BALOGUNYOMI KÖZÖS ÖNKORMÁNYZATI HIVATAL

Informatikai Biztonsági Szabályzat

(Balogunyom, Kisunyom, Sorokpolány, Sorkifalud, Sorkikápolna, Gyanógeregye, Nemeskolta,)

Verziószám: **ASP 1.0**

Iktatási szám: KÖH/29/ 2018

Dátum: 2018. április 1.

Balogunyom, 2018. március 12. **Jóváhagyta:** Dr. Varga Krisztina jegyző

Tartalomjegyzék

1. ÁLTALÁNOS RÉSZ 5

1.1. AZ INFORMATIKAI BIZTONSÁGI SZABÁLYZAT CÉLJA 5
1.2. SZABÁLYZAT HATÁLYA 5
1.3. MINŐSÍTÉS 6
1.4. KÖTELEZETTSÉGEK A DOKUMENTUMMAL KAPCSOLATBAN 6

2. SZERVEZETI BIZTONSÁG 6

2.1. INFORMÁCIÓBIZTONSÁG SZERVEZETI HÁTTERE 6
2.1.1. Jegyző 6
2.1.2. Elektronikus információs rendszer biztonságáért felelős személy 7
2.1.3. Rendszergazda 8
2.2. FELHASZNÁLÓK FELELŐSSÉGE 8
2.3. SZERZŐDÉSES PARTNER HOZZÁFÉRÉSE 9

3. VAGYONTÁRGYAK KEZELÉSE 10

3.1. VAGYONTÁRGYAKÉRT VISELT FELELŐSSÉG 10
3.2. INFORMATIKAI NYILVÁNTARTÁSOK 11
3.2.1. Elektronikus információs rendszerek nyilvántartása 11
3.2.2. Elektronikus információs rendszerelem leltár 11
3.2.3. Alapkonfigurációs nyilvántartás 11
3.2.4. Rendszerbiztonsági terv 12
3.3. KOCKÁZATKEZELÉS 12
3.3.1. Kockázatok elemzése 12
3.3.2. Kockázatok kezelése 13
3.4. BIZTONSÁGI OSZTÁLYBA, BIZTONSÁGI SZINTBE SOROLÁS 14
3.4.1. Végrehajtás gyakorisága 15
3.4.2. Cselekvési terv 15
3.5. SZERZŐI JOGOK VÉDELME 16
3.6. VAGYONTÁRGYAK ELFOGADHATÓ HASZNÁLATA 16
3.6.1. Illegális tevékenységek, szerzői és társjogok védelme 16
3.6.1.1. Megvásárolt termékek 16
3.6.1.2. Szerzői jogvédelem alá eső egyéb elektronikus dokumentumok, programok, termékek 17
3.6.2. Kifogásolható anyagok 17
3.6.3. Pazarlás 17
3.6.4. Nyomtatások 17

4. SZEMÉLYZETI BIZTONSÁG 18

4.1. ALKALMAZÁS ELŐTT 18
4.2. ALKALMAZÁS ALATT 19
4.2.1. Belső oktatások, továbbképzés 19
4.2.2. Képzési eljárásrend 19
4.2.3. Biztonságtudatossági képzés 20
4.2.4. Fegyelmi eljárás 20
4.3. ALKALMAZÁS MEGSZŰNÉSE 21
4.3.1. A hozzáférési jogok visszavonása 21
4.3.2. A vagyontárgyak visszaszolgáltatása 21
4.3.3. A munkakör változásának biztonsági kérdései 22

5. FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG 22

5.1. ALAPVETŐ NORMÁK 22
5.1.1. A Hivatal épületén kívül 22
5.1.2. Üres íróasztal, tiszta képernyő politika 23
5.1.3. Látogató kísérete 23
5.1.4. Belépés rendje 23
5.1.5. Belépések regisztrálása 23
5.1.6. Tűzvédelem 23
5.1.7. Villám és túlfeszültség védelem 23
5.1.8. Fizikai biztonsági incidensek jelzése 24
5.1.9. Irodákban elhelyezett informatikai eszközök védelme 24

6. KOMMUNIKÁCIÓ ÉS ÜZEMELTETÉS MENEDZSELÉSE 25

6.1. ÜZEMELTETÉSI ELJÁRÁSRENDEK 25
6.1.1. Dokumentáció készítése 25
6.1.2. Rendszeres tevékenységek 25
6.1.3. Karbantartás 25
6.1.4. Javítócsomagok, frissítések telepítése 26
6.1.4.1. Desktop környezet 27
6.1.4.2. Hálózati aktív eszközök 27
6.1.4.3. Szakrendszerek 27
6.1.4.4. Frissítések dokumentálása 27
6.1.5. Együttműködésen alapuló számítástechnikai eszközök 28
6.2. VÍRUSVÉDELEM 28
6.3. MENTÉSI REND 29
6.3.1. Általános követelmények 29
6.3.2. Mentési eljárásrend 30
6.3.3. Alkalmazások mentése 30
6.3.4. Adatok visszaállításának folyamata 30
6.3.5. Katasztrófamentés, teljes környezet mentés 31
6.4. HÁLÓZATBIZTONSÁG 31
6.4.1. Vezetékes hálózati végpontok 32
6.5. ADATTÁROLÁS ÉS ADATTOVÁBBÍTÁS SZABÁLYAI 32
6.5.1. Általános szabályok 32
6.5.2. Elektronikus levelezés szabályai 33
6.5.3. Internethasználat szabályai 33
6.6. NAPLÓZÁS 33
6.7. HORDOZHATÓ INFORMATIKAI ESZKÖZÖK HASZNÁLATA 34
6.8. RENDSZERFEJLESZTÉS 35
6.9. KRIPTOGRÁFIAI VÉDELEM 35

7. HOZZÁFÉRÉS-ELLENŐRZÉS 36

7.1. HOZZÁFÉRÉS-VÉDELEM 36
7.2. FELHASZNÁLÓ KEZELÉS 36
7.2.1. Általános elvárások 37
7.2.2. Jogosultságok igénylése 37
7.2.3. Jogosultsági igény jóváhagyása, továbbítása 37
7.2.4. Felhasználó felvétele 38
7.2.5. Jogosultságok módosítása 38
7.2.6. Felhasználó kilépése 39

7.3. KIEMELT FELHASZNÁLÓI JOGOSULTSÁG KEZELÉSE 39
7.3.1. Jogosultság igénylése 39
7.3.2. Kiemelt jogosultság használata 39
7.3.3. Jogosultság megvonása 39
7.3.4. ASP rendszerek jogosultság kezelése 40
7.4. TECHNIKAI AZONOSÍTÓK KEZELÉSE 40
7.5. FELHASZNÁLÓI AZONOSÍTÓ ÉS JOGOSULTSÁGOK HASZNÁLATA 41
7.5.1. Jelszókezelés szabályai 41
7.5.2. Kiemelt felhasználói és technikai azonosítók jelszavai 43
7.5.3. Külső harmadik fél hozzáférés védelme 43
7.5.4. Tanúsítványok használata 43
7.6. JOGOSULTSÁGOK NYILVÁNTARTÁSA 44
7.7. A JOGOSULTSÁGOK FELÜLVIZSGÁLATÁNAK RENDJE 44

8. NYILVÁNOSAN ELÉRHETŐ TARTALOM 45

9. INFORMÁCIÓS RENDSZEREK BESZERZÉSE, FEJLESZTÉSE ÉS KARBANTARTÁSA 45

9.1. FEJLESZTÉSEK BIZTONSÁGI KÖVETELMÉNYEINEK ELLENŐRZÉSE 46

10. AZ INFORMÁCIÓBIZTONSÁGI INCIDENSEK KEZELÉSE 46

10.1. JELENTÉSI KÖTELEZETTSÉG 46
10.2. BEJELENTÉSEK KEZELÉSE 46
10.3. ESEMÉNYKEZELŐ KÖZPONTOK JELZÉSE 47
10.4. FELHASZNÁLÓK TÁJÉKOZTATÁSA 47
10.5. TANULÁS A BIZTONSÁGI ESEMÉNYEKBŐL 47

11. A MŰKÖDÉS FOLYTONOSSÁGÁNAK IRÁNYÍTÁSA 47

12. MEGFELELŐSÉG 48

12.1. FELÜLVIZSGÁLAT, ELLENŐRZÉS 48
12.2. VEZETŐSÉGI ÁTVILÁGÍTÁS 49
12.3. HIVATAL INTÉZKEDÉSI TERVEINEK NYOMON KÖVETÉSE, FELÜLVIZSGÁLATA 49
12.3.1. Cselekvési terv felülvizsgálata 49
12.3.2. Informatikai biztonsági stratégia 50

13. MELLÉKLETEK 50

13.1. BIZTONSÁGI OSZTÁLYBA, BIZTONSÁGI SZINTBE SOROLÁS 50
13.2. ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGI OSZTÁLYBA SOROLÁSA 50
13.3. SZERVEZET BIZTONSÁGI SZINTBE SOROLÁSA 50

1. Általános rész

1.1. Az informatikai biztonsági szabályzat célja

Az informatikai biztonsági szabályzat (a továbbiakban: Szabályzat) azon alapvető biztonsági normákat és működési kereteket határozza meg, melyek érvényesítésével a Balogunyomi Közös Önkormányzati Hivatal elfogadható szintre csökkentheti az általa végzett adatkezelés és adatfeldolgozás kockázatait, egyúttal hozzájárulnak a vonatkozó jogszabályokban előírt követelmények teljesítéséhez. A Szabályzat rögzíti a hatálya alá eső adatok, információk informatikai rendszeren történő adatfeldolgozásával szemben támasztott alapvető biztonsági követelményeket valamint a legfontosabb szervezeti feladatokat és felelősségi köröket.

A Szabályzat további célja, hogy iránymutatással szolgáljon a Hivatal informatikai rendszereihez hozzáférési jogosultsággal rendelkező felhasználók számára az informatikai rendszerek helyes használatáról, ismertesse a helyes és biztonságos munkavégzés szabályait, a követendő eljárásokat, továbbá rögzítse a felhasználókkal szemben támasztott elvárásokat és követelményeket.

1.2. Szabályzat hatálya

A Szabályzat tárgyi hatálya kiterjed a Hivatal minden informatikai rendszerére, teljes informatikai környezetére, beleértve minden olyan adathordozót és informatikai eszközt, amin a Hivatal adatait tárolják, feldolgozzák, vagy ügyviteli folyamatait támogatják, illetve az azok létrehozásával, működtetésével, használatával kapcsolatos tevékenységekre.

A Szabályzat személyi hatálya kiterjed valamennyi, a feladatai ellátásához a Hivatal informatikai rendszereit, eszközeit használó, vagy azokhoz hozzáférő köztisztviselőre, ügykezelőre, Munka Törvénykönyve hatálya alá tartozó munkavállalóra, továbbá a Hivatalban megbízási, vagy egyéb jogviszony alapján az informatikai rendszerekhez bármilyen okból hozzáférő személyre (a továbbiakban együttesen felhasználó).

A Szabályzat területi hatálya kiterjed minden olyan épületre, helyiségre, ahol a tárgyi hatály alá eső eszközök megtalálhatók, illetve a tárgyi hatálya alá tartozó tevékenységeket végeznek.

Jelen szabályzatban foglalt elvárások és követelmények a jegyző jóváhagyásával kerültek kialakításra. Azon biztonsági területek esetében, melyeket jelen szabályzat nem fed le, vagy részletesen nem szabályoz, a jegyző határozza meg a követendő eljárásrendet és az alkalmazandó biztonsági elvárásokat, melyek meghatározásához szükség esetén bevonja az elektronikus információs rendszerek biztonságáért felelős személyt.

1.3. Minősítés

A Szabályzat bizalmas minősítésű, terjesztése kizárólag a Jegyző jóváhagyásával történhet. A Szabályzathoz hozzáférési jogosultsággal a Szabályzat személyi hatálya alá tartozók, továbbá a jegyző által feljogosított személyek rendelkezhetnek.

1.4. Kötelezettségek a dokumentummal kapcsolatban

A jegyző felelőssége a szabályzat napra készen tartása, így a jegyző feladata biztosítani, hogy szükség szerint, a Szabályzatot érintő jogszabályi, funkcionális, biztonsági, technológiai vagy egyéb változások esetén a Szabályzat felülvizsgálata megtörténjen.

2. Szervezeti biztonság

A Hivatal az informatikai biztonsággal kapcsolatos feladatok ellátását jelen fejezetben meghatározott résztvevők és szerepkörök feladatául és felelősségébe utalja.

2.1. Információbiztonság szervezeti háttere

2.1.1. Jegyző

Az informatikai biztonsági feladatok vezetői szintű tervezése, koordinálása, a szabályzatban előírt kontrollok működtetésének biztosítása és azok működésének felügyelete a jegyző feladata. A jegyző felelőssége továbbá az ügyvitel kialakítása során a Hivatalra vonatkozó informatikai biztonsággal kapcsolatos jogszabályi követelmények érvényre juttatása. A jegyző feladata továbbá:

- munkaviszony létesítésével és megszűntetésével kapcsolatos feladatok ellátása
- elektronikus információs rendszer biztonságáért felelős személy kinevezése
- elektronikus információs rendszerek felhasználói jogosultságainak engedélyezése
- fejlesztési igények engedélyezése
- döntés a védelmi intézkedésekről
- gondoskodik arról, hogy az informatikai szolgáltatás nyújtásához igénybe vett harmadik felek szerződéseiben az Informatikai Biztonsági Szabályzat elvárásai érvényre jussanak
- biztosítja a Hivatal munkatársainak rendszeres időközönkénti biztonságtudatossági oktatását, feladata a képzések tematikájának összeállítása, a képzések végrehajtása.
- cselekvési tervben előírt intézkedések előrehaladásának figyelemmel kísérése
- kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal
- biztonsági incidensek kivizsgálása

A jegyző a fenti feladatokat delegálhatja, figyelembe véve az összeférhetetlen feladatok esetén az egy személyhez történő delegálást.

2.1.2. Elektronikus információs rendszer biztonságáért felelős személy

Az elektronikus információs rendszer biztonságáért felelős személyt a jegyző nevezi ki vagy bízza meg. Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló információs rendszer védelméhez kapcsolódó feladat ellátásáért. Ennek során:

- közreműködik a Hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtésében és fenntartásában,
- támogatás nyújt az előző pontban meghatározott tevékenységek tervezésében, szervezésében, koordinálásában és ellenőrzésében,
- előkészíti a Hivatal elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
- felülvizsgálja a Hivatal informatikai biztonsági stratégiáját, szükség esetén aktualizálja,
- előkészíti a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását és a Hivatal biztonsági szintbe sorolását,
- véleményezi az elektronikus információs rendszerek biztonsága szempontjából a Hivatal információbiztonsági szabályzatait, szerződéseit,
- elősegíti a törvényi megfelelést a Hivatal valamennyi elektronikus információs rendszerének tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésben és kockázatkezelésben, karbantartásban vagy javításban közreműködők esetében,
- elősegíti a törvényi megfelelést abban az esetben, ha a Hivatal adatkezelési vagy adatfeldolgozó tevékenységre közreműködőt vesz igénybe,
- felülvizsgálja a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását, illetve a Hivatal biztonsági szintbe sorolását,
- jegyzői kérésre közreműködik az informatikai biztonsági incidensek kivizsgálásában,
- kockázatkezelési javaslatok kidolgozása, megvalósulásuk nyomon követése.

Az elektronikus információs rendszer biztonságáért felelős személy jogosult a Hivatal tevékenységeihez köthető közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében valamennyi adatot, illetve az elektronikus információs rendszerek biztonságában keletkezetett valamennyi dokumentumot bekérheti.

Az elektronikus információs rendszer biztonságáért felelős személyre vonatkozó követelményeket, valamint a feladatköröket a 2013. évi L. törvény szabályozza részletesen.

2.1.3. Rendszergazda

A rendszergazda a jegyző iránymutatásának megfelelően végzi feladatait. Szorosan együttműködik az elektronikus információs rendszer biztonságáért felelős személlyel az informatikai biztonsági követelmények kialakításában és végrehajtásában.

