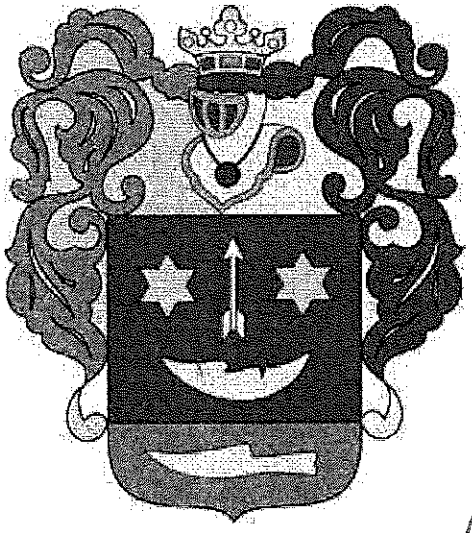
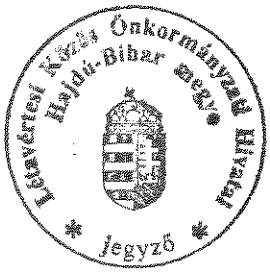
LÉTAVÉRTESI KÖZÖS ÖNKORMÁNYZATI HIVATAL

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT





.....

Jegyző

Létavértes, 2018. 06 hó 27 nap

Tartalom

I. Informatikai Biztonsági Szabályzat célja és hatálya

1. Célok és kötelezettségek

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, valamint a 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szerint az állami és önkormányzati szerveknek rendelkezniük kell Informatikai Biztonsági Szabályzattal. A szabályzat kialakításánál az említett jogszabályokon túl figyelembe kell venni az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendeletet, valamint a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. 30. § (1) bekezdése alapján Létavértesi Közös Önkormányzati Hivatal (továbbiakban: Hivatal) informatikai biztonsági szabályzatát a Hivatal jegyzője az alábbi szabályzat szerint határozza meg.

Az IBSZ célja, hogy biztosítsa a Hivatal alkalmazottai által kezelt adatok vonatkozásában az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok nyilvánosságra hozatalát, valamint megváltoztatását, valamint:

a) A jogkövető magatartás és a jó hírnév érdekében védje a szervezet értékeit,

b) A tudatosság, a szervezettség, a hatékonyság és a technikai megoldások használata segítségével növelje az információbiztonságot,

c) A megelőzés, a tájékoztatás, az oktatás, a felderítés és a szankcionálás eszközeivel segítse az intézkedések érvényesítését.

A Szabályzat célja továbbá biztosítani:

- az adat-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását,
- az üzemeltetett informatikai eszközök rendeltetésszerű használatát,
- a számítógépes rendszerek zavartalan üzemeltetését,
- az üzembiztonságot szolgáló karbantartást,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetését, illetve minimális mértékre való csökkentését,
- az adatállományok épségének megőrzését,
- az alkalmazott programok és adatállományok dokumentációjának nyilvántartását,
- a munkaállomásokon lekérdezhető adatok körének meghatározását,
- az adatállományok biztonságos mentését,
- az informatikai rendszerek zavartalan üzemeltetését,
- a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását,
- az adatvédelem és az adatbiztonság feltételeinek megteremtését

A jelen IBSZ a Hivatal szervezeti szintű információbiztonsági szabályozó rendszerének egyik alapvető eleme. Az IBSZ a hatályos jogszabályokkal, a Hivatal működési és ügyrendi előírásaival összhangban megteremti az elektronikus információs rendszerek és az azokban kezelt adatok biztonságát. Tartalmazza a Hivatal elektronikus információs rendszereivel kapcsolatba kerülő személyek felé támasztott minimum információbiztonsági követelményeket, továbbá meghatározza azokat az elvárásokat, kötelezettségeket és a felelősséget, amelyekre a biztonságos információellátás érdekében szükség van.
A Hivatal informatikai szolgáltatóival kötött szolgáltatási szerződéseknek és azok mellékleteinek összhangban kell lenniük jelen IBSZ-szel.

2. A Szabályzat személyi hatálya

Az Informatikai Biztonsági Szabályzat személyi hatálya kiterjed a Hivatal valamennyi szervezeti egységére, munkatársára, valamint azokra a személyekre, akik kapcsolatba

kerülnek a Hivatal elektronikus információs rendszereivel (használják, fejlesztik, telepítik, üzemeltetik, javítják. stb.), így:

a) a választott tisztségviselőkre (polgármester, alpolgármester, képviselők),

b) a közszolgálati jogviszony alapján foglalkoztatott munkatársakra,

c) a munkaviszony alapján foglalkoztatott munkatársakra,

d) a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyekre,

e) más szervezetek képviseletében a Hivatal munkahelyein tartózkodó személyekre.

3. A Szabályzat tárgyi hatálya

Az IBSZ tárgyi hatálya kiterjed a Hivatal adataival és adatainak kezelésével összefüggésben:

- a védelmet élvező elektronikus adatok teljes körére, függetlenül felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától,
- a Hivatal tulajdonában lévő, illetve az általa használt valamennyi informatikai berendezésre, valamint az informatikai eszközök műszaki dokumentációira,
- az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési)
- a rendszer és felhasználói programokra,
- az adatok felhasználására vonatkozó utasításokra
- az adathordozók tárolására, felhasználására.

A tárgyi hatály kiterjed az önkormányzati ASP központ által nyújtott szakrendszerek felhasználó oldali komponenseire, így

a) a munkaállomásokra,

b) a munkaállomásokon futó szoftverekre,

c) kártyaolvasóra,

d) e-személyire.

4. A Szabályzat területi hatálya

Az IBSZ területi hatálya kiterjed a Hivatal:

- Létavértesiszékhelyére,
- Kokadi Kirendeltségre,
- minden olyan épületre, helyiségre, ahol a tárgyi hatály alá eső eszközök megtalálhatók, illetve a tárgyi hatálya alá tartozó tevékenységet végeznek.

5. A Szabályzat időbeni hatálya

Jelen IBSZ a kiadás napján lép hatályba.

II. Hatásköri és illetékességi szabályok

Az IBSZ belső használatú dokumentum: a Hivatal elektronikus információs rendszerének felhasználói, illetve egyéb érintettek (a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyek, más szervezetek képviseletében a Hivatal munkahelyein tartózkodó személyek) megismerhetik és birtokolhatják, de illetékteleneknek nem adhatják tovább.

A szabályzat végrehajtásának ellenőrzése a Hivatal vezetőjének feladata.
A szabályzat alkalmazásáért és betartásáért a Hivatal minden egysége, minden dolgozója felelős.
E szabályzatban foglaltak be nem tartása, tartatása jogi, munkaügyi, illetve szerződésben meghatározott következményeket/eljárást von maga után.

III. Az IBSZ végrehajtás szabályai és eszközei

A Hivatal elektronikus információs rendszereit csak olyan személyek használhatják, akikmegfelelő számítástechnikai, informatikai ismeretekkel rendelkeznek.
Rendszeres belső oktatásokkal gondoskodni kell arról, hogy a felhasználókban tudatosodjanakaz alapvető információbiztonsági fogalmak, illetve ismerjék meg a munkájuk során felmerülőinformációbiztonsági fenyegetettségeket. Gondoskodni kell továbbá arról,

hogy a napi feladatokvégzése során a felhasználók kellőképpen felkészültek legyenek a jelen IBSZ-ben foglaltakbetartására. Ennek végrehajtására évente frissítő oktatást kell szervezni.

Új dolgozó munkába lépésekor a dolgozóval a munkába állás előtt az információbiztonságielőírásokat meg kell ismertetni.

A Hivatal személyügyekért felelős vezetőjének a feladata, hogy az elektronikus információsrendszerekhez való hozzáférési jogosultság megadása előtt ellenőrizze, hogy az érintett személya munkaköréhez meghatározott feltételeknekmegfelel-e. A vizsgálat magában foglalja az alábbiakat:

a) referenciák ellenőrzése,

b) a felvételre jelentkező életrajzának ellenőrzése a teljességre és pontosságra vonatkozóan,

c) a legmagasabb iskolai végzettség (szakképzettség) ellenőrzése,

d) nyelvtudást igazoló okiratok ellenőrzése,

e) hatóság által kibocsátott azonosító irat ellenőrzése,

f) erkölcsi bizonyítvány ellenőrzése.

A felelősségi köröket a munkaköri leírásokban rögzíteni kell.

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

Az önkormányzati ASP szakrendszerek felhasználóinak az ASP működtetője által biztosított e-learningképzésen kell részt venni a szakrendszerhez történő hozzáférés előtt.A kiemelt jogosultságokkal rendelkező munkatársak részére külön oktatást kell tartani.

Az információbiztonsági oktatások és továbbképzések tematikájának kidolgozása, a szükségesszakirodalom és tájékoztató anyagok biztosítása, valamint a képzés megtartása az elektronikus információs rendszerek biztonságáért felelős személy (továbbiakban: információbiztonsági felelős, rövidítve IBF)feladata.Az oktatáson, illetve továbbképzésen való részvétel az elektronikus információs rendszerrelkapcsolatba kerülő személyek számára kötelező és a megjelenést a résztvevők aláírásukkalkötelesek tanúsítani.

IV. Az IBSZ felülvizsgálata

Az IBSZ eseti módosítására kerül sor, ha a benne szereplő adatok megváltoztak, illetve, ha az IBSZ olyan kisebb mértékű kiegészítésekre szorul, amelyek nem érintik az aktuális biztonsági követelményeket.

Az IBSZ módosítására van szükség, ha a Hivatal elektronikus információs rendszereinek működésében vagy a Hivatal elektronikus információs rendszereinek működését meghatározó jogszabályi környezetben jelentős változások következnek be.

Az IBSZ-t legalább évente egy alkalommal felül kell vizsgálni.

Az IBSZ eseti módosításának, felülvizsgálatának kezdeményezése és a felülvizsgálat, valamint a módosítás elvégzése az elektronikus információs rendszerek biztonságáért felelős személy (IBF) feladata. A módosítások engedélyezése és az újabb változat jóváhagyása a jegyző hatásköre.

Az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet alapján a Hivatalnak 2018. január 1-ig csatlakoznia kellett az önkormányzati ASP rendszer valamennyi szakrendszeréhez.

A csatlakozás feltétele, hogy a Hivatal teljesítse az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben foglaltakat.

A jelen IBSZ az ASP csatlakozási projekt információi birtokában került felülvizsgálatra, amikor a Hivatal már valamennyi szakrendszerhez csatlakozik.

