Őri Közös Önkormányzati Hivatal

Informatikai Biztonsági Szabályzat

Érvénybe lépett:2015.10.19
Iktatószáma:
Kihirdetésének időpontja:
Módosítások Időpontjai:2017. október

Tartalom

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. Törvény (a továbbiakban: Infotv.) részletesen szabályozza a személyes adatok védelmével, és a közérdekű adatok nyilvánosságával kapcsolatos legfontosabb teendőket, illetőleg az alapvető jogok érvényesülését.

Magyarország Alaptörvényének VI. cikk 82) bekezdése értelmében „Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez”. Ezen alapvető jogok védelme és tiszteletben tartása az állam és az önkormányzatok elsőrendű kötelessége.

Őri Közös Önkormányzati Hivatalának Informatikai Biztonsági Szabályzatát az Infotv., a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény (a továbbiakban: Nytv.), az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, a 257/2016. (VIII.31) Korm.rendelet, a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII.15) BM rendelet illetve a kutatás és a közvetlen üzletszerzés célját szolgáló név és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvényben foglaltak alapján, továbbá a Nytv. 30. § (1) bekezdésben kapott felhatalmazás alapján, az államháztartásról szóló 2011. évi CXCV. törvény (a továbbiakban Áht.), a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény (a továbbiakban Ötv.) alapján Őri Közös Önkormányzati Hivatalának (továbbiakban: Hivatal) informatikai biztonsággal és adatvédelemmel összefüggő feladatait és eljárási rendjét figyelembe véve az Önkormányzati ASP rendszerről szóló 257/2016. (VIII.31.) Korm. rendeletet az alábbiak szerint szabályozom.

1. Bevezetés

1.1. Az IBSZ tárgya

Ez a dokumentum, a Hivatal által használt, üzemeltetett vagy felügyelt informatikai rendszerekre vonatkozóan tartalmazza a legfontosabb információtechnológiai, biztonsági feladatokat, továbbá meghatározza azokat az intézkedéseket, tevékenységeket, amelyekre a biztonságos működés érdekében szükség van.

1.2 Az IBSZ célja

Az IBSZ alapvető célja, hogy az informatikai rendszer működtetése, üzemeltetése során biztosítsa az adatvédelem elveinek, az információbiztonság követelményeinek érvényesülését. További cél, hogy a szabályzat egységes szerkezetbe foglalja a használatban lévő informatikai rendszerekkel és annak felhasználóival szemben támasztott informatikai biztonsági követelményeket.

A szabályzat célja ezen felül, hogy a Hivatal az informatikai szolgáltatás területén biztosítsa:

- az informatikára vonatkozó törvényi előírások érvényesítését,
- a folyamatos informatikai üzembiztonság fenntartását,
- az informatikai vagyon védelmét és megőrzését,
- az informatikai hálózat integritásának védelmét.

1.3 Információbiztonsági politika

Cél, hogy a Hivatal az ügyfelek adatait megvédje, a jogtalan adatfelhasználást és az adatvesztést megakadályozza. Az informatikai biztonság úgy legyen megszervezve, hogy a hatékony, külső és belső szabályok az ügyintézési tevékenységet támogassák.

Az információbiztonsági politikából kell származtatni minden további, részletesebb informatikai biztonsági tervezést és ezek megvalósítását.

1.4 Információbiztonsági stratégia

Az információbiztonsági stratégia kapcsot jelent az informatikai stratégia és a biztonsági stratégia között. Összehangolja az elsősorban informatikai-technológiai célokat a szervezet (átfogó kockázat alapú) biztonsági céljaival, és definiálja a közös működési területeket.

Az információbiztonsági stratégia célja, hogy a szervezet szakmai működési igényeinek jövőbeni változásaival összhangban meghatározza az információbiztonság fejlesztésének tervét.

A stratégia alapelvei: A Hivatal egységes és közös elvek mentén alakítja ki az információbiztonság szabályozását. A munkavégzés számára biztosítja az adatok pontos, megbízható tárolását, nyilvántartások vezetését és ezek hiteles, bizalmas és sértetlen továbbítását. A stratégia kiterjed az informatikai, az infrastrukturális, a fizikai és a humán faktorokra. Az egységes szabályozás megvalósítását követően mérésekre alapozva folyamatosan fejlesztésre kerül az információbiztonsági szabályozás és eljárás.

2. A szabályzat hatálya

2.1 Tárgyi hatály

Tárgyi hatálya kiterjed a Hivatal tulajdonában, kezelésében lévő valamennyi informatikai rendszerre és azok elemeire, az ott használt alkalmazásokra és adatbázisokra, valamint az általuk keletkeztetett, feldolgozott, tárolt, továbbított valamennyi adatra és információra (függetlenül azok megjelenési formájától). **Jelen szabályzat hatálya kiterjed az önkormányzatnál kezelt, keletkezett információkra, az informatikai rendszerben üzemeltetett valamennyi hardver és szoftver elemekre, amely felhasználja, feldolgozza, felügyeli, ellenőrzi, tárolja, továbbítja a keletkező illetve felhasznált adatokat. Továbbá kiterjed a rendszerelemek dokumentációira.**

2.2 Szervezeti hatály

Szervezeti hatálya kiterjed a Hivatal valamennyi szervezeti egységére és a Nemzetiségi Önkormányzatokra.

2.3 Személyi hatály

Személyi hatálya kiterjed a Hivatalban foglalkoztatott valamennyi közszolgálati tisztviselőre, ügyintézőire, a hivatal valamennyi munkatársára, közalkalmazottra és bármely formában létesített munka és egyéb jogviszony keretében foglalkoztatott munkavállalóra valamint azokra a személyekre, akik részt vesznek a keletkező, tárolt illetve továbbított adatok kezelésében (a továbbiakban: felhasználó).

2.4 Területi hatály

Területi hatálya kiterjed a Hivatal épületére, illetve telephelyeire is.

1. **Nyírparasznya Község Önkormányzata**
   (4822 Nyírparasznya, Szabadság út 23)
2. **Őr Község Önkormányzata**
   (4336 Őr, Kossuth út 2)

2.5 Időbeli hatály

Érvényes kiadásának napjától, visszavonásig.

2.6 Az IBSZ további hatálya

Idegen vagy vegyes tulajdonú, illetve kezelésű eszközök, rendszerek használata során figyelembe kell venni a társszervezet ide vonatkozó rendelkezéseit és előírásait, illetve a megkötött és az érvényes megállapodásokat.

A dokumentum azokat a szabályokat tartalmazza, amelyek betartását a Hivatal vezetője kötelező jelleggel elrendeli a dokumentum elfogadásával, és amelyeket alkalmazni kell a fenti informatikai rendszerek fejlesztése, telepítése és üzemeltetése során, a kívánt biztonsági szint elérése és fenntartása érdekében.

3. Általános hatásköri és illetékességi szabályok

3.1 A szabályzat kidolgoztatása, ellenőrzése és karbantartatása

Az IBSZ kidolgoztatása, ellenőrzése, majd karbantartatása a Hivatal vezetőjének feladata és hatásköre.

3.2 A szabályzat hatályba léptetése, a végrehajtás ellenőrzése

Az IBSZ hatályba léptetése kihirdetésével történik meg, végrehajtásának ellenőrzése a Hivatal vezetőjének feladata.

3.3 A szabályzat betartása és betartatása

A szabályzat alkalmazásáért és betartásáért a hivatali szervezet minden egysége, minden felhasználója felelős.

3.4 A szabályzat ellenőrzése

A Hivatal vezetője, az elkövetkező, minden év január hó 31. napjáig, éves ellenőrzési tervet készít a szabályzatban foglaltak ellenőrzésére, és kijelöli az informatikai biztonsági megbízottat.

4. Az IBSZ végrehajtása

4.1 A Végrehajtás szabályai

Az IBSZ betartása és betartatása a Hivatal minden felhasználójának és szervezeti egység vezetőjének munkaköri kötelessége.

Az IBSZ személyi hatálya alá tartozó valamennyi személynek ismernie kell azokat a követelményeket és feladatokat, amelyeket az IBSZ számára meghatároz.

A szervezeti egység vezetője gondoskodik róla, hogy a Hivatal alkalmazottai a megfelelő ismereteket megkapják.

A külső felek a hivatali kapcsolattartón keresztül ismerhetik meg a szabályokat.

Az IBSZ személyi hatálya alá tartozó valamennyi személy köteles a Hivatal vezetőjét, illetve az informatikai biztonsági megbízottat minden olyan tényről, eseményről értesíteni, amely az IBSZ rendelkezéseinek végrehajtását akadályozza, illetve ellentétes az IBSZ rendelkezéseivel.

4.2 A végrehajtás eszközei

Az IBSZ végrehajtásának eszközei:

- az egyes informatikai rendszerek oly módon történő kialakítása, beállítása, hogy az informatikai rendszer kikényszerítse az IBSZ rendelkezéseinek betartását,
- ismeretek oktatása, megismertetése és az ismeretek számonkérése,
- az IBSZ kötelező betartatása,
- az IBSZ betartását célzó rendszeres és időszaki ellenőrzések átfogó vagy cél jelleggel (tételes vagy szúrópróba szerű ellenőrzési módszerekkel),
- a hálózat rendszeres monitorozása a naplók és nyilvántartások pontos és napra kész vezetése, azok rendszeres ellenőrzése,

- a szervezeti egységvezető tájékoztatása a szervezeti egységet érintő ellenőrzési tapasztalatokról, fegyelmi vagy biztonsági eseményekről, az elkészített jegyzőkönyvek, jelentések, feljegyzések másolatának megküldése révén,
- a szabályzat rendszeres megsértőivel szembeni fegyelmi szankciók alkalmazása.

5. Az IBSZ felülvizsgálata

5.1 Időszakos felülvizsgálatok

Jelen szabályzatot a Hivatal vezetője köteles és jogosult időközönként, de legalább évente dokumentáltan felülvizsgálni, és a szükség esetén módosítani.

5.2 Változás miatti felülvizsgálat

Jelen szabályzatot a Hivatal vezetője köteles felülvizsgálni és szükség esetén módosítani: minden olyan szervezeti változás esetén, amely a benne hivatkozott szervezeti egységek bármelyikének megszűnésével vagy jelentős átalakulásával jár, súlyos informatikai biztonsági események („incidensek”) után, az esemény tanulságait figyelembe véve, minden olyan jogszabályváltozás esetén, amely a benne foglaltak érvényességét módosíthatja.

A Hivatal SZMSZ-nek változása esetén jelen szabályzatot kötelező jelleggel felül kell vizsgálni és a szükséges módosításokat át kell vezetni jelen dokumentumban.

5.3 Megfelelőségi vizsgálat

Évente egyszer a Hivatal vezetője köteles megfelelőségi vizsgálatot végezni, és ha szükséges, az IBSZ-t módosítani. A megfelelőségi vizsgálat során vizsgálja: az IBSZ betartásával kapcsolatos ellenőrzések eredményét, a felmerülő problémák és hibák jellegét és tanulságait, az időközben felmerülő informatikai és adatvédelmi eseményeket és az ezekkel összefüggő biztonsági vonzatokat.

5.4 Az IBSZ kapcsolódása

Az IBSZ megfelel a vonatkozó Magyar Informatikai Biztonsági Ajánlásoknak - Közigazgatási Informatikai Bizottság ajánlásai -, és elősegíti a Hivatal mindenkor hatályos Szervezeti és Működési Szabályzatában és kapcsolódó szabályzataiban, az adatvédelemmel és informatikai biztonsággal kapcsolatban megállapított feladatok végrehajtását.

6. Az információbiztonság szervezeti struktúrája, szerepkörök

A Hivatal egyes informatikai rendszereinek működtetésével kapcsolatos feladatokat külső szolgáltató látja el. Az információbiztonság megfelelőségéért, az IBSZ-ben foglaltak megtartásáért és annak megvalósításával kapcsolatos feladatok végrehajtásáért a Hivatal vezetője felelős.

6.1 A Hivatal vezetője a jegyző

az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L törvény alapján:

11. § (1) A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről a következők szerint:

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

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

c) az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,

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

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

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

i) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,

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

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

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

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

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

(2) Az (1) bekezdésben meghatározott feladatokért a szervezet vezetője az (1) bekezdés *k)* és *l)* pontjában meghatározott esetben is felelős, kivéve azokat az esetköröket, amikor jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót kell a szervezetnek igénybe venni.

(3)A jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve központi adatkezelő és adatfeldolgozó szolgáltató igénybevétele esetén az (1) és (2) bekezdésben meghatározott feltételek teljesítését a jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve a központi adatkezelő és adatfeldolgozó szolgáltató úgy biztosítja, hogy közreműködik a szervezet és az elektronikus információs rendszer biztonságáért felelős személy feladatai ellátásában a jogkörébe tartozó tevékenységek tekintetében. A két szervezet közötti feladatmegosztást kétoldalú szolgáltatási szerződések biztosítják, amelyek a központi szolgáltató felett felügyeletet gyakorló miniszter vagy megbízottja ellenjegyzésével lépnek hatályba. Az (1) bekezdés *a)* és *b)* pontjában meghatározott feladatok keretében a szervezeti szintű informatikai biztonsági szabályok kidolgozása abban az esetben is a szervezet vezetőjének felelőssége, ha a jogszabály által kijelölt központosított elektronikus és hírközlési szolgáltatót vesz igénybe.

12. § A szervezet vezetője köteles együttműködni a hatósággal. Ennek során:

a) a 11. § (1) bekezdés *c)* pontjában meghatározott, az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt,

b) a szervezet informatikai biztonsági szabályzatát tájékoztatás céljából megküldi,

c) az ellenőrzés lefolytatásához szükséges feltételeket biztosítja a hatóság részére.

6.2 Informatikai biztonsági megbízott, Elektronikus információs rendszer biztonságáért felelős személy

A Hivatalnál a vezető informatikai biztonsággal összefüggő tevékenységét az informatikai biztonsági megbízott támogatja. Részt vesz a biztonsággal kapcsolatos vezetői döntések előkészítésében, kivizsgálja az informatikai rendkívüli eseményeket, elvégzi a rendszeres biztonsági ellenőrzéseket, és hatáskörében intézkedik, vagy javaslatot tesz a hibák kijavítására. Munkája során szorosan együttműködik a biztonság megvalósításában résztvevő informatikai és egyéb szakemberekkel.

- Gondoskodik az ellenőrzés módszereinek és rendszerének kialakításáról és működtetéséről. Jóváhagyásra előkészíti az éves informatikai biztonsági ellenőrzési tervet és az IBSZ javításait.
- Feladata a Hivatal informatikai rendszerének olyan mértékű megismerése, hogy annak elemeit hatékonyan ellenőrizni tudja.
- Összehangolja a biztonságot meghatározó, befolyásoló területek tevékenységét az informatikai biztonság érdekében.
- A Hivatal vezetőjével együttműködve felügyeli a biztonsággal kapcsolatban készítendő tervek és szabályzatok elkészítését.
- Informatikai biztonsági szempontból ellenőrzi az informatikai rendszer szereplőinek tevékenységét.
- Az informatikai rendkívüli eseményeket, az esetleges rossz szándékú hozzáférési kísérletet, illetéktelen adatfelhasználást, visszaélést kivizsgálja, javaslatot tesz a szervezet vezetőjének a további intézkedésekre, a felelősségre vonásra.
- Az SZMSZ rendelkezései és a munkaköri leírások alapján ellenőrzi az informatikai rendszer szereplőinek jogosultsági szintjét és szükség esetén módosításukra javaslatot tesz.
- Ellenőrzi a fejlesztő rendszerek elkülönítésének megfelelőségét az éles rendszertől.
- Felügyeli az informatikai központokat, eszközöket és infrastruktúrát érintő karbantartási terveket.
- Felügyeli a beruházásokat, a fejlesztéseket és az üzemvitelt informatikai biztonsági szempontból, illetve javaslatot tesz rájuk.
- Az új biztonságtechnikai eszközök és szoftverek tesztelésére ajánlást ad.
- Szúrópróba-szerűen ellenőrzi: az egyes felhasználói gépek hardverkonfigurációját, és a telepített szoftvereket összeveti a felhasználónak engedélyezett szoftverek listájával, hogy a rendszerben aktuálisan beállított felhasználói jogosultságok megegyeznek-e a jóváhagyott (a jogosultsági nyilvántartásban is szereplő) jogosultságokkal, hogy a javításra kiszállított eszközökön adat ne kerüljön ki, az adathordozók selejtezését.