A rendszergazda feladata:

- A Hivatal informatikai igényeinek (hibák, változások) fogadása, informatikai hibák javítása, informatikai változási igények végrehajtása.
- Mentési és naplózási elvárások érvényre juttatása.
- Ügyviteli igényeknek megfelelő mentési rend kialakítása és mentési eljárások kidolgozása.
- Hatáskörébe tartozó informatikai rendszerek jogosultságadminisztrációs feladatainak ellátása, jogosultság nyilvántartás naprakészen tartása.
- A Hivatal elektronikus információs rendszereinek nyilvántartása, beleértve a hardver-, szoftver- és licencnyilvántartás elkészítését.
- Részvétel az informatikai biztonsági stratégia felülvizsgálatában, megvalósításában.
- Új elektronikus információs rendszer bevezetése esetén a felhasználók oktatása.
- Informatikai rendszerek beszerzésében való közreműködés.
- A Hivatal elektronikus információs rendszereivel kapcsolatos nyilvántartásainak évenkénti felülvizsgálata.

2.2. Felhasználók felelőssége

Felhasználó a Hivatal minden munkavállalója, foglalkoztatási formától függetlenül, aki az informatikai rendszereket használja. A felhasználók kötelezettsége a szabályzatban szereplő, illetve a jegyző által előírt védelmi intézkedések körültekintő betartása, alapvető elvárás a felhasználókkal szemben, hogy a napi munkavégzés során az informatikai rendszerek használata során jelen szabályzat szellemiségével összhangban járjanak el.

A felhasználó:

- Elszámoltatható minden olyan tevékenységért, amelyet a saját felhasználó azonosító kódja (user ID) alapján végeztek.
- Megakadályozza a kapott hozzáférési jogokkal való visszaélést azáltal, hogy megőrzi a hozzáférési kódok titkosságát.
- Betart minden, az informatikai rendszerek megfelelő használatára, tárolására és megsemmisítésére vonatkozó szabályt és az eszközöket a céljuknak megfelelően használja.
- A számítástechnikai berendezéseket, programokat előírás szerint használja.
- Jelenti az észlelt incidenseket, sebezhetőségeket, működésbeli problémákat a rendszergazdának és a jegyzőnek.

- Elvárható gondossággal jár el az adatkezelés során, mind az adatbevitel, mind a kimenő adatok elkészítése alkalmával.

2.3. Szerződéses partner hozzáférése

Harmadik fél szolgáltatásainak igénybe vétele előtt a jegyző feladata, az elektronikus információs rendszer biztonságáért felelős személlyel együttműködve, az informatikai biztonsággal kapcsolatos kockázatok előzetes felmérése, mely kockázatok értékelése alapján kell a későbbiekben kötendő szerződést elkészíteni.

Harmadik félnek tilos megengedni a hozzáférést az információkhoz, információ feldolgozó eszközökhöz, amíg a kellő óvintézkedések (pl. megfelelő titoktartási és bizalmassági nyilatkozat aláírása) foganatosítása nem történt meg, és a felek nem állapodtak meg a szerződésben.

A szerződőnek kötelezettséget kell vállalnia, hogy a szerződés teljesítésében részt vevő bármely személy vagy közreműködő szervezet, aki hozzáféréssel rendelkezik a jelen szabályzat hatálya alá tartozó informatikai erőforrásokhoz, mindenkor a Hivatal informatikai biztonsági szabályzatában foglalt előírásoknak megfelelően jár el.

A szerződések megkötésénél a szerződés tárgyának megfelelő információbiztonsági kockázatokra figyelemmel kell lenni és meg kell követelni az azok kezelésére vonatkozó előírásokat. Ilyen követelmények lehetnek:

- adatátadási és visszavételi követelmények, eljárások;
- fizikai biztonsági óvintézkedések, követelmények;
- a partner megszűnése illetve szerződésszegésének esete;
- rendelkezések az információbiztonsági incidensek és biztonsági sértések jelentésére;
- a szolgáltatás előirányzott szintje és a szolgáltatás el nem fogadható szintjei;
- igazolható teljesítési kritériumok meghatározása, figyelemmel kísérésük és jelentéstétel;
- szolgáltatás auditálásának lehetősége;
- szolgáltatás folytonossági követelmények.

A jegyző feladata, hogy szerződéses kötelezettségként követelje meg (kerüljön a szolgáltatási szerződésekben rögzítésre), hogy a szolgáltatási szerződés alapján a Hivatal által igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek a Hivatal elektronikus információbiztonsági követelményeinek.

3. Vagyontárgyak kezelése

3.1. Vagyontárgyakért viselt felelősség

A jegyző felelőssége, hogy a Hivatal informatikai rendszerein kezelt adatok, az azokat tároló adathordozók, illetve az azokat kezelő informatikai eszközök védelme a kezelt, illetve feldolgozott adatok érzékenységének és a kapcsolódó jogszabályi követelményeknek megfelelő módon valósuljon meg, értékelje az adatok informatikai eszközökön történő feldolgozásának kockázatait és a kockázatok elfogadható szinten tartásának figyelembe vételével alakítsa ki az ügyviteli, adatvédelmi, illetve informatikai biztonsági szabályokat. A jegyző felelőssége, hogy a selejtezés a rendszergazda bevonásával történjen és minden leselejtezett, de nem megsemmisített adathordozót a Hivatal elzártan tároljon. Az adathordozók megsemmisítése során olyan eljárást kell alkalmazni, mely biztosítja az adattartalmuk visszaállíthatatlanságát.

3.1.1. Adathordozók védelme

A Hivatal ügyviteli folyamataihoz, valamint a rendszergazda által használt külső adattárolóiról (pl. flash disk, USB pendrive, memóriakártya, hordozható HDD és SSD) nyilvántartást vezet.

3.1.2. Hozzáférés adathordozókhoz

Az adathordozókat alapértelmezetten a rendszergazda tárolja és tartja nyilván. A rendszergazda bocsájtja rendelkezésre az adathordozókat igény esetén meghatározott időre. Ettől az eljárástól eltérni csak a Jegyző engedélyével lehet.

A használni kívánt adattárolót a tárolásra kijelölt helyről kell kivenni és használatot követően oda is kell visszahelyezni. A munkaasztalokon csak a munkavégzéshez használatos adathordozók lehetnek.

Az adattárolókat minden felhasználónak rendeltetésszerűen kell használnia. A Hivatal adathordozóin csak munkavégzéshez szükséges adatokat lehet tárolni.

A felhasználók saját tulajdonú adathordozóit az informatikai hálózatra csak az informatikai feladatokért felelős személy engedélyével, vírusszűrés után csatlakoztathatják.

3.1.3. Adathordozók törlése

A meghibásodott, további felhasználásra alkalmatlan adathordozókat a rendszergazdának fizikai roncsolással kell megsemmisítenie.

Az adathordozókat selejtezés vagy az újrafelhasználásra való kibocsátás előtt a rendszergazdának helyreállíthatatlanságot biztosító törlési technikákkal és

eljárásokkal kell törölnie, így védve az adatok bizalmasságát. A biztonságos törlés eredményességét a rendszergazdának minden esetben ellenőriznie kell. Azokat az adathordozókat, amelyeket nem lehet biztonságosan törölni, újrafelhasználni tilos és meg kell semmisíteni.

3.2. Informatikai nyilvántartások

Az Ibtv. előírásainak megfelelően a Hivatalnak naprakész nyilvántartást kell vezetnie a Hivatal elektronikus információs rendszereiről.

3.2.1. Elektronikus információs rendszerek nyilvántartása

A jegyző felelőssége, hogy a Hivatal teljes körű, naprakész nyilvántartást vezessen a Hivatalban használt elektronikus információs rendszerekről. A nyilvántartásnak tartalmaznia kell az elektronikus információs rendszer:

- nevét
- funkcióját
- nyújtott szolgáltatását
- licencszámát
- szakterületi felelőst és elérhetőségét
- üzemeltetési felelőst és elérhetőségét
- továbbá releváns esetben a külső elérhetőségeket.

A rendszergazda feladata a nyilvántartás elkészítése és az évente történő felülvizsgálata.

3.2.2. Elektronikus információs rendszerelem leltár

Az elektronikus információs rendszerelem leltár a Hivatal hardver- és szoftvernyilvántartása. A nyilvántartás elkészítése és naprakészen tartása a rendszergazda feladata.

A nyilvántartásnak ki kell terjednie:

- az informatikai eszközök leltári és műszaki adataira;
- az informatikai eszközökre telepített szoftverekre, azok licencnyilvántartására, külön rögzítve;
  - a megvásárolt licenceket;
  - Hivatal megrendelésére fejlesztett termékek licenceire.

Az informatikai eszközök, illetve azok használatát érintő változások szabályozott keretek között történő végrehajtását az elektronikus információs rendszer biztonságáért felelős személy ellenőrzi.

3.2.3. Alapkonfigurációs nyilvántartás

A Hivatal által használt desktopok, laptopok és szerverek esetében egy alapkonfigurációs nyilvántartást kell készíteni, és folyamatosan aktualizálni. A nyilvántartás elkészítéséért és frissítéséért a rendszergazda felel.

A nyilvántartásnak legalább az alábbi tételeket kell tartalmaznia:

- alapértelmezett hardver;
- alapértelmezett operációs rendszer;
- alapértelmezetten telepítendő programok;
- alapértelmezett alkalmazott policy beállítások;
- alkalmazandó biztonsági beálltások;

Változások esetén azonnal, de legalább évente szükséges a nyilvántartás felülvizsgálata. A felülvizsgálat rendszeres végrehajtásáért az elektronikus információs rendszer biztonságáért felelős személy felel.

3.2.4. Rendszerbiztonsági terv

A Hivatalnak feladata minden hatókörébe tartozó elektronikus információs rendszerre (továbbiakban: EIR) vonatkozóan egy rendszerbiztonsági terv elkészítése.

A rendszerbiztonsági terv elkészítése a rendszergazda feladata. A rendszerbiztonsági tervben szerepeltetni kell:

- az elektronikus információs rendszer hatókörét, alapfeladatait, biztonságkritikus elemeit és alapfunkcióit;
- az EIR és az általa kezelt adatok biztonsági osztályát;
- EIR működési körülményeit és egyéb függőségeit;
- biztonsági követelményeket;
- érintett ügyviteli folyamatokat;
- mentést;
- rendelkezésre állást;
- azonosítás és hitelesítésre vonatkozó követelményeket;
- az adott EIR jogosultságkezelését;
- naplózást;
- a rendszerfelügyeletet;
- frissítésre vonatkozó információkat;
- amennyiben releváns kriptográfiai megoldásokat;
- vírusvédelemre és tartalomszűrésre vonatkozó információkat;
- valamint az egyéb rendszerspecifikus biztonsági követelményeket.

A rendszergazdának gondoskodnia kell arról, hogy a rendszerbiztonsági tervet az arra jogosultak megismerjék. A terveket évente vagy változások esetén felül kell vizsgálni.

3.3. Kockázatkezelés

3.3.1. Kockázatok elemzése

A Hivatalnak az elektronikus információs rendszerek teljes életciklusában meg kell valósítania és biztosítania kell az elektronikus információs rendszerekben kezelt adatok és információk bizalmasságát, sértetlenségét és rendelkezésre állását,

valamint az elektronikus információs rendszerek és elemeinek sértetlenségét és rendelkezésre állását zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

A vonatkozó jogszabályokkal összhangban a kockázatelemzés alapját képezi:

- Az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, és az elektronikus információs rendszerelemek sértetlenségének és rendelkezésre állásának sérüléséből, elvesztéséből bekövetkező kár, vagy káros hatás, terjedelme, nagysága.
- A kár bekövetkezésének, vagy a kárral, káros hatással fenyegető veszély mértéke, becsült valószínűsége.

A Hivatal a jogszabályi követelményekhez igazodva a CRAMM alapú kvalitatív kockázatelemzési módszertant használja. A kockázatelemzéshez használandó kvalitatív skálákat, illetve az alkalmazott kockázati mátrixot az elektronikus információs rendszer biztonságáért felelős személy javaslata alapján jegyző hagyja jóvá. A kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának sérüléséből, elvesztéséből bekövetkező kár, vagy káros hatás terjedelmét, nagyságát a szakterületek felelősei határozzák meg a jegyző által jóváhagyott kárértéktáblázat alapján.

A kockázatelemzés során vizsgálandó sérülékenységek és az ezeket kihasználni képes releváns fenyegetések azonosításáért, valamint a káresemények becsült bekövetkezési gyakoriságának meghatározásért és ez alapján a kockázatelemzés elkészítéséért az elektronikus információs rendszer biztonságáért felelős személy felel.

A jegyző felelőssége az elektronikus információs rendszer biztonságáért felelős személlyel együttműködve, gondoskodnia kockázatelemzés legalább háromévenként vagy szükség esetén, soron kívül dokumentált módon történő felülvizsgálatáról.

3.3.2. Kockázatok kezelése

Az elektronikus információs biztonságáért felelős személy feladata, hogy azonosítsa a nem elfogadható kockázatokat okozó sérülékenységeket, javaslatot tegyen az esetleges további kezelendő kockázatot okozó sérülékenységekről, valamint megvizsgálni, hogy a kockázatelemzés eredménye befolyásolhatja-e az elektronikus információs rendszerek biztonsági osztályba sorolását és erről tájékoztatni a jegyzőt.

Az elektronikus információs biztonságáért felelős személy feladata, hogy kockázatkezelési javaslatok kerüljenek kidolgozásra. A bevezetendő védelmi intézkedés javaslatokról, illetve a felvállalt kockázatokról a jegyző dönt, egyúttal a feladathoz határidőt és felelőst rendel, valamint biztosítja a feladat végrehajtásához szükséges erőforrások rendelkezésre állását.

A jegyző döntései alapján az elektronikus információs biztonságáért felelős személy által összeállított feladatterv végrehajtásának nyomon követése a jegyző felelősségi körébe tartozik.

Amennyiben a kockázatkezeléssel kapcsolatos vezetői döntések alapján változik az elektronikus információs rendszerek biztonsági osztályba sorolása, a jegyző felelőssége, hogy a Hivatal a 3.4. Biztonsági osztályba, biztonsági szintbe sorolás fejezetben leírtak szerint elvégezze a besorolást.

3.4. Biztonsági osztályba, biztonsági szintbe sorolás

Az elektronikus információs rendszerek, valamint az azokban kezelt adatok költséghatékony védelmének biztosítása érdekében a Hivatalnak a vonatkozó jogszabályokban leírtak szerint be kell sorolni az elektronikus információs rendszereket egy-egy (1-től 5-ig számozott) biztonsági osztályba a kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának kockázata alapján, valamint meg kell határozni a szervezet biztonsági szintjét.

Az elektronikus információs rendszerek biztonsági osztályba sorolását a vonatkozó jogszabályok szerint kockázatelemzés alapján kell elvégezni, oly módon, hogy a biztonsági osztályba sorolásnál nem a lehetséges legnagyobb kárértéket, hanem a releváns, bekövetkezési valószínűséggel korrigált fenyegetések által okozható kárt, káros hatást kell figyelembe venni.

A fentiekben leírtaknak megfelelően a Hivatal az elektronikus információs rendszerek biztonsági osztályba sorolását a 3.3. Kockázatkezelés pontban leírtak szerinti kockázatelemzési, kockázatkezelési feladatok eredményei alapján végzi el.

Az elektronikus információs rendszerek biztonságáért felelős személy feladata, hogy a kockázatelemzés, illetve a kockázatkezelési döntések alapján előkészítse az elektronikus információs rendszerek biztonsági osztályba sorolását és a Hivatal biztonsági szintbe történő besorolását. Az elektronikus információs fejlesztését, üzemeltetését végző, az üzemeltetésért felelős vagy információbiztonságért felelős szervezeti egységeket az elektronikus információs rendszerek védelmére való felkészültségük alapján a szervezettől elvárt, eltérő biztonsági szintekbe kell sorolni a jogszabályban meghatározott szempontok szerint. A Hivatal vagy a Hivatal szervezeti egységeinek biztonsági szintjének meghatározását az elektronikus információs rendszer felhasználásának módja határozza meg a jogszabályban meghatározott szempontok szerint.