V. Biztonsági szintbe sorolás

Létavértesi Közös Önkormányzati Hivatal nyilatkozatban rögzíti, hogy a 41/2015. (VII.15.) BM rendelet 2. melléklete alapján a Hivatal biztonsági szintje:

2-es (azaz kettes) besorolású

VI. Biztonsági osztályba sorolás

Létavértesi Közös Önkormányzati Hivatal nyilatkozatban rögzíti, hogy a 41/2015. (VII.15.) BM rendelet 1. melléklete alapján a Hivatal biztonsági osztálya:

2-es (azaz kettes) besorolású

Indoklás:

A Hivatal olyan elektronikus információs rendszert használ, amelyben csekély káresemény következhet be, mivel

- személyes adat sérülhet;
- az üzlet-, vagy ügymenete 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 eléri az érintett szervezet költségvetésének 1%-át.

A Hivatal központi üzemeltetésű és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszert vagy zárt célú elektronikus információs rendszert működtet.Az ASP specifikus rendszerek nem a Hivatal által működtetett rendszerek.

Védelmi intézkedések

Az ASP rendszerben kezelt adatok tekintetében a védelmi intézkedések megvalósulásának jelentős részét az ASP Központ biztosítja. Tekintettel azonban arra, hogy az adatkezelés a Hivatal helyszínein, a Hivatal munkavállalói és szerződött partnerei által is megvalósul, így biztonsági elvárások egy része a Hivatal hatáskörébe tartozik.

A nem az ASP rendszerben kezelt adatok tekintetében a védelmi intézkedéseka Hivatal hatáskörébe tartoznak.

I. Adminisztratív védelmi intézkedések

Az itt részletezett adminisztratív védelmi intézkedéseket egységesen, valamennyi elektronikus információs rendszerre vonatkozóan kell megvalósítani.

1. Szervezeti szintű alapfeladatok

1.1. Informatikai biztonsági szabályzat

A Hivatal megfogalmazta, dokumentálta, valamint kihirdette, az informatikai biztonsági szabályzatát. Az informatikai biztonsági szabályzat a Hivatal, képviselő-testülete hagyja jóvá.
Az informatikai biztonsági szabályzatát szükség szerint, de legalább évente egyszer az informatikai biztonsági rendszer felülvizsgálata során (belső audit) a Hivatal felülvizsgálja, szükség szerint módosítja. Az informatikai biztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor az informatikai biztonsági szabályzatot újra vizsgálja, szükség szerinti módosítja.
Jelen szabályzatban a Hivatal rögzíti az elektronikus információs rendszereinek mind a biztonsági osztályba sorolását és a szervezet biztonsági szintjét.

1.2. Az információbiztonság szervezeti struktúrája, szerepkörök

Az információbiztonság megteremtése és fenntartása olyan alapvető felelősség, amely szerint
nem tartozhat egyszemélyi felelősségi és hatáskörbe az elektronikus információs rendszerektervezése, fejlesztése, üzemeltetése és felügyelete.
Az információbiztonság megvalósítását, fenntartását és ellenőrzését a Hivatal a feladatok ésfelelősség szempontjából egymástól elhatárolt szervezeti keretek között valósítja meg.

A Hivatal vezetője az elektronikus információs rendszer biztonságáért felelős személyt nevez ki (akár szerződéses partner), aki ellátjaaz állami és hivatali szervek elektronikusinformációbiztonságáról szóló 2013. évi L. törvényben meghatározott feladatokat.
A Hivatal vezetője gondoskodik (szerződéses partner esetén szerződésben elvárja) a biztonságért felelős személy képzettségéről az idevonatkozó rendeletnek megfelelően.

Az információbiztonság megfelelőségéért,az IBSZ-ben foglaltak megtartásáért és annak megvalósításával kapcsolatos feladatok végrehajtásáért a Hivatal vezetője felelős.

A Hivatal információbiztonsági feladatainak ellátása során a következő szerepkörök érintettek:

- szervezet vezetője
- információbiztonsági felelős
- szervezeti egység vezetője
- rendszergazda
- adatgazda
- felhasználó
- külső személyek
- ASP adminisztrátor
- szakrendszeri adminisztrátor

1.2.1. Szervezet vezetője

A szervezet vezetője(jegyző) az Ibtv. alapján gondoskodik az elektronikus információs rendszerek védelméről akövetkezők szerint:

- biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
- biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
- az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,
- meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,
- gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,

- rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
- gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
- 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,
- ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
- ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az a törvényben foglaltak szerződéses kötelemként teljesüljenek,
- felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,
- megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

1.2.2. Elektronikus információs rendszer biztonságáért felelős személy

Az elektronikus információs rendszer biztonságáért felelős személy (továbbiakban: IBF) felel a Hivatalnál előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:

a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
b) elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
c) előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,

d) előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,
e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a hivatal e tárgykört érintő szabályzatait és szerződéseit,
f) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.

Az elektronikus információs rendszer biztonságáért felelős személy az Ibtv. hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet.
Amennyiben a Hivatal elektronikus információs rendszereinek mérete vagy biztonsági igényei indokolják, a szervezeten belül elektronikus információbiztonsági szervezeti egység hozható létre, amelyet az elektronikus információs rendszer biztonságáért felelős személy vezet.

Az elektronikus információs rendszer biztonságáért felelős személy biztosítja az Ibtv-ben meghatározott követelmények teljesülését

a) a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában,és kockázatkezelésében, karbantartásában vagy javításában közreműködők,

b) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők

a törvény hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

Az elektronikus információs rendszer biztonságáért felelős személy munkája során:

- Gondoskodik az ellenőrzés módszereinek és rendszerének kialakításáról és működtetéséről. Jóváhagyásra előkészíti az éves informatikai biztonsági ellenőrzési tervet és az IBSZ javításait.
- Olyan mértékben ismeri aHivatalinformatikairendszerét, hogyannakelemeit hatékonyan ellenőrizni tudja.

- Összehangoljaabiztonságotmeghatározó,befolyásolóterületektevékenységétazinformatikai biztonság érdekében.
- AHivatalvezetőjévelegyüttműködvefelügyeliabiztonsággalkapcsolatbankészítendőtervekés szabályzatok elkészítését.
- Informatikai biztonsági szempontból ellenőrzi az informatikai rendszer szereplőinek tevékenységét.
- Azinformatikairendkívülieseményeket, azesetlegesrosszszándékúhozzáférési kísérletet, illetéktelenadatfelhasználást,visszaéléstkivizsgálja,javaslatotteszaszervezetvezetőjéneka további intézkedésekre, a felelősségre vonásra.
- AzSZMSZrendelkezéseiésamunkakörileírásokalapjánellenőrziazinformatikairendszer 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.
- Felügyeliaberuházásokat,afejlesztéseketésazüzemviteltinformatikaibiztonságiszempontból, illetve javaslatot tesz rájuk.
- Az új biztonságtechnikai eszközök és szoftverek tesztelésére ajánlást ad.
- Szúrópróba szerűen ellenőrzi:azegyesfelhasználóigépekhardverkonfigurációját,ésatelepített szoftvereketösszevetiafelhasználónakengedélyezettszoftvereklistájával,hogyarendszerben aktuálisanbeállítottfelhasználóijogosultságokmegegyeznek-eajóváhagyott(ajogosultsági nyilvántartásbanisszereplő)jogosultságokkal,hogyajavításrakiszállítotteszközökönadatne kerüljön ki, az adathordozók selejtezését.
- Értékeli a rendszer eseménynaplóit.
- Ellenőrzi a víruskereső programokhasználatát.
- Ellenőrzi a dokumentációk meglétét és megfelelőségét (teljes körű, aktuális).
- Ellenőrzi,hogya vonatkozóinformatikaibiztonsági követelményeketarendszerekfejlesztési ésaz alkalmazási dokumentációiban is megjelenítik-e.

- Amennyiben új fenyegetéseket észlel, vagy hatékonyabb biztonsági intézkedések megtételét tartja szükségesnek, kezdeményezi a védelem erősítését.
- Azadott szakterületekvezetőivel egyeztetvemeghatározzaazegyesfeladatkörökhöztartozóan az informatikaibiztonsággalkapcsolatosanelsajátítandóismeretekkörét,ésellenőrziazelsajátítás tényét.
- Javaslatot tesz informatikai biztonságot erősítő továbbképzésre.
- AzIBSZ-téventefelülvizsgálja,ésjavaslatotteszagyakorlati tapasztalatok, előfordultinformatikai rendkívüliesemények,ajogszabályikörnyezetváltozásai,atechnikaifejlődés,azalkalmazottúj informatikaieszközök,újprogramrendszerek,fejlesztésiésvédelmieljárásokmiattszükségessé 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.
- Biztosítja az adat- és információvédelmi feladatok folyamatos belső ismertetését, felügyeli a képzési terv kidolgozását és oktatását.

1.2.3. Rendszergazda

Feladata:

- az Informatikai rendszer IBSZ-nek megfelelő működtetése,
- az Informatikai rendszer működtetéséhez szükséges valamennyi személyi és tárgyi feltétel biztosítása a biztonsági elvárások figyelembevételével,
- előterjeszteni a Hivatal informatikai fejlesztéseit az informatikai biztonság megvalósítása céljából,
- az érzékelt vagy ismert kockázatokról az Informatikai Biztonsági Felelőst és a jegyzőt tájékoztatni,

- az informatikai biztonságot érintő minden dokumentum és utasítás elkészítésében való aktív részvétel, az elkészült dokumentumok véleményezése, kihirdetésének biztosítása,
- közreműködni az Informatikai rendszer informatikai biztonságát érintő területek megvalósításában,
- biztosítja a veszélyforrások körében bekövetkezett változások folyamatos követését (vírusvédelem), és kezdeményezi a szükséges intézkedések meghozatalát
-

1.2.4. Szervezeti egység vezető

Feladata:

- 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).

1.2.5. Adatgazda

Az adatgazda annak a szervezeti egységnek a vezetője, ahol az adat keletkezik, illetve amelyhez jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését elrendeli.
Az adatgazda feladata:

- meghatározni az általa felügyelt adatokhoz hozzáférő személyeket, a szükséges-elégséges hozzáférési elv alapján.

Az adatgazda felelős:

- a hatáskörébe tartozó informatikai rendszerek hozzáférési jogosultságainak a szükséges minimális jogosultságok elve alapján történő engedélyezéséért.

1.2.6. Felhasználó

Felhasználó az egy adott elektronikus információs rendszert igénybe vevők köre.