- Értékeli a rendszer eseménynaplóit.
- Ellenőrzi a víruskereső programok használatát.
- Ellenőrzi a dokumentációk meglétét és megfelelőségét (teljes körű, aktuális).
- Ellenőrzi, hogy a vonatkozó informatikai biztonsági követelményeket a rendszerek fejlesztési és az alkalmazási dokumentációiban is megjelenítik-e.
- Amennyiben új fenyegetéseket észlel, vagy hatékonyabb biztonsági intézkedések megtételét tartja szükségesnek, kezdeményezi a védelem erősítését.
- Az adott szakterületek vezetőivel egyeztetve meghatározza az egyes feladatkörökhöz tartozóan az informatikai biztonsággal kapcsolatosan elsajátítandó ismeretek körét, és ellenőrzi az elsajátítás tényét.
- Informatikai biztonsági képzést szervezi a munkatársak részére, oktatási dokumentációt elkészíti.
- Javaslatot tesz informatikai biztonságot erősítő továbbképzésre.
- Az IBSZ-t évente felülvizsgálja, és javaslatot tesz a gyakorlati tapasztalatok, előfordult informatikai rendkívüli események, a jogszabályi környezet változásai, a technikai fejlődés, az alkalmazott új informatikai eszközök, új programrendszerek, fejlesztési és védelmi eljárások miatt szükségessé váló módosításokra.
- Munkakapcsolatot tart a szakigazgatási szervek központi szerveinek és a Hivatal szervezeti egységeinek dolgozóival és vezetőivel, az üzemeltetési feladatokat ellátó külső szervezetek munkatársaival.
- Szükség szerint informatikai képzésen vesz részt.

6.3 Szervezeti egység vezető

- gondoskodik arról, hogy a neki beosztott személyek megismerjék, és munkavégzésük során alkalmazzák az Informatikai Biztonsági Szabályzatot,
- ellenőrzi, hogy a neki beosztott személyek betartják-e az Informatikai Biztonsági Szabályzatot,
- informatikai kérdésekben dönt az Informatikai Biztonsági Szabályzatban részére delegált területeken (igénylések, engedélyek).

6.4 Speciális előírások a külső személyek – mint felhasználók – általi hozzáférésekkel kapcsolatban:

A Hivatal igénybe vehet állományába nem tartozó külső személyeket felhasználói jogosultságokkal időszakos vagy folyamatos feladatok végrehajtására. A Hivatal külső személlyel, való szerződéskötésével kapcsolatos eljárását a vonatkozó megállapodások szabályozzák. Egyéb esetben a külső személlyel szerződést kötő szervezeti egység vezetője felelős:

- a külső személy bevonása által okozott informatikai biztonsági kockázatok felméréséért és értékeléséért,
- az IBSZ szerinti követelmények kommunikálásáért és a vonatkozó szerződésbe történő beépítéséért, az alábbiak szerint
    - a Hivatal rendszereivel kapcsolatos vagy azokat érintő munkavégzés céljából érkező külső személy az Hivatalterületén a szerződés létrejötte után kizárólag a szerződéskötést

kezdeményező szervezeti egység vezetőjének tudtával és az általa kijelölt személy felügyelete mellett tartózkodhat,

- a külső személy a munkafolyamat egyeztetése során minden olyan munkafolyamatról köteles beszámolni a szerződéskötést kezdeményező szervezeti egység vezetőjének, amely bármilyen módon érinti az informatikai rendszer biztonságát,
- amennyiben az a munkavégzéshez feltétlenül szükséges, a Hivatal informatikai rendszereihez való hozzáféréshez ideiglenes és személyre szóló hozzáférési jogosultságot kell biztosítani, amelyről a szerződést kötő szervezeti egység vezetője gondoskodik,
- a Hivatal külső személlyel csak olyan szerződést köthet, amely a külső személy tekintetében biztosítja a vonatkozó titokvédelmi szabályok érvényesülését. A szerződéskötés során figyelembe kell venni az IBSZ előírásait, a jogszabályi előírásokat (különös tekintettel a szellemi alkotásokhoz fűződő, illetve szerzői, iparjogvédelmi, egyéb szellemi tulajdonhoz fűződő vagy egyéb személyhez fűződő jogokra)

- az informatikai biztonsági követelmények betartásának ellenőrzéséért, szükség esetén a felelősségre vonás (illetve jogkövetkezmények bevezetésének) kezdeményezéséért.

6.5 A Felhasználó

A Felhasználó – jogosultságtól és állományba tartozástól függetlenül –

- felelős az általa használt, az IBSZ hatálya alá eső eszközök rendeltetésszerű használatáért,
- felelős az általa elkövetett szabálytalanságért, valamint a keletkező károkért és hátrányért,
- köteles az IBSZ-ben megfogalmazott szabályokat megismerni és betartani, illetve ezek betartásában az informatikai rendszer használatát irányító személyekkel együttműködni,
- köteles a számára szervezett informatikai biztonsági oktatáson részt venni, az ismeretanyag elsajátításáról számot adni,
- köteles a rendelkezésére bocsátott számítástechnikai eszközöket megóvni,
- köteles a belépési jelszavát (jelszavait) az előírt időben változtatni, biztonságosan kezelni,
- köteles a felügyelet nélkül maradó munkahelyen (munkaállomáson) személyes adatot vagy nem nyilvános adatot tartalmazó dokumentumot/adathordozót elzárni,
- köteles a számítógépét (a munkahelyi munkaállomást) a helyiség elhagyása esetén lezárni úgy, hogy ahhoz csak jelszó vagy hardveres azonosító eszköz használatával lehessen hozzáférni,
- köteles az információbiztonságot érintő esemény gyanúja esetén az észlelt rendellenességekről tájékoztatni a közvetlen felettesét és az informatikai biztonsági megbízottat,
- köteles a folyó munka során nem használt nem nyilvános anyagokat, adathordozókat elzárni,
- köteles a munkahelyről történő eltávozáskor az addig használt – kivéve ha ez a rendszer(ek) más által történő használatát vagy a karbantartást akadályozza – eszközt szabályszerűen leállítani,
- köteles az általa használt eszközök biztonsági beállításait változtatás nélkül megőrizni,
- köteles az e-mail és internet használat során tartózkodni a biztonság szempontjából kockázatos tevékenységtől.

A Felhasználó – jogosultságtól és állományba tartozástól függetlenül – számára tilos

- a saját használatra kapott számítógép rendszerszintű beállításainak módosítása (ide nem értve az irodai programok felhasználói beállításait),
- a munkaállomására telepített aktív vírusvédelem kikapcsolása,
- belépési jelszavát (jelszavait), hardveres azonosító eszközét más személy rendelkezésére bocsátania, hozzáférhetővé tennie,
- a számítógép-hálózat fizikai megbontása, a számítástechnikai eszközök lecsatlakoztatása, illetve bármilyen számítástechnikai eszköz rácsatlakoztatása a hálózatra az informatikai biztonsági megbízott tudta nélkül,
- a számítástechnikai eszközökből összeállított konfigurációk megbontása, átalakítása,
- bármilyen szoftver installálása, internetről való letöltése, külső adathordozóról merevlemezre való másolása az informatikai biztonsági megbízott engedélye nélkül,
- a munkaállomásokon nem a Hivatalban rendszeresített vagy engedélyezett szoftverek (szórakoztató szoftverek, játékok, egyéb segédprogramok) installálása és futtatása,
- bármilyen eszköz számítástechnikai eszközökbe szerelése és annak használata,
- az általa használt hardveres azonosítóeszköz számítógépben való hagyása a munkaállomásáról való távozása esetén,
- ellenőrizetlen forrásból származó adatokat tartalmazó adathordozót az eszközökbe helyezni,
- más szerzői, iparjogvédelmi, egyéb szellemi tulajdonhoz fűződő vagy egyéb személyhez fűződő jogát vagy jogos érdekét sértő dokumentumokat, tartalmakat (zenéket, filmeket stb.) az eszközökön tárolni, oda le-, illetve onnan a hálózatra feltölteni,
- láncleveleket továbbítani, kéretlen levelekre válaszolni, ismeretlen tartalmú kéretlen levelek mellékleteit vagy linkjeit megnyitni,
- kereskedelmi célú hirdetéseket/reklámokat belső címzettek felé továbbítani (ide nem értve a Hivatal által kért vagy partnerei által küldött, a Hivatal által támogatott tevékenységekről – pl. kedvezményes beszerzés, munkavégzést segítő eszközök – szóló anyagokat),
- levelező listákra hivatali e-mail címmel feliratkozni, kivéve a munkavégzéshez szükséges
    - a Hivatal által megrendelt, működtetett vagy előfizetett szolgáltatások,
    - belső információs rendszerek,
    - közigazgatási, illetve nemzetközi vagy uniós szervek/szervezetek által biztosított szolgáltatások,
    - közigazgatási szervek által felügyelt szervek vagy szervezetek által biztosított szolgáltatások levelező listái,
    - más levelező listára történő feliratkozás a Hivatal vezetőjének külön engedélyével történhet;
- online játékokat használni,
- közösségi oldalakat látogatni és használni, kivéve ha ez a munkaköréhez kapcsolódik

7. Az információ vagyon védelmének szabályai

7.1 Az információ vagyon elszámoltatható kezelése

7.1.1 Titokvédelem

A Hivatal informatikai adatfeldolgozással és kezeléssel, valamint közzététellel foglalkozó minden munkatársának informatikai munkája során kötelessége betartani a Hivatal

- az adatkezelés és az adatvédelem általános szabályairól szóló szabályait,
- a közérdekű adatok elektronikus közzétételére vonatkozó tevékenységről szóló szabályzatát.

A Hivatal informatikai rendszeréről és eszközeiről csak a Hivatal vezetője szolgáltathat adatokat.

A Hivatal döntése alapján bevezetett alkalmazói rendszerek bevezetésében és felhasználásában közreműködő külső fél munkatársai és vezetői a Hivatalnál rendszeresített titoktartási nyilatkozat tételére kötelesek. A titoktartási kötelezettség kiterjed az alkalmazói rendszerekkel kapcsolatos, illetve ezek bevezetése során tudomásra jutó információkra.

Az alkalmazói rendszerek bevezetése és működtetése kapcsán a rendszerekkel kapcsolatba kerülő külső szervezeteknek, személyeknek felelősséget kell vállalniuk azért, hogy

- a tudomásukra jutott információkat kizárólag a Hivatal által meghatározott célokra használják fel,
- azokat harmadik személy részére a Hivatal képviselőjének írásos engedélye nélkül át nem adják,
- illetve a Hivatal tevékenységére vonatkozó információk rögzítésére semmiféle technikai eszközt vagy más eszközt nem alkalmazhatnak.

7.1.2 Adatvédelem

Minden felhasználó az általa végzett elektronikus adatfeldolgozás során személyesen felelős az adatvédelmi szabályok és információbiztonsági előírások betartásáért.

Külső fél munkavégzése során törekedni kell arra, hogy:

- a feladatához szükségtelen hivatali adat, információ ne kerüljön tudomására,
- a feltétlenül szükséges adat birtoklásáról és az információ megismeréséről nyilatkozzon, és ha szükséges titoktartási nyilatkozatot tegyen.

7.1.3 Információvédelem

A Hivatal számítógépeiről, szervereiről – a munkahelyi célú felhasználás kivételével – nem engedélyezett programok, adatállományok, illetve a munkavégzés során szerzett egyéb adatok, információk másolása, azok más, illetéktelen személyekkel történő megismertetése.

Nyomatképző berendezések (fénymásoló, nyomtató stb.) használata során gondoskodni kell a felesleges vagy rontott iratpéldányok megsemmisítéséről.

Az eszközök (monitorok, nyomtatók, fénymásolók) elhelyezése során biztosítani kell, hogy bizalmas információ illetéktelen tudomására ne juthasson.

Adathordozók és nyomtatványok tárolása során gondoskodni kell az illetéktelen személyek elleni hozzáférés megakadályozásáról.

7.1.4 Informatikai biztonság

Az Informatikai biztonsággal szemben támasztott követelmények:

- Rendelkezésre állás: a szolgáltatások és adatok elérhetősége biztosított az arra jogosult felhasználók számára. Biztosított a védelem a jogosulatlan hozzáféréstől és adatmódosítástól, törléstől, illetve a szolgáltatás elérhetőségének megakadályozásától.
- Sértetlenség: adat- és rendszerintegritás. Adatintegritással biztosítjuk, hogy adat nem módosulhat nem engedélyezett (nem tervezett) módon a tárolás, feldolgozás, adatátvitel során. Rendszerintegritáson azt érjük, hogy a rendszer a megvalósított funkciót, engedélyezetlen manipulációtól mentesen hajtja végre.
- Bizalmasság: az a követelmény, hogy a bizalmas, vagy magántermészetű információ nem jutott jogosulatlan kezekbe. Ez vonatkozik az adat tárolására, feldolgozására, átvitelére egyaránt.
- Felelősség: bármely entitás cselekvései követhetőek, és egyértelműen visszavezethetőek rá.
- Megbízhatóság: a különböző biztonsági intézkedések az irányítási, technológiai, működési vezérlés területén megfelelően működnek, és védik a rendszert és az általa feldolgozott adatot. A célok megvalósítottak, ha: a kívánt funkció jelen van és pontosan megvalósított. megfelelő védelem van a nem szándékos hibák ellen. megfelelő védelem van a szándékos hibák (behatolás stb.) ellen.

A Hivatal területén végzett minden tevékenység (építési és karbantartási munka, ügyfélforgalom bonyolítása, üzemeltetési feladatok ellátása, postaszolgálat, futárszolgálat) során figyelemmel kell lenni az IBSZ betartására és betartatására az informatikai biztonság követelményeinek maximális fenntartására.

7.2 Információbiztonság követelményei

7.2.1 Rendelkezésre állás

Az informatikai biztonsági megbízott feladata biztosítani az informatikai rendszerek folyamatos rendelkezésre állását az alábbi eszközök felhasználásának koordinálásával:

- rendszeres adatmentések és szoftvertelepítő készletek megfelelő biztosításával és megfelelő tárolásával,
- tartalék eszközök és alkatrészek biztosításával,
- helyreállítási módszerleírások, vészforgatókönyvek naprakész biztosításával.

7.2.2 Sértetlenség

Számítógép vagy programhibából eredő adatvesztés gyanúja esetén az - adatfeldolgozás szüneteltetése mellett – a kijelölt informatikust haladéktalanul értesíteni kell. Az értesítés módja lehet személyes, telefonos, vagy a kijelölt email címre küldött bejelentés. A probléma tisztázása után az informatikus útmutatása szerint kell folytatni az adatrögzítést, illetve adatfeldolgozást.

Az alkalmazások használata során az adatok felvitelét, módosítását, törlését kizárólag csak az aktuális felhasználói dokumentáció útmutatását követve lehet elvégezni.

Az alkalmazásokhoz és hálózati mappákhoz (könyvtárakhoz) való hozzáférés (jogosultságok) dokumentált engedélyeztetése útján gondoskodni kell arról, hogy jogosulatlan felhasználó azokat ne módosíthassa, és ne törölhesse.

A mentések és archívumok tárolása és őrzése során biztosítani kell az adatok sértetlenségét.

7.2.3 Bizalmasság

A Hivatal területén végzet minden ügyfélforgalmi és ügyfél kiszolgálási tevékenység során szem előtt kell tartani

- az ügyfelek adatainak és információinak,

- az ügyük elemeinek bizalmas jellegét, ezért az informatikai struktúrát és környezetet ennek megfelelően kell kialakítani.

7.3 Az információ vagyon osztályozása

7.3.1 Útmutató az információ vagyon osztályozásához

Az adatokat az alábbi szempontok szerint kell minősíteni.

A közérdekű, illetve a közérdekből nyilvános adatokat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény határozza meg.

A közérdekű adat nyilvánosságához fűződő jogok minősítéssel történő korlátozását a minősített adat védelméről szóló 2009. évi CLV. törvény szabályozza.

Az üzleti titok körébe tartozó adatokat az 1959. évi IV. Törvény (Ptk) 81. § határozza meg.

Az adatok minősítője, amennyiben azt jogszabály nem szabályozza, annak a szervezeti egységnek a vezetője, amelynek érdekkörébe az adat tartozik.

A rendszerekben nyilvánosnak csak a Hivatal vezetés által egyértelműen annak minősített információ tekinthető.

A nyilvános adatok kivételével, valamennyi adatot legalább érzékeny adatnak kell tekinteni és bizalmasként (védendő nem titkos adat) kell kezelni.

7.3.2 Az információ vagyon biztonsági osztályba sorolása

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban – ibtv.) 7. § (1) bekezdése értelmében annak érdekében, hogy a törvény hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából. Ugyanezen paragrafus (3) bekezdése szerint a biztonsági osztályba sorolást a szervezet informatikai biztonsági szabályzatában kell rögzíteni.