A biztonsági osztályba, illetve biztonsági szintbe sorolást az elektronikus információs rendszerek biztonságáért felelős személy előterjesztése alapján a jegyző hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért.

A jegyző a törvényben meghatározott feltételeknek megfelelő, az elektronikus információs rendszerre irányadó biztonsági osztálynál magasabb, kivételes esetben indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthat az elektronikus információs rendszerre vonatkozóan.

Az elektronikus információs rendszerek biztonságáért felelős személy feladata, hogy az elektronikus információs rendszerek biztonsági osztályba sorolását és a szervezet biztonsági szintjét jelen szabályzat 13.1. számú melléklete szerint rögzítse, valamint a biztonsági osztályba soroláshoz kapcsolódó hatósági adatszolgáltatást előkészítse és a jegyző számára előterjessze, aki gondoskodik az adatszolgáltatás teljesítéséről, illetve a módosított szabályzat érvénybe léptetéséről.

3.4.1. Végrehajtás gyakorisága

A biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.

A soron kívüli biztonsági osztályba sorolást az elektronikus információs rendszer biztonságát érintő jogszabályban meghatározott változás vagy új elektronikus információs rendszer bevezetése esetén szükséges elvégezni. A soron kívüli felülvizsgálatot akkor is el kell végezni, ha a Hivatal státuszában, illetve az általa kezelt vagy feldolgozott adatok vonatkozásában változás következik be.

Soron kívüli felülvizsgálatot kezdeményezhet a jegyző, tipikusan a működési környezetben bekövetkezett fenti változások esetén, illetve az elektronikus információs rendszerek biztonságáért felelős személy a kockázatelemzés eredményei alapján.

3.4.2. Cselekvési terv

A biztonsági osztályba soroláshoz kapcsolódóan a jegyző felelőssége az elektronikus információs rendszerek biztonságáért felelős személy szakmai támogatása melletti felülvizsgálata, hogy a Hivatal elektronikus információs rendszerei megfelelnek-e az adott biztonsági osztályra, illetve biztonsági szintre külön jogszabályban előírt fizikai, logikai és adminisztratív védelmi intézkedéseknek.

Ha a felülvizsgálat adott elektronikus információs rendszerre vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, illetve a szervezet biztonsági szintje alacsonyabb, mint a Hivatalra előírt biztonsági szint, akkor a jogszabályban meghatározott határidőn belül cselekvési tervet kell készíteni az elektronikus információs rendszerek biztonságáért felelős személy közreműködésével és szakmai irányításával, illetve az informatikai rendszerek üzemeltetési feladataival megbízottak bevonásával a hiányosság megszüntetésére, illetve az előírt biztonsági szint elérésére.

A cselekvési tervnek tartalmaznia kell a törvény által biztosított felkészülési időszakra a védelem elvárt erősségének eléréséhez szükséges biztonsági intézkedések fokozatos kivitelezésére vonatkozó feladatokat.

A cselekvési tervet a jegyző hagyja jóvá, a cselekvési tervben szereplő feladatok végrehajtásához felelőst rendel és biztosítja a szükséges erőforrások rendelkezésre állását.

3.5. Szerzői jogok védelme

A Hivatal eszközein szoftvereket (beleértve a hozzájuk tartozó dokumentációt) csak a felhasználási jog keretei szerint szabad telepíteni, másolni, futtatni, kivéve a törvény adta szabad felhasználás körében (így különösen biztonsági másolat készítése céljából). Egyetlen termék többszörös használata esetén a szoftver csak a licenc megállapodásnak megfelelően használható.

A Hivatal informatikai eszközeire szoftvereket a rendszergazda telepíthet, és olyan logikai biztonsági megoldásokat kell alkalmazni, mellyel biztosítható hogy rajta kívül más rendszerfelhasználó ne legyen képes programtelepítésekre.

Az informatikai rendszerek üzemeltetési feladataival megbízottak felelőssége, hogy csak akkor telepítsenek licencköteles programot informatikai rendszerre, ha előzetesen meggyőződtek róla, hogy azzal szerzői jogot, licenc megállapodást nem sértenek, a program jogszerű használatát igazoló bizonylatok, okiratok rendelkezésre állnak.

A rendszergazda feladata rendszeres időközönként (legalább kétévente) ellenőrizni automatikus, vagy manuális módszerekkel a hivatali szoftverhasználat jogtisztaságát, illetve szerzői jogvédett tartalmak (pl. zene, film, dokumentumok) jogosulatlan megosztását a Hivatal informatikai rendszerein.

Illegális szoftverek használata, illetve a Hivatal által nem engedélyezett szerzői jogvédett tartalmak tárolása esetén a használatban és megosztásban érintett felhasználóval szemben felelősségének megállapítása érdekében fegyelmi, kártérítési, illetve egyéb eljárás indulhat, mely eljárást az informatikai feladatokért felelős vezető kezdeményezheti az jegyző felé.

3.6. Vagyontárgyak elfogadható használata

3.6.1. Illegális tevékenységek, szerzői és társjogok védelme

Alapvetően tilos minden olyan adat tárolása, vagy feldolgozása a Hivatal informatikai eszközein, mely hatályos jogszabályokat sért. A felhasználó harmadik féltől beszerzett adatok esetén köteles a megfelelő gondossággal eljárni, törvénysértés gyanúját a 10.1. fejezetben leírtak szerint jelenteni.

3.6.1.1. Megvásárolt termékek

A felhasználóknak tilos minden, Hivatal által megvásárolt, vagy a partnerek által a Hivatal rendelkezésére bocsátott szoftveréről, szerzői vagy szabadalmi jog alá tartozó minden egyes anyagról

- másolatot készíteni;
- harmadik félnek átadni, vagy harmadik fél tulajdonát képező informatikai eszközre telepíteni, ott futtatni.

Minden olyan esetben, ha jogsértés történt és a felhasználó vagy felhasználók jogsértő magatartása bizonyítható, a Hivatal a felhasználóval szemben érvényesíteni fogja a jogsértés miatt elszenvedett károkat.

3.6.1.2. Szerzői jogvédelem alá eső egyéb elektronikus dokumentumok, programok, termékek

Hivatal informatikai eszközein tárolt és kezelt – harmadik féltől beszerzett - szerzői jogvédelem alá eső elektronikus dokumentumok védelme az adott terméket beszerző felhasználó felelőssége, amiben az eszközt használó felhasználók, illetve az eszköz üzemeltetési feladatait ellátó személyek kötelesek együttműködni.

Az internetről letöltött szerzői jogvédelem alá tartozó adatok, szoftverek (pl.: szoftver demo verziók stb.) kezelésekor a felhasználónak a gyártó licencpolitikáját minden esetben be kell tartania.

Minden olyan esetben, ha jogsértés történt és a felhasználó vagy felhasználók jogsértő magatartása bizonyítható, a jogsértés miatt elszenvedett károkat – a törvények adta mértékében - a felhasználóval szemben Hivatal érvényesíteni fogja.

3.6.2. Kifogásolható anyagok

Tilos a Hivatal informatikai eszközein tárolni, feldolgozni vagy továbbítani olyan anyagokat, melyek közízlést, vagy törvényt sértenek, mint például:

- betiltott filmeket, publikációkat;
- számítógépes játékot;
- pornográfiát, pedofíliát, erőszakot hirdető cikkeket, publikációkat;
- megbotránkoztató, a jó ízlés határait sértő anyagokat;
- gyűlöletkeltésre alkalmas, vagy vallási és kisebbségi érzelmeket sértő anyagokat.

3.6.3. Pazarlás

A felhasználónak kerülnie kell az informatikai erőforrások pazarlását, mivel ezzel más jogosult felhasználók tevékenységét akadályozhatja. A Hivatal a rendelkezésre álló informatikai erőforrások pazarlást biztonsági eseménynek tekinti.

Hivatal pazarlásnak tekinti például, de nem kizárólag

- az indokolatlan és túlzó mértékű nyomtatást;
- a merevlemez tároló kapacitás felesleges kihasználását, a munkakör ellátásához nem szükséges adatok tárolását;
- haszontalan vagy a felhasználó tevékenységével szorosan nem összeegyeztethető alkalmazások, programok szándékos futtatását;
- a hálózati forgalom szándékos növelését, beleértve a túlzó, pazarló internet használatot is.

3.6.4. Nyomtatások

A felhasználó kötelessége gondoskodni arról, hogy az általa kezelt adatok az arra kijelölt nyomtatón kerüljenek kinyomtatásra, a különösen érzékeny anyagokat a nyomtatás idejére sem lehet felügyelet nélkül hagyni, ha a nyomtatóhoz olyan is hozzáférhet, aki nem jogosult hozzáférni az érintett adatokhoz.

4. Személyzeti biztonság

4.1. Alkalmazás előtt

A jegyző felelőssége, hogy a Hivatal informatikai rendszereihez hozzáférő felhasználók esetén az adott feladat-, illetve munkakör betöltéshez szükséges képzettségre, tapasztalatra, gyakorlatra vonatkozó, illetve egyéb, a mindenkor hatályos jogszabályok és belső szabályozók által előírt követelmények ellenőrzése a jogviszony létesítése előtt megtörténjen, a jelölt a szükséges átvilágításon átessen.

A Hivatal informatikai rendszereihez hozzáférő minden felhasználóját munkába állását követően tájékoztatni kell az informatikai rendszerek használatára vonatkozó szabályokról, az új belépő számára biztosítani kell az informatikai biztonsági szabályok megismeréséhez és megértéséhez szükséges minden szükséges támogatást.

A szabályzatok megismeréséről aláírásával kell nyilatkoznia a munkatársnak, amely nyilatkozatot a jegyzőnek kell tárolnia. Az aláírt felhasználói nyilatkozat megléte előfeltétele az első jogosultság igénylés befogadásának.

4.1.1. A munkaviszony létesítésének előfeltételei

A jegyző felelőssége, hogy a Hivatal informatikai rendszereihez hozzáférő felhasználók esetén az adott feladat-, illetve munkakör betöltéshez szükséges képzettségre, tapasztalatra, gyakorlatra vonatkozó, illetve egyéb, a mindenkor hatályos jogszabályok és belső szabályozók által előírt követelmények ellenőrzése a jogviszony létesítése előtt megtörténjen, a jelölt a szükséges átvilágításon átessen.

A felvételi eljárás során a hatályos törvényi előírásoknak megfelelően ellenőrizni szükséges, hogy a jelölt rendelkezik a munkaköréhez előírt végzettséggel. A jogviszony létesítését a Kttv. rendelkezéseinek megfelelően kell végrehajtani.

A felvételi eljárás során minimum ellenőrizni szükséges:

- az önéletrajzot,
- a végzettségeket igazoló dokumentációkat,
- a három hónapnál nem régebbi erkölcsi bizonyítványt.

Plusz követelmények előírása nem szükséges, a felvételi eljárás során előnyként figyelembe vett előírásokat a jegyző határozza meg.

A felvételi eljárás során beadott dokumentáció ellenőrzése a Jegyző által kijelölt ügyintéző feladata.

A felvételt nyert személyt a felvételi eljárás eredményéről hagyományos postai úton vagy elektronikus formában értesítik. A munkába álláshoz szükséges kitöltendő nyilatkozatokat és adatlapokat megküldik a felvételt nyert személy részére, amelyeket az első munkanapon szükséges leadnia.

A Hivatal informatikai rendszereihez hozzáférő minden felhasználóját munkába állását követően tájékoztatni kell az informatikai rendszerek használatára vonatkozó szabályokról, az új belépő számára biztosítani kell az informatikai biztonsági szabályok megismeréséhez és megértéséhez szükséges minden szükséges támogatást.

4.1.2. Titoktartási nyilatkozat

A Hivatal köztisztviselője, a munkaviszonyban, illetve a közfoglalkoztatás keretében foglalkoztatott alkalmazottja, valamint szerződéses partnere csak előzetes titoktartási nyilatkozat megtételét követően férhet hozzá a munkakörének, megbízásának megfelelő jogosultságokkal jelen szabályzat hatálya alá eső adatokhoz, adathordozókhoz, informatikai rendszerekhez. Az első munkában töltött napon a köztisztviselők leteszik az esküt, aláírják az esküokmányt, valamint külön titoktartási nyilatkozatot is. Titoktartási nyilatkozatot kell tennie minden Hivatalban munkát vállalónak, függetlenül a foglalkoztatás formájától.

4.1.3. Próbaidő

A Hivatal új belépő esetén a Kttv.-nek megfelelően a közszolgálati jogviszonyban foglalkoztatottaknak hat hónap próbaidőt jelöl ki, míg az MT-seknek három hónapot.

A próbaidő alatt a jegyző felelőssége az új munkatárs számára a munkakör betöltéséhez szükséges oktatások megszervezése.

4.2. Alkalmazás alatt

4.2.1. Belső oktatások, továbbképzés

A jegyző feladata biztosítani, hogy a jogviszony fennállása alatt a felhasználó fenntartsa, szükség esetén megszerezze az általa ellátandó feladatkör betöltéséhez szükséges ismereteket, képzettségeket, képesítéseket, indokolt esetben biztosítsa a szükséges oktatások megtartását, illetve gondoskodjon róla, hogy a felhasználó részt vegyen a megfelelő képzéseken, továbbképzéseken.

4.2.2. Képzési eljárásrend

A Hivatal a 273/2012. (IX. 28.) Korm. rendelet előírásainak megfelelően, a közszolgálati jogviszonyban foglalkoztatott munkatársak részére éves és négyéves képzési tervet állít össze. A képzések kiválasztását a felhasználók a szakterületi vezetővel egyeztetve, majd jegyzői jóváhagyással végzik. A munkavállalók szakterületüknek megfelelő képzéseken vesznek részt. A képzési tervek összeállítása a jegyző felelősségi körébe tartozik.

A kötelező képzési terven kívül a munkatársak a szakterületi vezetővel egyeztetve jegyzői jóváhagyással egyedi szakmai továbbképzéseken is részt vehetnek.

Új rendszer bevezetése esetén a jegyző felelőssége a felhasználók oktatásának biztosítása. Az új rendszerhez hozzáférés csak azoknak a felhasználóknak adható, akik részesültek a képzésben és ezt aláírásukkal igazolták.

4.2.3. Biztonságtudatossági képzés

A jegyző felelőssége, hogy a Hivatal elektronikus információs rendszereinek felhasználói biztonságtudatossági képzések formájában megismerjék az alapvető biztonsági követelményeket. A biztonságtudatossági képzés az új felhasználók esetén már a kezdeti képzés részét kell, hogy képezze, továbbá a képzést legalább háromévente meg kell ismételni, illetve minden olyan elektronikus információs rendszerben vagy munkakörben történő változás esetén, mely ezt indokolttá teszi.

A képzésnek kötelezően:

- Fel kell hívnia a munkatársak figyelmét az informatikai biztonsági szabályzati rendszerben bekövetkezett változásokra.
- Ismertetnie kell azokat a sebezhetőségeket, melyek a felhasználó nem-biztonságtudatos magatartását használják ki.
- Ismertetnie kell az azonosított, súlyosnak minősített szabálysértéseket.
- Fel kell hívnia a figyelmet, hogy a megadott súlyos szabálysértések ismételt elkövetése milyen szankciókat von maga után.
- A szabályzatokban, jogszabályokban, szerződésekben előírt követelmények felfrissítése érdekében ismertetnie kell a betartandó szabályokat, kötelezettségeket, egy-egy az oktatásra kijelölt biztonsági terület esetében (pl. hozzáférés védelem témakörében a jelszókezelési szabályok stb.)

Az oktatásokon való részvétel kötelező a Hivatal informatikai rendszereihez hozzáférők számára, amely jelenlétet az oktatás végén a jelenléti ív aláírásával igazolnak.

4.2.4. Fegyelmi eljárás

Az informatikai rendszerek biztonságának gondatlan veszélyeztetése, az informatikai biztonsági szabályok megsértése, illetve a felhasználó súlyos mulasztása esetén a jegyző felelőssége a szükséges fegyelmi eljárás lefolytatása. A jegyző a fegyelmi eljárás megindításáról köteles írásban értesíteni az érintettet és a vizsgálat végrehajtására vizsgálóbiztost jelöl ki. Az IBSZ hatálya alá tartozó szabályok megszegése esetén a fegyelmi eljárás vizsgálóbiztosa a jegyző. A vizsgálatba a jegyző bevonhatja a rendszergazdát, az elektronikus információs rendszer biztonságáért felelős személyt és más külső szakértőket.