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,

A Felhasználó köteles:

- az IBSZ-ben megfogalmazott szabályokat megismerni és betartani, illetve ezek betartásában az informatikai rendszer használatát irányító személyekkel együttműködni,
- aszámáraszervezettinformatikaibiztonságioktatásonrésztvenni,azismeretanyag elsajátításáról számot adni,
- a rendelkezésére bocsátott számítástechnikai eszközöket megóvni,
- bizalmasan kezelni valamennyi felhasználói azonosítóját és jelszavát, vagy egyéb olyan tokent, kulcsot, ami a Hivatal informatikai rendszereihez biztosít hozzáférést,
- afelügyeletnélkülmaradómunkahelyen(munkaállomáson)személyesadatotvagynem nyilvános adatot tartalmazó dokumentumot/adathordozót elzárni,
- aszámítógépét(amunkahelyimunkaállomást)ahelyiségelhagyásaeseténlezárniúgy, hogy ahhoz csak jelszó vagy hardveres azonosító eszköz használatával lehessen hozzáférni,
- azinformációbiztonságotérintőeseménygyanújaeseténazészleltrendellenességekről tájékoztatni a közvetlen felettesét és az informatikai biztonsági megbízottat,
- biztonsági incidensek kivizsgálásakor együttműködni,
- a folyó munka során nem használt nem nyilvános anyagokat, adathordozókat elzárni,
- a munkahelyről történő eltávozáskor az addig használt –kivéve ha ez a rendszer(ek) más által történő használatát vagy a karbantartást akadályozza, - az általa használt eszközt szabályszerűen leállítani,
- az általa használt eszközök biztonsági beállításait változtatás nélkül megőrizni,
- aze-mailésinternethasználatsorántartózkodniabiztonságszempontjábólkockázatos tevékenységtől.

A Felhasználónak tilos:

- asajáthasználatrakapottszámítógéprendszerszintűbeállításainakmódosítása(idenemért veaz irodai programok felhasználói beállításait),
- a munkaállomására telepített aktív vírusvédelem kikapcsolása,
- belépésijelszavát(jelszavait),hardveresazonosítóeszközétmásszemélyrendelkezésére bocsátania, hozzáférhetővé tennie,
- illetéktelenül más felhasználó jogosultságának használata,
- a Hivatal hálózatának monitorozása, felderítése, jelszavak kipróbálása, illetve illetéktelen hozzáférések megkísérlése,
- 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) telepítése, 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 adathordozótaz eszközökbe helyezni,
- más szerzői, jogvédelmi,egyébszellemitulajdonhozfűződővagyegyébszemélyhezfűződő jogátvagyjogosérdekétsértődokumentumokat,tartalmakat(zenéket, filmeketstb.)az eszközökön tárolni, oda le-, illetve onnan a hálózatra feltölteni,
- lánclevelekettovábbítani,kéretlen levelekreválaszolni,ismeretlentartalmú kéretlenlevelek mellékleteit vagy linkjeit megnyitni,
- kereskedelmicélúhirdetéseket/reklámokatbelsőcímzettekfelétovábbítani(idenemértv ea

Hivataláltalkértvagypartnereiáltalküldött,aHivataláltaltámogatotttevékenységekről– 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.

1.2.7. Külső személyek – mint felhasználók

AHivataligénybevehetállományábanemtartozókülsőszemélyeketfelhasználóijogosultságokkal időszakosvagyfolyamatosfeladatokvégrehajtására.A Hivatal külső személlyel,valószerződéskötésével kapcsolatoseljárásátavonatkozómegállapodásokszabályozzák.Egyébesetbenakülsőszemállyel szerződést kötő szervezeti egység vezetője felelős:

- akülsőszemélybevonásaáltalokozottinformatikaibiztonságikockázatokfelméréséértés értékeléséért,
- azIBSZszerintikövetelményekkommunikálásáértésavonatkozószerződésbetörténő beépítéséért, az alábbiak szerint
  - aHivatalrendszereivelkapcsolatosvagyazokatérintőmunkavégzéscéljábólérkező külső személyaHivatalterületénaszerződéslétrejötteutánkizárólagaszerződéskötést kezdeményezőszervezetiegységvezetőjénektudtávalésazáltalakijelöltszemély felügyelete mellett tartózkodhat,
  - akülsőszemélyamunkafolyamategyeztetésesoránmindenolyanmunkafolyamatról köteles beszámolni a szerződéskötést kezdeményező szervezeti egység

vezetőjének, amely bármilyen módon érinti az informatikai rendszer biztonságát,

- amennyibenaza munkavégzéshezfeltétlenülszükséges,aHivatalinformatikai rendszereihezvalóhozzáféréshezideiglenesésszemélyreszólóhozzáférésijogosultságot kell biztosítani, amelyről a szerződést kötő szervezeti egység vezetője gondoskodik,
- a Hivatal külső személlyel csak olyan szerződést köthet, amely a külső személy tekintetében biztosítjaavonatkozótitokvédelmiszabályokérvényesülését.Aszerződéskötésso rán figyelembekellvenniazIBSZelőírásait,ajogszabályielőírásokat(különöstekintette la szellemi alkotásokhozfűződő,illetveszerzői,iparjogvédelmi,egyébszellemitulajdonhoz fűződő vagy egyéb személyhez fűződő jogokra

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

1.2.8. ASP adminisztrátor

Az önkormányzati ASP adminisztrátor feladata a bérlő fiók, tenant (önkormányzat, intézmény, nemzetiségi önkormányzat) szintű felhasználó kezelés, azaz

a) az adott tenant felhasználóinak felvétele és szakrendszeri szerepkör(ök)höz rendelése, annak adminisztrációja és karbantartása;

b) intézményi kapcsolattartóként az adott tenant felhasználók tanúsítvány igénylésének adminisztrációja és karbantartása, illetve a tanúsítványokat hordozó tokenek csoportos átvétele és felhasználók közötti kiosztása.

1.2.9. Szakrendszeri adminisztrátor

Az önkormányzat szakrendszeri adminisztrátor(ok) feladata a szakrendszer szintű jogosultságkezelés, azaz a szolgáltatást igénybe vevő felhasználók számára a szakrendszeri jogosultságok beállítása, adminisztrációja és karbantartása.

1.3. Intézkedési terv és mérföldkövei

A Hivatal vezetése intézkedési tervet készít az elektronikus információbiztonsági stratégia megvalósításához az ahhoz illeszkedő határidőkkel, felelősökkel, az esetleg felmerülő költségekkel és egyben mérföldköveket állapít meg. Az így elkészített intézkedési tervet legalább évente felülvizsgálja és karbantartja. Ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál (belső vagy külső vizsgálat során) hiányosságot állapítanak meg, vagy a meghatározott biztonsági szint alacsonyabb, mint az érintett hivatalra érvényes szint, akkor a Hivatal vezetése a vizsgálatot követő 90 napon belül felülvizsgálatot készít a hiányosság megszüntetése érdekében.

Az intézkedési tervet az IBF készíti elő a rendszergazda bevonásával és a jegyző hagyja jóvá.

1.4. Az elektronikus információs rendszerek nyilvántartása

A Hivatal minden használt szoftverre és szoftverlicencekre – a tárgyi eszköz nyilvántartástól független - nyilvántartást vezet, azt szükség szerint aktualizálja.A Hivatal az elektronikus rendszerek nyilvántartását egy korlátozottan, csak az érintettek számára hozzáférhető belső dokumentumban kezeli.

A nyilvántartásnál figyelembe kell venni a mindenkor érvényben lévő számviteli törvény előírásait, a Belügyminisztérium ajánlásait, valamint összhangban kell lennie az ügyviteli rendszerek (tárgyi eszköz) nyilvántartásával.

Minden rendszert a beszerzéssel egyidejűleg fel kell venni a nyilvántartásba. A nyilvántartásból rendszereszközt kivenni csak annak selejtezésekor lehet.

1.4.1. A nyilvántartás célja

Az elektronikus információs rendszerek nyilvántartásának célja:

- szoftvergazdálkodás optimalizálása
- a Hivatal szoftver- és hardvervagyonának nyilvántartása
- a karbantartási és fejlesztési munkálatok nyomon követése
- a Hivatal működéséhez szükséges informatikai feltételek biztosítása az optimalizált eszközhasználat segítségével

1.4.2. Felelősök

A Hivatal elektronikus információs rendszereinek nyilvántartását a rendszergazda végzi. A nyilvántartás karbantartásáért szintén a rendszergazda felel. Felülvizsgálatát, ellenőrzését az Informatikai Biztonsági Felelős végzi.

A nyilvántartásban a szoftverekről, alkalmazásokról az alábbi adatokat tartalmazza:

- szoftver neve, azonosítója
- szoftver gyártója
- a szoftver szállítója
- rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait
- szoftver verzió száma
- szoftver sorozatszáma
- licenc típusa
- licencek száma
- beszerzés dátuma
- aktiválás dátuma
- szoftver telepítésének helye

1.5. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

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

- emberi, fizikai és logikai erőforrásra
- eljárási és védelmi követelményszintre és folyamatra.

Belépő, új munkatárs hozzáférési jogkörét, illetve nem új belépő munkatárs hozzáférési jogkör változtatását a felettes vezetője határozza meg.

Új munkakörök kialakítása során az illetékes szervezeti egység vezetője tájékoztatja az informatikai vezetőt és IBF-et a munkakör feladatairól és tervezett jogosultságairól. Az informatikai vezető és az IBF javaslattal élhet a munkakör feladatainak biztonsági vonatkozásait illetően.

Az engedélyezési eljárás a 14. pontban meghatározott Hozzáférési eljárásrendben meghatározottak figyelembevételével történik.

Amennyiben külső személyek hozzáférési lehetőséget kell biztosítani, azt csak a 1.2.7. pontban leírtak szerint lehet megtenni. A hozzáférést mindaddig ki kell zárni, amíg a szükséges ellenőrzés nem valósult meg.

Abban az esetben, ha a feladat elvégzésére a harmadik fél alvállalkozót is igénybe vesz, a szerződésben pontosan meg kell nevezni az alvállalkozót, s meg kell határozni a rá vonatkozó hozzáférési jogosultságokat. A titoktartási kötelezettség a harmadik fél alvállalkozójára is vonatkozik.

A Hivatalban nincsenek azonosítás és hitelesítés nélkül engedélyezett tevékenységek.

2. Kockázatelemzés

2.1. Kockázatelemzési és kockázatkezelési eljárásrend

A Hivatal az elektronikus információs rendszerek teljes életciklusában megvalósítja és biztosítja az elektronikus információs rendszerekben kezelt adatok és információk bizalmasságát, sértetlenségét és rendelkezésre állását, valamint az elektronikus információs rendszerek és elemeinek sértetlenségét és rendelkezésre állását zárt, teljeskörű, folytonos és kockázatokkal arányos védelmét.

A vonatkozó jogszabályokkal összhangban a kockázatelemzés alapját képezi:

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

A kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának sérüléséből, elvesztéséből bekövetkező kár, vagy káros hatás nagyságát a szakterületek felelősei határozzák meg.
A kockázatelemzés során vizsgálandó sérülékenységek és ezeket kihasználni képes releváns fenyegetések azonosításáért, valamint a káresemények becsült bekövetkezési gyakoriságának meghatározásáért és ez alapján a kockázatelemzés elkészítéséért IBF felel.
A jegyző felelőssége az IBF-el együttműködve, gondoskodnia kockázatelemzés legalább háromévenként vagy szükség esetén, soron kívül dokumentált módon történő felülvizsgálatáról.

