ezért az informatikai irodavezető minden esetben tájékoztatja a Hivatal helyreállításért felelős vezetőjét, szükséges esetben kikéri döntését.

HELYREÁLLÍTÁSI SZEREPKÖR	FELELŐS
Helyreállítási Team vezetője	Jegyző
Helyreállítási Team informatikai vezetője	Informatikus
Helyreállítás hivatali operatív vezetője	Aljegyző, a helyreállítás vezetésére kijelölt hivatali felső vezető
Rendszerek szakmai felelősei	Helyreállítás vezetésére kijelölt szakmai vezető(k)
Informatikus támogatók	Helyreállítás szakmai végrehajtói, rendszertámogatás

A z egyes funkciókhoz aktuálisan rendelt felelős személyek adatait és elérhetőségét az Értesítési Listák tartalmazzák.

3.2 A helyreállítási team tagjai

A helyreállítási team tagjai számos felelősséget viselnek a vészhelyzeti felkészülés során és az esetlegesen bekövetkezett katasztrófa helyzet kezelésében is. Általában igaz, hogy a normál működés során folyamatosan követni kell a szervezetben, az szakmai követelményekben és az informatikai környezetben bekövetkezett változásokat és fel kell készülni az ebből fakadó követelményekre.

Biztosítani kell, hogy folyamatosan rendelkezésre álljanak a helyreállításhoz szükséges anyagi és emberi erőforrások.

- *Helyreállítási Team vezetője;* a jegyző katasztrófa helyzet esetén közvetlenül irányítja a helyreállítási tevékenységet. A helyreállítás szakmai vezető folyamatosan tájékoztatja a pillanatnyi helyzetről, vele konzultálva meghozza a szükséges döntéseket.

- *Helyreállítási Team informatikai vezetője;* informatikus vagy az őt helyettesítő (külső) munkatárs: A felkészülési időszakban az aljegyző irányítása szerint látja el feladatát, teljes körűen ismeri a katasztrófa utáni helyreállítás informatikai tevékenységeit.

- *Helyreállítás hivatali operatív vezetője;* az aljegyző, a helyreállítás vezetésére kijelölt hivatali szakmai felső vezető: a jegyző által kijelölt szakmai felső vezető, aki a Hivatal teljes működését átlátva, szakmai prioritások szerint meghatározza az informatikai rendszerek rendelkezésre állási követelményeit. A felkészülési időszakban egyezteti az informatikussal a meglévő technikai lehetőségeket, a kialakított helyreállítási képességeket. Megszervezi az szakmai területen belül, az informatikai rendszerek részleges vagy teljes kiesésére, vagy az egyes hivatali helyiségek pótlására vonatkozó ideiglenes intézkedési terveket. Az szakmai területeken biztosítja, hogy az érintett munkatársak a szükséges mértékben megismerjék az informatikai rendszerek helyreállítási terveit, továbbá az azokhoz fűződő feladataikat.

  Katasztrófa helyzet esetén a helyreállítási team informatikai vezetője (informatikus) folyamatos tájékoztatást nyújt számára a helyreállítás státuszáról. A helyreállítás hivatali operatív vezetője szükség szerint dönt a helyreállítási prioritásokról.

- *Rendszerek szakmai felelősei*; Helyreállítás vezetésére kijelölt szakmai vezetők: az általános helyreállítási feladatokon belül, a Hivatal vezetésének döntése szerint, egyes szakterületek vezetői külön feladatokat és felelősségeket viselnek az általuk irányított terület informatikai támogatásával, illetve annak folytonosságának biztosításával kapcsolatban. Feladatuk területükön meghatározni az informatikai rendszerek rendelkezésre állási követelményeit, s az elvárásokat az informatikai irodavezető vel egyeztetniük kell. Az esetleges vészhelyzetekre való felkészülés során meghatározzák a területük feladatait, kijelölik a felelősöket.

  Informatikai katasztrófa helyzet esetén irányítják területének munkatársait, a helyreállítás pillanatnyi helyzetének megfelelően szervezik a tevékenységeket.

- *Informatikai támogatók*; Helyreállítás szakmai végrehajtói, rendszertámogatás: feladatuk a helyreállítási felkészülés során a felelősségi körükbe tartozó rendszerek technikai felkészítése. Ebbe a feladatkörbe tartozik a rendszerek dokumentálása, a szükséges mentések elvégzése és azok frissítése és ellenőrzése, a technikai helyettesítő és tartalék megoldások megtervezése. Felelősségük a katasztrófa elhárítási tervek, azok végrehajthatóságának ellenőrzése és a rendszeres előírt tesztelések elvégzése és dokumentálása.

  Katasztrófa helyzet esetén a tervek szerinti intézkedéseket hajtják végre, közvetlen beszámolással az *Helyreállítási Team informatikai vezetője* felé tartoznak.

4 Kiinduló hatáselemzés

Gondosan megtervezett és megvalósított megelőző intézkedések esetén is lehetséges, hogy olyan meghibásodások, emberi tévedések és/vagy természeti katasztrófák történnek, amelyek a biztonsági rendszerek és szolgáltatások kiesését okozzák. A helyreállítási intézkedések megtervezéséhez szükséges kiinduló adatok meghatározása a szakmai terület elvárásai alapján a Kockázati Jelentésben került összefoglalásra.

Az egyes működési területekre, meghatározásra kerültek a maximálisan elfogadható kiesési idők, (MTO, Maximum Tolerable Outage), melyek időtartamig az adott szolgáltatás nélkülözhető. Ezek az időtartamok tekintendők a katasztrófa helyzet utáni visszaállítás cél-értékének, az úgynevezett sebezhetőségi ablaknak.