A fegyelmi eljárást a 31/2012. (III.7.) Kormányrendelet rendelkezéseinek megfelelően kell lefolytatni.

A fegyelmi vizsgálatról vizsgálati jegyzőkönyvet kell készíteni, valamint a vizsgálat eredményéről írásban szükséges tájékoztatni a jegyzőt.

A jelentésnek tartalmaznia kell:

- a biztonságsértés időpontját,

- a biztonságsértést elkövető nevét és beosztását,
- a tevékenység által közvetlenül okozott kárt,
- a tevékenységgel közvetve okozható kár becsült mértékét,
- a felelősségre vonás javasolt módját.

Amennyiben az információbiztonsági szabályokat nem a Hivatal személyi állományába tartozó személy sérti meg, a jegyző felelőssége érvényesíteni a vonatkozó szerződésben meghatározott és alkalmazható jogi és vagyoni következményeket, továbbá az egyéb jogi lépések lehetőségének vizsgálata és szükség esetén azok alkalmazása.

4.3. Alkalmazás megszűnése

4.3.1. A hozzáférési jogok visszavonása

A felhasználó informatikai rendszerekhez való hozzáférési jogát vissza kell vonni a jogviszonyának megszűnésekor, illetve módosítani kell a felhasználó feladatainak változása esetén. A jegyző felelőssége, hogy az egyes felhasználók jogviszonyának megszűnése esetén a Hivatal érintett munkatársait értesítse.

Általánosságban elmondható, hogy a jegyző felelőssége, hogy a felhasználók csak a feladatkörük ellátásához minimálisan szükséges jogosultságokkal rendelkezzenek az informatikai rendszereken. Ennek megfelelően a jegyző felelőssége, hogy:

- A Hivatal informatikai rendszerét üzemeltető megbízott értesüljön a jogosultságok megváltoztatásának szükségességéről.
- A jogviszony megszűnésekor az érintett felhasználó hozzáférési jogosultsága visszavonásra kerüljön minden olyan informatikai rendszeren, ahol a felhasználó a jogviszony keretében végzendő feladatai miatt kapott hozzáférést.
- A felhasználó feladatkörének változása esetén az új feladatokhoz már nem szükséges jogosultságok visszavonásra kerüljenek.
- Tartós távollét esetén a nem használt hozzáférések felfüggesztésre, illetve tiltásra kerüljenek.

A jogosultságok visszavonásakor a 7.3.4. fejezet rendelkezései az irányadóak.

4.3.2. A vagyontárgyak visszaszolgáltatása

Minden munkatárs köteles a részére átadott vagyontárgyat visszaszolgáltatni a jogviszony megszűnése előtt.

A kilépő munkatárs munkakörét a jegyző által előírt rendben köteles átadni és a munkáltatóval elszámolni. A munkakör-átadás és az elszámolás feltételeit a Hivatal köteles biztosítani.

A jegyzőnek meg kell győződnie arról, hogy a munkatárs minden munkával kapcsolatos adatot és információt, valamint munkájához használt eszközt (laptop, mobiltelefon, fényképezőgép stb.) átadott, valamint a jogosultságai és hozzáférései visszavonásra kerültek.

4.3.3. A munkakör változásának biztonsági kérdései

Áthelyezés esetén a jegyzőnek a szakterülettel együttműködve gondoskodnia kell a munkavállaló meglévő jogosultságainak visszavonásáról, majd az új munkakörnek megfelelő új jogosultságok igényléséről.

5. Fizikai és környezeti biztonság

Az informatikai rendszereken történő adatfeldolgozás biztonsága érdekében meg kell akadályozni az informatikai eszközökhöz történő jogosulatlan fizikai hozzáférést, illetve biztosítani kell az eszközök megbízható működéséhez szükséges környezeti feltételeket (pl. hőmérséklet, páratartalom).

A jegyző felelőssége biztosítani, hogy a Hivatal helyiségeinek kialakítása, illetve az informatikai eszközök elhelyezése során a helyi adottságokat figyelembe véve elfogadható szintre csökkentse az informatikai eszközök jogosulatlan fizikai hozzáféréséből eredő kockázatokat, a lehetőségekhez képest legoptimálisabb módon biztosítottak legyenek az egyes informatikai rendszerek megbízható működéséhez szükséges környezeti és infrastrukturális körülmények.

5.1. Alapvető normák

A felhasználók kötelesek betartani a jegyző által meghatározott fizikai védelmi intézkedéseket, önhatalmúlag nem változtathatják meg az eszközök elhelyezését, valamint kötelesek a napi munkavégzés során az alábbi alapvető viselkedési normákkal összhangban kezelni az informatikai eszközöket, illetve adathordozókat.

5.1.1. A Hivatal épületén kívül

Az alábbi szabályok érvényesek minden olyan helyiségre, ami nem Hivatal használatában, felügyeletében van. Így tipikusan ilyenek például az alábbiak:

- felhasználó lakása;
- közösségi közlekedés;
- közösségi helyek (pl. étterem, kávézó)
- egyéb közterület (pl. utca).

Az ilyen jellegű környezetben az alábbi szabályok betartásával lehet a Hivatal tulajdonú informatikai eszközöket tárolni, használni:

- Utcán, tömegközlekedési eszközön és egyéb nyilvános helyen a Hivatal tulajdonát képező informatikai eszközt – különös tekintettel az adathordozókra – nem szabad felügyelet nélkül hagyni.
- Tilos bekapcsolt és bejelentkezett, de nem zárolt laptopot, vagy egyéb hordozható eszközt felügyelet nélkül hagyni.
- Laptopon, hordozható eszközökön, hordozható adathordozón a feltétlen szükséges minimumra kell korlátozni az érzékeny adatok tárolását, ahol adottak ennek a technikai feltételei lehetőség szerint az érzékeny adatokat titkosítva kell tárolni (ennek egy tipikus módja, ha a laptopokon ki alakításra kerül egy titkosított partíció az érzékeny adatok tárolására).

5.1.2. Üres íróasztal, tiszta képernyő politika

Az irodahelyiségekben tárolt és kezelt adatok jogosulatlan felhasználása ellen minden belépésre jogosultnak fel kell lépnie. A szabályzat személyi hatálya alá tartozók

- Kötelesek az általuk kezelt adathordozókat csak a használat ideje alatt maguknál tartani.
- Kötelesek a papír alapú adathordozók kezelése során az iratkezelési szabályzat előírásait betartani.
- A részükre kiadott biztonsági eszközöket a hatályos szabályozások szellemében más személyek részére nem adhatják át.
- Kötelesek az informatika eszközről kijelentkezni vagy azt zárolni minden esetben, ha a tevékenységet befejezte vagy megszakítja oly módon, hogy az informatikai eszköz felügyelet nélkül marad.
- Kötelesek minden esetben a harmadik felek felügyeletéről gondoskodni, annak érdekben, hogy az ellenőrizetlenül ne férjen hozzá informatikai eszközhöz vagy egyéb adathordozóhoz.
- A munkanap végén a rendelkezésére bocsátott informatikai eszközt kikapcsolni. Ez alól a szabály alól a jegyző személyre, eszközre, munkafolyamatra vonatkozó felmentést adhat, ha ez szakmailag indokolt.

5.1.3. Látogató kísérete

Az irodahelyiségekben harmadik személy nem tartózkodhat felügyelet nélkül, az üres irodákat be kell zárni, annak érdekben, hogy ellenőrizetlenül ne férjen hozzá informatikai eszközhöz vagy egyéb adathordozóhoz.

Látogató fogadásakor a látogató felügyeletét az irodahelyiségben a felhasználónak biztosítani kell. Az irodahelyiségben a látogatóért a felhasználó felelősséggel tartozik.

5.1.4. Belépés rendje

Irodahelységek belépési pontját amennyiben a helységben nem tartózkodik senki sem, az utolsó távozó személynek zárnia kell.

5.1.5. Belépések regisztrálása

A Hivatali munkatárs, személyzet beléptetését az irodai helyiségekbe a Jegyző a felvétellel egyidejűleg engedélyezi mindaddig, amíg a munkatárs jogviszonya fennáll.

5.1.6. Tűzvédelem

A Hivatal helységeiben azok tűzveszélyességi osztályának megfelelő oltókészülékeket kell jól látható és könnyen hozzáférhető helyeken elhelyezni. Az oltókészülékek rendszeres ellenőrzéséről, cseréjéről gondoskodni kell.

5.1.7. Villám és túlfeszültség védelem

A Hivatal épületének rendelkeznie kell villám-, érintés- és túlfeszültség védelemmel. Ezen védelmi megoldások rendszeres karbantartásáról és felülvizsgálatáról a Jegyző feladata gondoskodni. A rendszeres felülvizsgálatokról készített jegyzőkönyveket a

Hivatal köteles megőrizni, és vizsgálatok eredményeképpen feltárt hiányosságok esetén a hiányosságok megszűntetéséről gondoskodni.

5.1.8. Fizikai biztonsági incidensek jelzése

Amennyiben a munkatársak fizikai biztonságot érintő eseményt tapasztalnak vagy a fizikai védelmi eszközök rendellenes működését, rongálását tapasztalják, azonnal jelenteniük kell közvetlen felettesük részére. A bejelentett incidensek kivizsgálásáért a Jegyző felel.

5.1.9. Irodákban elhelyezett informatikai eszközök védelme

A munkatársak nem bonthatják meg az informatikai eszközöket, ilyen tevékenységet csak és kizárólag a rendszergazda végezhet. Amennyiben a munkatársak az eszközök megbontásának tényét tapasztalják, vagy a gyanúja merül fel, abban az esetben kötelesek értesíteni a rendszergazdát.

Az ASP rendszereket futtató munkaállomások elhelyezését úgy szükséges megoldani, hogy az ügyfelek azokat ne tudják elérni és a monitor képét ne láthassák.

6. Kommunikáció és üzemeltetés menedzselése

A jegyző köteles gondoskodni róla, hogy az informatikai eszközök üzemeltetése során, az üzemeltetési feladatokkal megbízott rendszergazda az adott eszközön tárolt, feldolgozott adatok érzékenységének megfelelő védelmi megoldásokat, biztonsági beállításokat alkalmazzon, az üzemeltetési feladatok elvégzése során az elvárható gondossággal járjon el, ezáltal elfogadható szintre korlátozva az informatikai szolgáltatásokhoz való jogosulatlan logikai hozzáférésből, illetve az üzemeltetői hibákból fakadó kockázatok mértékét.

6.1. Üzemeltetési eljárásrendek

6.1.1. Dokumentáció készítése

A főbb üzemeltetési eljárásokra üzemeltetési eljárásrendeket kell kidolgozni, melyeknek összhangban kell lenniük a jelen szabályzattal. Az eljárásrendek kidolgozása az elektronikus információs rendszer biztonságáért felelős személy koordinációjával a rendszergazda feladata. A kész eljárásrendeket az Jegyzőnek jóvá kell hagynia.

Az eljárásrendek napra készen tartása az elektronikus információs rendszer biztonságáért felelős személy feladata.

Az üzemeltetés során, az informatikai rendszeren elvégzett tevékenységek (karbantartás, hibajavítás, változáskezelés stb.) főbb adatait (tevékenység, dátum, végző üzemeltető neve, főbb lépések, a művelet eredménye, felmerült problémák stb.) írásban, visszakereshető módon rögzíteni kell.

Az üzemeltetési eljárásrendek tárolása a hivatal fájlszerverén egy dedikált mappában történik, amelyhez csak a rendszergazda által felhatalmazott munkatársak jogosultak hozzáférni.

6.1.2. Rendszeres tevékenységek

A rendszeresen végrehajtandó üzemeltetési feladatok körét, végrehajtásuk gyakoriságát– jelen szabályzatban foglaltak figyelembe vételével – a rendszergazda határozza meg. A rendszeresen végrehajtandó üzemeltetési feladatokat a rendszergazdának az üzemeltetési eljárásrendben kell rögzítenie, megjelölve a végrehajtás módját, gyakoriságát, felelősét.

6.1.3. Karbantartás

A rendszergazda figyelemmel kíséri az üzemeltetett hardver és szoftver eszközöket, rendszeres időközönként tervszerűen, megelőző jelleggel elvégzik a karbantartásukat.

Az informatikai eszközök hardver karbantartását a rendszergazda végzi. A tervszerű megelőző karbantartás keretében el kell végezni az eszköz portalanítását, takarítását, a mozgóalkatrészek működőképességének ellenőrzését, szükség esetén cseréjét, ellenőrizni kell az eszköz burkolatának, csatlakozóinak épségét, meg kell vizsgálni, hogy fizikai behatás nem érte-e az eszközt, külsérelmi nyom nem látható-e az eszközön. A karbantartás keretében az üzemeltetőnek ellenőriznie kell, hogy az eszköz címkézése, konfigurációja, fizikai fellelhetősége megfelel-e a tárgyi eszköz nyilvántartás adatainak.

A karbantartás keretében az üzemeltető ellenőrizheti az eszközön futó programokat, az eszközön tárolt anyagokat, hogy azok nem sértik-e jelen szabályzat követelményeit (pl. engedély nélküli programok futtatása, szerzői jogvédelem alatt álló anyagok tárolása), illetve, hogy a felügyeleti programok megfelelően futnak-e, a programok frissítettségi szintje aktuális-e, szükség esetén telepíti a hiányzó frissítéseket.

A karbantartás megtörténtét, az elvégzett feladatokat dokumentálni kell. Ha a karbantartás során az üzemeltető olyan problémát észlelt, amit a karbantartás keretében nem lehetett elhárítani, akkor azt a jegyző felé kell jelezni, biztonsági esemény észlelése esetén a biztonsági események jelentésére vonatkozó szabályok szerint kell eljárni.

Az eszköz legutolsó hardverkarbantartásának időpontját az elektronikus információs rendszerelem leltárhoz kapcsolódóan nyilván kell tartani olyan módon, hogy lekérdezhetőek legyenek a legrégebben karbantartott eszközök. A karbantartás időpontját a karbantartást elvégző üzemeltető feladata felvezetni a nyilvántartásba. Ez a nyilvántartás képzi a karbantartások tervezésének alapját. A karbantartások tervezése során biztosítani kell, hogy legfeljebb háromévente minden eszköz karbantartása megtörténjen.

A karbantartások ütemezését, előrehaladását a jegyző hagyja jóvá, ellenőrzi, illetve felügyeli.

Az informatikai eszközök szoftver komponenseinek karbantartása során a rendszergazdának figyelemmel kell kísérni a szoftvergyártók, illetve fejlesztők által kiadott javítócsomagokat, különös tekintettel a biztonsági frissítésekre. Ahol ez lehetséges törekedni kell a frissítések nyomon követésének, telepítésének automatizált, központi management eszközzel támogatott módon történő végrehajtására, felügyeletére.

6.1.4. Javítócsomagok, frissítések telepítése

A Hivatal informatikai eszközeinek szoftverkomponenseire (alaprendszer, telepített alkalmazások) megjelenő, a gyártó, illetve a fejlesztő által kiadott javítócsomagok nyomon követése és telepítése a rendszergazda felelőssége és az adott rendszer üzemeltetőinek feladata az alábbiak szerint.

6.1.4.1. Desktop környezet

A desktop környezet munkaállomásainak frissítéseit lehetőség szerint automatizáltan, központi management eszközzel felügyelt módon kell nyomon követni, teríteni és felügyelni.

A frissítések telepítésének státuszát az alkalmazott központi felügyeleti megoldás segítségével a rendszergazdának kell ellenőriznie minimum heti gyakorisággal. Ha a frissítések telepítése valamelyik munkaállomáson elmaradást mutat, akkor az elmaradt frissítéseket telepíteni kell, az elmaradás okát ki kell vizsgálni, el kell hárítani.

A központi felügyeleti megoldással automatikusan nem frissíthető alkalmazásokról listát kell vezetni, megjelölve a frissítések nyomon követésének módját, gyakoriságát, a frissítések telepítésének módját. A listán szereplő alkalmazások frissítéseit legalább havonta ellenőrizni, szükség esetén telepíteni kell.