2.2. Biztonsági osztálybasorolás

A 41/2015. (VII. 15.) BM rendelet 1. melléklete határozza meg az elektronikus információs rendszerek biztonsági osztályba sorolásának szempontjait, a 4. melléklet a lehetséges védelmi intézkedéseket, a 3. melléklet pedig, hogy adott biztonsági osztályhoz mely pontokat kötelező megvalósítani a védelmi intézkedés katalógusból. Amennyiben valamely kötelező intézkedés az érintett szervezetnél nem valósult meg, a cselekvési tervben ki kell térni a teljesítésére.

A rendelet az egységes értelmezés és kommunikáció érdekében lehetőséget ad arra, hogy a NEIH a nevezett adatokra vonatkozó bejelentést kizárólag az Osztályba sorolás és védelmi intézkedés (OVI) űrlapon fogadja el. Az űrlap segítségével az érintett szervezet könnyebben sorolhatja biztonsági osztályba elektronikus információs rendszereit bizalmasság, sértetlenség és rendelkezésre állás szempontjából, valamint egységesen dokumentálhatja a megállapított osztályokhoz tartozó követelmények teljesülését vagy hiányát, végül meggyőződhet arról, hogy a rendszer pillanatnyilag mely biztonsági osztály követelményeit teljesíti maradéktalanul. Az űrlap a 4. verziótól kezdve támogatja a cselekvési terv összeállítását is azzal, hogy minden egyes intézkedéshez megadható a megvalósítás tervezett dátuma.

2.3. Biztonsági szintbe sorolás

A 41/2015. (VII.15.) BM rendelet 2. melléklete határozza meg a szervezeti egységek biztonsági szintbe sorolásának szempontjait és hogy adott biztonsági szintekhez mely védelmi intézkedéseket kell megvalósítani. Amennyiben valamely kötelező intézkedés az érintett szervezetnél nem valósul meg, cselekvési tervben kell kitérni a teljesítésére.

A rendelet egységes értelmezés és kommunikáció érdekében lehetőséget ad arra, hogy a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) a nevezett adatokra vonatkozó bejelentést kizárólag a Szintbe sorolás és védelmi intézkedés (SZVI) űrlapon fogadja el.

Az űrlap segítségével a biztonsági szintbe történő besorolás egyértelműen megtörténik, egységesen dokumentálható a megállapított szinthez tartozó követelmények teljesülése vagy hiánya.

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

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

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

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

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

2.4. Kockázatelemzés

Az információbiztonsági kockázatelemzés célja, hogy feltárja a Hivatal elektronikusinformációs rendszereire és az azokban kezelt adatokra ható fenyegető tényezőket,veszélyforrásokat (fenyegetettség elemzés), vizsgálja az elektronikus információs rendszer gyenge pontjait (sérülékenység vizsgálat), elemezze a veszélyforrások által a gyenge pontokon keresztül bekövetkező sikeres támadások bekövetkezési valószínűségét és az általuk okozott kár nagyságát (kockázatelemzés), valamint kezelje a Hivatal által el nem fogadható kockázatokat (kockázatkezelés).

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.

Az elektronikus információs biztonságáért felelős személy feladata, hogy azonosítsa a nem elfogadható kockázatokat okozó sérülékenységeket, javaslatot tegyen az esetleges további kezelendő kockázatot okozó sérülékenységekről, valamint megvizsgálni, hogy a

kockázatelemzés eredménye befolyásolhatja-e az elektronikus információs rendszerek biztonsági osztályba sorolását és erről tájékoztatni a jegyzőt.

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

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

Amennyiben a kockázatkezeléssel kapcsolatos vezetői döntések alapján változik az elektronikus információs rendszerek biztonsági osztályba sorolása, a jegyző felelőssége, hogy a Hivatal elvégezze az új besorolást.

A kockázatelemzéssel és kezeléssel kapcsolatos dokumentumok bizalmasnak minősülnek, ezért azok megismerésére az IBF, a rendszergazda, a jegyző, valamint a jegyző által írásban kijelölt személyek jogosultak.

3. Rendszer és szolgáltatás beszerzés

3.1. Külső elektronikus információs rendszerek szolgáltatásai

A Hivatal:

a) szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek az érintett Hivatal elektronikus információbiztonsági követelményeinek;

b) szerződésben határozza meg az érintett Hivatal felhasználóinak feladatait éskötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban;

c) külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

A beszerzésekre vonatkozó felhasználói és egyéb rendszerbővítési igényeket a szervezeti egység vezetője és/vagy a jegyző specifikálja, melynek során figyelembe veszi:

- a vonatkozó közbeszerzési eljárás lefolytatására vonatkozó előírásokat
- a Hivatal által alkalmazható szoftver-liszenszelési lehetőségeket
- az adott piaci kínálatot.

Az eszközök (hardver, szoftver) kiválasztásánál a fentiekben részletezett általános és gazdasági tényezőkmellett figyelembe kell venni az adott eszköz által nyújtott biztonsági funkciókat, megoldásokatis.

A hardver eszközök beszerzéséhez még az alábbi tényezők figyelembevétele szükséges:

- a hardver funkcionalitása, erőforrásai
- a hardver várható rendelkezésre állása (megbízhatóság)
- a hardver garanciális feltételei (garancia idő, műszaki tartalom)
- a hardver szakértői és technikai támogatottsága (tanácsadás, alkatrész biztosítás)

A szoftver megoldásoknál még az alábbi tényezők figyelembevétele szükséges:

- a szoftver funkcionalitása
- illeszkedés a platform szabványokhoz (kompatibilitás)
- a szoftver biztonsági megoldásai (jogosultság kezelés, titkosítás, AD integrálhatóság, stb.)
- a szoftver menedzselhetősége
- aszoftverhez biztosított support és rendelkezésre állás

3.2. Szolgáltatások minőségének ellenőrzése

A szolgáltatások minőségének ellenőrzésére szolgáltatásonként kontrollokat kell felállítani. Minimális kontrollok az alábbiak:

- Szolgáltatás minőségére vonatkozó kontrollok:

- A szolgáltatás rendelkezésre állása (pl: Internet esetén kiesett órák száma, vagy a hiba elhárításának megkezdése, stb.).
- A szolgáltatás minősége (pl. Internet esetén sávszélesség, vagy a hiba gyors és szakszerű elhárítása, stb.).

- A szolgáltató megbízhatóságára vonatkozó kontrollok:
  - A szolgáltató rendelkezésre állása.
  - A szolgáltató együttműködési készsége.
  - A szolgáltató szakmai kompetenciája.

A szolgáltatások minőségének ellenőrzését a rendszergazda végzi.

4. Üzletmenet- (ügymenet-) folytonosság tervezése

4.1. Vonatkozó eljárásrend

Az információk védelmének és a megfelelő rendelkezésre állásának biztosítása érdekében a Hivatal az alábbi módon teljesíti az üzletmenet-folytonossági elvárásokat:

a) biztosítjuk, hogy a kockázatok esetleges bekövetkezésekor a szolgáltatás kiesés ne legyen nagyobb a tervezetnél (ne sérüljön az SLA);

b) megfelelő alapot adunk a kockázatok csökkentésére irányuló hatékony intézkedések végrehajtásához és eredményességük nyomon követéséhez;

c) meghatározzuk azokat az intézkedéseket, amelyek ahhoz szükségesek, hogy a Hivatal folyamatos működése biztosítva legyen;

d) meghatározzuk azokat az intézkedéseket, feladatokat, melyeket az esetleges folytonosság megszakadásra felkészülésként, illetve bekövetkezésekor a kár enyhítéseként, illetve a helyreállításért kell tenni;

e) biztosítjuk, hogy az üzletmenet-folytonosság és a szolgáltatások rendelkezésre állása személyes felelősséghez köthető legyen;

4.2. Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

A Hivatal működésének folytonosságával kapcsolatos feladatok tervezése, irányítása, koordinálása, a szükséges erőforrások rendelkezésre állásának biztosítása a jegyző

feladata. A feladat keretében a jegyző alapvetően biztosítja, hogy informatikai szolgáltatás kiesésével járó esemény esetén:

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

A fentieket figyelembe véve a vonatkozó kockázatokat szem előtt tartva a Hivatal informatikai rendszereit úgy kell kialakítani, valamint a külső szolgáltató által nyújtott informatikai szolgáltatásokra olyan rendelkezésre állási követelményeket kell kikötni, hogy azok költséghatékonyan támogassák a Hivatal feladatait, illetve az azok alapján az érintett ügyviteli folyamatokra levezethető rendelkezésre állási követelményeket kapjunk.
A fenti követelmények érdekében számba kell venni a Hivatal működését támogató informatikai szolgáltatásokat, a szolgáltatások rendelkezésre állását veszélyeztető lehetséges rendkívüli eseményeket és meg kell határozni meghatározni, hogy milyen preventív, detektív, illetve korrektív intézkedések bevezetésével csökkenthetőek az informatikai szolgáltatások kieséséből származó kockázatok elfogadható szintre.
A meghatározott - informatikai szolgáltatás kiesésével járó - rendkívüli esemény bekövetkezése esetén végrehajtandó alternatív folyamat szükségességének meghatározásakor az érintett ügyviteli folyamatok rendelkezésre állási követelményei mellett figyelembe kell venni a Hivatal által használt informatikai rendszerek rendelkezésre állási képességeit (hogyan és mennyi idő alatt lehet a rendszert újraindítani egy esetleges meghibásodást követően és az újraindítás során mikori adatokat lehet a rendszerbe visszatölteni), illetve a külső féltől igénybe vett informatikai szolgáltatások esetén az azokra vállalt rendelkezésre állási paramétereket.
A fenti szempontok figyelembe vételével a jegyző felelőssége meghatározni a Hivatal által alkalmazott kockázatkezelő intézkedéseket; valamint a bevezetett intézkedések

működésének biztosítása és felügyelete (pl. az esetlegesen szükségesnek ítélt folytonossági tervek oktatása, tesztelése, rendszeres felülvizsgálata; az informatikai rendszerekre meghatározott rendelkezésre állási képességeket biztosító intézkedések működtetése).

4.3. A folyamatos működésre felkészítő képzés

A jegyző felelőssége az elektronikus információs rendszer folyamatos működésére felkészítő képzés megszervezése, amikor a rendszer változásai azt szükségessé teszik.

4.4. Az elektronikus információs rendszer mentései

A Hivatal a rendszerbiztonsági és üzletmenet-folytonossági elvárásokkal összhangban:

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

b) meghatározott gyakorisággal elmenti az elektronikus információs rendszerben tárolt rendszerszintű információkat, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;

c) meghatározott gyakorisággal elmenti az elektronikus információs rendszer dokumentációját, köztük a biztonságra vonatkozókat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;

d) megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen.

A munkaállomások

A mentéseket a szerverektől elkülönítve, legalább külön helyiségben kell tárolni, védve mind a különböző fizikai káreseményektől (tűz, csőtörés-vízbetörés, stb.), mind az illetéktelen hozzáféréstől (lopás, illegális másolás).

A 466/2017. (XII. 28.) Kormányrendeletben foglalt archiválási kötelezettségnek a Hivatal az önkormányzati ASP rendszer útján tesz eleget.