7.3.3 Információ vagyon biztonsági szintjei

A Hivatal biztonsági osztályba sorolását a 77/2013 (XII.19) NFM rendelet alapján lefolytatott kockázatelemzés végrehajtásával lehet meghatározni. A rendelet alapján a következő biztonsági szintekbe lehet a szervezet elektronikus információs rendszereit és a szervezetet besorolni:

Az 1. biztonsági osztály esetében csak jelentéktelen káresemény következhet be, mivel

- az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot;
- nincs bizalomvesztés, a probléma kisebb, az érintett szervezeten belül marad, és azon belül meg is oldható;
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest jelentéktelen.

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

- személyes adat sérülhet;
- az üzlet-, vagy ügymenet szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat, vagy elektronikus információs rendszer sérülhet;
- a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;

- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest csekély.

A 3. biztonsági osztály esetében közepes káresemény következhet be, mivel

- különleges személyes adat, vagy nagy tömegű személyes adatok sérülhetnek;
- az üzlet-, vagy ügymenet szempontjából közepes értékű, vagy az érintett szervezet szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat sérülhet;
- a lehetséges társadalmi-politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek;
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest közepes.

A 4. biztonsági osztály esetében nagy káresemény következhet be, mivel

- nagy tömegű különleges személyes adat sérülhet;
- személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket);
- az üzlet-, vagy ügymenet szempontjából nagy értékű, üzleti titkot, vagy az érintett szervezet szempontjából különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet;
- a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, az érintett szervezet vezetésében személyi konzekvenciákat kell alkalmazni;
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest jelentős.

Az 5. biztonsági osztály esetében kiemelkedően nagy káresemény következhet be, mivel

- kiemelten nagy tömegű különleges személyes adat sérül;
- emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;
- a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;
- az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;
- a lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetését, szellemi és anyagi erőforrásait meghaladó, különösen nagy értékű üzleti titok, az érintett szervezet szempontjából kiemelten érzékeny információt képező adat sérül.

Az Ibtv. 9. § 1.-2. pontja alapján a szervezet biztonsági szintjének a szervezet elektronikus rendszereinek legmagasabb biztonsági szintbe sorolásával azonos besorolású, de legalább 2-es besorolási szintűnek kell lennie, továbbá az Ibtv. 10. § (8). pontja alapján a szervezet biztonsági szintbe sorolását a szervezet vezetőjének jóvá kell hagynia.

A kockázatelemzés eredményeképp megállapításra került, hogy a Hivatal elektronikus információs rendszereinek biztonsági osztály szerinti besorolása a 2-es szintet érte el, amely megegyezik a szervezetre vonatkozó legalább 2-es szintű besorolási fokozattal.

A szakrendszerek vonatkozásában a következő biztonsági osztály kerül meghatározásra:

Szakrendszer	Biztonsági Osztály
Adó rendszer	4
Keretrendszer	4
Gazdálkodási rendszer	3

Az Ibtv. 8. § (1) pontja alapján a biztonsági osztályba sorolást legalább három évenként, vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.

7.4 Védelem módszerei

7.4.1 Általános védelem

A Hivatal informatikai hálózatában az internet kijárat védelme érdekében biztonsági és védelmi megoldásokat kell alkalmazni. Gondoskodni kell a hálózat fizikai elemeinek védelméről, azaz:

- a vezetékek és végpontok illetéktelenek általi hozzáférésének megakadályozásáról,
- vezeték nélküli kapcsolatok megfelelő titkosításáról,
- eszközhöz való illetéktelen hozzáférés megakadályozásáról.

7.4.2 Proaktív védelem (kezdeményező védelem)

Gondoskodni kell a Hivatal informatikai rendszerének behatolás elleni védeleméről, az erre vonatkozó szakmai előírások és a biztonsági szabályok betartása mellett.

Az informatikai rendszert automatikus vírusvédelmi rendszerrel kell ellátni, üzemeltetését és felügyeletét helyi szinten biztosítva.

A vírusvédelmi rendszert oly módon kell konfigurálni, hogy

- minden kimeneti és bemeneti eszköz és csatorna esetében folyamatos legyen a valósidejű vírusfigyelés,
- a vírusvédelmi szoftver vírustalálat esetén a vírust távolítsa el az érintett fájlból, vagy a fájlt helyezze karanténba,
- a vírusvédelmi szoftver vírusincidens esetén értesítést küldjön az informatikai megbízott részére.
- a kliens gépeken teljes víruskeresés történjen heti egy alkalommal olyan időszakban, amikor a legtöbb kliens gép be van kapcsolva, de a gépek leterheltsége a lehető legkisebb (pl. a hét közepén, ebédidőben, ügyfélfogadási időn kívül).

Amennyiben a Hivatal lokális szervert üzemeltet, a szerverek esetén alkalmazandó vírusvédelmi eljárások:

- Minden szerverhez, amelyhez kereskedelmi forgalomban beszerezhető vírusvédelmi szoftver, azt be kell szerezni, és telepíteni kell. Biztosítani kell, hogy a szerveroldali vírusvédelmi szoftver, víruskereső motor és vírusminta adatbázisa automatikusan frissüljön.

- A levelező szerver esetében a levelezésért felelős alkalmazásba beépülő, a levélforgalom vizsgálatát végző vírusvédelmi szoftvert kell alkalmazni.

Az elektronikus levelezés biztonsági irányelveinek érvényesítéséről a levelező rendszer üzemeltetője felelős. Az irányelvek a következők:

- a folyamatos üzembiztonság megvalósítása,
- az elektronikus küldemények adatintegritásának megtartása,
- a levelezőrendszer vírusvédelmének biztosítása és folyamatos frissítése,
- az elektronikus levelező eszközök, elsősorban a szerverek fizikai és logikai védelme (szoftverfrissítések, service packok és security-patch fájlok telepítése).

7.4.3 Defenzív védelem (védekező, megelőző védelem)

A Hivatal területén és szervezeti egységeinél informatikai hálózatot, illetve vezetékes vagy mobil internet kapcsolatot Hivatal vezetője engedélyezhet, hagyhat jóvá és hozhat létre.

Két internet kapcsolat egyszerre egy eszközön nem használható (pl.: LAN és mobil internet).

A használatra kapott számítógép rendszerszintű beállításainak módosítása nem engedélyezett. (Ebbe nem értendők bele az irodai programok felhasználói beállításai).

A felhasználónak a vírusvédelmi programot inaktívvá tenni, a beállításokat megváltoztatni, a vírusvédelmet eltávolítani nem engedélyezett.

Vírussal fertőzött fájlt vagy elektronikus adathordozót bármilyen formában továbbítani, továbbadni, illetve fertőzött állománnyal munkát végezni nem engedélyezett!

A Hivatal informatikai rendszerébe és informatikai eszközén csak azon szoftvert szabad telepíteni és használni, amelyik:

- a Hivatal által jóváhagyott, telepítésre kiadott és engedélyezett nyílt forráskódú szoftver, vagy
- szerzői jog szerint biztosított licencigazolással, illetve más jogi igazolással rendelkező, illetve tulajdonosi vagy használói szerződéssel biztosított hivatalos forrásból származó jogtiszta szoftver, vagy
- a szakigazgatási szervek szakmai irányító szervei felelősségi körébe tartózó és részükről rendelkezésre bocsátott telepítési utasítással vagy más megállapodással kiadott szoftver.

8. A HR erőforrásokra vonatkozó biztonsági szabályok

8.1 Munkaköri biztonsági előírások

ASP rendszert használó Hivatalként a hivatal szervezeti egységvezetőjének feladata és felelőssége, hogy meghatározza az egyes, ASP szakrendszer munkakörökhöz tartozó feladatok és felelősségek meghatározása.

Alkalmassági vizsgálat keretében a humánpolitikai munkatárs felelőssége, hogy a foglalkoztatás előtt a betöltendő ASP rendszerhez kapcsolódó munkakör kockázataival arányos mértékű megfelelőségi vizsgálatot végezzen a foglalkoztatni kívánt munkatárs vonatkozásában.

8.1.1 Általános biztonsági kötelezettségek

Minden, a jelen szabályzat hatálya alá eső személyre a következő, általános kötelezettségek érvényesek:

- Az informatikai rendszerek használata csak hivatalos célokra engedélyezett.
- A használt informatikai eszközpark kezelésével kapcsolatos kezelési és biztonsági ismereteket el kell sajátítani, és készség szintjére kell fejleszteni.
- A rendszerekbe csak szabályszerűen, a személyes felhasználó-azonosító kóddal szabad bejelentkezni.
- Az informatikai rendszerekben csak azokat a feladatokat szabad elvégezni, amelyek a felhasználó vagy üzemeltető munkájának ellátásához szükségesek, függetlenül attól, hogy a rendszer esetleg ennél szélesebb körű tevékenységet enged meg.
- Minden személynek biztosítania kell, hogy felhasználó-azonosítóját más felhasználók ne tudják használni.
- A képernyőket, nyomtatókat úgy kell elhelyezni, hogy azok minél kevesebb lehetőséget biztosítsanak illetéktelen betekintésre.
- A Hivatal által rendszeresített biztonsági funkciókat (például automatikus képernyővédő-aktiválás) kikapcsolni, megkerülni tilos.
- A Hivatal eszközein csak a Hivatal által engedélyezett eszközöket és programokat szabad használni.
- Tartózkodni kell minden olyan tevékenységtől, amely az informatikai rendszerben kárt okoz a biztonság, a sértetlenség és teljesítmény terén.
- Az információtechnológiai biztonságra és az adatvédelemre vonatkozó minden egyéb utasítást és jogszabályt be kell tartani.
- Esetleges meghibásodás esetén törekedni kell a további károsodás megelőzésére (a hiba jelentésével, a további használat mellőzésével stb.).
- A felhasználónak vagy üzemeltetőnek ismernie kell a segítségkérés és hibajelentés módját. Amennyiben ez az ismeret nem áll rendelkezésére, hiba esetén értesítenie kell a munkahelyi vezetőjét, külső személyek esetén a Hivatal kijelölt kapcsolattartóját.
- Az informatikai biztonságot veszélyeztető eseményről vagy ennek gyanújáról értesíteni kell a kijelölt informatikust, az informatikai biztonsági megbízottat és a Hivatal vezetőjét, külső személyek esetén a Hivatal kijelölt kapcsolattartóját.
- A közvetlen munkahelyi vezető (külső személyek esetén a Hivatal kijelölt kapcsolattartója) a felelős azért, hogy a fenti szabályokat az érintettekkel ismertesse.

8.1.2 A jelszókezelés általános szabályai

A felhasználó a számítógépre csak saját nevében és jelszavával léphet be, és az alkalmazásokat csak saját nevében használhatja.

A jelszó érvényességi idejét, ezzel együtt a jelszócsere gyakoriságát az informatikai rendszer központi szabályozása vagy a használt rendszer működése határozza meg. A jelszó cseréjét ezen értesítés hiányában legalább 90 naponta kötelező elvégezni. Ha az informatika rendszer lehetővé teszi, törekedni kell arra, hogy a jelszócsere kikényszerítésre kerüljön, illetve a felhasználó e-mailes értesítést kapjon a jelszó csere szükségességéről

A felhasználó jelszókezelési szabályai:

- jelszavak nem hozhatók nyilvánosságra.

- a jelszavak biztonságának megőrzéséért a felhasználó személyesen felel,
- a felhasználó a jelszavát nem oszthatja meg senkivel,
- ha a felhasználónak a legkisebb gyanúja is felmerül, a jelszó biztonságának integritása felől, azt köteles azonnal megváltoztatni és gyanújáról az informatikai biztonsági megbízottat értesíteni,
- más felhasználó azonosítóját átmeneti jelleggel sem szabad használni,
- a felhasználó köteles a jelszavát az előírt gyakorisággal és módon megváltoztatni.

A felhasználói azonosító kialakításáról, és az informatikai rendszerbe történő felvételéről a kijelölt informatikus gondoskodik, és alapértelmezett jelszóval adja át az első belépéshez szükséges információt a felhasználónak, akinek a jelszót az első belépés után kötelessége azonnal megváltoztatni.

Új belépő, vagy új hozzáférés kiosztása esetén a kijelölt informatikus szóban ismerteti a felhasználóval a munkájához szükséges felhasználó nevét és induló jelszavát és az első belépést követően elkészíti az informatikai eszközein a szükséges beállításokat.

Ha a felhasználónak tudomása vagy gyanúja támad arról, hogy jelszava valakinek tudomására jutott, akkor erről a tényről az informatikai biztonsági megbízottat tájékoztatni kell és a jelszót azonnal meg kell változtatnia.

8.1.3 Titoktartási nyilatkozat

A Hivatal bármilyen informatikai rendszerével, eszközével, szoftverével kapcsolatba csak az a munkavállaló kerülhet (kivéve azon központi szakmai irányító felettes szervek munkatársai vagy a szervezettel kapcsolatban álló megbízott partnerek, amelyek a központi szervnél már titoktartási nyilatkozatot tettek), aki a szükséges titoktartási nyilatkozatokat megtette.

A Hivatal állományába kerülő munkatársnak a titoktartási kötelezettségét „Belépési és Titoktartási Nyilatkozat” aláírásával kell bizonyítania.

A Külső Félnek „Titoktartási nyilatkozat (Külső Fél)” nyilatkozat aláírásával kell vállalnia a titoktartási kötelezettséget.

A nyilatkozatok e szabályzat hatálybalépését követően a Hivatalnál már alkalmazásban álló dolgozóknak is 30 napon belül meg kell tenniük a mellékletben található nyilatkozat megfelelő részeinek kitöltésével. A nyilatkozat kitöltéséért, aláírásáért és átadásáért a dolgozó felettes vezetője a felelős.

8.2 Felhasználók oktatása, képzése

8.2.1 Informatikai biztonsági oktatás és képzés

A Hivatal rendszereit csak olyan személyek használhatják, akik megfelelő informatikai ismeretekkel rendelkeznek. Az új belépő közszolgálati tisztviselőt az illetékes szervezeti egység vezetője utasítja a szükséges informatikai ismeretek megismerésére. Ezt követően a kijelölt informatikus tájékoztatja a felhasználót az informatikai rendszer használatához szükséges alapvető ismeretekről és eljárásokról, a rá vonatkozó informatikai szabályzatok elérhetőségéről, és felkéri annak megismerésére és betartására. A szükséges informatikai ismeretek és az informatikai szabályzatok megismerésének tényét a dolgozó aláírásával igazolja.

Az informatikai biztonsági megbízott legalább évente egyszer informatikai oktatást szervez az IBSZ szabályaiból azon dolgozók részére, akiknek:

- az IBSZ ismeretét számon kérő tesztje sikertelen volt,
- az informatikai biztonsági megbízott ellenőrzései során részére róható szabálysértés merült fel,

- az informatikai szabályzat be nem tartásával kapcsolatos fegyelemsértést követtek el.

A belső informatikai biztonsági oktatások és továbbképzések tematikájának kidolgozásáért, a szükséges tájékoztató anyagok biztosításáért az informatikai biztonsági megbízott felelős. Az oktatás lehet közvetlen (előadás) és közvetett (elektronikus úton megvalósuló). A számonkérés lehetőleg elektronikus úton történjen.

Az oktatáson, illetve továbbképzésen való részvétel az informatikai rendszerek felhasználói számára kötelezőek.

Minden felhasználó köteles a vonatkozó informatikai-szakmai szabályzatokat megismerni és betartani, illetve köteles ezek betartása során az informatikai rendszer használatát irányító személyekkel együttműködni.

A Hivatal azon munkatársainak, akik az ASP rendszert kezelik, adatott visznek fel illetve továbbítanak ASP oktatáson kell részt venniük, amely alapján a rendszert az elvárásoknak megfelelően, önállóan is használni tudják.

8.2.2 Informatikai biztonság értékelése

Minden felhasználó köteles a vonatkozó informatikai-szakmai és adatvédelmi szabályzatok áttanulmányozása után évente egyszer egy IBSZ elemeit tartalmazó tesztet (papíron vagy elektronikus úton) kitölteni, melyben felmérhető a szabályzatok ismerete. A sikertelen tesztet kitöltő felhasználó (50% alatti eredmény esetén) a szervezeti egység vezetője útján kötelezhető az informatikai biztonsági megbízott által szervezett oktatáson való részvételre.

Az új belépő dolgozó belépését követő két héten belül köteles az informatikai biztonsági megbízott által készített és részére rendelkezésére bocsátott tesztet kitölteni.

Az informatika biztonsági megbízott évente egyszer köteles jelentést készíteni a Hivatal vezetője részére a felhasználók oktatásáról és a tesztek eredményéről.