A desktop környezet munkaállomásai esetén a frissítések nyomon követése, telepítése, illetve felügyelete a rendszergazda feladata.

6.1.4.2. Hálózati aktív eszközök

A hálózati eszközök frissítéseinek nyomon követése, telepítése a rendszergazda feladata. A frissítések ellenőrzését havi rendszerességgel kell elvégezni. A frissítések telepítése előtt a hálózati eszköz konfigurációjáról mentést kell készíteni.

6.1.4.3. Szakrendszerek

A szakrendszerek frissítése az adott rendszer fejlesztője által alkalmazott gyakorlatnak megfelelően, jellemzően a fejlesztő értesítése alapján történik. A működőképesség fenntartása érdekében a frissítések időzítése előtt a rendszergazdának fel kell mérnie a frissítések okozta kockázatokat és azt össze kell vetni a frissítés szükségességével, illetve a frissítéstől remélt előnyök fontosságával.

A szakrendszerek frissítéseinek nyomon követésével, telepítésével kapcsolatos feladatokat, illetve a feladatok végrehajtásának módját üzemeltetési eljárásrendben kell rögzítenie az adott szakrendszer üzemeltetőjének. Az egyes rendszerek frissítésével kapcsolatos eljárások elkészítését a rendszergazda végzi.

6.1.4.4. Frissítések dokumentálása

A javítócsomagok telepítésével kapcsolatos feladatait az érintett üzemeltetőnek üzemeltetési eljárásrendben kell rögzíteni. Az üzemeltetési eljárásrend szakmai minőségbiztosítása a rendszergazda feladata. A frissítésekkel kapcsolatos feladatok elvégzését a feladatot végrehajtó üzemeltetőnek kell dokumentálnia. A dokumentálás módjával kapcsolatos speciális követelményeket az üzemeltetési eljárásrendben kell rögzíteni.

6.1.5. Együttműködésen alapuló számítástechnikai eszközök

Az elektronikus információs rendszereknek meg kell gátolnia az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha a Hivatal engedélyezte azt, és a fizikailag az eszköznél lévő felhasználó közvetlen kijelzést kap a távoli aktivitásról.

6.2. Vírusvédelem

Hivatal minden munkaállomásán és szerverén vírusvédelmi rendszernek kell üzemelnie, mely minden, az adathálózatról fogadott illetve oda továbbított adatállományt átvizsgál.

A vírusvédelmi rendszernek biztosítania kell:

- a vírus-adatbázis rendszeres és automatikus frissítését a vírusvédelmi rendszer minden elemén;
- a vírusvédelmi rendszernek (az üzemeltetési szempontból indokolt kivételek figyelembe vételével) minden állomány megnyitásakor el kell végeznie a vírusellenőrzést (on-access ellenőrzés);
- azon gyanúsnak ítélt illetve kártékony kódra hasonlító jelsorozatok (nem irtható vírusok) karanténba helyezését, melyek biztonságos eltávolítása nem lehetséges;
- a vírusfertőzések, illetve fertőzött állományok kezelésének naplózását;
- a vírusvédelmi rendszernek riasztást kell tudnia küldeni;
- a vírusvédelmi rendszert a felhasználó ne kapcsolhassa ki, beállításait ne változtathassa meg.

Mind a szerverek, mind a munkaállomások esetén a rendszergazda feladata a vírusvédelmi rendszerek beállításainak a meghatározása. A vírusvédelmi rendszer beállításait (az alkalmazandó policyt) általános esetben az alapkonfiguráció nyilvántartásban, míg egyedi beállítások alkalmazása esetén az érintett elektronikus információs rendszer rendszerbiztonsági tervében kell rögzítenie a rendszergazdának.

A vírusvédelmi rendszer napi üzemeltetési feladatait, vírusvédelmi rendszer működésének felügyeletét a rendszergazda végzi az üzemeltetési eljárásrendben rögzítettek szerint. A vírusvédelmi rendszer megfelelő működését, a frissítések végrehajtásának ellenőrzését legalább heti gyakorisággal ellenőrizni kell.

A felhasználó rendelkezésére bocsátott informatikai eszközön vírusvédelmi rendszert kell üzemeltetni. A vírusvédelmi rendszert a felhasználónak tilos kikapcsolnia vagy módosítania, illetve tilos módosítani annak beállításait. Abban az esetben, ha a vírusvédelmi rendszer vagy a felhasználó kártékony kódot – pl.: vírust -, vagy annak gyanúját észleli, akkor a felhasználó kötelessége azonnal jelenteni az eseményt az adott eszköz üzemeltetési feladataival megbízott rendszergazdának.

A felhasználónak tilos a rendelkezésére bocsátott informatikai eszközökön szándékosan kártékony kódokat, illetve Hivatal informatikai biztonsági rendszereinek állapotát bármilyen formában feltérképező szoftvereket tárolni, működtetni, módosítani (mutációkat létrehozni), illetve fejleszteni.

6.3. Mentési rend

6.3.1. Általános követelmények

A Jegyző feladata biztosítani a Hivatal működése szempontjából kritikus adatok, szoftverek, konfigurációs beállítások megfelelő tartalékolását. A Hivatal informatikai rendszereinek, illetve az informatikai rendszereken kezelt adatoknak a mentését, megőrzését, tárolását úgy kell megoldani, hogy a mentések típusa, gyakorisága és példányszáma elfogadható adatvesztési kockázatot eredményezzen, valamint az archiválásra vonatkozó jogszabályi követelményeket teljesíthesse.

A Hivatalnak olyan mentési megoldásokat kell alkalmazni, illetve olyan mentési eljárást kell működtetni, ami biztosítani tudja, hogy az informatikai eszközök sérülése, meghibásodása, illetve a tárolt adatok sérülése használhatatlanná válása esetén rendelkezésre álljon olyan mentés, amely segítségével a kiesett informatikai szolgáltatás elfogadható időn belül újraindítható, illetve amelynek visszaállításával az elvesztett adatmennyiség mértéke még kezelhető szinten marad. Azon adatok esetén, amelyek hosszú távú megőrzését a Hivatal elektronikus formában biztosítja a mentésnek alkalmasnak kell lenni az adatok jogszabályban előírt megőrzési idejének végéig történő visszaállítására.

A fenti követelményeknek megfelelő mentő infrastruktúra, illetve mentési eljárások tervezése, kialakítása a rendszergazda szakmai támogatásával a Jegyző feladata, a Hivatal működése szempontjából kritikus adatok, szoftverek, konfigurációs beállítások megfelelő tartalékolásával kapcsolatos tevékenységek felügyelete, ellenőrzése a rendszergazda feladata. A rendszergazda feladata meghatározni, hogy az egyes informatikai rendszerek esetén milyen jellegű mentéssel (pl. logikai mentés, fájl szintű fizikai mentés, mentőagenttel készített mentés) tudja biztosítani a Hivatal a kezelt adatok konzisztens módon történő visszaállítását, figyelembe véve az adatok tárolásának és használatának módját, illetve a nyitott fájlok mentésével kapcsolatos esetleges problémákat.

Az alkalmazandó mentési stratégiára a mentendő adatok mennyisége, a mentés lefutására rendelkezésre álló idő, az alkalmazott mentőmegoldások, valamint a megőrzési idők és a rendelkezésre állási követelmények figyelembe vételével ugyancsak a rendszergazda ad javaslatot.

A fentieknek megfelelően a jegyzőnek az alábbi irányelveket javasolt figyelembe vennie:

- Az adatok mentése illetve archiválása mellett az adatok visszaállításához szükséges valamennyi egyéb adat és szoftver komponens is visszaállíthatóan

mentésre, illetve archiválásra kerüljön, vagy mentésük illetve archivált állományuk létezzen.

- A mentésre, illetve archiválásra alkalmazott adathordozó megválasztása az adathordozó felhasználhatóságának gyártói korlátozásai – pl. adatmegőrzési idő, újraírhatóság száma, tárolási előírások stb. - figyelembe vételével történjen.
- A mentéseket tartalmazó adathordozók kezelése a rajtuk tárolt adatok érzékenységének megfelelően történjen, valamint a forrásrendszerrel azonos szintű biztonságos fizikai hozzáférés védelem mellett kerüljenek megőrzésre.
- A mentett és az archív állományok adatainak a visszatöltéséhez szükséges berendezés mindenkor a rendelkezésre álljon.

6.3.2. Mentési eljárásrend

A kialakított mentési stratégiát, az alkalmazott mentőkörnyezet illetve mentési eljárás leírását, a mentések technikai paramétereit, a mentőmédiák kezelésével kapcsolatos feladatokat, a mentésekkel kapcsolatos feladatok végrehajtásának módját, a rendszergazdának mentési eljárásrendben kell dokumentálni.

A mentési rendnek minimálisan tartalmaznia kell az alábbiakat:

- Mentendő rendszer neve
- Mentendő adatterületek
- Mentés gyakorisága
- Mentési típusa (teljes, inkrementális, differenciális, stb.)
- Mentés példányszáma
- Alkalmazandó mentő média
- Mentő média tárolása, kezelése
- Mentő média, mentett állományok névkonvenciója
- Mentés megőrzési ideje
- Mentés végrehajtásának felelőse
- Mentésből történő visszaállítás felelőse
- Mentési jogok futásának ellenőrzése
- Mentett állományok visszatöltési tesztjeinek gyakorisága

6.3.3. Alkalmazások mentése

Az alkalmazások mentési módszerének meghatározását úgy kell elvégezni, hogy egy konzisztens állapot kerüljön mentésre. Amennyiben azt az alkalmazás vagy a mentési rendszer jellemzői megköveteli, ehhez szükség lehet az alkalmazás és/vagy adatbázisa elérhetőségének korlátozására a mentés idejére.

6.3.4. Adatok visszaállításának folyamata

Sérült, törölt, elveszett adatok mentésből történő visszaállítását a felhasználók e-mailen kezdeményezhetik a rendszergazdánál, az adatvisszatöltés indokának megjelölésével.

Adatvesztéssel járó adatvisszatöltés csak az adat tulajdonosának jóváhagyásával történhet, ezért ilyen esetben a rendszergazda e-mailen kéri az adatvisszatöltés jóváhagyását a várható adatvesztés mértékének megjelölésével.

Az adatvisszatöltés tényét, technikai részleteit a rendszergazdának dokumentálni kell, a mentésből történő visszaállításhoz tartozó teljes levelezés mentésével. A mentésből történő visszatöltés eredményének tesztelését az igénylő feladata elvégezni, illetve megszervezni a rendszergazdától kapott értesítés alapján.

Üzemeltetési célú rendszer-visszaállítás esetén a mentésből történő visszaállítást a rendszergazdának dokumentálni kell. Ha a visszatöltés nem járt adatvesztéssel, akkor a tesztelés és a visszatöltés jóváhagyása a rendszergazda feladata. A visszatöltés okát, tényét, eredményét és a kapcsolódó levelezést dokumentálni kell.

6.3.5. Katasztrófamentés, teljes környezet mentés

A Hivatalnak az informatikai rendszerek futtatókörnyezetéről olyan mentéssel kell rendelkeznie, ami a költséghatékonysági szempontokat is figyelembe véve legrövidebb időn belül lehetővé teszi az informatikai rendszer, illetve a kezelt adatok mentésből történő visszatöltésére alkalmas futtatókörnyezet újraindítását, ami minimálisan lehet a kiszolgáló rendszerállapotának a mentése, de lehetőség szerint a rendszer teljes futtatókörnyezetének visszaállítására alkalmas image, virtuális környezetben futó rendszerek esetén valamilyen VHD szintű mentés. A rendszerkörnyezet hatékony visszaállítására alkalmas mentési megoldásról a Jegyző dönt a rendszergazda bevonásával. Az elektronikus információs rendszer biztonságáért felelős személynek vizsgálnia kell, hogy a javasolt megoldás mennyire felel meg a szakterületek által támasztott rendelkezésre állási követelményeknek. Feladatok és felelősségek

A jegyző által meghatározott követelményeknek megfelelő mentési megoldás kialakítása és a mentések elkészítésével és ellenőrzésével kapcsolatos feladatok szükséges gyakorisággal történő végrehajtása az adott eszköz üzemeltetési feladataival megbízott feladata.

A felhasználó felelőssége, hogy az általa használt eszközön (munkaállomáson, laptopon) tárolt azon adatokról, állományokról, amelyek sérülése, elvesztése jelentősen hátráltatná a napi munkavégzést, illetve amelyek pótlása utólag nem lehetséges, vagy túl nagy terhet jelentene a Hivatalra nézve valamiféle mentés készüljön. Az adott eszköz üzemeltetési feladatainak ellátásáért felelős feladata tájékoztatni a felhasználót, hogy mit kell tennie az állományok mentése érdekében (pl. külső adathordozóra írás, hálózati megosztásra történő másolás stb.).

A jegyző joga a mentési feladatok végrehajtásának ellenőrzése, számon kérése.

6.4. Hálózatbiztonság

A hálózatbiztonsági intézkedések célja az adathálózaton keresztül megvalósuló, a Hivatal informatikai rendszerein kezelt adatok biztonságát kompromittáló, illetve a

Hivatal normál működéséhez szükséges informatikai szolgáltatások elérhetőségét korlátozó biztonsági események kockázatát elfogadható szintre csökkenteni.

A jegyző felelőssége biztosítani, hogy a Hivatal informatikai rendszerei által használt hálózati szolgáltatásokat megvalósító eszközök biztosítsák az informatikai rendszerek számára a kezelt adatok érzékenységének megfelelő szintű védelmet. Az eszközök üzemeltetése olyan módon történjen, hogy üzemeltetői hiba, félrekonfigurálás, vagy az eszközök biztonsági beállításainak gyengesége, hiányosságai lehetőség szerint ne jelentsenek támadási felületet a belső hálózaton lévő eszközökre nézve. Az alkalmazott határvédelmi megoldásnak a szükséges minimumra kell korlátozni a külső hálózat irányából a Hivatal informatikai rendszereire irányuló adatforgalmat, azon informatikai eszközöket, amelyek nem futtatnak nyilvános szolgáltatást, külső hálózat irányából ne lehessen elérni.

A rendszergazdának a minimális hozzáférési szabályoknak eleget tevő módon (minden tiltott, ami nem engedélyezett) korlátozni kell a hozzáférést a hálózati eszközökhöz és az azok által nyújtott szolgáltatásokhoz.

A rendszergazdának a tűzfalakhoz és az egyéb hálózati eszközökhöz történő privilegizált hozzáférést szigorúan korlátozni kell, az engedélyezett hozzáféréseket titkosított kapcsolaton keresztül együtt szabad engedélyezni.

A Hivatal internetkapcsolatának beállásait, logikai és fizikai struktúráját a rendszergazdának dokumentálnia kell.

6.4.1. Vezetékes hálózati végpontok

A Hivatal strukturált kábelezéssel megvalósított vezetékes hálózatot üzemeltet. Hálózati végpontok felügyelet nélküli nyilvános hozzáférést lehetővé tevő helyen nem lehetnek. A nem használt végpontokat hálózati eszközökről le kell csatlakoztatni, de legalább logikai szintű beállítással tiltani kell a használatukat.

A felhasználók a hálózati kábelezést nem bonthatják meg, a végpontokra idegen, nem a Hivatal tulajdonában lévő eszközt nem csatlakoztathatnak.

6.5. Adattárolás és adattovábbítás szabályai

6.5.1. Általános szabályok

A jegyző felelőssége, hogy a kialakított ügyviteli rend biztosítsa, hogy a napi feladatok keretében végzett adattárolás és adattovábbítás az adatok érzékenységének, illetve a vonatkozó jogszabályi követelményeknek megfelelően történjen. A felhasználóknak a kialakított ügyviteli rendtől önhatalmúlag eltérni tilos. A jegyző jogosult az adatok tárolásával, továbbításával kapcsolatban a normál ügyrend által előírt adatkezelési feladatok mellett tovább intézkedéseket előírni.