4.5. Az elektronikus információs rendszer helyreállítása és újraindítása

Az ügymenet-folytonosság tervezése során ki kell dolgozni az elektronikus információs rendszerek helyreállítási terveit, melyek a katasztrófahelyzetek kezelésére vonatkozóan a következőket kell tartalmaznia:

a) katasztrófát követő helyreállítandó célállapot;

b) a katasztrófa események definíciója;

c) a katasztrófa tényét eldöntő, a folyamat inicializálásáért felelős személyt, személyeket;

d) a helyreállítási terv hatóköre;

e) a megelőzés érdekében végzett tevékenységeket;

f) felkészülés a katasztrófa elhárítására;

g) katasztrófa esetén végrehajtandó tevékenységek;

h) elektronikus információs rendszerek vészleállításának és újraindításának folyamatát leíródokumentumot;

i) a helyreállítási terv tesztelése, karbantartása.

Az elektronikus információs rendszerekre vonatkozó helyreállítási tervek elkészítéséről, teszteléséről és folyamatos karbantartásáról a rendszergazda gondoskodik. A terv készítési tevékenységeket az IBF-nek információbiztonsági szempontból támogatnia és rendszeresen ellenőriznie kell.

A terveket minden olyan esetben aktualizálni kell, amikor jelentősen megváltozik az infokommunikációs infrastruktúra (pl.: új elektronikus információs rendszer bevezetése, új nagyteljesítményű hardverelemek változása).

A rendszergazdának - mindezeken túl - gondoskodnia kell az elektronikus információs rendszer helyreállításához szükséges mentések meglétéről, elérhetőségéről.

5. Emberi tényezőket figyelembe vevő - személy - biztonság

5.1. Munkaköri felelősség és az alkalmazás feltételei

A foglalkoztatottakat a Hivatalban végzendő tevékenység megkezdése előtt informatikai biztonsági képzésben kell részesíteni. A munkaköri leírásokban meg kell határozni az általános és az adott munkakörhöz tartozó információbiztonsági feladatokat és felelősségeket.

A Hivatalnak tájékoztatnia kell a dolgozókat arról, hogy milyen jogi felelősségük és kötelezettségük van az információbiztonsági előírások betartására vonatkozóan. A dolgozók információbiztonsági felelőssége arra az esetre is vonatkozik, ha nem a Hivatalban (pl. otthon), illetve a normál munkaidőn kívül dolgozik.

A munkahelyi vezető közvetlenül felelős azért, hogy az ellenőrzése alá tartozó felhasználók betartsák az IBSZ előírásait.

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

a) az új felhasználók kezdeti képzésének részeként;

b) amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;

c) a Hivatal vezetése által meghatározott gyakorisággal, de minimum évente egyszer

A munkatársak felelősek a képzési előírások betartásáért, a képzések során leadott anyagok elsajátításáért.

5.2. Eljárás jogviszony megszűnésekor

A jogviszony megszüntetésekor a következő feladatok végrehajtása szükséges:

a) Jogosultságok megszüntetése, úgy hogy a régi állapot mentésre vagy dokumentálásra kerül. Ezáltal a használt szoftverekhez való hozzáférés megszűnik.

b) A felhasználó elektronikusan tárolt információit, e-mailjeit és egyéb általa létrehozott adatot menteni, archiválni kell az általa használt informatikai eszközről, szerver tárhelyről, illetve bármely egyéb adathordozóról.

c) Az így archivált adatokat a törvényi előírásoknak megfelelően tárolni kell, illetve ha szükséges a megadott idő után törölni a rendszerből.

d) a munkavállaló Hivatali e-mail címének ideiglenes átirányítása az adott felelős vezetőnek vagy az általa kijelölt személy címére.

e) Külső vagy távmunka esetén a hálózathoz való csatlakozás lehetőségét meg kell szüntetni, a kapcsolat létrehozását tiltani kell.

A fenti feladatok végrehajtásáért a rendszergazda a felelős. A rendszergazda megfelelő időbeni tájékoztatásáért (adott esetben még a felhasználó értesítése előtt), hogy a fenti lépéseket megfelelő előkészületek alapján időben el tudja végezni, a szervezeti egység, és a jegyző felelős.

5.3. Eljárás jogviszony jelentős megváltozása esetén

Munkavállaló áthelyezése vagy feladatkörének jelentős megváltozása esetén az érintett felelős vezető igénylésére az alábbi intézkedéseket kell alkalmazni:

- Az érintett felelős vezetőnek meg kell igényelnie a munkavállaló számára azokat a hozzáféréseket, amik szükségesek az adott munka elvégzéséhez, és amelyre a felhasználó az új munkaköre által jogosultságot szerez.
- Az eszköznyilvántartás alapján a rendszergazdának el kell döntenie, hogy a munkavállaló eddigi munkavégzésére bocsájtott eszközök megfelelnek-e az új feladatok teljes körű ellátásához. Amennyiben az eszközök biztosítják a szükséges erőforrásokat, úgy átadás-átvételi jegyzőkönyvet nem kell felvenni, csupán a nyilvántartásban kell jelezni az eszköz elhelyezésének megváltozását.
- A szoftverekhez, alkalmazásokhoz való hozzáférését ellenőrizni kell. Azokhoz a szoftverekhez, amikhez az érintett felelős vezető nem igényelt hozzáférést, a felhasználó korábbi hozzáféréseit le kell tiltani. Az újakhoz a megfelelő jogosultságot meg kell adni.

5.4. Fegyelmi intézkedések

A Hivatal:

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

5.5. Viselkedési szabályok az interneten

a) A Hivatal tiltja és számon kéri a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét;

b) A Hivatal tiltja a belső szabályzatában meghatározott, interneten megvalósuló tevékenységeket (pl.: chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták, stb.);

c) tilthatja a közösségi oldalak használatát, magánpostafiók elérését, és más, a Hivataltól idegen tevékenységet.

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

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

Az internet és az IT rendszer kizárólag a Hivatalai munkát segíti, tehát kizárólag munkahelyi célra engedi használni azokat. A rendszergazda (ill. erre feljogosított, megbízott személy) jogosult ellenőrizni az internet használatát, hogy a felhasználók betartották-e a tiltásra vonatkozó szabályokat, valamint a hálózati kommunikációt, az egyes IT eszközök jogos és szakszerű használatát.

5.5.1. A web böngészés szabályai

Az Internethez való kapcsolódás csak és kizárólag a munkavégzést szolgálja!

Az Internet és az elektronikus levelezés használatának főbb szabályai:

- A nem munkavégzést szolgáló hálózati sávszélesség foglalása (pl. nagyméretű állományok letöltése), és adatok kiszolgálón történő tárolása esetén a felhasználó figyelmeztetésben részesül. Ismételt előfordulás esetén az rendszergazda jelentést tesz az IBF-nek, aki eljár az ügyben a jegyző felé.
- Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, kiiktatása. Ebbe a körbe tartoznak a vírusellenőrző és Internet böngésző kontrollok is.
- Tilos internetes vagy más jellegű szolgáltatást nyújtó külső féllel hálózati kapcsolat kialakítása.
- Tilos az elektronikus információs rendszerek használata a Hivatali értékekkel összhangban nem álló célokra, vagyis pl. szexuális jellegű fájlok fogadására, küldésére, fenyegetésre vagy megfélemlítésre, megkülönböztetésre, gyűlölködésre, fegyverekkel és illegális drogokkal való kereskedésre, erőszakra, internetes- illetve szerencsejátékokra, bármilyen kereskedelmi, illetve jogellenes tevékenységre.
- Az internetről csak Hivatali célból lehet fájlokat letölteni! Tilos fájlletöltő szolgáltatások használata. Különösen tilos jogvédett, illetve illegális tartalmak, fájlok letöltése, tárolása!

Az internetes oldalak elérése monitorozásra és naplózásra kerülhet, a munkával összefüggésbe nem hozható oldalak elérhetőségét az informatikai üzemeltetés jogosult korlátozni.

5.5.2. Az elektronikus levelezés szabályai

A Hivatal fontosnak tartja a munkatársai hatékony belső és külső kommunikációját ezért elektronikus levelezési lehetőséget biztosít. A Hivatal által nyújtott elektronikus levelezési szolgáltatás igénybevételének a következők a szabályai.

- A levelek nem képviselhetnek a hatályos magyar jogszabályokba ütköző magatartásformát.
- A levelek nem sérthetik mások becsületét, emberi jogait, faji, nemzetiségi hovatartozását, vallási, politikai világnézetét.
- A levelezés nem veszélyeztetheti a hálózati infrastruktúra működését.
- A Hivatal által biztosított elektronikus levél cím és az elektronikus levelezési szolgáltatás kizárólag társasági munkavégzés céljára biztosított, ezért a felhasználóknak tilos a Hivatali email címüket nem társasági minőségben használni (pl.: regisztráció letöltési weboldalakra, online játék oldalakra, közösségi oldalakra stb.)!
- A Hivatal által nem támogatott külső levelezőrendszer (pl.: Gmail, Freemail) használata munkavégzésre nem engedélyezett.
- Az e-mail a munkavégzéssel kapcsolatos levelezést szolgálja, ahol az egy felhasználóra eső tárterület korlátozott, és ennek túllépése esetén a rendszer figyelmeztetést küld, további figyelmeztetési határok átlépése esetén pedig megszűnhet a további levelezési lehetőség.
- Az elektronikus levelek és csatolmányok védelmi előírásai megegyeznek az egyéb dokumentumok védelmének előírásaival.
- A felhasználók alapértelmezésben a levelezés során csak a saját postaládájukat tudják kezelni, mások postaládáit nem látják.
- Ismeretlen helyről származó e-mail-t megnyitni nem szabad, mert maga a levél vagy annak csatolmánya vírus lehet, ezért ezeket olvasatlanul törölni kell. Bizonytalanság esetén a levelet olvasatlanul továbbítani kell a rendszergazdának, elemzés céljából.
- Tilos a levélbombák, levelezési láncok küldése, illetve továbbküldése.
- Tilos a levelek fejlécének megváltoztatása, hamis levelek küldése.
- Tilos a levelezési címet olyan kereskedelmi listára feltenni, amelyről az államháztartás szervezete levelező rendszerét e-mail szeméttel (spam) terhelhetik meg.

6. Tudatosság és képzés

6.1. Képzési eljárásrend

A Hivatal rendszeres képzésben részesíti az információs rendszer felhasználóit. A képzések gyakoriságát az információs rendszerek változásainak és egyéb igényeknek a figyelembevételével határozzuk meg, de évente legalább egyszer belső oktatáson vesz részt minden munkavállaló. A szervezetbe újonnan belépő munkavállalókat a lehető leghamarabb alapképzésben részesítjük. Rendkívüli oktatást tart a Hivatal rendszereiben történő incidens után.