Az informatika biztonsági megbízott évente egyszer köteles jelentést készíteni az IBSZ szabályait figyelembe véve az informatikai folyamatok felhasználókat érintő ellenőrzéséről.

9. Az informatikai biztonsági incidensek kezelése

9.1 IT biztonsági incidensek jelentési kötelezettsége

Az informatikai rendszereket érintő (vagy vele összefüggésbe hozható) bármilyen bekövetkezett, vagy előre látható biztonsági eseményt (betörés, lopás, tűz, víz, villámcsapás, balesetveszélyes eszköz, eszköz elvesztése vagy eltűnése stb.) a Hivatal vezetője felé az eseményt észlelőnek azonnal jelezni kell.

Vészhelyzet vagy rendkívüli helyzet esetén (pl.: betörés, tűz, villámcsapás stb.) az IT eszközöket és adathordozó eszközöket tároló helyiségekbe biztonsági kulccsal, illetve biztonsági kóddal lehet bejutni utólagos jelentési kötelezettség mellett.

A felhasználó köteles jelezni az informatikai biztonsági megbízottnak bármely, az informatikai biztonságot érintő gyanús eseményt (pl.: előző nap lekapcsolt, de reggel bekapcsolva talált gépet), vagy ezzel kapcsolatos gyanúját.

9.2 IT biztonsági incidensek jelentésének módja

Az informatikai rendszereket érintő (vagy vele összefüggésbe hozható) biztonsági eseményeket az alábbi módon kell bejelenteni:

Felhasználói hiba észlelés: Haladéktalanul értesíteni kell telefonon vagy személyesen a kijelölt informatikust, az esemény bekövetkezte után, lehetőleg azonnal, írásban (e-mail), vagy elektronikus

„helpdesk” rendszeren (amennyiben rendszerbe van állítva ilyen) keresztül a hiba és bekövetkezésének körülményeinek pontos leírásával. Központi üzemeltetésű szakmai alkalmazással kapcsolatos probléma esetén a szakigazgatási szerv ügyintézőjének a hibát közvetlenül a központi szakigazgatási szerv felé kell bejelenteni, a szervezeti egység vezetőjének tájékoztatása mellett.

Biztonsági esemény esetén: Haladéktalanul telefonon értesíteni kell az informatikai biztonsági megbízottat, aki az esemény jellegétől függően intézkedik, indokolt esetben tájékoztatja a Hivatal vezetőjét. Az eseményt követően az eseményről jegyzőkönyvet kell készíteni, és azt a Hivatal vezetője részére írásban meg kell elküldeni (e-mail, levél).

9.3 IT biztonsági hiányosságok jelentési kötelezettsége

Az informatikai rendszer bármely felhasználói pontján jelentkező, a hálózattal, eszközzel, illetve adott alkalmazással kapcsolatban felmerülő rendellenes működés, jelenség, vírusjelzés, futási hiba esetén használója köteles a tapasztalt jelenséget, és ha van, a jelenséget kísérő hibaüzenetet regisztrálni és haladéktalanul bejelenteni az informatikai biztonsági megbízott felé.

9.4 Incidensek nyilvántartása és kivizsgálása

Az informatikai incidenseket a kijelölt informatikus és az információs biztonsági megbízott számára írásban (e-mail, levél) kell megküldeni. Amennyiben van elektronikus igény és hibabejelentő rendszer (helpdesk – összefoglalóan incidens bejelentő és nyilvántartó rendszer) az incidens bejelentését azon kell megtenni.

A kijelölt informatikus vagy az informatikai biztonsági megbízott a rendelkezésre álló nyilvántartásokat („helpdesk” alkalmazás digitális adatait, papíralapú eseménynaplókat, belépési naplókat) félévente elemzi, és a tanulságokat felhasználja:

- beszerzések tervezésénél,
- selejtezések tervezésénél,
- biztonsági konzekvenciák levonásakor,
- beszámoló készítésekor,
- IBSZ felülvizsgálatakor.

9.5 Visszajelzés a biztonsági incidensekről

A kijelölt informatikus a hiba elhárítása érdekében intézkedik, vagy a probléma elhárítását elvégzi, a hiba megszüntetéséről és a további teendőkről a felhasználót folyamatosan tájékoztatja. Helyettesítő eszköz biztosításával gondoskodik a felhasználó munkavégzési lehetőségéről.

9.6 Eljárás a biztonsági előírások megsértőivel szemben

Az informatikai rendszer rendellenes működése vagy a biztonságot veszélyeztető esemény elhárítása érdekében az informatikai eszközök használatát, a hálózat működését, az internet és levelezés használatát a kijelölt informatikus részben vagy egészében korlátozhatja vagy leállíthatja a Hivatal vezetőjével történt tájékoztatást vagy egyeztetést követően.

A Hivatal szankciókat alkalmazhat az internethasználat és elektronikus levelezés szabályainak megszegése esetén, ha a felhasználó az internetezés során a figyelmeztetését követően is szándékosan és rendszeresen:

- megszegi az internethasználat szabályait,
- vagy olyan magatartás tanúsít, melyek által súlyosan vét a munkahelyi etikai szabályok ellen,
- vagy tiltott tartalmú kategóriába sorolt oldalakat látogat (kivéve egyedi írásos engedéllyel),
- vagy tiltott tevékenységet folytat.

Az IBSZ szándékos, vagy az ismeret hiányából eredő megszegőjével szemben az informatikai biztonsági megbízott a Hivatal vezetője felé figyelmeztető felszólítást vagy fegyelmi eljárást kezdeményezhet.

10. A fizikai és környezeti infrastruktúra biztonsága

10.1 Védett, biztonságos területek

10.1.1 Fizikai biztonsági elkülönítés

Az informatikai infrastruktúra elemeinek és a helyiségeknek a kockázatokkal és a tágabb értelemben vett értékükkel arányos fizikai védelmet kell biztosítani.

Az informatikai rendszer kritikussága és a benne kezelt adatok besorolásának kockázata alapján a helyiségeket biztonsági zónák szerint kell besorolni. A biztonsági követelményeknek megfelelően, lehetőség szerint úgy kell a helyiségeket kialakítani, hogy a rendszerek és adatok megfelelő fizikai és környezeti védelmét garantálni tudják. A kialakított információbiztonsági zónákban történő munkavégzésre – a zónát veszélyeztető fenyegetettségek függvényében – más-más informatikai biztonsági követelmények vonatkoznak.

10.1.2 Kiemelten védendő területek

Informatikai központoknak minősülnek azon helyiségek, melyek működő szerverek és hálózati elosztó elemek (router, switch) elhelyezésére és működtetésére szolgálnak, kivételt képeznek azon egyéb helyiségek, melyekben zárt, kulccsal biztosított rack szekrény található.

Az informatikai biztonsági zónákba való belépési jogosultságot személyre szólóan, az adott személy feladata alapján kell meghatározni. Állandó vagy egyedi belépési jogosultságot a Hivatal vezetője adhat.

10.1.3 Munkavégzés szabályai az informatikai központokban

A belépési jogosultsággal nem rendelkezők az informatikai központban csak az arra jogosultak felügyelete mellett tartózkodhatnak.

Az informatikai központokba belépési jogosultsággal nem rendelkező személyek esetén, ha belépés munkavégzés, szemle, felmérés, ellenőrzés céljából történik, az eseményt a belépési naplóban rögzíteni kell.

Abban az esetben, ha az informatikai központba (pl.: szerverszoba) valamilyen okból (szemle, ellenőrzés, szerelés stb.) belépési jogosultsággal nem rendelkező személynek be kell jutni, arról előzetes egyeztetés mellett a kijelölt informatikus vagy az informatikai biztonsági megbízott gondoskodik.

A szerverszobában nem engedélyezett:

- az eszközök közelében ételt, italt fogyasztani,
- tűz vagy robbanásveszélyes anyagot tárolni.

Törekedni kell arra, hogy az informatikai központban a helyiség funkciójától eltérő anyagot vagy eszközt ne tároljanak.

Az informatikai központ helyiségeiben elhelyezett szerver- és nem szerverként működő számítógépeket, hálózati eszközöket, az informatikai központokban használt klímaberendezéseket és biztonsági berendezéseket az év minden napján, a nap 24 órájában folyamatosan kell üzemeltetni.

Az informatikai központok számítógépeire telepített szoftverek karbantartását kijelölt informatikus végzi.

A szerverek mellett gépkönyvet kell elhelyezni és az abban feltüntetett adatokat naprakészen kell tartani.

A Hivatal vezetőjét értesíteni kell az informatikai központok területén érzékelt, különös jelentőséggel bíró egyéb események bekövetkezéséről (pl.: betörési kísérlet).

A hálózati eszközök üzemeltetése és felügyelete a szakmai irányító központi szervekkel együttműködve történik.

10.1.4 Kontrollok

A szerverek üzemeltetéséről a kijelölt informatikus eseménynaplót vezet papír alapon vagy elektronikus formában.

Az informatikai központok belépési naplóinak kötelező vezetése az ellenőrzött körülmények kikényszerítésének eszköze.

10.1.5 Ellenőrzés

Az informatikai központok üzemeltetési feltételeit és az ott készült naplókat az informatikai biztonsági megbízott legalább évente egyszer szúrópróba szerű ellenőrzés során megvizsgálja, és jelentést készít a tapasztalatairól a Hivatal vezetőjének.

10.2 Eszközbiztonság

10.2.1 Eszközök

Az informatikai eszközök nyilvántartásáért az Hivatal vezetője tartozik felelősséggel. A kijelölt dolgozó az eszközöket az informatikai eszköznyilvántartásban tartja nyilván, és a változásokat lehetőség szerint azonnal, de legkésőbb három napon belül aktualizálja, a változásokról a Hivatal vezetőjét értesíti.

10.2.2 Eszközök életciklusa

Az informatikai eszközök üzembe helyezésére és selejtezésére, csak a Hivatal vezetője által kijelölt informatikus jogosult a Hivatal leltározási és selejtezési szabályzatai előírásait betartva. Az eszközök használata és tárolása során biztosítani kell annak fizikai védelmét. Az eszközök teljes életciklusa alatt kötelező annak nyilvántartása, és mozgatásának dokumentálása (üzembe helyezési dokumentum, átadás-átvétel nyomtatvány, szállítók, selejtezési bizonylat).

10.2.3 Eszközök elhelyezése és védelme

Az informatikai berendezéseket, eszközöket fizikai valójukban is védeni kell a biztonságot fenyegető veszélyektől és a káros környezeti hatásoktól. A környezeti veszélyek és kockázatok mérséklése érdekében:

- a berendezéseket úgy kell elhelyezni, hogy lehetőleg megakadályozza az illetéktelen hozzáférést,
- a különleges védelmet igénylő, fokozott és kiemelt biztonsági osztályba tartozó eszközöket elkülönítetten kell elhelyezni és használni,
- a környezeti hatások és a lehetséges veszélyforrások folyamatos vizsgálatával és elemzésével kell törekedni a szükséges működési feltételek biztosítására.

Az informatikai eszközök rendeltetésszerű használatáért a számviteli leltárban az eszköz használójaként kijelölt hivatali alkalmazott a felelős, vagy az a személy, aki vezetői utasításra és engedélyével azt használta. Közös használatú eszköz esetén az eszközök rendeltetésszerű használatáért, az a személy a felelős, akit a vezető adott esetben kijelöl eszközök felügyeletére (csoportvezető, ügyeletes, munkafelelős stb.).

A munkája során számítógépet használó felhasználó köteles az általa működtetett számítógépet és az ahhoz csatlakoztatott eszközöket:

- a rendeltetésnek megfelelően, munkavégzés céljából, szakszerűen, a Hivatal érdekeit szem előtt tartva az Informatikai Biztonsági Szabályzatban meghatározott módon használni,

- kikapcsolni, ha előre láthatóan hosszabb (1 órát meghaladó) ideig nem használja (pl. értekezlet, megbeszélés, tárgyalás, ebédidő),
- a munka befejeztével valamennyi eszközt kikapcsolni (kivéve akkor, ha ezzel ellentétes állandó vagy egyedi írásos utasítást, illetve tájékoztatást nem kap).

Az informatikai eszközök használata során nem engedélyezett:

- az eszközt illetéktelen személynek átengedni.
- az eszköz közelében folyadékot, éghető anyagot, illetve felette, alatta vagy rajta az eszköz rendeltetésétől eltérő anyagot, tárgyat elhelyezni és tárolni,
- nem engedélyezett az eszközt a telepítési helyéről elmozdítani és elvinni a kijelölt informatikus engedélye és közreműködése nélkül (kivételt képeznek a mobil eszközök).

Az informatikai eszközöknek a munkafeladattól eltérő célra történő használatához a szervezeti egység vezetőjének engedélye és az informatikai biztonsági megbízott hozzájárulása szükséges.

Az informatikai eszközökhöz bármilyen külső eszközt, illetve kábelt csatlakoztatni csak a kijelölt informatikus engedélyével vagy közreműködésével lehet. Az informatikus által már csatlakoztatott és beüzemelt eszköz további használata visszavonásig engedélyezett (pl.: pendrive, fényképezőgép).

Címkét, jelölést, feliratot csak a kijelölt informatikus helyezhet az informatikai eszközökre, illetve távolíthat el onnét. Az eszközök burkolatát megbontatni nem engedélyezett. Alkatrészt csak a kijelölt informatikus helyezhet be az eszközbe, illetve szerelhet ki az eszközből.

Az ügyfélszolgálatot bonyolító helységekben az informatikai eszközöket (pl.: monitor, billentyűzet, nyomtató) lehetőleg úgy kell elhelyezni, hogy illetéktelen ne lásson rá, megelőzve ezzel a jelszavak és bizalmas információk kiszivárgását.

10.2.4 Tápellátás

Az informatikai eszközök a vonatkozó szabványnak megfelelően kizárólag védőföldeléssel ellátott 230 V feszültségű elektromos hálózati dugaszoló aljzatba csatlakoztathatók.

A kijelölt informatikusnak törekedni kell arra, hogy a szervezeti szintű alkalmazások működését befolyásoló informatikai és távközlési eszközök (pl.: szerverek, rack szekrény stb.) szünetmentes tápegységekkel legyenek ellátva.

10.2.5 Kábelezés biztonsága

A Hivatal területén az informatikai rendszert, áramellátó hálózatot, telefonhálózatot érintő bármilyen beavatkozást, építést, karbantartást, átalakítást csak az informatikai biztonsági megbízott tájékoztatása után, annak jóváhagyásával, és felügyeletével lehet végezni.

A kábeleket a kábelrendező és a csatlakozó aljzatok között rögzített csatornában kell vezetni, a lengőkábelek nem keresztezhetnek közlekedési utat. A hálózat valamennyi elemét olyan környezetben kell elhelyezni, ahol a jogosulatlan fizikai hozzáférés megakadályozott.

10.2.6 Eszközök karbantartása

Az informatikai eszközök rendelkezésre állásának biztosítása érdekében a kijelölt informatikus szükség szerint, illetve tervezett és a felhasználókkal egyeztetett módon karbantartást végez.

Az informatikai eszközök és berendezések folyamatos használata és rendelkezésre állásának biztosítása érdekében: a specifikációban javasolt időközönként el kell végezni a berendezések karbantartását, a berendezések kezelését, illetve javítását csak megfelelő szakképzettséggel rendelkező személyek

végezhetik, az informatikai eszközök külső helyszínen történő javítása, karbantartása esetén gondoskodni kell az eszközön tárolt adatok védelméről.

10.2.7 Eszközök használata a Hivatal területén kívül

A Hivatal tulajdonát képező mobil informatikai eszközöket (pl.: laptop) a Hivatal területén kívül csak az érintett szervezeti egység vezetőjének írásos engedélyével rendelkező személyek használhatják az informatikai biztonsági megbízott hozzájárulásával, a nyilvántartási előírások betartása mellett.

A mobil informatikai eszköz (laptop) az arra felhatalmazott személy részére történő átadásakor a kijelölt informatikusa tárolási nyilatkozatot készít, mely tartalmazza az eszköz műszaki adatait, az átadás-átvétel adatait és az eszközön telepített szoftverek adatait.

Kiadott mobil eszközt rendszeresen felülvizsgálat céljából a kijelölt informatikusnak be kell mutatni. A mobil eszközön vírusvédelmi rendszer telepítéséről és folyamatos frissítéséről gondoskodni kell.

A kijelölt informatikus köteles az eszköz átadása során felvilágosítani a dolgozót a mobil informatikai eszközök használatának veszélyeiről, kockázatairól, amit a dolgozó a tárolási nyilatkozaton aláírásával igazol, és az eszközért felelősséget vállal.