Azok az események, melyek hatása az adott eszközre vonatkozó sebezhetőségi ablakon belül helyreállíthatók, nem tekinthetők katasztrófa helyzetnek.

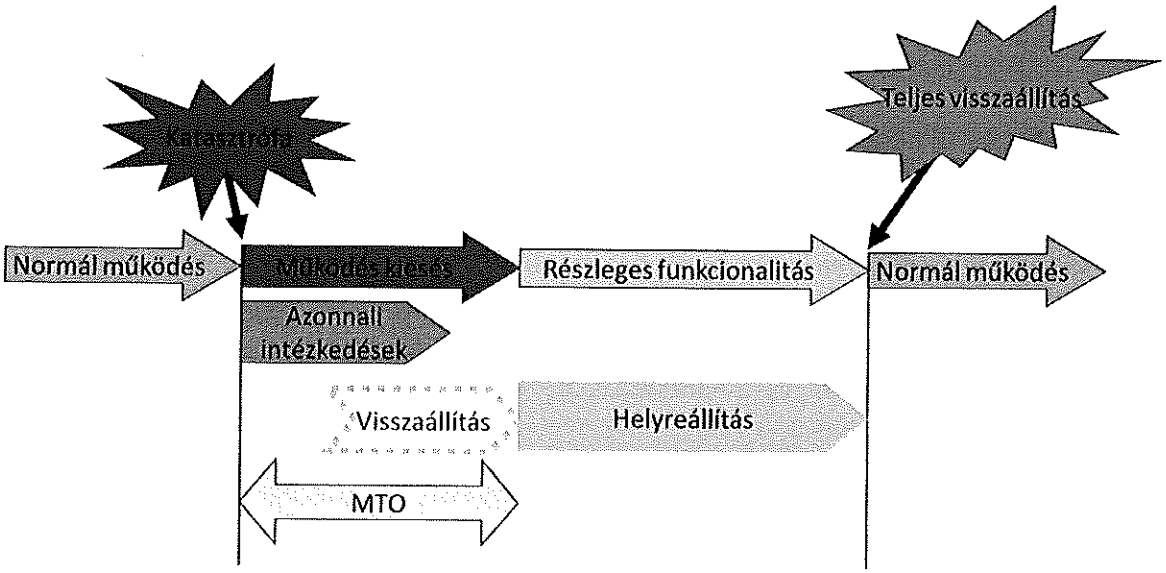
A katasztrófa helyreállítási tervezés során az a cél, hogy legalább az adott funkció visszaállítási ideje a sebezhetőségi ablakon belül maradjon. A biztonsági architektúra több elemének sérülése esetén nem kerül meghatározásra a szakmai prioritások alapján a visszaállítási sorrend, mivel a sorrendet a technikai lehetőségek határozzák meg. Az informatikai alap infrastruktúra nagyobb arányú sérülése esetén a visszaállítás, illetve helyreállítás során informatikai szempontból meg kell állapítani a helyreállítási tevékenységek sorrendjét, melyek az architektúra tulajdonságaiból következnek, például a hálózati működés helyreállítása előbb történik, mint a tartományvezérlők helyreállítása.)

A Hivatal követelményei szerint:

- Elfogadható kiesési idő:
  - kritikus rendszereknél: 24 óra,
  - egyéb kategóriák: egy hét,
  - maximum: egy hónapon belül valamennyi funkciónak működnie kell.
- Az események szakmai hatás szerinti kategorizálása:
  - szakmailag kritikus hiba,
  - szakmailag nem kritikus hiba.
- A kritikus hibák következményeik szerint az alábbi kategóriákba kerültek:
  - indifferens,
  - kisebb hiba,
  - súlyos hiba,
  - katasztrofális hiba,

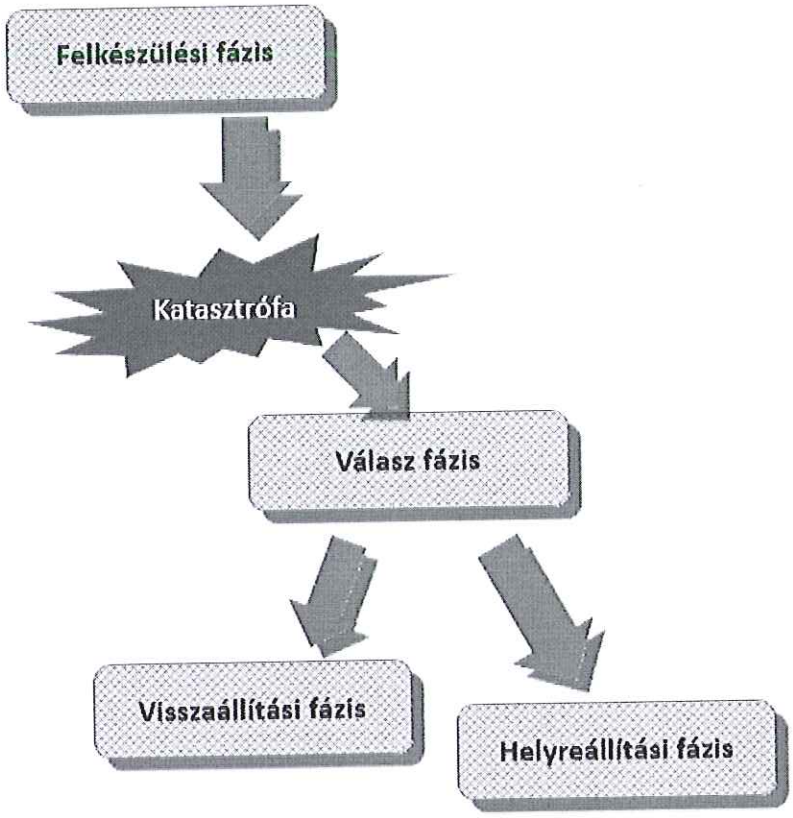
5 A katasztrófa kezelés fázisai

A katasztrófa helyzet bekövetkeztét, annak helyreállítási lépéseit szemlélteti az alábbi ábra.