A Hivatal vezetése:

- felelős a képzési kritériumok meghatározásáért
- biztosítja a képzéshez a szükséges erőforrásokat
- gondoskodik a képzések fontosságának tudatosításáról a teljes szervezetben

Az információbiztonsági felelős:

- felelős a képzési rendszer kialakításáért, fenntartásáért
- felelős a szükséges oktatások megtartásáért

A munkatársak:

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

6.2. Biztonságtudatosság képzés

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

A képzésen kötelezően:

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

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

6.2.1. Alkalmazás előtt

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

A Hivatal informatikai rendszereihez hozzáférő minden felhasználóját munkába állását követően, és az informatikai rendszer használatát megelőzően tájékoztatjuk az informatikai rendszerek használatára vonatkozó szabályokról, az új belépő számára biztosítjuk az informatikai biztonsági szabályok megismeréséhez és megértéséhez szükséges minden szükséges támogatást.

6.2.2. Belső oktatások, továbbképzés

A jegyző feladata biztosítani, hogy a jogviszony fennállása alatt a felhasználó fenntartsa, szükség esetén megszerezze az általa ellátandó feladatkör betöltéséhez szükséges ismereteket, képzettségeket, képesítéseket, indokolt esetben biztosítsa a szükséges

oktatások megtartását, illetve gondoskodjon róla, hogy a felhasználó részt vegyen a megfelelő képzéseken, továbbképzéseken.

II. Fizikai védelmi intézkedések

7. Fizikai védelmi eljárásrend

A fizikai környezeti biztonság megteremtése, illetve fenntartása érdekében a vonatkozó jogszabályok, a biztonsági és tűzvédelmi szabványok, valamint a helyi szabályok és rendelkezések előírásainak maradéktalanul meg kell felelni.

Az informatikai rendszer fizikai környezetének kialakítása, működtetése és használata során az általános biztonsági előírások szerint kell eljárni, az alábbiak szerint:

- az informatikai szolgáltatásokat biztosító eszközöket (szerverek, hálózati eszközök, UPS, internet átjárók, stb) fizikailag védett, biztonságos helyre kell telepíteni, és a környezetet a berendezések gyártói által megadott fizikai feltételek szerint kell kialakítani, fenntartani,
- a környezeti fizikai feltételeket (hőmérséklet, páratartalom, áramszolgáltatás stb.) folyamatosan ellenőrizni kell,
- a megbízható működés biztosítása céljából a körülményeknek megfelelő legfontosabb klímatechnikai, épületgépészeti, áramellátó tartalékberendezésekről szükség esetén gondoskodni kell

7.1. Biztonsági zónák

Mind az infrastruktúrát, mind az információt meg kell védeni a jogosulatlan hozzáféréstől, a sérüléstől, valamint az illetéktelen felhasználástól.

Az illetéktelen károkozás és jogtalan hozzáférések megakadályozása érdekében fel kell mérni a lehetséges kockázatokat, melyek alapján ki kell jelölni a biztonsági zónákat. A biztonsági zónák védelmének arányban kell állnia a megállapított kockázatokkal.

7.2. Biztonsági határok

A biztonsági határok kijelölése során figyelni kell azokra a területekre, ahol információ-feldolgozó eszközök vannak telepítve. Biztonságos zóna lehet egy lezárt iroda, vagy néhány helyiség, amelyek vagy maguk zárhatók, vagy amelyekben zárható szekrények,

páncélszekrények vannak.Informatikai központoknak minősülnek azon helyiségek, melyek működő szerverek és hálózati elosztó elemek (router, switch) elhelyezésére és működtetésére szolgálnak.

7.3. A fizikai belépés ellenőrzése

A biztonságos területekre vagy biztonságos zónákba való belépést, beléptetést ellenőrizni kell. A védett zónák bejárati ajtajában a kulcsot nem lehet bent hagyni, ha az ajtó nyitva van, akkor a védett zónát nem szabad őrizetlenül hagyni.

Az informatikai biztonsági zónákba való belépési jogosultságot személyre szólóan, az adott személy feladata alapján kell meghatározni.A belépési jogosultsággal nem rendelkezők az informatikai központban csak az arra jogosultak felügyelete mellett tartózkodhatnak.

A Hivatalnak össze kell állítania azon személyek listáját, akik jogosultak a védett és az érzékeny területekre történő belépésre. A listát a jegyző hagyja jóvá. A biztonságos területekhez való hozzáférési jogokat rendszeresen át kell vizsgálni és frissíteni. Az átvizsgálást és frissítést az Informatikai Biztonsági Felelős végzi.

7.4. Az irodák, a helyiségek és az eszközök biztonsága

Az informatikai rendszerek környezetét a biztonsági osztályának megfelelő fizikai-, mechanikai-, elektronikai-, személyi védelemmel kell biztosítani.

A Hivatalnak az irodák, a szobák és a szerverszoba védelmét az alábbiak szerint kell szabályozni:

- a kulcsokat nem szabad nyilvános, idegenek számára is könnyen hozzáférhető helyen tárolni
- a védett és érzékeny helyiségek átlagos kinézetűek legyenek, ne hívják fel magukra a figyelmet, ne legyen rajtuk olyan jelzés, amelyből kiderül a funkciójuk
- a fénymásoló és nyomtató berendezéseket, a fax készülékeket védett területen belül kell elhelyezni
- a dokumentumok tárolása védett területen történjen
- azokban az időszakokban, amikor a helyiségek felügyelet nélkül maradnak, az ajtókat és ablakokat zárva kell tartani

Az alkalmazott védelmi formák körét az Informatikai Biztonsági Felelős határozza meg az informatikai biztonságpolitika és az adott létesítmény védelmi igényeinek és speciális feltételeinek figyelembevételével.

7.5. Tiszta íróasztal, tiszta képernyő politika

A Hivatal munkatársainak be kell tartania a „tiszta íróasztal" elvet az adathordozókra vonatkozóan, független azok megjelenési formájától (papír alapú, egyéb számítástechnikai adathordozó, pl.: pendrive). Valamint be kell tartania a „tiszta képernyő" szabályt a használt informatikai eszközre, munkaállomásra vonatkozóan.

A „tiszta íróasztal, tiszta képernyő" irányelvének betartására az adathordozókat ajánlatos arra alkalmas, zárható szekrényben őrizni/tárolni, amikor nincsen használatban, különösen munkaidőn kívüli időszakban.

A felhasználóknak gondoskodniuk kell arról, hogy íróasztalukon csak azok az adathordozók legyenek, melyek az aktuális munkafolyamatokhoz szükségesek.

A munkaállomásokat nem hagyhatják bejelentkeztetett állapotban felügyelet nélkül. A hosszabb ideig inaktív munkaállomásokat rendszer szinten blokkolni kell.

Az informatikai rendszerekben tárolt bizalmas adatok nyomtatása nem történhet felügyelet nélkül. (Akinek szükséges helyi nyomtató, vagy kódos nyomtatás a központi nyomtatókra, stb) A Hivatalnak olyan intézkedéseket kell hozni, melyek megakadályozzák az illetéktelen nyomtatást, vagy a nyomtatás során keletkezett papír alapú anyag illetéktelen kézbe kerülését. Annak betartásáért a felelős vezető felel.

7.6. Munkavégzés a biztonsági zónákban

A biztonságos zónákban való munkavégzés estén legfontosabb szabály, hogy a biztonságos zónákban nem engedhető meg a felügyelet nélküli munkavégzés. Egyrészt a biztonság

érdekében, másrészt a rosszindulatú tevékenység megelőzésére. Ezért a személyzet nélkül hagyott biztonsági zónákat fizikailag le kell zárni, és időről időre ellenőrizni.

A biztonságos zónákban való munkavégzésre csak állandó vagy eseti jogosultsággal rendelkezőknek szabad belépni. A hozzáférési jogosultság megadásért az Informatikai Biztonsági Felelős felel.

7.7. A berendezések fizikai védelme

Az informatikai berendezéseket fizikai valójukban is védeni kell. A védelemi intézkedésekre azért van szükség, hogy csökkentsük az adatokhoz való illetéktelen hozzáférés kockázatát.

A központi hardver erőforrások, az azokon üzemeltetett alkalmazások információvédelmének érdekében olyan helyiségekbe kerüljenek, melyek kielégítik a rájuk vonatkozó biztonsági követelményeket. Gondoskodni kell a megfelelő és szükséges mechanikai védelmükről.

Az informatikai rendszer adat- és üzembiztonságának megfelelő szinten tartása érdekében lehetőleg redundáns megoldásokat kell alkalmazni.

7.8. A berendezések elhelyezése és védelme

A berendezéseket úgy kell elhelyezni, hogy csökkentsük a környezeti fenyegetések és vészhelyzetek kockázatát, valamint a jogtalan hozzáférés lehetőségét.

Az érzékeny adatokat tároló eszközöket, a munkaállomásokat úgy kell elhelyezni, hogy a munkavégzés közbeni ügyfél általi rálátás kockázatát elkerüljük.

A központi hardvereszközök védelmére speciális intézkedéseket kell alkalmazni. Az informatikai rendszer biztonságos működésének érdekében a központi számítógépparkban (szerver szobák) klimatizált légteret, szünetmentes tápellátást, tűzjelző és –oltó berendezést kell biztosítani.

7.9. Tápellátás

Azinformatikaieszközökavonatkozószabványnakmegfelelőenkizárólagvédőföldelésselellátott 230V feszültségű elektromos hálózati dugaszoló aljzatba csatlakoztathatók.A kijelölt informatikusnak törekedni kell arra, hogy a szervezeti szintű alkalmazások működését

befolyásoló informatikaiéstávközlésieszközök(pl.: szerverek,rackszekrénystb.)szünetmentestápegységekkel legyenek ellátva.

7.10. A kábelezés biztonsága

Az áramellátás kábelezését, valamint az adattovábbító és informatikai szolgáltatások ellátásában használt távközlési kábeleket meg kell védeni a zavarásoktól, illetéktelen hozzáféréstől és a sérülésektől.

Ahol csak lehetséges ajánlatos az adatfeldolgozó rendszerekhez csatlakozó kábeleket zárt burkolatban vezetni (gégecső, védőcső, kábelcsatorna), a véletlen károkozás, vagy jogosulatlan lehallgatás elkerülésének érdekében.

A kábelezés biztonságáért a rendszergazda felel.

7.11. A berendezések karbantartása

Az informatikai eszközökön javítást, módosítást, illetve új eszközök telepítését csak a rendszergazdák, vagy az Informatikai Biztonsági Felelős által engedélyezett és ellenőrzött külső vállalkozó végezhet.

Adathordozók esetében, ha a javítás nem szerződött, a titoktartási szerződést nem elfogadott külső helyszínen történik, az adattartalmat törölni, az el- és visszaszállítást pedig dokumentálni kell.

A tervezett karbantartások mértéke és gyakorisága feleljen meg a gyártói előírásoknak és ajánlásoknak, de minimum évente egyszer legyen elvégezve.