A mobil eszközöket használó személyeknek:

- nem engedélyezett az eszközt gépjárműben, idegen helyen felügyelet nélkül hagyni,
- a repülés, vagy vonatút alatt a személyi számítógépet kézipoggyászként kell szállítani,
- a Hivatal területén kívül, idegen helyen történő tárolás esetén (szálloda, lakás) fokozott figyelmet kell fordítani a jogosulatlan hozzáférés, az adatok esetleges módosítása, megrongálása, vagy ellopása elleni védelemre,
- nem engedélyezett az eszköz engedély nélküli átruházása vagy adatainak közlése,
- nem engedélyezett megfelelő védelem nélkül idegen hálózathoz csatlakoztatni az eszközt,
- nem engedélyezett a gépet bármilyen indokolatlan veszélynek kitenni vagy nem rendeltetésszerűen használni.

Mobil adathordozót a felhasználók számára az adott szervezeti egység vezetője a „Mobil adathordozó engedélyezése” adatlapon kérhet a kijelölt informatikustól. Ezen az adatlapon kérheti a külső adathordozó egységek (USB, HDD) hozzáférésének egyedi engedélyezését is. Az engedélyezést és az eszköz átadását követően az adatlapot az Adathordozó nyilvántartáshoz kell csatolni.

Az adatokat a mobil adathordozóról a feladat elvégzése után, védett hálózati meghajtóra való felmásolást követően, le kell törölni és az adathordozót a tároló helyre vissza kell adni az esemény dokumentálása mellett.

A kódolatlan mobil adathordozó eszközök rendkívül nagy kockázati veszélyforrást jelentenek, ezért a felhasználók csak informatikai ellenőrzés mellett használhatják. A hivatali adathordozón magánjellegű adatot tárolni nem engedélyezett, magánjellegű adathordozót hivatali célra használni nem engedélyezett, azon hivatali adatot tárolni nem szabad.

A Hivatal informatikai rendszerébe kapcsolt munkaállomásokon csak olyan adathordozót lehet használni, arról adatokat beolvasni, melyen előtte a rendszeresített és telepített víruskereső programmal vírusellenőrzést végeztek.

A mobil infokommunikációs eszközök, mobil adathordozók felhasználói felelősek az eszközön található adatok esetleges kiszivárgásáért, az eszköz elvesztéséért, eltűnéséért, megsérüléséért. A mobil

infokommunikációs eszközök, mobil adathordozók eltűnése, ellopása esetén annak tényét haladéktalanul a Hivatal vezetője felé jelentenie kell a szükséges intézkedések megtétele érdekében.

A felhasználók egyes feladatok elvégzése érdekében, a részükre biztosított, nyilvántartott és egyedi azonosítóval ellátott, hivatali tulajdonú mobil adathordozóra (pendrive, mobil HDD) kimenthetik a feladathoz kapcsolódó állományaikat.

10.2.8 Eszközkivonási biztonsági intézkedések, újrafelhasználás

Megsemmisítésre kijelölt eszközöket és kellékanyagokat megsemmisítésig a használatban lévő eszközöktől elkülönítetten kell tárolni és kezelni figyelembe véve:

- a veszélyes anyagok tárolására és a megsemmisítésre vonatkozó szabályokat (fizikai védelem, szállítás),
- a leltározási és selejtezési szabályzat előírásait,
- az adatvédelem biztonsági követelményeit (hozzáférés elleni védelem).

Az olyan hivatali helyiségeket, ahol informatikai eszközökkel történik a munkavégzés, vagy informatikai eszközt tárolnak, lehetőség szerint zárral kell ellátni, és a helyiséget távollét esetén vagyonvédelmi és biztonsági okokból zárva kell tartani.

Az informatikai berendezések végleges használaton kívül helyezése előtt gondoskodni kell az összes adat, szoftver visszaállíthatatlan eltávolításáról és felülírásáról, vagy a beépített adathordozó eltávolításáról és megfelelő tárolásáról.

Külső fél által javításra elszállított informatikai eszközből el kell távolítani a beépített adathordozót, ha ez nem megoldható a külső félnek titoktartási nyilatkozatot kell tennie. A nyilatkozat megtagadása esetén az adathordozó nem adható át a külső fél részére.

10.2.9 Kontrollok

Informatikai eszközökkel kapcsolatos eszközmozgatást, csatlakoztatást, lecsatlakoztatást, szerelést, eszközátadást, selejtezést és üzembe helyezést csak a kijelölt informatikus végezhet.

Az informatikai eszközökkel kapcsolatos minden telephelyen belüli és kívüli mozgatásról dokumentumot kell készíteni: tárolási nyilatkozat, mobil adathordozó engedélyezése, adathordozó nyilvántartás, átadás-átvételi adatlap, szállítói kísérőlapok, munkalapok, üzembe helyezési dokumentum, selejtezési dokumentum.

10.2.10 Ellenőrzés

Az informatikai eszközök biztonsági beállításait, illetve háttértárolóinak tartalmát a kijelölt informatikusnak szúrópróbaszerűen, de legalább évente egyszer ellenőriznie kell. A felhasználónak az eszköz átadásával az ellenőrzés elvégzését segítenie kell.

Az informatikusnak az ellenőrzés tényét mobil informatikai eszközök esetén a tárolási nyilatkozat második oldalán tett bejegyzéssel kell dokumentálnia. Az ellenőrzés során fokozott figyelmet kell fordítani a következőkre:

- az adott eszközön a biztonsági beállítások, vírusvédelmi és egyéb biztonsági rendszerek beállításai megfelelnek-e az előírtaknak,
- az állományok lokális tárolására vonatkozó szabályokat a felhasználók betartják-e,
- az eszközön fellelhető naplóállományokban nincs-e nyoma rendellenes műveleteknek, jogosulatlan használatnak.

10.3 Általános biztonsági előírások

A Hivatal vezetője gondoskodik:

- az informatikai eszközök fizikai védelmét biztosító eszközök és berendezések meglétének és működőképességének rendszeres ellenőrzéséről, a tervezett karbantartásáról,
- az informatikai eszközök működéséhez szükséges megfelelő fizikai környezet biztosításáról,
- a hálózati központi egységek (Rack szekrény) fizikai környezetének biztosításáról,
- a megfelelő elektromos hálózat, villám és túlfeszültség, valamint érintésvédelmi berendezések meglétéről és működésének biztosításáról,
- a behatolás elleni védelem és riasztórendszer körülmények szerinti kialakításáról (pl.: zárt terek, beléptető rendszer, elektromos behatolás jelző, mozgás érzékelő, belső térvédelem)
- a megfelelő tűzvédelmi rendszerről: füstjelző és riasztó rendszer kialakításáról, automata tűzoltó rendszer kialakításáról, vagy kézi tűzoltó készülékek (elektromos berendezések tűzének oltására alkalmas gázzal oltó készülék) elhelyezéséről;
- a hálózati központi egységek klímájáról (hűtéséről) oly módon, hogy az információtechnológiai eszközök környezeti hőmérséklete működés közben 15–25 C° között legyen.

Az informatikai objektumok közüzemi ellátását (áramellátás, fűtés, szellőzés, vízszolgáltatás stb.) a vonatkozó szabályzatok és hatósági előírások szerint kell biztosítani.

Különálló szerverszobában vizesblokk kialakítása nem engedélyezett. A szerverszobát védeni kell szennyvíz, illetve esővíz bejutása ellen. A kialakítás során törekedni kell arra, hogy felette vizesblokk ne helyezkedjen el.

Az informatikai központokban (szerverszobákban) végzett építési és karbantartási munkákat a kijelölt informatikus, vagy az informatikai biztonsági megbízott felügyeli.

Az üzemeltetés és hibaelhárítás során jelentkező alkatrészbeszerzések, javítások és a rendszer fejlesztésére irányuló beszerzések szakmai előkészítése a kijelölt informatikus feladata.

A teljes körű védelemről lehetőség szerint már a helyiségek kialakítása során gondoskodni kell. Az informatikai központok üzemeltetése során biztosítani kell a mechanikai (építészeti) és a technikai (elektronikai) védelmet:

- elektromos vagy fizikai (rács) védelmi eszközöket kell alkalmazni a nyílászárókon keresztül történő bejutás megakadályozása érdekében, beltéri vagy földszinti, illetve könnyen elérhető kültéri nyílászárók esetében egyaránt,
- gondoskodni kell arról, hogy a szerverszobába kívülről nyitott nyílászárón vagy szellőzőn keresztül idegen anyagot bedobni ne lehessen,
- a szerverszobára kívülről lehetőleg ne lehessen rálátni (pl. ablakon),
- az ajtónak kulccsal és/vagy mágneskártyával, illetve kóddal zárhatónak kell lennie, a kulcshoz vagy a mágneskártyához, illetve kódhoz való hozzájutás csak naplózottan történhet, a kijelölt informatikus – vészhelyzetet, rendkívüli helyzetet kivéve - előzetes értesítésével és tudtával (aláírással, keltezéssel.

11. A hálózat és rendszer üzemeltetés biztonsága

11.1 Az üzemeltetés folyamatai és a felelősségek

11.1.1 Dokumentált üzemeltetési folyamatok

A rendszer napi üzemeltetéséhez tartozik a működés felügyelete, a mentések elvégzése, és hiba esetén az eszközök javítása.

A rendszer üzemeltetését ellátó kijelölt informatikusnak ismernie kell a Hivatal rendszereszközeinek, operációs rendszereinek, adatbázisainak működését, az operációs és alkalmazói rendszerek hibaüzeneteit és a behatolás detektáló rendszerfigyelmeztető üzeneteit. A szükséges reagálásokat tartalmazó leírást tudnia kell alkalmazni.

A rendszer felügyelete a felhasználói programok és adatbázisok, a szerverek és alapszoftverek és a hálózat működésének folyamatos figyelemmel kísérését kívánja meg. A kijelölt informatikusnak rendszeresen el kell végeznie azokat az – üzemeltetési dokumentációban részletesen felsorolt – tevékenységeket, amelyek alapján meggyőződhet arról, hogy a rendszer üzemszerűen működik.

A rendszer valamennyi hardver/szoftver eleméről nyilvántartást kell vezetni. A nyilvántartásnak tartalmaznia kell a szerverek, munkaállomások pontos és naprakész hardver konfigurációját, a működtető szoftverek egyedi beállításait és elhelyezkedését, az értük felelős személy nevét.

Készítendő és naprakészen vezetendő nyilvántartások:

- tárolási nyilatkozat,
- mobil adathordozó engedélyezése,
- szoftvernyilvántartás,
- jogosultság nyilvántartás,
- szerverek esemény naplója,
- eszköz átadás-átvételi adatlap.

Az üzembiztonság érdekében a szerverek operációs rendszereit (a beállításokkal együtt) lehetőség szerint tartalék adathordozón is tárolni kell, amelyekről az adatok szükség esetén azonnal betölthetőek.

11.1.2 Az üzemeltetési folyamat változásainak kezelése

Szoftvert a számítógépre csak a kijelölt informatikus tölthet le, másolhat és telepíthet, valamint a számítógépről csak a kijelölt informatikus távolíthat el.

A felhasználó a munkaállomás használata során a munkaállomásra telepített alkalmazásokat használhatja. Új alkalmazások telepítését vagy a meglévő alkalmazásokat illető jogosultság változást a szervezeti egység vezetője engedélyével az erre szolgáló és a szabályzat mellékletét képező adatlapon igényelhet. Az informatikai biztonsági megbízott jogosult az igény felülvizsgálatára, és ha szükséges, biztonsági okból annak elutasítására.

A felhasználó a számítógépre telepített alkalmazásokat a felhasználói leírás szerinti módon, szakszerűen köteles használni.

A központ hivatalok, illetve szakigazgatási szervek szakmai irányító szervei által üzemeltetett alkalmazásokhoz kapcsolódó jogosultságokra vonatkozó igényléseket, változásjelentőket és levelezéseket – amennyiben azt nem a kijelölt informatikus intézi – a szervezeti egységek vezetői kötelesek másodpéldányban megküldeni a kijelölt informatikus és az informatikai biztonsági megbízott részére.

A központilag, szolgáltatásként biztosított alkalmazások használatánál, valamint a szakigazgatási szervek szakmai irányító szervei által kiadott és üzemeltetett alkalmazások használata során a szolgáltatást biztosító szervezet által kiadott előírások szerint kell eljárni.

11.1.3 Hibakezelési, hibaelhárítási rendszer

Az informatikai hiba és igénybejelentéseket elektronikus úton a kijelölt informatikus email címre küldött levéllel kell megtenni. Amennyiben a hiba elhárítása (kritikus) nem tűr halasztást, a hiba bejelentés telefonon is megtehető, azonban ebben az esetben is a hibabejelentő munkatársnak a fent megadott email címre küldött levélben a hiba bejelentést utólag meg kell tennie.

Súlyos hibák kezelése: olyan esetben, ha a hiba a Hivatal rendszereinek működésére komoly kihatással van (pl. üzembiztonságot veszélyeztető helyzet, katasztrófahelyzet áll fenn), vagy más jellegű, de rendkívül fontos eset következik be (pl. bűncselekmény gyanúja áll fenn) az észlelő köteles haladéktalanul értesíteni a Hivatal vezetőjét.

A szoftvereket és adatokat harmadik fél számára másolni és továbbadni nem engedélyezett. Kivételt képez a szoftverekről és adatokról való biztonsági másolatok kijelölt informatikus által történő elkészítése, mely a rendelkezésre állás folyamatosságát hivatott biztosítani.

A szoftverek adathordozóit, üzemeltetési és felhasználói dokumentációját, licenc dokumentációját a kijelölt informatikus vagy informatikai biztonsági megbízott tárolja és tartja nyilván.

11.1.4 A fejlesztés és az éles környezet elkülönítése

Fejlesztés során az éles környezet mellett külön fejlesztői, külön teszt környezet kialakítása szükséges. A teszt környezetnek tartalmaznia kell mindazon elemeket, amelyekben valamely módosításra sor kerül. A teszt környezetnek, a tesztelni kívánt elem kivételével, lehetőleg ugyanolyan beállításúnak kell lennie, mint az éles környezet.

A fejlesztői környezetből tesztelés nélkül semmilyen elem sem kerülhet át az éles környezetbe. Nem éles környezetben csak olyan próbaadatok használhatók, amelyek nem sértik az éles környezetbeli adatokra vonatkozó adatvédelmi szabályokat.

A külső fejlesztő személy hozzáférését az éles környezethez, csak rendkívüli esetben lehet megengedni, ha ez feltétlenül szükséges az üzemeltetés folyamatosságának biztosításához vagy más kiemelten fontos cél eléréséhez. Az ilyen hozzáférést a Hivatal vezetője minden alkalommal külön, írásban engedélyezi. Az engedélyben jelölni kell a feladatvégzés célját. A fejlesztő által elvégzett munkákat, a munkáját végig figyelemmel kísérő kijelölt kapcsolattartója részletesen dokumentálja a naplókban. A fejlesztő munkájának megkezdése előtt a rendszerről mentést kell készíteni. A fejlesztő munkájának befejezése után az éles rendszerhez adott jogosultságát haladéktalanul meg kell vonni.

11.1.5 Külső erőforrások kezelése

A külső üzemeltetői erőforrások (harmadik fél) bevonása esetén pontosan meg kell határozni a feladatok és a felelősségek megosztását, a korábban meghatározott biztonsági követelmények rögzítése mellett.

11.1.6 Kontrollok

A fejlesztési folyamatok teljes szakasza alatt a Hivatal kijelölt kapcsolattartója felügyeli és ellenőrzi a munkálatokat. Minden kritikus lépésről tájékoztatja a Hivatal vezetőjét.

11.1.7 Ellenőrzés

Az informatikai biztonsági megbízott ellenőrzi a fejlesztési folyamatok alatt eseti jelleggel, hogy megfelel-e az ügymenet az IBSZ szabályainak.

11.2 Végpont védelem

11.2.1 Végpontvédelem követelményei

A hálózati végpontok és az azokra csatlakoztatott eszközök végpont védelméről minden informatikai eszköz esetében gondoskodni kell. A védelem során gondoskodni kell, hogy:

- illetéktelenek ne férjenek szabadon maradt hálózati végpontokhoz,
- illetéktelenek ne léphessenek be a számítógépekbe,
- ne legyen támadható vezeték nélküli vagy vezetékes kapcsolat a rendszerben,
- a felhasználók ne tölthessen le, illetve ne másolhassanak ki engedély nélkül adatot a számítógépekről.

A Hivatal területén hálózati végpontot csak ellenőrzött körülmények között lehet létesíteni. Az ügyfélforgalom bonyolítására szolgáló helyeken (pl. ügyfélváró, folyosó) a használaton kívüli végpontoknak az aktív, és passzív hálózati elemekkel (switch, hub stb.) való kapcsolatát meg kell szüntetni, a strukturált hálózatról le kell választani.