6.5.2. Elektronikus levelezés szabályai

- Tilos minden olyan, a Hivatal informatikai rendszerén kívülről bejövő levelet megnyitni, amely szemmel láthatóan nem a Hivatal tevékenységével kapcsolatos és a levél megnyitását a felhasználó kockázatosnak ítéli, valamint akinek ez nem munkaköri kötelessége, annak tilos megnyitni azon leveleket, amelyek feladója a fogadó személy által nem kellően azonosítható.
- „Forward”-al tovább küldött levelek esetén ügyeljünk rá, hogy az lehetőleg ne tartalmazza a küldő, illetve a többi címzett e-mailcímét, ha az kifejezetten nem szükséges, mert így az érintettek tudta és beleegyezése nélkül adjuk ki az e-mail címeket.
- Nem javasolt a Hivatal levelező rendszerét magánlevelezésre használni, ha mégis a tevékenységével össze nem függő e-mail érkezik a felhasználó postafiókjába, elolvasás után azt célszerű mielőbb törölni.
- Hivatalos e-mail címet külső helyen regisztrációs adatként, vagy magáncélból megadni nem javasolt.
- Tilos kéretlen reklám-, lánc-, átverésre irányuló levelekre, válaszolni, továbbítani, vagy bárminemű más cselekedetet végrehajtani.
- Hivatal fenntartja magának a jogot, hogy az elektronikus leveleket szűrje és korlátozza.
- Hivatal jogosult a belső és a kimenő levelek szúrópróba szerű vizsgálatára.

6.5.3. Internethasználat szabályai

Az internet használata munkavégzés céljából engedélyezett. A Jegyző utasításának megfelelően az internet használat korlátozásra kerülhet, a Hivatal a használatot utólagosan ellenőrizheti.

A felhasználók számára a munkavégzéshez nem szükséges honlapok böngészőből történő elérése nem engedélyezett, amelyet technikai eszközzel is kikényszeríthet a Hivatal, fehér-, illetve feketelistás szűrést alkalmazva. Alapértelmezetten tiltani kell a közösségi oldalak, társ- vagy partnerkereső oldalak, magán postafiókok, pornográf és szexuális jellegű és tartalmú oldalak megtekintését, illetve használatát.

A jegyző felelőssége meghatározni, hogy milyen tartalmú fehér- vagy feketelistás szűrést kell alkalmazni. Az engedélyezett vagy tiltott oldalakat a jegyző engedélye alapján a rendszergazda feladata beállítani.

Az internetről nem engedélyezett semmilyen szoftver, illetve fájl letöltése, illetve telepítése, kivételt képeznek ez alól a rendszergazda, valamint ha a fájl a Hivatal ügymenetéhez elengedhetetlen.

6.6. Naplózás

A számon kérhetőség és hibakezelés biztosítása érdekében az informatikai eszközöknek az informatikai rendszer működéséről és különösen az informatikai biztonsági eseményekről helyi naplóállományt kell generálni.

A jegyző felelőssége, hogy a kialakított naplózási rendszer a szükséges mértékben biztosítsa a számon kérhetőséget és az auditálhatóságot, tegye lehetővé a bekövetkezett fontosabb események utólagos kivizsgálását, különös tekintettel azokra, melyek a rendszer biztonságát érintik.

Amennyiben a jegyző másként nem rendelkezik az informatikai eszközök minimálisan az alapértelmezett naplózási beállítások szerinti eseményeket naplózni kell. Az adott informatikai eszköz üzemeltetéséért felelős személy, ha azt az üzemeltetési, üzemeltethetőségi szempontok indokolják, saját hatáskörben módosíthatja az alapértelmezett naplóbeállításokat, az jegyző tájékoztatása mellett. A naplóállományokat meghibásodás vagy biztonsági incidens esetén, eseti jelleggel kell vizsgálni. Meghibásodás esetén a naplóállományok vizsgálata a hibajavításban eljáró üzemeltető feladata. A naplóállományok rendszeres átvizsgálását a rendszergazdának feladata végrehajtani, hiba vagy biztonsági incidens esetén azonnal, egyéb esetben féléves rendszerességgel.

A rendszergazda felelőssége a rendszereket úgy beállítani, hogy azok a naplókat a jegyző által meghatározott időtartamra visszamenőlegesen megőrizzék.

Olyan elektronikus információs rendszert szükséges használnia a Hivatalnak, mely biztosítja, hogy a felhasználói tevékenységek személyre szólóan nyomon követhetők legyenek.

A Hivatalban lehetőség szerint olyan rendszerek használata engedélyezett, melyek biztosítják a naplóbejegyzések időbélyeggel történő ellátását.

A rendszergazda felelőssége a rendszerek naplóinak hozzáférését olyan módon korlátozni, hogy ahhoz jogosulatlanul hozzáférni, illetve törölni, tartalmát módosítani ne lehessen.

A rendszergazda köteles a mentési rendszert úgy beállítani, hogy a Hivatal kiszolgálóin üzemelő rendszerek naplóinak mentése az adott rendszer mentésével együtt megtörténjen. A rendszergazdának a munkaállomásokon üzemelő szakalkalmazások mentését olyan módon kell megoldania, hogy az kiterjedjen az alkalmazás működése során keletkezett naplók mentésére is.

Új rendszer bevezetése vagy nagyobb frissítés esetén a rendszergazda felelőssége annak ellenőrzése, hogy az új, illetve módosított alkalmazás a Hivatalnak a naplózásra vonatkozó követelményeket kielégíti-e, és az esetlegesen szükséges módosításokat az üzemeltetőkkel elvégeztesse.

6.7. Hordozható informatikai eszközök használata

Tekintettel arra, hogy a hordozható eszközök könnyen mozgathatók, a hordozható eszközre kiemelt figyelmet kell szentelni a lopások, elvesztések, fizikai sérülések elkerülésére.

Hordozható informatikai eszközt a Hivatalban és a munkatárs lakásán kívül tilos magára hagyva tárolni, vagy bekapcsolt állapotban szállítani. (Például e szabály szerint nem engedélyezett felügyelet nélkül hagyni az eszközt autóban, bemutató alkalmával a pódiumon, tárgyalás szünetében az asztalon, portán stb.) Ezen felül a hordozható eszközt a használat ideiglenes, akár rövid idejű felfüggesztése esetén is zárolni kell, oly módon, hogy az eszköz használatát csak a felhasználói jelszó megadásával lehessen folytatni, ezáltal akadályozva a jogosulatlan hozzáférést lehetőségét.

A felhasználónak kötelessége az eszközt elrejtett módon szállítani.

Abban az esetben, ha a hordozható informatikai eszköz vagy valamely perifériája fizikailag megsérül, roncsolódik, elvész, megsemmisül vagy a külső felületen elváltozás tapasztalható, a munkatársnak kötelessége azt jelezni a rendszergazdának, aki a körülmények ismeretében dönt róla, hogy ki kell-e vizsgálni az esetet, illetve biztonsági esemény gyanúja esetén értesíti a jegyzőt.

A hordozható eszközt TILOS együtt szállítani olyan adathordozókkal vagy egyéb eszközökkel, melyek felhasználása meggyorsítja a hordozható eszköz biztonsági rendszerének megkerülését. Ugyanakkor a felhasználónak kötelessége elérhetőségét elhelyeznie a hordozható eszköz mellett annak érdekében, hogy az eszköz elvesztése esetén a becsületes megtaláló, azt vissza tudja szolgáltatni.

6.8. Rendszerfejlesztés

A Hivatal informatikai rendszereinek továbbfejlesztési irányait a felhasználói igények, illetve a vonatkozó jogszabályi követelmények összegyűjtésével és kiértékelésével a jegyző feladata meghatározni és szükség esetén a képviselő testület elé terjeszteni.

A felhasználók igényeiket közvetlen munkahelyi vezetőjükön keresztül jelezhetik. A megvalósítás módjáról – szükség esetén az igénylővel egyeztetve – a jegyző dönt. A módosításoknál figyelembe kell venni jelen szabályzatnak történő megfelelést.

6.9. Kriptográfiai védelem

A Hivatal elektronikus információs rendszereiben alkalmazott kriptográfiai eszközök kiválasztásánál figyelembe kell venni, hogy a törvényi előírásoknak megfelelő titkosítási algoritmusok kerüljenek kiválasztásra és azok a kezelt adatok besorolásának megfelelően kerüljenek alkalmazásra,

A rendszergazdának gondoskodnia kell róla, hogy a Hivatalban alkalmazott kriptográfiai kulcsokhoz csak azon személyek férhessenek hozzá, akiknek ehhez a munkájuk során feltétlen szükségük van. A kulcsokat biztonságos módon, csak a felhasználó számára hozzáférhetően illetve páncélszekrényben kell tárolni.

7. Hozzáférés-ellenőrzés

7.1. Hozzáférés-védelem

A Hivatal kizárólag nyilvánosan hozzáférhető adatokat tartalmazó elektronikus információs rendszereinek elérése során felhasználói szintű hozzáférés-védelem használata nem elvárás.

A nem kizárólag nyilvános adatokat tartalmazó elektronikus információs rendszereknek rendelkezni kell a felhasználók azonosítását, hitelesítését megbízható módon lehetővé tevő hozzáférés-védelmi rendszerrel. Az elektronikus információs rendszer hozzáférés-védelmi rendszerének biztosítania kell, hogy azokat a funkciókat, amelyek alkalmasak a kezelt adatok valamely védendő biztonsági kritériumának (bizalmasságának, sértetlenségének, rendelkezésre állásának) kompromittálására azonosítás és hitelesítés nélkül ne lehessen használni.

A rendszerek authentikációjának beállítása során törekedni kell a felhasználói azonosítók egységes, központi felületen történő kezelésére. Azon rendszerek esetén, amelyek lehetővé teszik, hogy a felhasználók azonosítása, hitelesítése központi címtárban tárolt adatok alapján történjen, ott lehetőség szerint kerülni kell a lokális felhasználók használatát, ettől csak üzemeltetési szempontból indokolt esetben, a jegyző jóváhagyásával lehet eltérni.

A rendszerekben lehetőség szerint személyhez rendelt azonosítókat kell használni, ettől eltérni – azaz felhasználói csoport által közösen használt azonosító használatára – csak a jegyző írásbeli engedélye esetén szabad, mely engedélynek indoklást kell tartalmaznia arról, hogy milyen technikai, ügyvitelszervezései vagy egyéb oka van annak, hogy személyhez rendelt azonosítók nem használhatók.

A Hivatal informatikai hálózatában csak a jegyző által jóváhagyott informatikai eszköz telepíthető. A hivatal felhasználója alapértelmezetten nem lehet jogosult az informatikai eszközön kiemelt felhasználói jog használatára, mely szabály alól jegyzői engedéllyel el lehet térni, azonban ilyen esetekben külön nyilvántartással kell rendelkeznie a Hivatalnak ezen többletjogosultsággal rendelkező felhasználókról, továbbá indokolni szükséges a többletjogosultság használatát.

7.2. Felhasználó kezelés

A jegyző feladata és felelőssége, hogy a felhasználók felvétele, kilépése, áthelyezése, az esetleges átszervezések, illetve a felhasználók feladatkörének változtatása kapcsán olyan munkarendet alakítson ki, ami biztosítja, hogy a felhasználók az informatikai rendszerekhez mindenkor csak a feladatkörük ellátásához szükséges jogosultságokkal férjenek hozzá. E követelmények teljesítése érdekében centralizált jogosultságkezelési és nyilvántartási, a jogosultságkezelés teljes életciklusára kiterjedő folyamatot kell kialakítani és működtetni a Hivatalban.

7.2.1. Általános elvárások

- Új felhasználó felvétele esetén csak a feladatköre ellátásához szükséges informatikai rendszerekhez és csak a szükséges jogosultságok erejéig kapjon hozzáférést.
- A hozzáférés csak akkor bocsátható a felhasználó rendelkezésére, ha minden feltétel biztosított ahhoz, hogy azt a felhasználó biztonságosan, jelen szabályzatban leírtakkal összhangban tudja használni.
- Áthelyezés, átszervezés, illetve a felhasználó feladatkörének változása esetén, a már nem szükséges hozzáférések, jogosultságok kerüljenek visszavonásra.
- Kilépés, tartós távollét, a felhasználó jogviszonyának megszűnése, vagy felfüggesztése esetén a felhasználó hozzáférési jogosultságai visszavonásra, tiltásra kerüljenek.

A fenti általános követelmények egyformán érvényesek a Hivatal saját informatikai rendszerein, a külső szolgáltatótól igénybe vett rendszerek esetén, illetve minden olyan internetes szolgáltatás esetén, ahová a felhasználók a Hivatal tevékenységével kapcsolatos feladatokhoz regisztrált hozzáférést használnak.

A jegyző felelőssége, hogy a fenti követelmények maradéktalan teljesítése érdekében minden érintett informatikai rendszer esetén az adott rendszer üzemeltetési feladatait ellátó személy értesítést kapjon a felhasználó hozzáférési jogosultságainak szükséges módosításáról.

7.2.2. Jogosultságok igénylése

A Hivatal informatikai rendszereihez jogosultságokat a Hivatal munkatársai a jegyzőtől igényelhetnek, írásban vagy szóban. A hozzáférési jogosultságot igényelni a Hivatal belső informatikai infrastruktúráján futó alapszolgáltatások eléréséhez és használatához, belső alkalmazások, külső szolgáltató által biztosított alkalmazások és szolgáltatások, illetve központi szolgáltatások igénybevételéhez lehetséges.

Új munkatárs munkába lépésekor a jegyző határozza meg a munkatárs munkakörének megfelelő rendszerhozzáféréseket, és a rendszerekben beállítandó jogosultságokat.

7.2.3. Jogosultsági igény jóváhagyása, továbbítása

A jegyző felelős az igényelt hozzáférési jogosultságok jóváhagyásáról dönteni. A jegyzőnek a döntésének megfelelően írásban szükséges rögzítenie a jóváhagyott jogosultságokat, és továbbítani a rendszergazdának, illetve az adott rendszer üzemeltetőjének (amennyiben nem a rendszergazda látja el az adott rendszer rendszerüzemeltetési feladatait) a kért és beállítandó jogosultságokat.

A jogosultsági igények továbbítása email-en vagy papír alapon is történhet. Az igénynek minimálisan kell tartalmaznia, hogy:

- mely felhasználóhoz kapcsolódóan történt az igénybejelentés,
- mely rendszerhez kapcsolódik az igény,
- milyen rendszeren belüli jogosultság beállítása szükséges.

A fenti adatokon felül az adott rendszer üzemeltetője (pl. központi rendszerek esetében) egyéb adatok megadását illetve egyedi jogosultság bejelentő formanyomtatvány használatát is megkövetelheti, melynek megfelelően szükséges a jegyzőnek az igénylést végrehajtani.

Érvénytelen az igénylés, ha nem tartalmaz minden olyan információt, mely alapján az üzemeltető be tudja állítani a kérvény alapján az igényelt jogosultságokat, továbbá, ha az igénylés e-mail esetén nem a jegyző e-mailcíméről érkezett, papír alapú igény esetén nem tartalmazza a jegyző aláírását.

A jegyző felelőssége a jóváhagyott és beállításra továbbított jogosultsági igények papír alapon történő megőrzése (e-mailen történt igénylés esetén az e-mail nyomtatásával) az igényléstől számított 3 évig. A jegyző feladta, hogy minden jóváhagyott jogosultsági igényről írásban tájékoztassa a Hivatal rendszergazdáját.

Az érintett informatikai rendszerek üzemeltetési feladatait ellátók kötelesek a jegyző által jóváhagyott igények alapján végrehajtani a jogosultsági igények beállítását az érintett rendszerekben.