A normál működést megszakító esemény után az adott funkcióban működés kiesés következik be. A katasztrófa helyreállítás tervezése során azt a célt kell elérni, hogy a működés kiesés az azonnal megtett intézkedések hatására megszűnjön, legalább részleges funkcionalitással vissza lehessen állítani a szolgáltatás – ez a visszaállítási fázis, melynek az elvárások szerint az MTO, a maximálisan tolerálható kiesés értékén belül kell lennie. Ezek után a teljes funkcionalitás helyreállítása következhet, de ahhoz már nem kötődnek kritikus időpontok.

- A katasztrófa kezelés fázisai az alábbiak:
  - felkészülési fázis
  - válasz fázis
  - visszaállítási fázis
  - helyreállítási fázis



5.1 Felkészülési fázis

Az esetlegesen bekövetkező katasztrófa helyzetre fel kell készülni. Az üzemeltetési szereplőknek meg kell tenniük azokat a lépéseket, mellyel biztosítják, hogy katasztrófa helyzet bekövetkezése esetén rendelkezésre álljanak mindazok az erőforrások, melyek a hatékony válasz lépésekhez szükségesek. Az erőforrások részben személyi, részben szervezési-szabályozási, részben műszaki-technikai jellegűek. (Hozzáértő, felkészült támogató szakemberek, szabályozások, folyamatok, továbbá tartalék technikai eszközök.)

A felkészülési fázis során kell

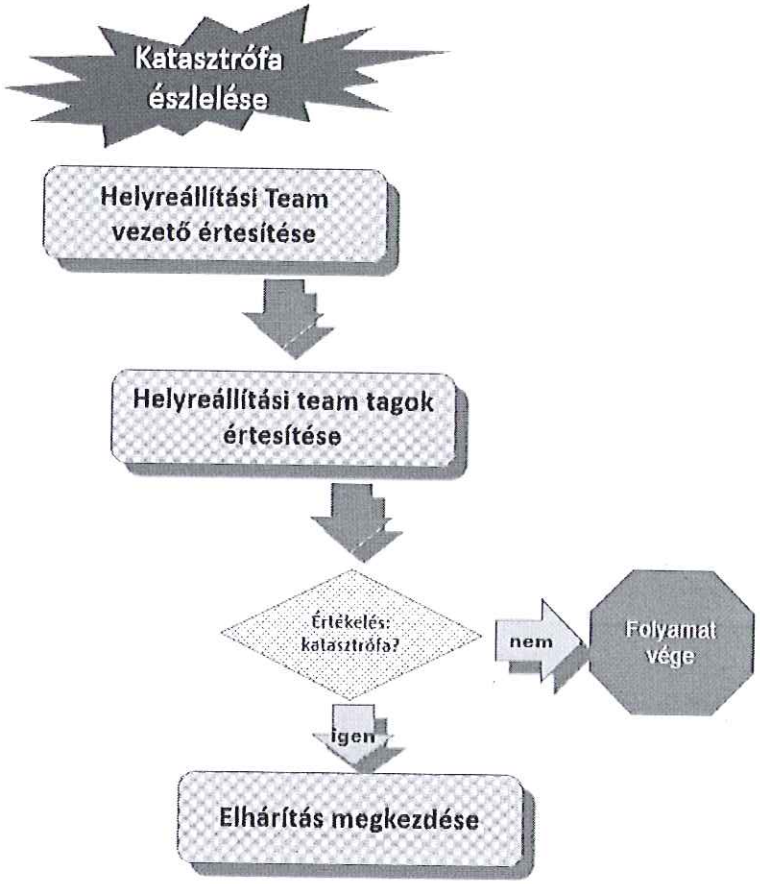
- létrehozni a katasztrófa helyreállításban részt vevő csoportokat, meghatározni a felelősségi köröket, személyeket hozzárendelni az egyes funkciókhoz,
- összeállítani a szükséges dokumentációt,
    - mentés-visszaállítási terveket,
    - egyéb dokumentumokat, helyreállítási folyamatokat, értesítési listákat stb.
- megfelelő szerződéses rendelkezésre állást biztosítani a beszállítók és támogató cégek részéről,
- a katasztrófa tervet tesztelni és oktatni.

A felkészülési fázisban figyelembe kell venni a szakterületek helyreállítási prioritásait, melyeket a hivatali Ügymenet Folytonossági Szabályzatban meghatározott RTO és RPO értékek határoznak meg.

5.2 Válasz fázis

A katasztrófa helyzet bekövetkezése esetén kell az úgynevezett „válasz fázis"-ban meghatározott intézkedéseket végrehajtani.

A „válasz fázis" folyamatán belül történik meg a katasztrófa felismerése, az érintettek értesítése, riasztása, továbbá a szükséges intézkedések meghozatala.