A Hivatal belső informatikai rendszeréhez való, nyilvános internet felőli hozzáféréshez az informatikai biztonsági megbízott felé az adott szervezeti egység vezetője által benyújtott írásos és indoklással ellátott kérelemmel igényelhető jogosultság. A kapcsolat kiépítésének hardveres és szoftveres követelménye van, amely költségekkel párosul.

Vezeték nélküli kapcsolat a Hivatal területén csak a Hivatal vezetőjének engedélyével létesíthető egyedi tervezés, megvalósítás, nyilvántartás, ellenőrzés mellett.

A vezeték nélküli kapcsolatot legalább WAP2-PSK titkosítással kell létrehozni.

11.2.2 Végpontvédelem alá eső végponti eszközök

Minden olyan asztali vagy hordozható számítógépet, végpont védelemmel kell ellátni, mely alkalmas: hálózathoz csatlakozásra, adatok kimásolására és továbbítására, USB adathordozó eszköz csatlakozásra, vezeték nélküli kapcsolatok létesítésére. A vírusvédelmi rendszert a Hivatal minden számítógépére telepíteni kell. Nem engedélyezett olyan eszközt az informatikai hálózathoz csatlakoztatni, amelyen nincs telepítve vírusvédelem. A használaton kívül helyezett informatikai berendezés és a Hivatal összes hálózata közötti összeköttetést meg kell szüntetni. Bármilyen eszközt csak a kijelölt informatikus csatlakoztathat az informatikai hálózatra. Bármilyen eszközt (kivéve a mobil eszköz) csak a kijelölt informatikus távolíthat el az informatikai hálózatról. Idegen, nem hivatali illetve helyi önkormányzati tulajdonú, nem a hivatal illetve helyi önkormányzati által bérelt, használt eszköz csatlakoztatása nem engedélyezett.

11.2.3 Végpontvédelem szabályozása

A végpontvédelmi intézkedések nem akadályozhatják az alapvető működési feladatokat ezért biztosítani kell a munka során használt engedélyezett (nyilvántartott) és a feladat végrehajtásához szükséges eszközök (nyomtató, szkenner, fényképezőgép, kamera stb.) zavartalan működését. Biztosítani kell, hogy hetente minden, víruskereső szoftverrel ellátott szerveren és kliensen teljes víruskeresés fusson le, de lehetőleg különböző időpontokban.

11.2.4 Kontrollok

A kijelölt informatikus jogosult a vírusvédelmi rendszer telepítésére, beállítására, eltávolítására, ellenőrzésére, frissítésére a munkaállomásokon és szervereken.

A kijelölt informatikusnak kötelessége gondoskodni a vírusvédelmi rendszer naprakészen tartásáról és működtetéséről.

11.2.5 Ellenőrzés

A kijelölt informatikus általános feladatai:

- elvégzi a vírusvédelmi szoftverek megfelelő beállítását, a rendszer konfigurálását,
- ellenőrzi a vírusvédelmi rendszerek rendszeres frissítését,
- listát készít a rendszeresen manuálisan frissítendő számítógépekről (pl. mobileszközökről, a nyilvántartás szerinti eszközöket frissíti, és a frissülés megtörténtét ellenőrizi a számítógépeken és a vírusvédelmi szoftver program nyilvántartásaiban,
- megbizonyosodik róla, hogy az informatikai rendszerébe kapcsolt munkaállomáson, szerveren, egyéb informatikai eszközön a vírusvédelmi program telepítve van, és a vírusdefiníciós adatbázisa naprakész,
- tájékoztatja a felhasználókat a vírusvédelmi eszközök működéséről, használatáról,
- megvizsgálja a felhasználók jelzése alapján a vírusgyanús eseteket,
- elvégzi a vírusfertőzés bekövetkeztekor a szükséges vírusmentesítési lépéseket,
- figyelemmel kíséri a vírusvédelem hatékonyságát.

11.3 Adatmentési és naplózási feladatok

11.3.1 Adatmentés és telepítő szoftvermentés

A mentési és visszaállítási eljárásokat úgy kell kialakítani, hogy az üzemeltetett rendszerek előre nem látható esemény (katasztrófa, vagy hardver, illetve szoftver meghibásodása, emberi mulasztás) bekövetkezte után, szükség esetén helyreállíthatók legyenek, biztosítva a folyamatos napi működést. Biztosítani kell, hogy az üzemidő kiesés, adatsérülés, adatvesztés minimális legyen. A mentések archiválások elvégzéséhez nagy tárolókapacitású mentőegység szükséges, amelyek beszerzéséről gondoskodni kell.

11.3.2 Naplózás

Tűzvédelmi mentésről rendszeres mentési naplót kell vezetni a kijelölt informatikusnak.

Egyedi mentésnél a mentés elvégzéséről mentési és archiválási adatlapot kell készíteni, és a mentési és archiválási nyilvántartáshoz kell csatolni. A mentett állomány törlését, ha szükséges csak ez után lehet elvégezni.

11.3.3 Naplók kezelésének szabályai

Tűzvédelmi mentésről rendszeresen a napi mentés után azonnal bejegyzést kell tenni a naplóba.

Egyedi mentésnél a mentés elvégzésével, illetve az adathordozó elhelyezésével egy időben kell kitölteni az adatlapot és ezt követően az adatlapot a mentési és archiválási nyilvántartáshoz felvezetni.

Az adatlapokat és a nyilvántartást a mentés helyétől és az adathordozók tárolási helyétől különböző helyen kell elhelyezni.

11.3.4 Kontrollok

Az adatlapok tartalmi változásakor (mentés, selejtezés) a mentett állomány szakmai felelősét tájékoztatni kell, és ennek tényét rögzíteni az adatlapon (aláírással igazolja a tudomásul vételt).

11.3.5 Ellenőrzés

A mentéssel kapcsolatos adatlapokat és nyilvántartást az informatikai biztonsági megbízott legalább évente egyszer szúrópróbaszerűen ellenőrzi és a Hivatal vezetőjét jelentésben tájékoztatja az ellenőrzés eredményéről.

11.4 Hálózat menedzsment

11.4.1 Hálózat felügyelete

A hálózat felügyeletét a kijelölt informatikus látja el, együttműködve a NISZ, KEKKH és a szakigazgatási szervek szakmai irányító szerveinek munkatársaival.

11.4.2 Dokumentálás

A hálózatfelügyelettel kapcsolatos események dokumentálásáról gondoskodni kell.

11.4.3 Kontrollok

A hálózat feletti kontrollt a kijelölt informatikus, a NISZ, KEKKH és a szakigazgatási szervek szakmai irányító szerveinek munkatársai közösen gyakorolják.

11.4.4 Ellenőrzés

A hálózat feletti ellenőrzést a kijelölt informatikus, a NISZ, KEKKH és a szakigazgatási szervek szakmai irányító szerveinek munkatársai közösen gyakorolják.

11.5 Adathordozók kezelése és biztonsága

11.5.1 Adathordozók és eszközök kezelése és tárolása

A mobil adathordozó eszközök (pl. pendrive, külső HDD) kiadása, állapotváltozása, visszavétele során a kijelölt informatikusnak az igénylő által benyújtott, kitöltött és engedélyezett „Mobil adathordozó eszköz engedélyezése adatlapot” az „Adathordozó nyilvántartáshoz” kell felvezetni és csatolni. Az eszközön szerepelnie kell az adathordozó egyedi azonosítójának (pl.: leltári szám, gyári szám, vagy képzett azonosító).

A mentés elkészítéséhez használt adathordozó típusok kiválasztásánál az alábbiakat kell figyelembe venni

- a mentendő adatmennyiségnek megfelelő tárolókapacitás,
- a megfelelő adatmegőrzési idő (legalább 5 év, különleges beavatkozás, speciális eljárások alkalmazása nélkül),
- megfelelő ellenállás a környezeti viszonyoknak (hőmérséklet, páratartalom, fény stb.),
- adat visszaállítás esetére szükséges eljárások és eszközök rendelkezésre állása.

11.5.2 Mentések tárolása

A Hivatal elektronikus szoftvereinek telepítő készletei, illetve adatainak mentésére és archiválására használt adathordozói, a mentés dokumentuma, a helyreállítást biztosító leírások:

- biztonságos módon, a mentés helyétől (telepítés helyétől) különböző helyen elhelyezett lemez fémszekrényben (tűzbiztos szekrény ajánlott),
- vagy amennyiben lehetőség nyílik rá a törekedni kell a mentés helyétől (telepítés helyétől) különböző tűzszakaszban elhelyezkedő helyiségben tárolandók és az elhelyezésükre: megfelelő mechanikai védelemmel (pl. ablakráccsal, biztonsági zárral) ellátott, elektronikus védelemmel (riasztórendszerbe integrált, füst- és vagy hőérzékelővel) ellátott, lehetőleg regisztrált kulcsfelvétellel hozzáférhető, közművezetékektől mentes helyiséget kell kijelölni.

11.5.3 Dokumentálás

A mobil adathordozó eszközöket az engedélyezési adatlapokon és a kapcsolódó nyilvántartásban kell nyilvántartani.

Az operációs rendszerek, programok, eszközkezelők telepítő állományait tartalmazó adathordozóiról szoftvernyilvántartást kell vezetni, mely történhet digitális formában is, illetve az informatikai nyilvántartás keretében.

11.5.4 Kontrollok

A mentések, archívumok tárolási ideje alatt az adatok integritásának megőrzése a kijelölt informatikus feladata.

11.5.5 Ellenőrzés

A kijelölt informatikus feladata az adattárolók műszaki állapotának, tárolásának, ellenőrzése.

11.6 Adathordozók selejtezésének biztonsági szabályai

A kijelölt informatikusnak, az adathordozó típusától, valamint a rögzítés módjától függően eltérő időközönként, de évente legalább egyszer ellenőrizni kell az adathordozó használhatóságának mértékét. Az adathordozók természetes fizikai romlása és elhasználódása következtében előálló biztonságcsökkenés miatt a működtetendő programokról és hasznos adatokat tartalmazó adathordozókról, ha az adathordozó megközelíti (élettartam -10%) a gyártó által javasolt felhasználási időtartamot, és az adathordozót nem lehet selejtezni, akkor másolatot kell készíteni róla.

Ha az adathordozó selejtezhető, a selejtezéshez az érintett szakterület képviselőjének hozzájárulása szükséges, melyet az adathordozóhoz kapcsolódó mentési és archiválási adatlapon aláírásával hitelesít. A selejtezés tényét a mentési és archiválási nyilvántartásában is be kell jegyezni. Az archiválásra kerülő adatok körét és rendszerét a mentési rend határozza meg.

12. A rendszerek hozzáférési jogosultságainak kezelése

12.1 Hozzáférés kezelési szabályok

12.1.1 Általános szabályok

A szervezeti egység vezetője írásban köteles tájékoztatni az informatikai biztonsági megbízottat a felhasználókra vonatkozó minden változásról (felvétel, munkakörváltozás, munkaviszony megszűnés), mely az informatikai vagy kommunikációs rendszert érinti. A felhasználó részére a szervezeti egység vezetője kéri meg a szakalkalmazásokhoz történő hozzáférések kiosztást, törlését.

A szervezeti egységek vezetői a felhasználóval kapcsolatban felmerülő egyéb informatikai igényeket írásban (e-mailben vagy levélben) nyújtják be az informatikai biztonsági megbízott és a kijelölt informatikus felé pl.:

- informatikusi beavatkozás igénylés,
- informatikai eszközigénylés, mozgatás, áthelyezés és átvezetés,
- informatikai rendszerhez hozzáférési változási igény (igénylés, módosítás vagy törlés).
- alkalmazástelepítési vagy - eltávolítási igény,
- inaktívvá válás esetén újra aktiválás kérése,
- munkavégzési hely vagy feladat változása esetén egyedi vagy tömeges eszközmozgatási és telepítési igény,
- hálózattal kapcsolatos igény (kiépítés, bővítés, elbontás),

- informatikai szolgáltatáshoz, alkalmazáshoz, hálózati mappához (könyvtár) való hozzáférés, valamint ezekkel kapcsolatos jogosultság változása (igénylés, módosítás vagy törlés).

A kijelölt informatikus elvégzi az informatikai rendszerben:

- az adatok átvezetését, a szükséges beállításokat,
- letiltja vagy engedélyezi az informatikai szolgáltatásokat (pl.: levelezés, internet, hálózati mappa elérése, nyomtatás stb.),
- szükség esetén, továbbítja az illetékes szervezetek, a szakigazgatási szervek központi szervei, központi informatikai szolgáltatók felé az előírt információkat,
- elvégzi a jogosultságok nyilvántartását:
    - amennyiben az adott rendszerből az informatikus által lekérdezhető, akkor a jogosultságok rendszerben történő átvezetésével,
    - egyéb esetben külön (elektronikus vagy papíralapú) jogosultsági nyilvántartás.
- a kijelölt informatikus átadja, átveszi, átvezeti, beállítja, törli, az informatikai eszközöket és jogokat a belépő, kilépő, meglévő felhasználóknak.
- elvégzi az informatikai eszközök nyilvántartására vonatkozó alábbi teendőket:
    - az eszközök mozgásáról eszköz átadás-átvételi adatlapot nyomtat,
    - a kinyomtatott adatlapot az érintett felhasználóval aláírattatja,
    - az aláírt adatlapot átadja az érintett felhasználónak, valamint a változások analitikus nyilvántartáson történő átvezetése érdekében a leltárvezetésért felelős dolgozónak.
- kilépő dolgozó vagy munkakör változás esetén elvégzi és igazolja a nyilvántartás szerint a dolgozó nevén lévő eszközök átvezetését, valamint jogosultságainak kivezetését a rendszerből.

ASP rendszer bevezetéséhez kapcsolódóan a szervezet vezetőjének irányítása alatt:

- A Keretrendszerben (ASP.KERET) „Tenant” került létrehozásra és felvételre került a Tenantadminisztrátor.
- Adatbázisok létrehozása a szakrendszerekben.
- Tenanat felhasználók felvétele és szerepkörök összerendelése.
- Tanúsítványok elkészítése és hozzárendelése.
- Tanúsítványok kiosztása a felhasználóknak.

A tenant adminisztrátorok rendszerbe történő „felvitelét” az ASP Központ végzi.

12.1.2 Authentikáció

A Hivatal informatikai rendszerét úgy kell kialakítani és olyan szoftvereket szabad használni, hogy a rendszerébe felhasználó csak authentikáció után jelentkezhessen be.

12.1.3 Authorizáció

A Hivatal informatikai rendszerébe csak az engedélyezett felhasználónak lehet azonosítót és jelszót adni.

12.1.4 Szerepkörök

Hálózati rendszergazdai jogosultság kizárólag a Hivatal vezetőjének írásos engedélyével adható.

Hálózati felhasználói jogosultságot a szervezeti egység vezetőjének írásban tett kérelmére a kijelölt informatikus adja meg.

Számítógépen helyi (lokális) rendszergazdai jog csak a Hivatal vezetőjének egyedi írásos engedélyével, nem személyhez kötött módon adható kizárólag üzemeltetési indok alapján.

12.1.5 Jogosultsági mátrix

Hálózati rendszergazdai jogosultság kizárólag a rendszergazdai feladatokat ellátó kijelölt informatikus részére adható.

Az azonosítónak egyedinek, személyhez kapcsolhatónak kell lennie. Az induló jelszó kiosztására, az adminisztrátori jelszó kezelésére ugyanazok a szabályok érvényesek, mint a felhasználói jelszó kezelésére.

A Hivatal vezetőjének egyedi engedélye alapján kap valamely belső vagy külső munkatárs adminisztrátori/üzemeltetői jogokat.

A nem személyhez köthető adminisztrátori (root, superuser, teljes jogú adminisztrátor stb.) azonosító ne legyen napi használatban, az csak olyankor használható, amikor elengedhetetlen.

12.1.6 ASP jogosultság:

A tenant adminisztrátorok rendszerbe történő „felvitelét” az ASP Központ végzi. A privilegizált joggal rendelkező felhasználók a munkatársaik részére további jogosultságot tudnak osztani, ezen tevékenységet a jegyző felelősségi és hatáskörébe tartozóan tudják végezni.

A rendszer használata során a privilegizált joggal rendelkező munkatársak a privilegizált jog használatát munkavégzésükhöz csak indokolt esetben használhatják.

A privilegizált joghoz tartozó bejelentkezési azonosítókat zárt borítékban, biztonságos helyen kell tárolni.

A nem személyhez köthető adminisztrátori azonosítókat és jelszavakat lezárt, és az adminisztrátor által aláírt borítékban a Hivatal vezetője őrzi elzártan.