Garanciális eszközt csak a gyártó által megadott módon és feltételekkel lehet javítani, szerelni, a karbantartásokat ezek alapján kell ütemezni.

A rendszeres és tervezett karbantartásoknak minél nagyobb mértékben hozzá kell járulniuk a kockázatok csökkentéséhez.

7.12. Berendezések védelme a Hivatal területén kívül

A felhasználókszámára mobiladathordozó használatátazadottszervezetiegységvezetője vagy a Hivatal jegyzője előzetesen kell engedélyezzen. A mobil eszközök (pl. notebook) használatára a munkaállomásokra vonatkozó szabályok érvényesek. A mobil eszközök

adattárolóit minden esetben megfelelő titkosítással kell ellátni, hogy esetleges elveszítésük esetén, még az eszköz megbontásával se legyen lehetőség hozzáférni az adatokhoz.
Amobilinformatikaieszközazarrafelhatalmazottszemélyrészéretörténőátadásakorátadás-átvételi jegyzőkönyv készül,melytartalmazzaazeszközműszakiadatait,azátadás-átvétel adatait és az eszközön telepített szoftverek adatait.Kiadott mobil eszközt felülvizsgálat céljából a kijelölt informatikusnak rendszeresen be kell mutatni. A mobil eszközön vírusvédelmi rendszer telepítéséről és folyamatos frissítéséről gondoskodni kell.Akijelöltinformatikuskötelesazeszközátadásasoránfelvilágosítaniadolgozótamobilinformatikai
eszközökhasználatánakveszélyeiről,kockázatairól,amitadolgozóatárolásinyilatkozatonaláírásával igazol, és az eszközért felelősséget vállal.
A mobil eszközöket használó személyeknek:
-nem engedélyezett az eszközt gépjárműben, idegen helyen felügyelet nélkül hagyni,
-utazás alatt a személyi számítógépet mindig felügyelettel (kézipoggyászként) kell szállítani,
-aHivatalterületénkívül,idegenhelyentörténőtárolásesetén(szálloda,lakás)fokozottfigyelmet kellfordítaniajogosulatlanhozzáférés,azadatokesetlegesmódosítása,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.

Akódolatlanmobiladathordozóeszközökrendkívülnagykockázativeszélyforrástjelentenek,ezért a felhasználókcsakinformatikaiellenőrzésmelletthasználhatják.
Ahivataliadathordozónmagánjellegű adatot tárolni nem engedélyezett, magánjellegű adathordozót hivatali célra használni nem engedélyezett, azon hivatali adatot tárolni nem szabad.
AHivatalinformatikairendszerébekapcsoltmunkaállomásokoncsakolyanadathordozótlehethasználni,
arróladatokatbeolvasni,melyenelőttearendszeresítettéstelepítettvíruskeresőprogrammal vírusellenőrzést
végeztek.Amobilinfokommunikációseszközök,mobiladathordozókfelhasználóifelelősekazeszk

özöntalálható
adatokesetlegeskiszivárgásáért,azeszközelvesztéséért,eltűnéséért,megsérüléséért.Amobil infokommunikációs eszközök, mobil adathordozók eltűnése, ellopása esetén annak tényét haladéktalanul a Hivatal vezetője felé jelentenie kell a szükséges intézkedések megtétele érdekében.Afelhasználókegyesfeladatokelvégzéseérdekében,arészükrebiztosított,nyilvántart ottésegyedi
azonosítóvalellátott,hivatalitulajdonúmobiladathordozóra(pendrive,mobilHDD)kimenthetika feladathoz kapcsolódó állományaikat. A mobil adathordozókat minden esetben megfelelő titkosítással kell ellátni, hogy esetleges elveszítésük esetén, se legyen lehetőség hozzáférni az adatokhoz.

7.13. A berendezések biztonságos tárolása és újrafelhasználása

A berendezéseket úgy kell tárolni, hogy csökkentsük a környezeti fenyegetések kockázatát, valamint a jogtalan hozzáférés lehetőségét.
Az érzékeny információt tartalmazó tárolóeszközöket vagy meg kell fizikailag semmisíteni, vagy biztonságosan felül kell írni az egyszerűtörlési művelet alkalmazása helyett.
Az érzékeny információt tartalmazó, de sérült tárolóeszközök tartalmának kritikussága alapján kell meghatározni, hogy az adott eszköz megsemmisítésre vagy javításra kerüljön.

7.14. Eszközök selejtezése, elvitele

A Hivatal vagyonleltárába tartozó valamennyi eszközre vonatkozóan a Hivatal belső szabályozásának megfelelő irányelveket.
Megsemmisítésre kijelölt eszközöket és kellékanyagokat megsemmisítésig a használatban lévő eszközöktől elkülönítetten kell tárolni és kezelni figyelembe véve:
-a veszélyesanyagoktárolásáraésamegsemmisítésrevonatkozószabályokat(fizikaivédelem, szállítás),
-a leltározási és selejtezési szabályzat előírásait,
-az adatvédelem biztonsági követelményeit (hozzáférés elleni védelem)
Azinformatikaiberendezésekvéglegeshasználatonkívülhelyezéseelőttgondoskodnikellazössze sadat,
szoftvervisszaállíthatatlaneltávolításárólésfelülírásáról,vagyabeépítettadathordozóeltávolítás árólés megfelelő tárolásáról.

7.15. Az elektronikus információs rendszer elemeinek elhelyezése

A Hivatal úgy helyezi el az elektronikus információs rendszer elemeit, hogy a legkisebb mértékre csökkentse a szervezet által meghatározott fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét.

III. Logikai védelmi intézkedések

8. Általános védelmi intézkedések

8.1. Személy biztonság

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed az érintett szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki az érintett szervezet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem az érintett szervezet tagja, a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

8.2. Rendszerbiztonsági terv

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

a) összhangban áll az Informatikai Biztonságpolitikával és a Biztonságtervezési Eljárásrenddel, valamint igazodik a szervezet felépítéséhez és architektúrájához,

b) meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait (biztosítandó szolgáltatásait és azok elvárt szolgáltatási szintjeit [angolul SLA]), biztonságkritikus elemeit és alapfunkcióit;

c) meghatározza az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát;

d) meghatározza az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;

e) a vonatkozó rendszerdokumentáció keretébe foglalja az elektronikus információs rendszer biztonsági követelményeit (naplózás, mentés és helyreállítás, üzletmenet-folytonosság);

f) meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és azok bővítését, végrehajtja a jogszabály szerinti biztonsági feladatokat;

g) gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is);

h) belső szabályozásában, vagy a rendszerbiztonsági tervben meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszer rendszerbiztonsági tervét (belső audit);

i) frissíti a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások, és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;

j) elvégzi a szükséges belső egyeztetéseket;

k) gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

Kivételek

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

8.3. Cselekvési terv

Az érintett szervezet cselekvési tervet készít, ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg;

a) a cselekvési tervben dokumentálja a megállapított hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeit;

b) frissíti a meglévő cselekvési tervet az érintett szervezet által meghatározott gyakorisággal a biztonsági értékelések, biztonsági hatáselemzések és a folyamatos felügyelet eredményei alapján.

A jegyző felelőssége biztosítani az elektronikus információs rendszerek biztonságáért felelős személy szakmai támogatása mellett a cselekvési terv előrehaladásának folyamatos nyomon követését és a fontosabb mérföldkövek mentén a feladatok előre haladásának értékelését. A jegyző elrendelheti, illetve az elektronikus információs rendszerek biztonságáért felelős

személy kezdeményezheti a készre jelentett feladatok utóvizsgálatát, amit utólag beépítünk az éves ellenőrzési tervbe.

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

8.4. Személyi biztonság

A Hivatal:

a) megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat a rájuk vonatkozó szabályokat, felelősségüket az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet;

b) Az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja;

c) meghatározott gyakorisággal felülvizsgálja és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat a rájuk vonatkozó szabályokat, felelősségüket az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet a viselkedési szabályok betartását;

d) gondoskodik arról, hogy a c) pont szerinti változás esetén a hozzáféréssel rendelkezők tekintetében a b) pont szerinti eljárás megtörténjen;

e) meghatározza az érintett szervezeten kívüli irányban megvalósuló követelményeket;

9. Rendszer és szolgáltatás beszerzés

9.1. A rendszer fejlesztési életciklusa

Az informatikai eszközök különböző beszerzési eljárásmódjainak alkalmazásánál fokozottan szem előtt kell tartani, hogy a szóban forgó eszköz megfeleljen a jelen szabályzatban rögzített informatikai biztonsági követelményeknek.

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

Fejlesztés esetén már a rendszer tervezésénél fokozottan figyelembe kell venni az informatikai biztonsági előírásokat, ajánlásokat.

A Szervezet a fejlesztési életciklus egészére meghatározza és dokumentálja az információbiztonsági szerepköröket és felelősségeket, valamint a szervezetre érvényes szabályok szerint kijelöli ezen szerepköröket betöltő, felelős személyeket.

A rendszer életciklus szakaszai a következők:

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

10.Konfigurációkezelés

10.1. Eljárásrend

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

10.2. Alapkonfiguráció

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

10.3. Elektronikus információs rendszerelem leltár

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

a) pontosan tükrözze az elektronikus információs rendszer aktuális állapotát,

b) az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet, valamint azok licenceit tartalmazza;

c) legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez.

10.4. Szoftverhasználat korlátozásai

A Hivatal:

a) kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi, vagy más jogszabályoknak;

b) a másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát;

c) ellenőrzi és dokumentálja az állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

10.5. A felhasználó által telepített szoftverek

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

11.Karbantartás

11.1. Rendszer karbantartási eljárásrend

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

11.2. Rendszeres karbantartás

A Hivatal által megbízott személyek vagy vállalkozók:

a) a karbantartásokat és javításokat ütemezetten hajtatja végre, dokumentáltatja és felülvizsgáltatja a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a Hivatal követelményeinek megfelelően;

b) jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;

c) az ezért felelős személyek jóváhagyásához köti az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a Hivatali létesítményből;

d) az elszállítás előtt (amennyiben szükséges) minden adatot és információt - mentést követően - töröl a berendezésről;

e) ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;

f) csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási a számítástechnikai eszközökön javítást, módosítást, illetve új eszközök telepítését csak a rendszergazdák, vagy az általuk megbízott és ellenőrzött külső vállalkozó végezhet;

g) számítógépek esetében, ha a javítás titoktartási szerződés által nem kötött külső helyszínen történik, az esetleges adattartalmat töröljük, az el- és visszaszállítást pedig dokumentáljuk

h) a nem javítható eszközöket a leírtaknak megfelelően selejtezzük, esetleges adattartalmukat pedig - szükség esetén véglegesen és helyreállíthatatlanul - töröljük

i) a tervezett karbantartások mértéke és gyakorisága megfelel a gyártói előírásoknak és ajánlásoknak, de minimum évente egyszer elvégzésre kerül;

j) minél nagyobb mértékben járuljon hozzá a kockázatok (a működési szabályok betartásával] csökkentéséhez, a helyes és rendszeres karbantartottság révén;

12.Adathordozók védelme

12.1. Adathordozók védelmére vonatkozó eljárásrend

A Hivatal az alábbi hordozható adathordozókat különbözteti meg, ezek használatát engedélyezi:

- CD/DVD lemez
- pendrive
- notebook
- hordozható/külső winchester

Az adathordozók védelmének célja, hogy a fizikai védelmet szabályozzák, a megfelelő eljárásokkal védjék a dokumentumokat, a számítógép adathordozóit, a bemenet/kimenet adatait és a rendszer dokumentációját a jogosulatlan megszerzéstől, módosítástól, eltávolítástól és rongálástól.