Az egyes lépések:

1. bejelentés érkezése a katasztrófa helyzetről
2. helyreállítási team tagok értesítése
3. helyzet értékelése: valóban katasztrófa helyzet van-e?
4. Amennyibe igen, akkor a katasztrófa helyzet kommunikálása az érintettek felé és az helyreállítás (visszaállítás) megkezdése

A kialakult helyzet értékelése

A legfontosabb tényezők, amelyek katasztrófahelyzetre, vagy katasztrófa közeli helyzetre utalhatnak:

a) természeti katasztrófa (tűz, vízbetörés stb.) vagy támadás következtében megsérültek a szerverterem vagy a hivatali épületek informatikai infrastruktúra kritikus elemei;

b) megrongálódtak az adatátviteli rendszer elemei, épület belső kábelezése;

c) támogató infrastruktúra kiesése lépett fel (elektromos áramellátás szünetel vagy szünetelt, telekommunikációs problémák stb.);

d) minden olyan egyéb esemény, amely az informatikai szolgáltatások leállását okozhatja;

e) az informatikai infrastruktúra észlelt, a szokásos módon nem helyreállítható rendellenes működés vagy meghibásodása.

Döntés a katasztrófa helyzet kihirdetéséről

Amint a Helyreállítási Team Vezető értesül a kialakult helyzetről, mérlegelnie kell az esemény súlyát, szükség esetén konzultál a Helyreállítási Team tagjaival és dönt a riasztás elfogadásáról és a katasztrófa helyzet kihirdetéséről, illetve arról, hogy az esemény kezelése megoldható-e normál üzemeltetési feladatként.

Kommunikációs és adminisztrációs terv

A katasztrófa helyreállítási tevékenységgel kapcsolatos külső kommunikációt kizárólag a Hivatal vezetése által felhatalmazott személyek folytathatnak. Ez a kommunikáció kiterjed a

- ügyfelek közvetlen tájékoztatására (hirdetmény, weblap stb.),
- érintett hatóságok előírt tájékoztatására,
- média tájékoztatására.

Az elektronikus információs rendszerek biztonságáért felelős személy megadja a jogszabályban előírt tájékoztatás a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) felé.

A munkatársaknak tilos felhatalmazás nélkül szervezeten kívüli személyeknek az felmerült eseményről tájékoztatást adniuk.

5.3 Visszaállítási fázis

A visszaállítási fázis során meg kell teremteni az eszközök, rendszerek működőképességét, lehetőség szerinti átállítását tartalék erőforrásokra vagy megkerülő megoldásokra.

Amennyiben kiépítésre kerültek a katasztrófában érintett eszközökkel párhuzamos erőforrások, akkor elsődlegesen azokat kell aktiválni. Az aktiválás előtt a párhuzamos alrendszerek működőképességét ellenőrizni kell. Ha tartalék eszközökkel lett megtervezve a visszaállítási folyamat, akkor azokat kell aktiválni.

A visszaállítási fázis mellett, illetve helyett a helyreállítási tevékenységet is el kell indítani.

5.4 Helyreállítási fázis

A helyreállítási fázis során a rendszerek funkcionalitásait az eredetivel azonos szinten helyre kell állítani, vagy az eredetivel egyenértékű erőforrások bevonásával, vagy az eredeti eszközök javításával, helyre állításával. Ez a fázis akkor ér véget, ha a biztonsági rendszer legalább az eredetivel azonos módon képes működni.

A fázis lépései:

- kárfelmérés
- helyreállítás tervezése
- kárkövetkezmények elhárítása
- normál működés helyreállítása

5.5 A katasztrófa kezelés alkalmazhatósága

A fenti folyamatok alkalmazhatóságához szükséges az egyes lépések tesztelése, továbbá a részt vevő szereplők oktatása, a folyamatok gyakorlása.

6 A Helyreállítási Szabályzat karbantartása

6.1 A katasztrófa helyreállítási dokumentumok tárolása

A helyreállítási terveket, vonatkozó értesítési kistákat és az egyéb, a helyreállításhoz szükséges dokumentumokat több helyen kell tárolni, annak érdekében, hogy bármelyik helyszín kiesése esetén az intézkedéshez szükséges dokumentumok elérhetők legyenek. Jelen szabályzatot és a kapcsolódó dokumentumokat kinyomtatva és elektronikus formában (pendrive-on vagy CD/DVD lemezen) is el kell helyezni az alábbi helyszíneken:

- A jegyzőnél, a jegyzői iroda zárt iratszekrényében,
- Informatikus irodájában,

A helyreállítási dokumentumok szerves kiegészítői a rendszer mentések, (adattrezor archívumok), melyek tárolási helye egyrészt szerverteremben van, másrészt a másrészt a mentések másodlagos tárolási helyén.

6.2 A dokumentumok frissítése

A katasztrófa helyreállítási terveket rendszeresen felül kell vizsgálni és szükség szerint frissíteni kell. A felülvizsgálatot évente legalább egyszer, tervezetten végre kell hajtani, illetve minden esetben el kell végezni soron kívül, ha az üzemeltetési környezetben, szervezetekben, eljárásrendekben jelentős változás következett be.

6.3 A Szabályzat tesztelése

6.3.1 A tesztelés tervezése

Az Informatikai katasztrófa helyreállítási terv tesztelésére éves tervet kell készíteni. A terv elkészítéséért és a tesztelés végrehajtásáért a Helyreállítási Team vezetője a felelős.

A teszt terv tartalmazza a következőket:

- a teszt végrehajtásának időpontját és helyszínét,
- a teszt módszerét és az alkalmazott eljárást,
- a tesztben résztvevők körét.

Annak érdekében, hogy meg lehessen győződni az összes rendszer-elem rendelkezésre állásáról, a közreműködők rendszer-ismeretéről és a visszaállítási folyamatok hiánytalan működőképességéről, a katasztrófa helyreállítási terveket tesztelni kell. Első alkalommal a terveket a bevezetés előtt kell tesztelni, soron kívüli tesztelés szükséges továbbá minden, az üzemeltetési környezetben történt jelentős változás esetén is.