7.2.4. Felhasználó felvétele

A Hivatal üzemeltetési hatáskörében lévő rendszerek esetében a jogosultságot beállító rendszergazdának az alábbi szabályok szerint eljárnia:

1. Új felhasználó esetében az érintett rendszer(ek)ben létre kell hoznia a hozzáféréshez szükséges azonosítókat, üzemeltetőnek törekedni kell a felhasználói azonosító egységes képzési szabályára.
2. Az érintett rendszer(ek)ben az létre kell hoznia a használathoz szükséges objektumokat (pl. postafiók, saját mappa a fájlszerveren).
3. Az érintett rendszer(ek)ben a felhasználót az igénylésben meghatározottak szerint hozzáférési jogosultsággal ruházza fel.
4. A rendszergazda feladata gondoskodni a kapcsolódó nyilvántartások (pl. jogosultság, licenc) frissítéséről.
5. A felhasználó kezdeti jelszavát a rendszergazda köteles megválasztani, a rendszergazda feladata felhívni a felhasználó figyelmét, hogy az első bejelentkezés alkalmával változtassa azt meg.
6. A rendszergazdának a jelszót a felhasználónak úgy kell átadnia, hogy annak bizalmassága ne sérüljön.

Nem hivatali hatáskörben üzemeltetett rendszerek esetében a rendszer üzemeltetését végző fél feladata a belső eljárásrendjének megfelelően regisztrálni az érintett rendszerben az igénylésben szereplő jogosultságokat.

7.2.5. Jogosultságok módosítása

Hozzáférési jogosultságok módosítása (új jog kiadása, meglévő jog elvétele) a 7.2.2 és 7.2.3-aspontban leírtak szerint történik.

7.2.6. Felhasználó kilépése

A jogviszony megszűnésekor jegyzői felelőssége gondoskodni arról, hogy a kilépő munkatárs esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzze (pl. hozzáférések megszüntetése, jogosultságok visszavonása).

A távozó munkavállaló jogosultságainak visszavonását a jegyzőnek kell írásban (e-mailen, papíron) kezdeményeznie, minden olyan informatikai rendszerre kiterjedően (helyi rendszerek, külső harmadik félnél üzemeltetett rendszerek esetében is), melyhez hozzáférési jogosultsággal rendelkezett a kilépő személy. A kilépéskor, a Hivatal által üzemeltett rendszerekben, a jogosultságot visszavonó rendszergazdának írásban kell igazolnia, hogy a kilépő munkatárs hozzáféréseit minden általa üzemeltetett rendszerben megszüntette, illetve ha az ő közreműködésével történt a külső rendszerekben lévő jogosultságok visszavonása úgy ezen rendszerekben végrehajtott változásokról is értesítenie kell a jegyzőt. Ha nincs lehetőség a jogosultságok visszavonására, akkor a jelszó megváltoztatásával kell megakadályozni az azonosító használatát. Ilyen esetben a megváltoztatott jelszót a jegyzőnek kell zárt borítékban elzárt helyen tárolnia.

Abban az esetben, ha a felhasználó jogviszonya, illetve a kapott hozzáférés oka megszűnik, akkor a Hivatal fenntartja a jogot, hogy a felhasználó által kezelt adatokat a jegyző engedélyével mások számára - pl. a munkahelyi vezető vagy az általa kijelölt munkatárs számára - hozzáférhetővé tegye, vagy archiválja. A munkaviszony megszűnése előtt a felhasználónak kötelessége felhasználói azonosítóját átadni, személyes használatú adatait törölni. A felhasználó a Hivatal tulajdonát képező adatokat kilépéskor nem semmisíthet meg!

7.3. Kiemelt felhasználói jogosultság kezelése

7.3.1. Jogosultság igénylése

A Hivatal felhasználói számára az informatikai rendszerekhez kiemelt felhasználó jogosultság a jegyző írásos beleegyezésével adható ki. A jogosultságigénylés a 7.2.2 fejezet előírásai szerint kell végrehajtani. A kiemelt felhasználói jogosultságokról a rendszergazdának a normál felhasználói jogosultságokhoz hasonlóan nyilvántartást kell vezetni.

7.3.2. Kiemelt jogosultság használata

Kiemelt felhasználói jogot biztosító felhasználói azonosítóval kizárólag üzemeltetési feladatok, illetve olyan ügyviteli tevékenységek (pl. kiemelt felhasználói jogosultság szükséges ügyviteli alkalmazás használatához) láthatók el, melyek megkövetelik ezen azonosító használatát.

7.3.3. Jogosultság megvonása

A jegyző kezdeményezheti a kiemelt felhasználói jogosultság azonnali hatállyal történő megvonását. A jogosult munkakörének megváltozása, kilépése azonnal a jog

megszüntetését vonja maga után. A kiemelt felhasználói jogok visszavonásának módja:

1. Azon rendszereken, ahol a kiemelt felhasználói jog nem köthető személyhez, ott a kiemelt felhasználói jelszót haladéktalanul meg kell változtatni.
2. Azon rendszerek esetén, ahol az adminisztrátori szerep a felhasználói azonosítóhoz rendelt, ott a felhasználó és a szerep kapcsolatát meg kell szüntetni.

7.3.4. ASP rendszerek jogosultság kezelése

Az ASP rendszerek jogosultságkezelését végző tenant adminisztrátorok rendszerbe történő felvétele a Hivatal által az ASP Központnak megküldött adatlap alapján történik.

A tenant adminisztrátorok a munkatársaik részére további jogosultságot oszthatnak, amelyeket a jegyző felelőssége jóváhagyni, a privilegizált joggal rendelkező tenant adminisztrátoroktól elvárt, hogy csak indokolt esetben használják a jogaikat, valamint a bejelentkezési azonosítóikat zárt borítékban, biztonságosan zárható helyen kell tárolni.

A tenant adminisztrátor feladatai:

- új felhasználók rögzítése;
- meglévő felhasználók adatainak módosítása;
- felhasználók zárolása;
- felhasználói jogosultságok kiosztása, módosítása, megvonása;
- helyettesítések beállítása, eltávolítása;
- felhasználói csoportok létrehozása, módosítása, törlése;
- üzleti napló megtekintése.

Az ASP munkaállomásokat csak a Jegyző által kijelölt személyek vehetik használatba, amely személyek listáját a kincstár felé szükséges leadni. A felhasználóknak rendelkeznie kell elektronikus személyi igazolvánnyal a munkaállomások használatba vételéhez, amelyet a rendszergazda feladata hozzárendelni a felhasználókhoz, hogy a leolvasó készülékkel be tudjanak jelentkezni az ASP rendszerekbe. Az elektronikus személyi igazolványt csak a tulajdonosa használhatja az ASP rendszer authentikációs folyamat céljából, azt másnak átadni a rendszer használatához tilos.

7.4. Technikai azonosítók kezelése

A technikai azonosítók igénylése és kezelése a kiemelt felhasználói azonosítókéval megegyező módon történik. A hozzáférési jogosultságokról vezetett nyilvántartásnak tartalmaznia kell a technikai azonosítókat is, feltüntetve a technikai azonosító használatának célját, valamint a technikai azonosító felelősét.

7.5. Felhasználói azonosító és jogosultságok használata

Minden felhasználó felelős a feladatköre ellátásához kapott informatikai hozzáférésekhez tartozó azonosító és hitelesítő adatok védelméért, biztonságos használatáért. Egyes rendszerek az azonosításhoz szükséges felhasználói név és a hitelesítéshez szükséges jelszó mellett megkövetelhetik további azonosító, illetve hitelesítő eszközök – pl. tokenek, chip kártyák, tanúsítványok – használatát. Ezek szintén fokozott körültekintéssel, a kapcsolódó szabályok megismerése és betartása mellett kezelendők.

A hitelesítő adatok (például a felhasználói jelszó) védelme a felhasználó kötelessége és felelőssége. A jelszókezeléssel kapcsolatos mulasztásért a felhasználó felel.

Az ASP rendszerbe történő belépéshez szükséges a Keretrendszerben rögzített felhasználóhoz rendelni az elektronikus személyi igazolványát. Ennek hiányában ideiglenesen a Hivatal részére kiosztott tanúsítványt használva engedélyezett bejelentkezni az ASP rendszerekbe.

A több felhasználó által közösen használt azonosítókhoz tartozó jelszót haladéktalanul meg kell változtatni, ha a jelszót ismerők bármelyikének a jogosultsága megszűnik (pl. áthelyezés, munkaviszony megszűnése).

Technikai azonosítót a felhasználók a napi feladataik elvégzéséhez nem használhatnak. A technikai azonosítók jelszavát haladéktalanul meg kell változtatni, ha az azt ismerő munkatársak valamelyikének a Hivatallal való kapcsolata (pl. munkaviszony, szerződés) megszűnik.

7.5.1. Jelszókezelés szabályai

A felhasználó számára annak érdekében, hogy csökkentse a részére átadott felhasználói azonosítókkal esetlegesen elkövethető visszaéléseket, az alábbi irányelvek követése javasolt:

a. Jelszókezeléssel kapcsolatos irányelvek:
   - A jelszavakat tilos jogosulatlanok számára hozzáférhető helyen leírva tárolni, a leírással szemben az emlékezetben tartás preferált!
   - A jelszót csak és kizárólag az alkalmazás igénybevételét lehetővé tevő bejelentkezési ablakba szabad begépelni! Ha a felhasználó a bejelentkezési ablaknál bármilyen rendellenességet tapasztal, ne gépelje be a jelszavát, azonnal értesítse az informatikai rendszer üzemeltetésével megbízott kollégát.
   - A személyhez rendelt jelszavakat másokkal megosztani TILOS! A felhasználó, a részére kiosztott jogosultsággal elkövetett visszaélésekért, biztonságsértésért - akár az a személyhez rendelt felhasználói név/jelszó pár átadásának vagy eltulajdonításának következménye - személyesen, a tényleges károkozóval egyetemlegesen felel!

- A felhasználó a részére kiadott felhasználói azonosítókat és jelszavakat csak azokon az eszközökön használja, melyek hozzáféréséhez kapta. Nem célszerű azt más, esetleg szabadon hozzáférhető, rendszereken használni.

- A jelszavakat javasolt rendszeresen, pl.: 90 naponta megváltoztatni, ez alól kivétel az az eset, amikor a jelszó illetéktelenek birtokába jut vagy ennek veszélye áll fenn, mert ekkor azonnali jelszóváltoztatás kötelező!

- Jelszó kompromittálódása esetén azt azonnal meg kell változtatni, valamint a biztonsági események jelentésénél leírtak szerint jelezni kell az informatikai rendszer üzemeltetésével megbízott felé és értesíteni kell a felhasználó közvetlen felettesét.

b. A biztonságos jelszó nem azt jelenti, hogy a felhasználó kitalál egy számára kedves szót, amit jelszónak tekint, hanem olyan szó vagy betűsorozat alkalmazása, mely mások által nehezen kitalálható és visszafejthető, a felhasználó személyéhez a lehető legkisebb mértékben köthető. Ellenkező esetben a támadó – aki ismeretekkel rendelkezik a felhasználóról és a környezetéről – képes szótárat készíteni a lehetséges szavakból és visszafejteni a felhasználói jelszavakat.

   Annak érdekében, hogy e visszaélések ne történjenek meg, az alábbi jelszóválasztási vezérelveket is javasolt figyelembe venni:

   - a jelszó hossza legalább 8 karakter hosszú legyen, vagy ha ezt az adott informatikai rendszer nem támogatja, akkor a rendszer által használható maximális hosszúság.
   - A jelszó SOHASE legyen személyes, személyhez köthető szó; mint pl.: a kedvenc autó típusa, az űzött sportág neve, születési idő, telefonszám, a kedvenc háziállat, gyerekek vagy házastárs neve, kedvenc étel vagy könyv címe.
   - SOHA sem lehet a jelszó azonos a felhasználói névvel vagy a felhasználó valódi nevével, illetve a felhasználói név nem lehet része a jelszónak.
   - A jelszavakat TILOS szótárakból választani, mert a legtöbb jelszótörő program szótárat használ a próbálgatáskor.
   - A jelszavak megválasztásakor vegyesen használjon a felhasználó betűket (kis- és nagybetű vegyesen: a-z, A-Z), számokat, egyéb írásjeleket (*@&(_+...) és üres karaktert.
   - A jelszóban nem fordulhat elő ugyanaz a karakter egymás mellett álló pozícióban kettőnél többször.
   - A billentyűzeten egymás mellett álló karakterek sorozata sem elfogadható.
   - A jelszó megválasztásakor törekedni kell arra, hogy könnyen gépelhető és megjegyezhető legyen (pl. „Boci boci tarka, Se füle se farka” alapján a jelszó képzési szabálya lehet: minden kezdőbetű az adott szó hosszával kiegészítve, „B4b4t5,S2f4s2f5”).

c. Tekintettel arra, hogy a felhasználó jelszava a biztonság szempontjából kiemelten védendő, ezért egyes informatikai rendszerek adott számú sikertelen bejelentkezési kísérletet esetén automatikusan kitiltják az adott felhasználót, így védve a felhasználót attól, hogy a támadó jogosulatlanul a felhasználó nevében kárt okozzon. Ilyen esetben az adott rendszer üzemeltetési feladataiért felelős munkatársat kell keresni új jelszó igénylése miatt.

7.5.2. Kiemelt felhasználói és technikai azonosítók jelszavai

A rendszerek kiemelt felhasználói azonosítói és a technikai azonosítók esetén a felhasználói jelszókezelés szabályain túl a jelszó megőrzését, hozzáférhetőségét a Hivatal rendszergazdájának biztosítania kell olyan módon, hogy a jelszavakhoz illetéktelenek ne férjenek hozzá. A megőrzés, illetve hozzáférhetővé tétel módját a jegyző határozza meg, és bármikor ellenőrizheti (pl. a jelszó páncélszekrényben zárt borítékban vagy védett fájlban való tárolásával).

A kiemelt felhasználói és technikai jelszavak esetén a jelszó hosszának minimálisan 12 karakteresnek kell lennie.

7.5.3. Külső harmadik fél hozzáférés védelme

A külső felek hozzáférésének biztonságát szerződés szintjén is meg kell határozni és ennek kapcsán ki kell térni az adminisztrációhoz és az adatok bizalmas kezeléséhez kapcsolódó követelményekre is. Kiszervezés esetén a felek között megkötött szerződésben ki kell térni a kockázatok és az információs rendszerekhez és hálózatokhoz kapcsolódó biztonsági ellenőrzések és eljárások kérdésére.

7.5.4. Tanúsítványok használata

A Hivatal elektronikus információs rendszerei külső felhasználók hitelesítéséhez csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat fogadja el.

A szakrendszerekhez használt külső tanúsítványokat a jegyző feladata igényelni a Hivatal rendszergazdájának támogatása mellett. A Hivatal rendszergazdájának feladata a Hivatal által használt tanúsítványokról naprakész nyilvántartást vezetni, mely nyilvántartásnak tartalmaznia kell a tanúsítványhoz kapcsolódó rendszert, a tanúsítvány lejáratát. A rendszergazda feladata ezen tanúsítványok lejáratát megelőző egy hónappal kezdeményezni a jegyzőnél az új tanúsítvány beszerzését.

A hitelesítés szolgáltatótól beszerzett tanúsítványok privát kulcsáról a Hivatal rendszergazdájának másolatot kell készítenie és a jegyző által meghatározott helyen kell tárolni.

7.6. Jogosultságok nyilvántartása

A Hivatal centralizált jogosultságkezelési és –nyilvántartási rendszert működtet. Ennek keretében minden használt elektronikus információs rendszerről, beleértve –

- a belső hálózatában üzemelő, belső üzemeltetésű,
- a belső hálózatában üzemelő, harmadik fél által üzemeltetett, valamint
- a belső hálózatán kívül harmadik fél által üzemeltetett

rendszert – egységes jogosultság nyilvántartást kell vezetni. A jogosultság nyilvántartás naprakészen tartása és annak biztonságos tárolása a jegyző felelőssége.

A nyilvántartásnak tartalmaznia kell az adott rendszerben aktuálisan létező felhasználói azonosítókat, az azonosítókat birtokló, használó munkatárs(ak) nevét, valamint a rendszerben beállított jogosultságainak felsorolását, a kiemelt és technikai azonosítók mellett.

Az aktuális jogosultság nyilvántartás elkészítése, karbantartása a Hivatal rendszergazdájának a feladata.

7.7. A jogosultságok felülvizsgálatának rendje

A jegyző bármikor jogosult a fenti követelmények teljesülését ellenőrizni, vagy ilyen jellegű ellenőrzést elrendelni, de legalább éves rendszerességgel szükséges végrehajtani a jogosultságok felülvizsgálatát.