12.2 A felhasználók hozzáférési jogainak kezelése

12.2.1 Felhasználó nyilvántartás

A Hivatal informatikai rendszerében felvett és ott jogosultságokat kapott felhasználókat, a jogosultság nyilvántartás segítségével annak vezetésére kötelezett, kijelölt informatikus tartja nyilván és naprakészen.

12.2.2 Felhasználói privilégiumok kezelése

A felhasználók hálózati mappákhoz való hozzáférésének jogosultsági szintjeit az adott felhasználó szervezeti egységének vezetője állapítja meg (adja, módosítja, elveszi) a benyújtott kérelemben, amit a kijelölt informatikus a dokumentum szerint beállít.

Az informatikai eszközöket, ha hozzáférhetősége vagy fontossága miatt indokolt (számítógép, nyomtató, multifunkciós eszköz, switch stb.), és ha az eszköz operációs rendszere megengedi, valamint a hálózathoz való hozzáférést minden esetben felhasználói azonosítóval (felhasználói név + jelszó) kell védeni.

12.2.3 Felhasználói jogosultság- és jelszókezelés

A felhasználók részére jogosultságot, csak az „12.1.1 általános szabályok” részben leírtak szerint lehet igényelni és kiosztani, valamint beállítani.

Jelszavak kezelése a 8.1.2. „A jelszókezelés általános szabályai” részben leírtak szerint kell, hogy történjen.

A felhasználók azonosítása egyedi, jellemző, ellenőrizhető és hitelesítésre alkalmas, úgynevezett felhasználói azonosító használatával valósul meg az informatikai rendszerben (felhasználói azonosító = felhasználói név + jelszó).

A javasolt névkonvenció, a felhasználói név képzésének szabálya: „vezeteknev.keresztnev” ékezet nélkül. Ha felhasználónak három neve van, akkor keresztnév helyére az általa választott, használni kívánt nevet kell írni. Név előtagot, illetve titulust nem kell szerepeltetni. Azonos nevű személyek esetén a keresztnév utáni sorszámmal kell egyedivé tenni a felhasználói nevet.

12.2.4 Felhasználói elérési jogok felülvizsgálata

A felhasználói jogosultságokat a kijelölt informatikusnak az érintett szervezeti egység vezetőkkel évente felül kell vizsgálni.

Az érintett szervezeti egység vezetőnek bejelentési jogosultsága van, ha a felhasználóval kapcsolatban munkaköri, vagy munkafeladat változás merül fel. Változás esetén az általános szabályok értelmében, bejelentést kell tennie.

12.2.5 Az adminisztrátori/üzemeltetői jogok és felülvizsgálatuk

Az adminisztrátori jogokat személyi változás, munkaköri változás esetén és feltétel nélkül évente felül kell vizsgálni. A Hivatal vezetőjének engedélye alapján kaphat valamely belső vagy külső munkatárs adminisztrátori/üzemeltetői jogokat.

12.2.6 Felügyelet nélkül hagyott felhasználói eszközök felelőssége

A nem használt (tartalék, javításra váró vagy javításból érkezett informatikai eszközök) tárolásáról a kijelölt informatikus gondoskodik.

A rövid, eltávozással járó szünet (1 óra vagy kevesebb) idejére a számítógépet a felhasználónak a hozzáférés ellen zárolni kell.

A munkaállomást illetéktelen személy (pl. ügyfél) jelenléte mellett a felhasználó nem hagyhatja felügyelet nélkül.

A használaton kívüli állapotban lévő (lekapcsolt) eszközöket a felhasználó csak illetéktelen személy elől elzárt helyen hagyhatja.

12.2.7 Dokumentálás

Felhasználó igények és jogosultságok bejelentése az erre szolgáló adatlapon történik.

Az adatlapokat a jogosultsági nyilvántartásban kell felvezetni.

12.2.8 Kontrollok

A kijelölt informatikus feladata az informatikai rendszerek oly módon történő konfigurálása, hogy a belépések és a belépési kísérletek a teljes adattartalommal naplózásra kerüljenek.

A szervereken és számítógépen tárolt naplókat a kijelölt informatikus a rendszer karbantartása során szúrópróbaszerűen vagy módszeresen ellenőrizheti. Biztonsági eseményt követően a naplókat az eseménnyel egyező időszakra vonatkozóan ellenőrizni és archiválni kell.

12.2.9 Ellenőrzés

A jogosultságok nyilvántartását és jelszókezelést az informatikai biztonsági megbízott évente egyszer szúrópróbaszerűen ellenőrzi, és a Hivatal vezetőjét jelentésben tájékoztatja az ellenőrzés eredményéről.

12.3 A hálózati hozzáférés védelme

12.3.1 Hálózati szolgáltatások használatának politikája

A Hivatal informatikai rendszerének elemeit adminisztrálási célból az internet felől elérni csak titkosított kapcsolaton keresztül, legalább kétkomponensű authentikáció után megengedett. Az ilyen kapcsolat kiépítésére a Hivatal vezetője adhat engedélyt.

Minden adminisztrátori tevékenységnek egyértelműen személyhez köthetőnek kell lennie.

12.3.2 Kötelező elérési útvonal

Külső hálózatról az informatikai rendszerek csak az erre a célra dedikált védelmi rendszeren (tűzfalak, zónák stb.) keresztül lehetnek elérhetők.

12.3.3 Hálózati részek elválasztása

Az internet és a hivatali rendszerek különböző zónái között a kijelölt informatikus és a szakmai irányító szervek közösen gondoskodnak arról, hogy a tűzfalak biztosítsák az elválasztást.

12.3.4 Hálózati kapcsolatok és a routolás vezérlése

Az internet és az informatikai rendszerek különböző zónái között a hálózaton routolás történjen.

12.3.5 Dokumentálás

A hálózati hozzáféréseket érintő döntésekről és eseményekről, valamint beállításokról írásos feljegyzést kell készíteni az Hivatal vezetője felé a kijelölt informatikusnak, melyet az informatikai biztonsági megbízott archivál.

12.3.6 Kontrollok

A hálózati hozzáférések felett a kijelölt informatikus és szakmai irányító szervek közösen gyakorolnak felügyeletet.

12.3.7 Ellenőrzés

Az informatikai biztonsági megbízott, vagy a Hivatal vezetője által megbízott más személy évente legalább egyszer, gyakorlati szúrópróba-szerű auditot végez. Ennek során az IBSZ hatálya alá tartozó területeken a rendszer sebezhetőségére irányuló támadáspróbával meggyőződik a hálózati integritás állapotáról. Az audittal megbízott személy a teszt eredményét dokumentálja.

Az informatikai biztonsági megbízott az éves ellenőrzések során szúrópróbaszerűen ellenőrzi a hálózattal kapcsolatos dokumentumokat és azok lényeges elemeit éves jelentésében szerepelteti.

12.4 Az operációs rendszer hozzáférés védelme

12.4.1 Felhasználó jogosultságkezelés

Minden felhasználó köteles a saját felhasználói nevével használni a Hivatal informatikai eszközeit.

A számítógép-programokhoz, rendszerprogramokhoz és adatokhoz csak a kijelölt informatikus számára megengedett hozzáférés biztosítása. Ezt az operációs rendszerek védelmi rendszerének kell biztosítania, és csak ennek megfelelő operációs rendszereket szabad használni.

Az informatikai központban működő rendszerek rendszergazdai és adminisztrátori jogait nyilvántartó dokumentumot a Hivatal vezetője hagyja jóvá. Ebből egy-egy példányt kell tárolni minden érintett informatikai központban.

12.4.2 „Single sing-on (SSO)”

Automatikus, a felhasználó számára észrevétlen beléptetés minden jelszó alapú alkalmazásba, ami lehetővé teszi, hogy egy adott rendszerbe való belépéskor mindössze csak egyszer azonosítsa magát a felhasználó és ezután a rendszer minden erőforrásához és szolgáltatásához további authentikáció nélkül hozzáfér.

Teljes informatikai megfelelőség biztosítása. (Tűzfal, vírusvédelem)

A Hivatali Kapu használatával kapcsolatos szabályokat „A Hivatali Kapu használatáról” kiadott szabályzat tartalmazza.

12.4.3 Biztonsági Policy

Az informatikai rendszerbe belépő felhasználókhoz rendelt biztonsági policy-k meghatározása és beállítása az informatikai biztonsági megbízott és a szakmai irányító szervek közös döntése és akarata szerint kell, hogy megvalósuljon.

12.4.4 Jogosultságigénylés

A jogosultságok igénylését a 12.1.1. pont alatti részben leírtak szerint kell megvalósítani.

12.4.5 Dokumentálás

A hozzáféréseket érintő döntésekről és eseményekről, valamint beállításokról írásos feljegyzést kell készíteni az Hivatal vezetője felé a kijelölt informatikusnak, melyet az informatikai biztonsági megbízott archivál.

12.4.6 Kontrollok

A jogosultságok engedélyezési folyamata során az engedélyező és jóváhagyó személyek gyakorolnak kontrollt az engedélyek jogossága és megfelelősége felett.

12.4.7 Ellenőrzés

Az informatikai biztonsági megbízott az éves ellenőrzések során szúrópróbaszerűen ellenőrzi a jogosultság igénylések jogosságát és megfelelőségét, valamint a nyilvántartások naprakész korrekt vezetését, és tesz jelentést a Hivatal vezetője felé az ellenőrzések tapasztalatairól.

ASP rendszerbe történő belépés, authentikáció

Az ASP elsődleges authentikációs eszköze az eSZIG. A használatához alkalmazott kártyaolvasó a hatóság által bevizsgált elfogadott eszköz.

A személyi igazolványkártyát csak a tulajdonosa használhatja, azt ASP rendszer authentikációs folyamat céljából másnak átadni tilos!

12.5 Az alkalmazások hozzáférés védelme

12.5.1 Felhasználó jogosultságkezelés

A felhasználó csak a számára meghatározott információkhoz férhet hozzá. Minden egyéb hozzáférési kísérletet biztonsági eseményként kell kezelni. A jogosultságokat a 12.1.1. pont alatti részben leírtak szerint kell megvalósítani.

12.5.2 Single sign-on (SSO)

Az informatikai rendszerbe belépő felhasználókhoz kapcsolt Single sing-on (hálózati authentikáció, egypontos bejelentkezés több alkalmazásba) biztosítása az érintett alkalmazások üzemeltetőjének és a hálózat üzemeltetőjének megállapodása alapján történik. A megállapodásban kell rögzíteni a beállítással kapcsolatos feltételeket.

Új, saját fejlesztésű rendszerek bevezetésekor a Single Sign-On módszer alkalmazására kell törekedni.

12.5.3 Biztonsági Policy

Az informatikai rendszerbe belépő felhasználókhoz rendelt biztonsági policy-k meghatározása és beállítása az informatikai biztonsági megbízott és a szakmai irányító szervek közös döntése és akarata szerint kell, hogy megvalósuljon.

12.5.4 Jogosultságigénylés

A jogosultságok igénylését a 12.1.1. pont alatti részben leírtak szerint kell megvalósítani.

12.5.5 Dokumentálás

A jogosultság igényléseket a kijelölt informatikusa továbbítja az alkalmazás üzemeltetője felé (a szükséges formában), majd az adatlapokat a jogosultsági nyilvántartásba felvezeti.

12.5.6 Kontrollok

A jogosultságok engedélyezési folyamata során az engedélyező és jóváhagyó személyek gyakorolnak kontrolt az engedélyek jogossága és megfelelősége felett.

12.5.7 Ellenőrzés

Az informatikai biztonsági megbízott az éves ellenőrzések során szúrópróbaszerűen ellenőrzi az alkalmazáshoz igényelt jogosultság igénylések jogosságát és megfelelőségét, valamint a nyilvántartások naprakész korrekt vezetését és tesz jelentést a Hivatal vezetője felé az ellenőrzések tapasztalatairól.

12.6 A távmunka hozzáférés szabályozása

12.6.1 A távmunka szabályai

A Hivatal hálózatában távmunka végzést a Hivatal vezetője engedélyezhet a megfelelő informatikai biztonság biztosítása mellett, indokolt esetben, írásbeli kérelem alapján.

12.6.2 A belső és külső felhasználók

A Hivatal hálózatába bejelentkező személyek (külső és belső felhasználó) felett az informatikai biztonsági megbízott gyakorol kontrollt a nyilvántartásain és ellenőrzésein keresztül.

12.6.3 A távmunka biztonsági követelményei

A Hivatal hálózatában csak a Hivatal vezetőjének engedélyével, az általa biztosított eszközökkel az általa megadott módon és az alábbi biztonsági követelmények betartása mellett végezhető távmunka:

- a távmunkához a Hivatal tulajdonában lévő eszközt kell használni, és az eszközt védeni kell a megfelelő biztonsági és vírusvédelmi szoftverekkel,
- nem engedélyezett a távmunkához használt eszközt más célra használni.

12.6.4 A távmunka biztonsági eszközei

A távmunka eszközeinek és beállításainak feltételei meg kell, hogy feleljenek a Hivatalon belüli használatra előírt biztonsági feltételeknek.

12.6.5 Dokumentálás

A távmunka igénylések és engedélyezések levelezései és a megfelelő adatlapok képezik a távmunka dokumentációját.

12.6.6 Kontrollok

A távmunka engedélyezési folyamata során az engedélyező és jóváhagyó személyek gyakorolnak kontrolt az távmunka jogossága és megfelelősége felett.

12.6.7 Ellenőrzés

Az informatikai biztonsági megbízott az éves ellenőrzések során szúrópróbaszerűen ellenőrzi a dokumentációt. Megszemléli a távmunkához biztosított eszközt, és jelentést tesz a Hivatal vezetője felé az ellenőrzések tapasztalatairól.

12.7 A rendszer hozzáférés és használat monitorozása

12.7.1 A rendszer használat monitorozása

A kijelölt informatikus a Hivatal informatikai rendszerének megfelelő működése és biztonsága érdekében a számítógépes hálózatot, valamint az internet szolgáltatást monitorozhatja.

12.7.2 Eseménynapló

A rendszerekben az operációs rendszerek, az adatbázis kezelő és az alkalmazás esemény és hiba naplózását aktív állapotban kell tartani.

Minden szerverről a kijelölt informatikusnak digitális, vagy papír alapú eseménynaplót kell vezetnie, melyben rögzíti a szerverrel kapcsolatos szoftveres és hardveres beavatkozásokat és eseményeket (telepítés, frissítés, hibajelzés, riasztása, leállás, lemerevedés, szerelés, javítás, bővítés stb.).

12.7.3 A rendszer órák szinkronizálása

A rendszer valamennyi, időinformáció kezelésére alkalmas elemének egységes időalapot kell biztosítani.

12.7.4 Dokumentálás

A rendszer monitorozása során jegyzőkönyvet kell készíteni a vizsgált időszak és terület, valamint a tapasztalatok tekintetében.

Az informatikai központok belépési naplóit és a szerver eseménynaplókat naprakészen kell vezetni.

12.7.5 Kontrollok

A rendszer monitorozása során be kell tartani az adatvédelemre és a személyiségi jogokra vonatkozó törvényi előírásokat.

12.7.6 Ellenőrzés

Az informatikai biztonsági megbízott az éves ellenőrzések során szúrópróbaszerűen ellenőrzi a naplókat és jegyzőkönyveket. Tapasztalatairól jelentést tesz a Hivatal vezetőjének.

13. A rendszerfejlesztés és követés biztonsági szabályai

13.1 A rendszerek biztonsági követelményei

13.1.1 Az elemzés és a specifikáció biztonsági követelményei

A meglévő szoftverek továbbfejlesztését vagy új programok bevezetését a szakmai területek vezetője írásos fejlesztési igénnyel kezdeményezheti.

A Hivatal számára szoftverek bevezetését, fejlesztését és az általa használt szoftverek továbbfejlesztését a Hivatal vezetőjének engedélyével és hozzájárulásával lehet végezni.

Az integrált szolgáltatást nyújtó kész szoftverek a Hivatal döntése alapján történő vásárlásánál, valamint a Hivatal saját fejlesztésű alkalmazásai esetében az erre épülő informatikai rendszerek bevezetésének tervezésénél az alábbiak szerint kell eljárni:

Írásban meg kell határozni a tervezett rendszer által nyújtandó szolgáltatások körét.

Meg kell tervezni a rendszer biztonsági modelljét, amelyben az alapvető védelmi igényeket szövegesen is rögzítik.

A hardver és szoftver komponensekkel, valamint az adatfeldolgozás folyamatával kapcsolatos adatbiztonsági elvárásokat meg kell fogalmazni.