A tesztelési eljárások és azok elvárt gyakorisága az alábbi táblázatban került összefoglalásra:

Teszt módszer	Teszt gyakorisága	Megjegyzés
Ellenőrző listás tesztelés	esetileg	kisebb erőforrás ráfordítású
Szóbeli tesztelés	negyedévente	részvevők teljes köre érintett
Szimulációs tesztelés	eseti elrendelés alapján	Vezetői döntés szerint
Párhuzamos tesztelés	nem alkalmazható	A jövőbeni tervezett fejlesztések után, párhuzamos infrastruktúra esetén lehetséges
Teljes leállás-visszaállítás	csak infrastruktúra frissítés vagy csere esetén	eseti döntés alapján, normál üzem mellett nem alkalmazható

6.4 A tesztelés módszerei

Különböző mélységű és bonyolultságú tesztelési eljárások együttes alkalmazásával érhető el a kívánatos célt, miszerint a teszt segítségével kerül ellenőrzésre a terv hatékonysága, feltárásra kerülnek az esetleges hiányosságok és begyakorolható a helyreállítási tevékenység végrehajtása. Az egyes tesztelési eljárások egymásra épülnek, a bonyolultabbat nem érdemes addig elvégezni, amíg az azt megelőző egyszerűbb tesztek sikeresen elvégzésre nem kerülnek.

Az alkalmazandó teszt módszerek a következők:

- Ellenőrző listás tesztelés (Checklist Testing)
- Szóbeli tesztelés (Walk Through Testing)
- Szimulációs tesztelés (Simulation Testing)
- Párhuzamos tesztelés (Parallel Testing)
- Teljes leállás-visszaállítás tesztelés (Full Interruption Testing)

Az összetettebb tesztek hosszabb időt, nagyobb emberi erőforrás felhasználást és járulékos költséget igényelnek. Ezeket a szempontokat a teszt előkészítésénél figyelembe kell venni.

6.4.1 Ellenőrző listás tesztelés (Checklist testing)

A teszt ciklust ezzel a teszttel célszerű kezdeni és abban az esetben kell tovább lépni, mikor ez a teszt eredményesen lezárult.

Alapvetően a katasztrófa helyreállítási terv és kapcsolódó dokumentumainak, valamint mellékleteinek meglétét és aktualitását kell ellenőrizni, elsősorban a következőkre kiterjedően:

- vészhelyzeti értesítési listák ellenőrzése

- tartalék eszközök rendelkezésre állása
- mentések elérhetősége, teljessége és ellenőrzöttsége
- visszaállítási utasítások megléte és teljessége
- egyéb kapcsolódó dokumentumok megléte és teljessége

6.4.2 Szóbeli tesztelés (Walk Through Testing)

A résztvevők szóban egy fiktív katasztrófahelyzetet szimulálva a Helyreállítási Szabályzat dokumentáció lépéseit követve lépésről lépésre ellenőrzik a terv hatékonyságát, gyenge pontjait. A teszt csak szóbeli ellenőrzést foglal magába, a résztvevők irodai körülmények között végzik az ellenőrzést, amely fő területei:

- feladatszegmensek,
- input / output adatok, dokumentumok,
- értesítési utak, módok, kontaktszemélyek,
- adattárolás, rögzítés.

A tesztelést az *Helyreállítási Team Vezetője* irányítja, a hozzászólásoknak a feladatok funkcionális egymásra épülésének sorrendjében kell követniük egymást. Minden szóbeli tesztelést meg kell, hogy előzzön egy sikeres ellenőrző listás tesztelés.

6.4.3 Helyzet-szimulációs tesztelés (Simulation Testing)

A helyzet-szimulációs teszt esetén a teszt időpontjáról csak a Helyreállítási Team Vezető és helyettese tudhat. A teszt során a központi kiszolgálók, vagy az hivatali épületek informatikai hálózata valamely kritikus elemének váratlan kiesését kell szimulálni. A riasztás után a valódi katasztrófa helyzethez leginkább hasonlító módon kell elvégezni a Katasztrófa Helyreállítási terv minden lépését, beleértve az érintett informatikai rendszerek visszaállítását is. Csak azok az anyagok és információk használhatók, amelyek egy tényleges katasztrófa helyzetben rendelkezésre állnak.

A tesztelést olyan mélységig szabad elvégezni, hogy a már rendelkezésre álló architektúra működőképességét ne érintse. A szóbeli teszteléshez képest jelentős különbség, hogy a tesztre az érintettek nem tudnak felkészülni, így valamennyi erőforrás, folyamat, személy, dokumentum rendelkezésre állását a teszt időpontjában kell bizonyítani.

Minden helyzet-szimulációs tesztelést meg kell, hogy előzzön egy sikeres szóbeli tesztelés.

6.4.4 Párhuzamos tesztelés (Parallel testing):

A párhuzamos tesztelés a tesztelési módszertanok fontos része, mert azoknak a katasztrófahelyzeteknek a kezelését vizsgálja, ahol a visszaállítás az alternatív helyszínen történik az ott tárolt tartalék eszközökön és back-up adatokból.

A párhuzamos tesztelés megvalósításához független helyreállítási teszt környezet kialakítása szükséges.. A tesztelés során különös gondossággal kell eljárni, hogy az elsődleges helyszín adatai

sértetlenek maradjanak. Az alternatív helyszínen történő tesztelés csak a tervezett rész-funkcionalitásra szorítkozik.