8. Nyilvánosan elérhető tartalom

A Hivatal nyilvánosan elérhető rendszerként definiálja például a Hivatal publikus weboldalát.

A publikus felületeken való közzétételt és a médiával való kommunikációt a jegyző szabályozza, a Hivatal külső kommunikációjáért a jegyző a felelős.

A Hivatali honlap tartalommenedzsmentjét az erre kijelölt hivatali belső személyek és külső szolgáltató végzi.

A publikált információk csak nyilvános adatokat és információkat tartalmazhatnak. A jegyző havonta áttekinti a honlapot és nem nyilvános adat kikerülése esetén eltávolítatja azt.

9. Információs rendszerek beszerzése, fejlesztése és karbantartása

Hivatal rendszereinek fejlesztése során a jegyző felelőssége, hogy az informatikai rendszer, szolgáltatás beszerzése, fejlesztése esetén a kapcsolódó biztonsági követelmények már a tervezés során felmérésre és meghatározásra kerüljenek és azok teljesülését a fejlesztés, beszerzés során a Hivatal ellenőrizze. Az éles használatba vétel feltétele legyen a meghatározott biztonsági követelmények teljesítése. A biztonsági követelmények meghatározásakor alapvetően jelen szabályzat előírásai, illetve a kapcsolódó jogszabályi követelmények tekintendők irányadónak. Tipikusan ilyen, a biztonság szempontjából kiemelt jelentőséggel bíró területek lehetnek a következők:

- felhasználók azonosítása, hitelesítése;
- jogosultságok kezelése, szerepkörök kialakítása;
- naplózás;
- biztonsági beállítások és biztonsági rendszerrel kapcsolatos adatok védelme;
- kommunikáció védelme;
- kezelt adatok bizalmasságának, sértetlenségének védelme;
- rendszerek, szolgáltatások biztonsági megerősítése;
- biztonsági javítások telepítése;
- tesztelés;
- az adatok mentési gyakoriságára és megőrzési idejére, valamint a rendszer újraindítási idejére vonatkozó üzleti követelményeknek megfelelően legyen biztosítva.

A rendszergazdának az új számítástechnikai eszköz beszerzése során:

- biztosítania kell, hogy az informatikai biztonság szempontjából a tervezett biztonsági követelménynek megfelelő kapacitású eszköz kerüljön beszerzésre;
- gondoskodnia kell a megfelelő felhasználói terméktámogatásról és karbantartás biztosításáról;
- gondoskodnia kell a rendelkezésre állás elvesztéséből eredő kockázatok csökkentéséről;
- gondoskodnia kell arról, hogy a Hivatal minden munkaállomásán csak olyan operációs rendszerek legyenek használatban, amelyek a process isolation funkciót támogatják.

9.1. Fejlesztések biztonsági követelményeinek ellenőrzése

Informatikai fejlesztések esetén – legyen az új rendszer fejlesztése vagy meglévő rendszer továbbfejlesztése – a tervezési fázisban megfogalmazott nem funkcionális követelmények részeként rögzített biztonsági követelményeket a fejlesztés elfogadásának előfeltételként tételesen tesztelni szükséges, és csak sikeres teszteket követően veheti át a Hivatal a fejlesztés eredménytermékét. Indokolt esetben a jegyző elrendelhet technológiai vizsgálatokat a fejlesztett termékek biztonsági hiányosságainak feltérképezésére.

10. Az információbiztonsági incidensek kezelése

10.1. Jelentési kötelezettség

Hivatal minden felhasználójának kötelessége megakadályozni a tárolt adatvagyon, a személyi tulajdon ellen irányuló magatartást, visszaélést, károkozást, hűtlen kezelést, a belső utasítások megsértését. Minden felhasználó kötelessége az általa feltárt biztonsági eseményt vagy tudomására jutott sebezhetőséget, biztonsági fogyatékosságokat vagy a fentiekben felsorolt cselekményeket jelentenie.

A szerződéses partnernek jeleznie kell az általa szállított vagy karbantartott termékkel vagy általa üzemeltetett szolgáltatással kapcsolatban felmerülő biztonsági problémákat Hivatal felé.

A külső fejlesztő vagy más szerződéses partner köteles az általa támogatott szoftver termékben feltárt, biztonsági kockázatot (sebezhetőséget) jelentő hibákat haladéktalanul Hivatal tudomására hozni.

A biztonsági eseményt haladéktalanul jelenteni kell a jegyzőnek és az érintett informatikai rendszer üzemeltetési feladataival megbízottnak.

10.2. Bejelentések kezelése

A jegyző felelőssége – szükség esetén további közreműködők bevonásával – a biztonsági esemény kivizsgálása, értékelése és az esetlegesen szükségesnek ítélt, azonnali és eredményes intézkedések meghozatala, azok bevezetésének felügyelte. Az érintett informatikai rendszer(ek) üzemeltetési feladataival megbízott(ak)

köteles(ek) a jegyzővel a biztonsági esemény kezelésében együttműködni, a jegyző utasításainak megfelelően az adott rendszerben szükséges módosításokról gondoskodni.

A jegyző jogosult szükség esetén – azonnali intézkedés formájában – az elérhető informatikai szolgáltatások körét korlátozni.

A feltárt vagy bekövetkezett biztonsági események kezelésére azonnali és eredményes, előre meghatározott biztonsági intézkedéseket kell bevezetni, amelyekkel csökkenthetőek a jövőbeli előfordulásukból keletkező károk.

10.3. Eseménykezelő központok jelzése

Az eseménykezelő központok által kiadott riasztásokat a rendszergazda kezeli. A riasztásokat minden esetben ki kell vizsgálni, tesztelés vagy ellenőrzés formájában, meghatározva, hogy azok fenn állnak-e a Hivatal informatikai rendszerében. A tesztelés alapján megállapított követelményeket – beleértve a tesztelés típusával és gyakoriságával kapcsolatos követelményeket is – dokumentálnia kell az informatikai rendszergazdáknak.

Amennyiben a riasztás további intézkedéseket igényel, úgy az elektronikus információs rendszer biztonságáért felelős személynek védelmi intézkedéseket kell kidolgoznia és bevezetnie.

10.4. Felhasználók tájékoztatása

Ha az azonnali javító intézkedés bevezetése a felhasználók által elérhető szolgáltatások korlátozásával jár, akkor minden érintett felhasználót tájékoztatni kell. A korlátozások visszavonásáról szintén értesíteni kell az érintett felhasználókat.

10.5. Tanulás a biztonsági eseményekből

A biztonsági esemény elhárítását követően meg kell vizsgálni, hogy van-e lehetőség, illetve a kapcsolódó kockázatok figyelembe vételével indokolt-e olyan jellegű intézkedések bevezetése, amelyek alkalmasak a bekövetkezett, vagy ahhoz hasonló biztonsági események jövőbeli előfordulását meggátolni, vagy azok bekövetkezés valószínűségét, esetleges káros hatásait a szükséges mértékben csökkenteni.

11. A működés folytonosságának irányítása

A Hivatal működésének folytonosságával kapcsolatos feladatok tervezése, irányítása, koordinálása, a szükséges erőforrások rendelkezésre állásának biztosítása a jegyző feladata. A feladat keretében a jegyzőnek alapvetően biztosítania kell, hogy informatikai szolgáltatás kiesésével járó rendkívüli esemény esetén:

- Az informatikai szolgáltatás elfogadható időn belül és elfogadható adatveszteség mellett újraindítható legyen.

- Az informatikai szolgáltatás kiesésének idejére azon kritikus fontosságú folyamatoknál, ahol ez indokolt a kieső informatikai szolgáltatás használata nélkül működtethető alternatív folyamat biztosítsa a szükséges minimális szinten a működést.
- A Hivatal működését érintő rendkívüli esemény esetén a Hivatal a szükséges tájékoztatási feladatokat szervezett módon végrehajtsa.
- Az informatikai szolgáltatás újraindítását követően az ügyviteli folyamatok a normál működési szintnek megfelelően, a normál ügyviteli rend szerint folytathatóak legyenek.

A fentieket figyelembe véve a vonatkozó kockázatokat szem előtt tartva a Hivatal informatikai rendszereit úgy kell kialakítani, illetve tartalékolni, valamint a külső szolgáltató által nyújtott informatikai szolgáltatásokra olyan rendelkezésre állási követelményeket javasolt kikötni, hogy azok költséghatékonyan támogassák a Hivatal feladatait, illetve az azok alapján az érintett ügyviteli folyamatokra levezethető rendelkezésre állási követelményeket.

A fenti követelmények érdekében számba kell venni a Hivatal működését támogató informatikai szolgáltatásokat, a szolgáltatások rendelkezésre állását veszélyeztető lehetséges rendkívüli eseményeket és meg kell határozni, hogy milyen preventív, detektív, illetve korrektív intézkedések bevezetésével csökkenthetőek az informatikai szolgáltatások kieséséből származó kockázatok elfogadható szintre.

A meghatározott – informatikai szolgáltatás kiesésével járó – rendkívüli esemény bekövetkezése esetén végrehajtandó alternatív folyamat szükségességének meghatározásakor az érintett ügyviteli folyamatok rendelkezésre állási követelményei mellett figyelembe kell venni a Hivatal által használt informatikai rendszerek rendelkezésre állási képességeit (hogyan és mennyi idő alatt lehet a rendszert újraindítani egy esetleges meghibásodást követően és az újraindítás során mikori adatokat lehet a rendszerbe visszatölteni), illetve a külső féltől igénybe vett informatikai szolgáltatások esetén az azokra vállalt rendelkezésre állási paramétereket.

A fenti szempontok figyelembe vételével a jegyző felelőssége meghatározni a Hivatal által alkalmazott kockázatkezelő intézkedéseket, valamint a bevezetett intézkedések működésének biztosítása és felügyelete (pl. az esetlegesen szükségesnek ítélt folytonossági tervek oktatása, tesztelése, rendszeres felülvizsgálata, az informatikai rendszerekre meghatározott rendelkezésre állási képességeket biztosító intézkedések működtetése).

12. Megfelelőség

12.1. Felülvizsgálat, ellenőrzés

- A Szabályzat előírásainak betartását, illetve az egyes információ, rendszer vagy alkalmazás érdekében bevezetett intézkedések megfelelőségét és

hatékonyságát a jegyző jogosult belső, vagy külső erőforrás bevonásával ellenőrizni, illetve ellenőriztetni. Az ellenőrzések során a jegyző felelőssége az ellenőrzés szakszerű lefolytatásához szükséges kompetencia biztosítása, illetve az ellenőrzés függetlensége érdekében az összeférhetetlenségek kizárása. Az ellenőrzési tevékenységeket az informatikai kockázatelemzéssel összhangban, az informatikai rendszer működési környezetében bekövetkezett jelentős változás esetén, de legalább háromévente végre kell hajtani. Az ellenőrzési tevékenységet ellenőrzési terv alapján szükséges végrehajtani, amely terv elkészítéséért az elektronikus információs rendszer biztonságáért felelős személy fele. Az ellenőrzési tervnek ki kell terjednie minden szabályozási folyamat és kontroll működésének ellenőrzésére. Az ellenőrzés történhet manuális módon, az ellenőrzést végző felelős által végrehajtott rendszerbeállítások manuális ellenőrzésével, és/vagy

- automatizáltan, célszoftver alkalmazásával.

Az ellenőrzést végző által alkalmazott ellenőrzési módszert az elektronikus információs rendszer biztonságáért felelős személynek a feladata jóváhagyni.

A felülvizsgálatok során tapasztalt hiányosságok, nem megfelelőségek értékelése során, a vonatkozó kockázatok, valamint a Hivatal költség- és haszonelemzés módszertanának figyelembe vételével kell mérlegelni további intézkedések, kiegészítő kontrollok szükségességét. Az egyedi kontroll eljárások tesztelésének gyakoriságát és mélységét ahhoz kell igazítani, hogy milyen biztonsággal jár a kontrollok nem megfelelő működése. A nem elfogadhatónak minősített kockázatok kezelésére a jegyző védelmi intézkedési javaslatok kidolgozását rendelheti el. A jegyző felelőssége a szükségesnek ítélt kockázatcsökkentő intézkedések meghatározása, a bevezetésükhöz szükséges erőforrások biztosítása, valamint az intézkedések bevezetésének felügyelete.

Abban az esetben, ha az ellenőrzés súlyos rendellenességet vagy szabályszegést tár fel a jegyző jogköre a fegyelmi eljárás szükségességének mérlegelése, illetve szükség esetén a fegyelmi eljárás lefolytatása.

12.2. Vezetőségi átvilágítás

A jegyző feladata az éves feljegyzés formájában az informatikai biztonsággal kapcsolatos tevékenység értékelése.

12.3. Hivatal intézkedési terveinek nyomon követése, felülvizsgálata

12.3.1. Cselekvési terv felülvizsgálata

A jegyző felelőssége biztosítani az elektronikus információs rendszerek biztonságáért felelős személy szakmai támogatása mellett a cselekvési terv előrehaladásának folyamatos nyomon követését és a fontosabb mérföldkövek mentén a feladatok előre haladásának értékelését. A jegyző elrendelheti, illetve az elektronikus információs rendszerek biztonságáért felelős személy kezdeményezheti a készre jelentett feladatok utóvizsgálatát, amit utólag be kell építeni az éves ellenőrzési tervbe.

Ha a cselekvési terv feladatainak előrehaladásában a cselekvési terv végrehajtását veszélyeztető probléma jelentkezik, akkor a jegyző feladata rendelkezni a probléma kezelésének módjáról, szükség esetén a cselekvési terv átütemezéséről.

12.3.2. Informatikai biztonsági stratégia

A Hivatal Informatikai Biztonsági stratégia dokumentumát éves rendszerességgel célszerű felülvizsgálni, mely felülvizsgálat keretében értékelni kell a stratégiai célok megvalósulását, figyelembe véve a Hivatal költség- és haszonelemzési módszertanát is, az esetlegesen felmerülő új stratégiai célokkal történő kiegészítését, megvalósult stratégiai célok kivezetését a dokumentumból. A felülvizsgálat végrehajtásáért a jegyző felel mely felülvizsgálatba szükséges bevonnia az elektronikus információs rendszer biztonságáért felelős személyt és a rendszergazdát. A felülvizsgálat alapján módosított dokumentumot a jegyző köteles jóváhagyni.

13. Mellékletek

13.1. Biztonsági osztályba, biztonsági szintbe sorolás

Az informatikai biztonsági szabályzat tartalmazza a Hivatal által elvárt biztonsági szintet, valamint a Hivatal egyes elektronikus információs rendszereinek elvárt biztonsági osztályát.

13.2. Elektronikus információs rendszerek biztonsági osztályba sorolása

A 41-es BM rendelet 1. § szerint az elektronikus információs rendszerek biztonsági osztályba sorolását az 1. mellékletben foglaltak szerint kockázatelemzés alapján kell elvégezni (1.2.).

A Hivatal elektronikus információs rendszereinek irányadó biztonsági osztályát a fentiek figyelembe vételével a jegyző az alábbiak szerint határozta meg:

Ssz.	Elektronikus információs rendszer megnevezése	Kockázati szint			Irányadó biztonsági osztály
		B	S	R	
1.	Központi webes rendszerek	2	2	2	2
2.	Terminál (utalás)	2	2	2	2
3.	ASZA	2	2	2	2
4.	Irodai környezet	2	2	2	2
5.	Jogtár	2	2	2	2
6.	ASP rendszerek	2	2	2	2

13.3. Szervezet biztonsági szintbe sorolása

A 41/2015. (VII.15.) BM rendelet 2. melléklete alapján a Hivatal informatikai területet a **4**-es biztonsági szintbe sorolom, mivel elektronikus információs rendszert üzemeltet.

A 41/2015. (VII.15). BM rendelet 2. melléklete alapján a Hivatal szakterületi egységeit, az informatikai terület kivételével, **3**-as biztonsági szintbe sorolom, mivel kritikus adatot kezel és feladatai ellátásához szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti.

A fentiek alapján a Hivatal egészére vonatkozó biztonsági szintként a **4**-es biztonsági szintet jelölöm meg, tekintettel arra, hogy a Hivatal egészére a legmagasabb biztonsági szint az irányadó.