Meg kell tervezni az információbiztonsági rendszer működtetéséhez szükséges feltételrendszert. El kell készíteni az adatok mentésének és meghatározott idejű megőrzésének előírását,

A biztonsági szempontok figyelembe vételével megvalósítási tanulmányt és rendszertervet kell készíteni, amit a megbízó, a fejlesztő és az informatikai biztonsági megbízott egyeztetés után elfogad.

13.1.2 A rendszerfejlesztés biztonsági követelményei

A Hivatal szervereihez és alkalmazásaihoz hozzáférést külső vagy belső fejlesztőnek fejlesztési, tesztelési célból az informatikai biztonsági megbízott adhat.

A Hivatal hálózatán a központi szervek által fejlesztett szoftverek tervezésében, fejlesztésében, tesztelésében, bevezetésében a Hivatal munkatársai a Hivatal vezetőjének tudtával és engedélyével vehetnek részt.

A szakigazgatási szervek szakmai irányító szerveinek, illetve a szakigazgatási szerveknek a Hivatal hálózatában és eszközein történő új szakmai rendszer bevezetése esetén a szoftvertelepítéssel kapcsolatos igényüket a Hivatal vezetője felé kell benyújtani.

13.1.3 A rendszer változáskezelésének biztonsági követelményei

Az informatikai rendszerben változtatásokat az alábbi elvek betartása mellett lehet tenni:

- A Hivatal által üzemeltetett rendszerprogramok (alapszoftver) illetve a felhasználói programok telepítését a központi számítógépekre (szerverekre) és munkaállomásokra csak a kijelölt informatikus végezheti el. Jogosultságot a Hivatal vezetője engedélyezhet.
- Az alapszoftverrel kapcsolatos bármely konfigurálási, hangolási műveletet csak a kijelölt informatikus, illetve – előzetes jóváhagyása mellett – az erre felhatalmazott üzemeltető végezhet. Az alkalmazói szoftvereken végzendő, azok bármely funkcióját megváltoztató művelethez a Hivatal vezetőjének engedélye szükséges. A verzióváltás és egyéb, jelentős beavatkozást igénylő hangolás elvégzéséhez a Hivatal vezetőjének engedélye szükséges.
- A felmerült változtatási igényeket kielégítő beállításokat teszt környezetben a Hivatal vezetője által meghatározott időszakon át, munkarendszerűen tesztelni és üzemeltetni kell.
- Teljes körű tesztelési eljárásokkal kell megbizonyosodni a biztonsági modellben megfogalmazott elvárások érvényesüléséről új rendszer bevezetése előtt.
- Próbaüzem és terhelési próbák során meg kell vizsgálni az új rendszer üzembiztonságát és megbízhatóságát még a bevezetés előtt.
- A tesztelésről készített jelentés felhasználásával dönt, a Hivatal vezetője a beállítások, illetve alkalmazások bevezetéséről.
- A Hivatal informatikai rendszerébe beállításokat, illetve alkalmazásokat helyi előzetes tesztelés nélkül csak a központi szakmai irányító szervek alkalmazási igazolása mellett szabad alkalmazni.
- Alapszoftvert és alkalmazói szoftvert csak érvényes, arra vonatkozó licence alapján szabad felhasználni.

13.1.4 Változáskövetési folyamatok

A Hivatal rendszerében a változtatásokat csak a változás folyamatainak dokumentált követésével, és a döntési pontoknál előzetes hatásvizsgálatok (biztonsági, költség) elvégzése után, annak figyelembe vételével lehet végrehajtani, a Hivatal vezetőjének írásos engedélyével.

13.1.5 Az operációs rendszer változásainak technikai felülvizsgálata

A Hivatal rendszerében az operációs rendszer verzióváltásai, illetve szerviz csomagok telepítését, frissítéseket meg kell, hogy előzze az operációs rendszer változásának hatásfelmérése, figyelembe véve a Hivatal munkafeladatait, eszközparkját és hálózati adottságait. A lehetséges kockázatokat és

sérülékenységet meg kell ismerni. A szerviz csomagok és frissítések esetében kockázatok felmérése a frissítéseket menedzselő szervezet feladata.

13.1.6 Álcázott csatornák és „Trójai" programok

A rendszerben használt szoftvereket csak megbízható forrásból (ismert szállítótól) szabad beszerezni az álcázott csatornán keresztüli beavatkozás és „Trójai" programok bejuttatásának kivédésére.

13.1.7 Külső cég által végzett (vállalkozói szerződés keretében) szoftverfejlesztés

A külső céggel végeztetett szoftverfejlesztés esetén rögzíteni kell a tulajdonosi, használati és licenc jogokat. Rögzíteni kell a követés módját, formáját és minimális időtartamát.

A Hivatal rendszerében végzett, külső cég általi szoftverfejlesztés esetén vizsgálni kell:

- az informatikai biztonsági veszélyeket és kockázatokat a fejlesztés során,
- a fejlesztő szervezet megbízhatóságát,
- a fejlesztésre vonatkozó szerződésben a fejlesztőnek garanciát kell vállalnia arra, hogy a fejlesztett alkalmazás nem jelent kockázatot az informatikai biztonságra.

13.1.8 Dokumentálás

A Hivatal rendszerben végzett rendszerfejlesztés minden elemét (felmérés, javaslat, tesztelés, döntés, bevezetés, monitoring) dokumentálni kell. A külső cég által végzett fejlesztést csak szigorú szerződési feltételek között szabad végezni.

13.1.10 Kontrollok

A Hivatali rendszerben végzett rendszerfejlesztés felett a Hivatal vezetője gyakorol felügyeletet. Az általa kijelölt informatikus végzi a kapcsolattartói feladatokat.

13.1.11 Ellenőrzés

Az informatikai biztonsági megbízott az éves ellenőrzések során szúrópróbaszerűen ellenőrzi a rendszerfejlesztési dokumentációkat, és jegyzőkönyveket készít a tapasztalatairól a Hivatal vezetőjének.

13.2 Titkosítási tevékenységek

13.2.1 Titkosítás szabályai

Az alkalmazott kriptográfiai eszközöknek meg kell felelniük a magyar törvényi előírásoknak.

13.2.2 Nyílt kulcsú titkosítás

Nyílt kulcsú titkosítást csak a Hivatal vezetőjének engedélyével lehet alkalmazni. A titkosítási rendszer kialakítása és a rendszer nyilvántartása a kijelölt informatikus feladata.

A nyílt kulcsú titkosítás eszközeinek és jelszavainak kezeléséért és megőrzéséért a kulcsot alkalmazó felhasználó felelős.

A nyílt kulcsú titkosítás azonosítóit és a titkos kulcsok jelszavait a kijelölt informatikus kezelésében zárt helyen, zárt borítékban kell tárolni. A boríték a Hivatal vezetőjének utasítására bontható fel.

13.2.3 Fájlrendszer tikosítása

A fájlrendszerek titkosítását az informatikai biztonsági megbízott engedélyével lehet alkalmazni a mobil adathordozóknál és mobil informatikai eszközöknél.

A rendelkezése álló szoftver telepítése és beállítása, és a titkosított rendszer használatának nyilvántartása a kijelölt informatikus feladata.

A fájlrendszer titkosítás eszközeinek és jelszavainak kezeléséért és megőrzéséért a felhasználó felelős.

A fájlrendszer titkosításának azonosítóit és jelszavait a kijelölt informatikus kezelésében zárt helyen, zárt borítékban kell tárolni. A boríték a Hivatal vezetőjének utasítására bontható fel.

13.2.4 Adatátvitel titkosítása

Az alkalmazott kriptográfiai eszközöknek meg kell felelniük a magyar törvényi előírásoknak.

13.2.5 Elektronikus aláírás

Elektronikus aláírást, csak a Hivatal vezetőjének engedélyével lehet alkalmazni.

A rendszer nyilvántartása a kijelölt informatikus feladata.

Az elektronikus aláírás eszközeinek és jelszavainak kezeléséért és megőrzéséért a felhasználó felelős.

13.2.6 Kontrollok

Kontrollokat a titkosítási és hitelesítési rendszerek felett a kijelölt informatikus gyakorolja.

13.2.7 Ellenőrzés

A titkosítási és hitelesítési rendszerek alkalmazását az informatikai biztonsági megbízott évente ellenőrzi.

14. Biztonsági kockázatmenedzsment

14.1 Informatikai biztonság kockázatelemzés

A Hivatal informatikai biztonsági megbízottja évente egyszer a rendelkezésre álló információk alapján kockázatelemzést köteles készíteni.

A kockázatelemzés során az egyes veszélyforrások által képviselt kockázatokat kell megállapítani, illetve feltárni. A kockázat meghatározása a veszély megvalósulásának valószínűsége és az okozható kár alapján, vagy más nézőpontból az adott veszélyt képviselő sérülékenység kihasználhatósága és ennek hatása alapján történik.

A Hivatal informatikai biztonsági megbízottja elemzés során a kockázatokat kategóriákba sorolja. A tanulságokat jelentésben tárja a Hivatal vezetője elé.

A Hivatal informatikai biztonsági megbízottja, az Ibtv. 8. § (1) pontja alapján a Hivatal biztonsági osztályba sorolását legalább három évenként, vagy szükség esetén soron kívül, dokumentált módon felül vizsgálja.

14.2 Informatikai biztonság kockázatértékelés

A kockázat elemzésről szóló jelentés alapján a Hivatal vezetője a kockázatokat értékeli, és gondoskodik a megelőzésükhöz szükséges intézkedések meghozataláról.

Az informatikai biztonsági osztályba soroló vizsgálati jelenés alapján a Hivatal vezetője az eredményeket értékeli és gondoskodik a szükséges intézkedések meghozataláról.

14.3 Informatikai biztonság kockázatkezelés

A kockázatkezelési folyamatok során a Hivatal vezetője igénybe veheti külső felek közreműködését.

14.4 Informatikai biztonság kockázatmenedzselés szabályai

A kockázatkezelés lépései:

- kockázatok feltárása, csoportosítása és hatáselemzése,
- szükséges lépések, módszerek meghatározása és hatáselemzés,
- megoldási tervek és alternatívák készítése,
- döntés és megvalósítás,

- monitoring és utóellenőrzés.

A kockázatkezelés szabályai:

- Valós kockázatokat kell figyelembe venni.
- Minden körülményt figyelembe kell venni.
- A súlyosság mértéke szerint kell haladni a kockázat megoldása és elhárítása során.
- A megoldások közül azt a módszert (eszköz kell választani), amelyik a legnagyobb eredményt hozza a legkisebb erőforrás ráfordítással.
- A kockázatkezelésre fordított erőforrások, a védekezés költségei arányosak kell, hogy legyenek a kockázat mértékével.

15. Ellenőrzés

15.1 Az informatikai biztonság dokumentálása

15.1.1 Az Informatikai biztonság dokumentálás szabályai

Az Informatikai biztonság dokumentumaival szemben támasztott követelmények:

- Rendelkezésre állás: a jogosultságok engedélyeztetése és nyilvántartása révén biztosítja a jogosulatlan hozzáférést.
- Sértetlenség: Adatintegritás biztosítása a mentési és archiválási nyilvántartások naprakész vezetésével és a mentések megfelelő tárolásával. Rendszerintegritás fenntartása a megfelelő ellenőrzött szoftverek használatával és a szoftvernyilvántartások vezetésével.
- Bizalmasság: az adatok illetéktelen kiszivárgása biztosítható a mentési adatlapok és nyilvántartások vezetésével, a mentések előírt tárolási szabályainak betartásával, az adatvédelmi szabályok betartásával.
- Felelősség: a cselekvések követhetőek és egyértelműen visszavezethetőek, a mentések, a számítógép naplók, valamint a szervernaplók elemzéséből.
- Megbízhatóság: az IBSZ intézkedései a rendszer megbízhatóságának biztosítására törekednek. A megbízhatóság az alapvető szabályok betartása mellett biztosítható.

Közbeszerzési tevékenység során meg kell felelni a közbeszerzésre vonatkozó normatíváknak és belső szabályozásoknak.

15.1.2 A dokumentum portfólió

A dokumentum portfolió részét képezik:

- Az IBSZ szabályai által előírt és napra készen vezetett adatlapok, naplók és nyilvántartások.
- Az informatikai munka során készített feljegyzések, jelentések, jegyzőkönyvek.
- Közbeszerzési dokumentumok.

15.1.3 Kontrollok

Az informatikai biztonság kontrollja az alábbi eszközökkel biztosítható:

- Dokumentált eszközkezelés (üzembe helyezési, eszközátadási, eszközszállítási, leltározási és selejtezési események dokumentálása).

- A jogosultságok és hozzáférések adatlapokkal történő dokumentálása.
- Ellenőrzött szoftverkezelés (jogtisztaság, tesztelt szoftverek, szoftvernyilvántartás vezetése, telepítés jogosultság szabályozása).
- Mentések és archívumok készítésére és tárolására vonatkozó előírások és kapcsolódó nyilvántartások vezetése.
- A munkahelyek, hálózatok, informatikai központok kialakítására és üzemeltetésére vonatkozó előírások betartása, kapcsolódó események naplózása.
- Hibakezelési rendszer alkalmazása és ellenőrzése, elemzése.
- Az informatikai biztonsági többszintű ellenőrzése.

15.1.4 Ellenőrzés

Az informatikai biztonsági megbízott az éves ellenőrzések során szúrópróbaszerűen ellenőrzi az informatikai biztonsági dokumentumokat és jelentés formájában a Hivatal vezetőjét tájékoztatja.

15.2 Az informatikai biztonság ellenőrzés szabályai

15.2.1 Az alkalmazandó szabályok meghatározása

Az informatikai biztonsági megbízott az éves ellenőrzések során szúrópróbaszerűen ellenőrzi az informatikai biztonsági dokumentumokat és jelentés formájában a Hivatal vezetőjét tájékoztatja.

15.2.2 A biztonsági ellenőrzés rendszere

Az informatikai biztonsági ellenőrzések területei:

- Környezeti veszélyek – pl. természeti károk, tűz stb.
- Fizikai veszélyek – lopás, rongálás, fizikai betörés.
- Informatikai veszélyek – vírusok, számítógépes betörés stb.
- Humán veszélyek – szabotázs, gondatlanság, tudatlanság, felelőtlenség stb.
- Szervezeti veszélyek – szervezeti problémák, irányítási gondok stb.

Az informatikai biztonsági ellenőrzések rendszere a Hivatalban:

- Alapszintű ellenőrzés:
- a kijelölt informatikus által.

Középszintű ellenőrzés:

- a szervezeti egység vezetők személyes részvételével,
- informatikai biztonsági megbízott ellenőrzései,
- a belső ellenőrzések,

Felsőszintű ellenőrzés:

- központi szakmai irányító szervek, hatóságok ellenőrzései felügyeleti kontrolja, illetve ellenőrzése.

15.2.3 Jogszabályi tényállások és szankciók

Ha a Hivatal alkalmazottja az informatikai biztonsági szabályok megszegésével olyan magatartást tanúsít, amely bűncselekmény gyanúját veti fel, az informatikai biztonsági megbízott jelzése alapján a

munkáltatói jog gyakorlója - a tudomására jutását követően haladéktalanul - feljelentést tesz ellene az illetékes nyomozóhatóságnál.

15.2.4 Kártérítési felelősség

Ha a Hivatal alkalmazottja az informatikai biztonsági szabályokat vétkesen megszegve a Hivatalnak kárt okoz, az informatikai biztonsági megbízott jelzése alapján a kártérítési eljárás kezdeményezhető vele szemben.

15.2.5 Fegyelmi felelősség

Ha a Hivatal alkalmazottja az informatikai biztonsági szabályokat vétkesen megszegi, az informatikai biztonsági megbízott jelzése alapján indokolt esetben fegyelmi eljárást kezdeményezhető vele szemben.

A fegyelmi és kártérítési eljárás lefolytatására a Hivatal Szervezeti és Működési Szabályzatának fegyelmi és kártérítési felelősségre vonatkozó rendelkezéseit kell alkalmazni.

16. Mellékletek

1. számú melléklet: Titoktartási és elfogadási nyilatkozat.

2. számú melléklet: Felhasználó regisztrációs munkalap.

3. számú melléklet: Rendszeres mentési napló.

4. számú melléklet: Kilépő dolgozó informatikai nyilatkozata.

5. számú melléklet: Belépő dolgozó titoktartási nyilatkozat.

6. számú melléklet: Mobil eszközre vonatkozó tárolási nyilatkozat.

7. számú melléklet: Mobil adathordozó eszköz engedélyezése.

8. számú melléklet: Adathordozó nyilvántartás

17. Záró rendelkezések

Jelen szabályzat a kiadás napján lép hatályba

……., ……

…….

jegyző