6.4.5 Teljes leállás-visszaállítás tesztelés (Full Interruption testing)

A teljes leállás-visszaállítás teszt hivatott egy valódi katasztrófa helyzet „élethű" modellezésére, ahol bizonyos rendszerek teljes leállítását és a katasztrófa helyzetnek megfelelő visszaállítását kell elvégezni.

Ez a teszt jelentős és közvetlen negatív hatással van az érintett szakmai folyamatokra, ezért csak Hivatal vezetőségének engedélyével hajtható végre gondosan kimunkált részletes tervezést követően.

A teljes leállás-visszaállítás teszt alkalmazásától a teszt ciklus többi elemének rendszeres elvégzése esetén el lehet tekinteni. Végrehajtása viszont indokolt lehet abban az esetben, amikor az informatikai infrastruktúra általános karbantartása történik, illetve fejlesztési vagy hibajavítási okokból részleges vagy teljes leállás szükséges.

6.4.6 Teszt kiértékelése

Közvetlenül a teszt befejezését követően a résztvevőknek ki kell értékelniük a teszt teljes folyamatát. A kiértékelésnek ki kell terjednie legalább a következőkre:

- a katasztrófa-elhárításért tett intézkedések a meghatározott időn belül megtörténnek-e, azaz teljesültek-e az MTO értékek,
- a visszaállítás és a helyreállítás garantálja-e az előre meghatározott funkcionalitást,
- mennyire folyamatos a visszaállítási és helyreállítási tevékenység, vannak-e szakadási pontok,
- az információáramlás, feladatdelegálás megfelelően zajlik-e,
- az egyes szereplők mennyire vannak tisztában az elvégzendő feladatokkal és rendelkezne-e a szükséges szakmai hozzáértéssel,
- vannak-e a Helyreállítási Szabályzatban (beleértve a mellékleteket és a kapcsolódó utasításokat) olyan pontok, amelyek megfogalmazása, ennek következtében az ellátandó feladat nem egyértelmű.

A kiértékelésről részletes feljegyzést (jegyzőkönyvet) kell készíteni, amelyet a tesztelés vezetőjének alá kell írnia.

A teszt kiértékelése során meg kell állapítani az esetlegesen szükséges módosításokat, kiegészítéseket és azokat át kell vezetni a katasztrófa elhárítási terveken.

6.5 Aktiválási terv

A katasztrófa helyreállítási terv aktiválási tervét külön dokumentumban kell rögzíteni.

Az aktiválási terv része a katasztrófa helyreállítást végző csapatok szakmai összetétele, az aktuálisan részt vevő személyek (funkciók) és szervezetek.

Meghatározásra kerülnek azok a feltételek, amelyek esetében IT katasztrófa helyzetet kell kihirdetni, el kell indítani a riasztást és a helyreállítási tervek aktiválását.

6.6 Értesítési listák

A katasztrófa helyreállítási tervekhez értesítési listákat kell készíteni, melyek tartalmazzák, hogy adott esemény bekövetkezte esetén mely szervezeteket, személyeket, milyen sorrendben kell értesíteni.

A katasztrófa helyreállításban részt vevő szervezeteknek biztosítaniuk kell, hogy a megadott kontaktok minden esetben elérhetők legyenek, ezért célszerűen állandó, ügyleti telefonszámokat kell az egyes funkciókhoz rendelni. Így biztosítható, hogy szabadság, betegség esetén is a Helyreállítási Team Vezető azonnal elérhesse a támogatást végző személyt.

Az értesítési listákat karban kell tartani. A központi rendszerekhez tartozó értesítési lista karban tartásáért felelős a Helyreállítási Team Vezetője (informatikai irodavezető).

6.7 A Szabályzat oktatása

Az informatikai rendszerek katasztrófa helyzetére, illetve annak hatékony helyreállítási módjára fel kell készíteni valamennyi személyt, aki a katasztrófa helyzet észlelésében, kommunikálásában, helyreállításában részt vehet.

A rendszerek természeténél fogva a katasztrófa helyzet érintheti a központi rendszerek üzemeltetőit, az hivatali épületek informatikai üzemeltetőit, a rendszereinek beszállítóit, támogatóit. Ennek megfelelően a katasztrófa helyreállítási tervek oktatásának teljes körűnek kell lennie, ugyanakkor differenciáltnak is az egyes érintettek munkakörének, tevékenységének megfelelően.

Az oktatási anyag elkészítésénél figyelembe kell venni

- a Katasztrófa Helyreállítási Tervben időközben történt módosításokat,
- a Katasztrófa Helyreállítási Terv tesztelésének eredményeit, tanulságait,
- az esetlegesen bekövetkezett katasztrófák, üzemzavarok tapasztalatait.

<u>Általános oktatás</u>

A Katasztrófa Helyreállítási Szabályzatban nem nevesített munkakörökben dolgozók általános jellegű oktatást kapnak. Az oktatásnak tartalmaznia kell az adott munkakörhöz igazodóan:

- a munkavégzés közben fellépő lehetséges problémákat,
- az ismert problémák kezelésének módját,
- a közvetlen hibaelhárítási eszkalációs feladatokat.

Ezeket az ismereteket a rendszeres információbiztonsági oktatások keretében kell a munkatársaknak átadni.

Helyreállítási Team tagok oktatása

A Katasztrófa Helyreállítási Szabályzatban nevesített munkakörökben dolgozók oktatását a „szükséges tudás" figyelembe vételével kell megvalósítani (tehát nem kell minden érintett munkatársat teljes körű oktatásban részesíteni).

A team-tagoknak évente egyszer vagy módosítást követően a Katasztrófa Helyreállítási Szabályzat tartalmával kapcsolatban oktatást kell tartani. Az újonnan kinevezett team-tagok részére, külön rendkívüli oktatást kell szervezni.

Az oktatási tematikát és a tesztelési tervet össze kell hangolni, mert ezek egymást segítő, kiegészítő tevékenységek.

A Helyreállítási Team Vezető feladata és felelőssége az oktatás megszervezése, megfelelő szakértők, szakemberek bevonása az oktatás különböző fázisaiba, tananyag és az esetleges vizsgakérdések összeállítása valamint az oktató biztosítása.

A Vezetőnek oktatási tervet kell kidolgoznia, amelyben megjelöli:

- az oktatni kívánt szervezeteket/személyeket,
- az oktatások időpontját,
- az oktatási tematikát és
- az oktatások helyszínét, módszerét, mely történhet online, telekonferencia, videokonferencia formájában.

Az oktatásokat meg lehet tartani a katasztrófa terv tesztelése előtt, illetve azzal egyidejűleg. A tesztelés vezetőjének meg kell győződnie arról, hogy valamennyi szükséges ismeret eljutott a megfelelő személyekhez. Az ismeretek átadását dokumentálni kell.

Az oktatási ütemtervet a Helyreállítási Team Vezetőhöz kell előterjeszteni jóváhagyásra.

Az éves oktatási tervet úgy kell kialakítani, hogy a következő feladatok gyakorlása, oktatása része legyen az oktatási tervnek:

- problémák feltárása
- vészhelyzeti kommunikáció
- visszaállítási tevékenység gyakorlása
- dokumentálási feladatok
- üzemzavarok kiértékelése

7 Katasztrófahelyzet kezelése

Általánosságban elmondható az Hivatal elektronikus információs rendszereiről, hogy a kritikus elemek védettek, redundáns vagy hibatűrő tervezésűek. A redundancia biztosítja az egyszeres meghibásodás elleni védelmet, a kiszolgálók professzionális hibatűrő eszközök, de egyes esetekben előfordul duplikálás nélküli eszköz vagy szolgáltatás. Az óvintézkedések ellenére előfordulhat, hogy a rendszerek esetleges halmozódó hibák, külső támadás (DDoS vagy hacker támadás) vagy egyéb, rendkívüli behatás következtében működésképtelenné válnak.

7.1 Általános katasztrófa kezelési megfontolások

7.1.1 Emberi életek mentése

Amennyiben a bekövetkező események miatt emberélet kerül veszélybe, minden egyéb tevékenységet megelőzően az emberek mentése, a közvetlen életveszély elhárítása mindenkinek feladata, függetlenül beosztásától és felelősségi körétől.

7.1.2 Katasztrófa kiterjedésének megakadályozása

A közvetlen életveszély elmúltával gondoskodni kell a katasztrófa kiterjedésének megakadályozásáról, (pl. tűz oltása), valamint a veszélyeztetett informatikai eszközök és más vagyontárgyak mentéséről. A technikai mentés hatókörének meghatározása és a szükséges erőforrások biztosítása a Helyreállítási Team Vezető feladata.

Tűz, illetve üzemi hőmérsékletet meghaladó hőmérséklet, vízbetörés, vagy az eszközöknek helyet adó helyiség egyéb sérülése esetén minden, a szerverszobákban lévő eszközt szakszerűen le kell állítani (amennyiben az emberéletet nem veszélyeztet), majd lokálisan áramtalanítani kell és az eszközöket a helyszínről el kell távolítani. A helyszínről eltávolított eszközök és dokumentumok fizikai védelméről gondoskodni kell.

7.1.3 Károk felmérése és a bizonyítékok megvédése

Az emberélet mentését és az eszközök védelmét követően meg kell állapítani a bekövetkezett károk mértékét, kiterjedését a helyreállítás mielőbbi megkezdése érdekében.

Amennyiben felmerül annak a gyanúja, hogy a katasztrófa helyzet szándékos cselekedet, vagy emberi mulasztás következménye, akkor már az eszközök mentése, biztonságba helyezése során gondoskodni kell arról, hogy a káresettel kapcsolatos bizonyítékok megőrzésre kerüljenek. Az elhárítás során az Helyreállítási Team Vezető dönt arról, hogy szükséges-e a bizonyítékok gyűjtése és esetlegesen külső szakértő bevonása.

7.2 Központi kiszolgálók teljes helyreállítási terve

A Hivatal *az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról* szóló, *466/2017. (XII. 28.) Korm. rendelet* előírásai szerint, valamennyi rendszerének teljes helyreállítását biztosító mentéseket továbbít a Kormányzati Adattrezor részére. Az adattrezor archiválás teljes folyamatát a Hivatal Archiválási Szabályzata írja elő.

Az adattrezor-archiválás biztosítja a Hivatal elektronikus információs rendszereiben tárolt adatok független, külső biztonságos tárhelyen történő elhelyezését, mely katasztrófa helyzet esetén elérhető.

E mellett a Hivatal biztosítja ugyanezen adatok helyi biztonságos tárolását, az informatikai így biztosított az adatok többszörös, biztonságos tárolása a központi infrastruktúrától elkülönített helyeken.

Az Archiválási Szabályzat részletesen meghatározza:

- az archiválási folyamat résztvevőit;
- az archiválás technikai folyamatát;
- a mentésre kerülő adatok körét és a mentési infrastruktúrát, továbbá a mentés menetét;
- a teljes visszatöltéshez szükséges minimál infrastruktúrát;
- a visszatöltés menetét;
- a visszatöltés ellenőrzését.

7.2.1 Tartalék infrastruktúra

A háttér informatikai kiszolgáló infrastruktúra kialakítása során törekedni kell arra, hogy a teljes informatikai kiszolgáló rendszer minimális konfigurációs követelményeinek megfeleljen. Az eszközök költséghatékonysági okok miatt a normál működési rendben más funkciót is betölthetnek, de katasztrófa helyzet esetén biztosítaniuk kell a helyreállítást.

7.3 Általános helyreállítási intézkedések

7.3.1 A helyreállítás előkészítése

A meghibásodás természetétől és a meghibásodott eszköz(ök) jellegétől függően szükség lehet a helyreállítás megkezdéséhez a következőkre:

- tartalék eszközök (hardver)
- operációs rendszer és alkalmazás telepítő készletek
- mentések
- külső cég (szállító) támogatása

Az előkészítési fázis a felsoroltak helyszínre juttatását és a szükséges kapcsolatfelvételeket foglalja magába.

7.3.2 A helyreállítás végrehajtása

A visszaállítást a vonatkozó visszaállítási utasítások alapján kell elvégezni. Jelen dokumentum mellékletében meghatározásra kerültek a központi kiszolgáló infrastruktúra meghibásodása esetén szükséges lépések.

7.3.3 A helyreállítás megfelelőségének ellenőrzése

Az eredményes visszaállítást követően az adott szolgáltatás szakmai felelősével igazoltatni kell a szolgáltatás megfelelőségét és erről feljegyzésnek kell készülnie, amit az informatika tűzbiztos szekrényében tárolunk elektronikus formában.

7.3.4 A katasztrófa elhárítási tevékenység dokumentálása

Az üzemzavar elhárítását követően a teljes elhárítási tevékenységről feljegyzést kell készíteni, amely tartalmazza legalább a következőket:

- az üzemzavar leírása
- az elvégzett tevékenységek
- a felhasznált anyagok (hardverek)
- a telepített szoftverek
- az üzemzavar elhárítást végző személy (felelős)
- további bevont személyek
- a tesztelés módja és eredménye

7.3.5 Az informatikai rendszerek helyreállítási sorrendje

Az szakmai hatáselemzés és az informatikai terület szakmai megfontolása alapján kerül meghatározásra a visszaállítási sorrend, amelyet akkor kell figyelembe venni, ha több rendszer egyidejű kiesése esetén nem biztosítható a párhuzamos munkavégzés, ezért fontossági sorrendet kell felállítani.

Az informatikai rendszerek visszaállítási sorrendje a következő:

- Központi szerverekkel kapcsolatos esemény során:
  1. Szerverek
  2. Storage-ok
  3. Virtuális szerverek
  4. Hálózat
  5. Tűzfalak
  6. Alkalmazások

7.3.6 Az informatikai üzemzavar elhárításhoz szükséges erőforrások biztosítása

Annak érdekében, hogy a visszaállítások valóban elvégezhetők legyenek, a szükséges erőforrásokat biztosítani kell. Az erőforrások két kategóriába soroljuk:

- emberi erőforrások
- technikai erőforrások

7.3.7 Értesítési listák

Az emberi erőforrások esetén meg kell határozni:

- a feladatot végző konkrét személyt, vagy a hozzá kapcsolódó funkciót,
- alkalmazás felelőst
- a feladatot végző személy helyettesítésének rendjét
- az elérhetőségeket (munkahely, mobil telefon)

Az emberi erőforrásokat a Mellékletben meghatározott Értesítési listák tartalmazza. Üzemzavarok esetén a kompetens személyzet rendelkezésre állása döntő tényező, ezért ezt a mellékletet különös gondossággal kell naprakészen tartani.

Az informatikai rendszerek üzemeltetéséhez, a telekommunikációs szolgáltatásokhoz külső szállítók kapcsolódnak, melyeknek a közreműködése hibaelhárítás esetén nélkülözhetetlen. A Mellékletben szereplő dokumentum tartalmazza mindazokat a támogatói kapcsolatokat, külső szakértőket és elérhetőségüket, akik bevonása adott esetben szükséges egy üzemzavar elhárításához. A külső támogatók listája tartalmazza a következőket:

- a szállító neve
- a szállító vezető képviselője és elérhetősége
- kapcsolattartó és elérhetősége
- a támogatott IT eszközök, rendszerek
- rendelkezésre állási paraméterek
- a vonatkozó szerződés megnevezése és elérhetősége

8 Mellékletek

Jelen Katasztrófa Helyreállítási Szabályzatot az egyéb dokumentumokban foglalt kiegészítésekkel kell együtt kezelni. **A mellékletek bizalmas műszaki-technikai információkat tartalmaznak, ezért azokat kizárólag az elhárítási tevékenységben részt vevő munkatársak ismerhetik meg, azok közzététele tilos.**

8.1 Aktiválási kézikönyv

Az Aktiválási kézikönyv határozza meg katasztrófa helyzet kihirdetésének feltételeit, az egyes scenáriók esetén követendő eljárásokat.

Tartalmazza a tartalékolási előírásokat, mind az irodaépületek, mind az informatikai erőforrások tekintetében.

Rendelkezik a helyreállítás technikai lépéseiről.

8.2 Értesítési listák

Az értesítési listák a visszaállításhoz, illetve a helyreállításhoz szükséges kompetenciákkal rendelkező személyek, illetve szervezetek hatékony eléréséhez szükségesek.

A nyilvántartásokat az aktualizált adatokkal feltöltve, az *Aktiválási Kézikönyv*-ben megjelölt módon és helyeken kell tárolni, vészhelyzet esetén biztosítva a hivatali és informatikai felelősök, illetve támogató szolgáltatók gyors elérhetőségét.