A Hivatal az adathordozókat informatikai eszköznek tekinti, melyekről nyilvántartást vezet. Azoknak az adathordozóknak, melyek bármilyen okból, kivéve megsemmisítés, használaton kívül vannak, szintén szerepelniük kell a nyilvántartásban, melynek használton kívül helyezését jelölni kell.

A Hivatalban csak a Hivatal tulajdonában lévő, regisztrált adathordozót lehet használni. Adathordozó igénylését a rendszergazdához kell benyújtania a felelős vezetőnek.

Az eszközhasználatot, a Hivatal elektronikus információs rendszereihez történő csatlakoztatása után, a Hivatal minden előzetes értesítés nélkül figyelheti, monitorozhatja.

12.2. Hozzáférés adathordozókhoz

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

A használni kívánt adattárolót a tárolásra kijelölt helyről vesszük ki és használatot követően oda is helyezzük vissza. A munkaasztalokon csak a munkavégzéshez használatos adathordozók

Az adattárolóknak minden felhasználónak rendeltetésszerűen használja. A Hivatal adathordozóin csak munkavégzéshez szükséges adatokat tároljuk.

A felhasználók saját tulajdonú adathordozóit az informatikai hálózatra nem csatlakoztathatnak.

12.3. Adathordozók törlése

Az adathordozókat selejtezés vagy az újrafelhasználásra való kibocsátás előtt a rendszergazda helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törli, így védve az adatok bizalmasságát. A biztonságos törlés eredményességét a rendszergazda minden esetben ellenőrzi. A meghibásodott, további felhasználásra alkalmatlan adathordozókat a rendszergazda fizikai roncsolással megsemmisíti.

Az adathordozók újrahasznosítása vagy mások rendelkezésre bocsátása előtt minden esetben gondoskodni kell arról, hogy az infokommunikációs eszközökön tárolt információk visszaállíthatatlanul eltávolításra kerüljenek. Ennek érdekében

- a rajtuk tárolt adatokat törölni kell;
- a törlést az adattárolón lévő adatok gazdájának jóvá kell hagynia;
- garanciális eszközök esetén, ha az eszköz hibája miatt az adatok törlésére nincs mód, az IBF dönt az eszköz cserére történő kiadhatóságáról, vagy megsemmisítéséről.

Az adatok megfelelő módon történő eltávolításáért az adatgazda a felelős. Az adatok eltávolítását a rendszergazda végzi. Az adatok eltávolítását jegyzőkönyvezni kell.

Csak a bizonyíthatóan visszaállíthatatlanul törölt adathordozókat lehet újra felhasználni. Azokat az adathordozókat újrahasznosítani nem lehet, amiket sérülés vagy elhasználódás miatt nem lehet helyreállíthatatlanul törölni. Az ilyen adathordozókat a Hivatal belső szabályai szerint selejtezni kell, ha az előírás úgy határozza meg, az adathordozót meg kell semmisíteni.

12.4. Adathordozók használata

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

13.Azonosítás és hitelesítés

13.1. Azonosítási és hitelesítési eljárásrend

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

13.2. Azonosító kezelés

A Hivatal:

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

13.3. Hitelesítésre szolgáló eszközök kezelése

A Hivatal vezetése által kijelölt személy:

a) ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát;

b) meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;

c) biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;

d) dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket;

e) megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során;

f) meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;

g) a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket;

h) megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;

i) megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;

j) lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

13.4. A hitelesítésre szolgáló eszköz visszacsatolása

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

13.5. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

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

14.Hozzáférés ellenőrzése

14.1. Hozzáférés ellenőrzési eljárásrend

A felhasználó részére az informatikai rendszerbe való belépést engedélyezni csak és kizárólag abban az esetben szabad, ha a felhasználó valamilyen módon azonosítja magát.

Az informatikai rendszer erőforrásait és felhasználóinak hozzáférési jogait egységes elvek alapján határozza meg és osztja ki a Hivatal.

Az informatikai rendszer felhasználóinak hozzáférési jogait a Hivatal központilag nyilvántartja.

A központi jogosultság-nyilvántartási rendszer tartalmazza a jogosultság kezeléshez kapcsolódó mindazon adatokat, amelyekből egyértelműen megállapítható, hogy kinek, milyen rendszerhez, milyen jogosultságai vannak.

Az informatikai rendszerben haladéktalanul meg kell szüntetni/fel kell függeszteni azon személyek hozzáférési jogait, akiknek jogviszonya a hivatallal megszűnt. A jogviszony megszűnését a szervezeti egység, vagy a Hivatal vezetője írásban előre jelzi az informatikusnak a jogosultság kizárása időpontjának megjelölésével.

A hozzáférési jogok kezelését jelen eljárásrendben foglaltak szerint kell megvalósítani akövetkező alapelvek alkalmazásával:

a) Minden felhasználó csak a feladatellátásához szükséges, minimális jogosultságot kapja meg.

b) A felhasználók a munkaállomásukon nem rendelkezhetnek rendszergazda jogokkal.

c) A rendszergazda a rendszerek adminisztrálásához használt adminisztrátori azonosítóját a napi munkavégzése során nem használhatja. A napi munkavégzéshez normál felhasználói jogú azonosítót kell használnia.

d) Az önkormányzati ASP szakrendszerekhez történő hozzáféréseket a működtető által megfogalmazott eljárásrend alapján kell kezelni.

14.2. Felhasználói fiókok kezelése

A felhasználók csak jóváhagyott hozzáférés-védelmi megoldásokat alkalmazhatnak.

A jogosultságok és a hozzáférés menedzselésekor az alábbi alapelveket kell figyelembe venni:

a) A meghatározott jogosultságok alkalmazásával minimalizálható legyen a rosszindulatú vagy egyéb jogosulatlan hozzáférés kockázata.

b) Az elektronikus információs rendszerrel kapcsolatba kerülő személyeknek a munkájuk ellátásához szükséges minimális jogosultságokat kell biztosítani, a munkavégzésük időtartamára.

c) Az azonos tevékenységet ellátó felhasználók jogosultságai szerepkörök szintjén legyenek kialakítva, és a felhasználók a kialakított szerepkörökbe kerüljenek besorolásra.

d) Az összeférhetetlenségi szabályokat figyelembe kell venni.

e) Az elektronikus információs rendszerben alkalmazott hozzáférési jogosultságokat adminisztrálni kell.

f) Törekedni kell arra, hogy a jogosultságok automatizált módon kerüljenek nyilvántartásba, szükség esetén, papír alapon kell a nyilvántartást vezetni.

g) Minden egyes elektronikus információs rendszerhez, csak a megfelelő adminisztrálást követően lehet felhasználói jogosultságot adni, módosítani, és felfüggeszteni, illetve visszavonni.

h) Az éles elektronikus információs rendszerekben a fejlesztők hozzáférési jogosultságokkal nem rendelkezhetnek.

A felhasználók nyilvántartásba vételi szabályainak és a követendő eljárásrend kidolgozásakor a következőket kell figyelembe venni:

a) A felhasználói tevékenység ellenőrizhetősége és nyomon követhetősége érdekében a felhasználók elektronikus információs rendszerekben történő azonosítására egyedi felhasználó azonosítókat kell alkalmazni.

b) A csoportos felhasználó azonosítók használatát tiltani kell.

c) A felhasználói hozzáférési jogosultságokat a szervezeti egység vezetője határozza meg. A jogosultság meghatározása során figyelembe kell venni:

- a felhasználó munkakörét és az azzal kapcsolatos feladatait,
- a munkaköri feladatok végrehajtásához minimálisan szükséges jogosultságok elvét,
- a felhasználó jogviszonyát,
- a felhasználó munkahelyét.

14.3. A hozzáférés ellenőrzésének szabályai

A hozzáférés-védelmi rendszert a biztonsági osztálynak megfelelően kell megtervezni. A hozzáférési jogosultságok odaítélését a feladatteljesítés követelményeihez igazodva kell megállapítani.

A Hivatal a legkevesebb jogosultság elv betartásával a felhasználók és az alkalmazások erőforrásokhoz való hozzáférését csak a legszükségesebbekre korlátozza. Ennek érdekében meg kell határozni a felhasználók munkájához szükséges jogosultságok minimális halmazát. A felhasználók pedig ehhez a halmazhoz kapnak csak hozzáférést (se többhöz, se kevesebbhez).

14.4. Azonosítás és hitelesítés nélkül engedélyezett tevékenységek

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

14.5. A munkaszakasz zárolása

Ha a felhasználó szünetelteti a munkaállomáson végzett tevékenységét, ki kell jelentkeznie, vagy zárolnia kell a számítógépet, vagy automatikus képernyővédőt kell alkalmazni a domain policy-ban, melynek időzített aktiválása a munkaállomás kihasználatlansága esetén nem lehet több 10 percnél. A rendszernek ez után újra kell indítania az azonosítási és a jogosultság ellenőrzési folyamatot, a felhasználó csak az újbóli bejelentkezés, illetve jelszó megadás után folytathatja a munkát. A megnyitott alkalmazásokat, a használatot követően a felhasználónak be kell zárnia. A felügyelet nélkül hagyott felhasználói munkaállomások védelme érdekében a munkaállomások beállításait a rendszergazdák végzik. A felhasználóknak tilos a rendszergazdák által beállított paraméterek törlése, megváltoztatása.

14.6. Külső elektronikus információs rendszerek használata

Az érintett szervezet:

- meghatározza, hogy milyen feltételek és szabályok betartása mellett jogosult a felhasználó egy külső rendszerből hozzáférni az elektronikus információs rendszerhez;
- meghatározza, hogy külső elektronikus információs rendszerek segítségével hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani az érintett szervezet által ellenőrzött információkat.

14.7. Nyilvánosan elérhető tartalom

Az érintett szervezet:

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

15.Rendszer és információ sértetlenség

15.1. Rendszer és információ sértetlenségre vonatkozó eljárásrend

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

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

15.2. Hibajavítás

A Hivatal:

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

b) telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket a szervezet feladatellátásának hatékonysága, az előre nem látható következmények szempontjából;

c) a biztonságkritikus szoftvereket frissítésük kiadását követő 1 hónapon belül telepíti, vagy telepítteti;

d) beépíti a hibajavítást a konfigurációkezelési folyamatba.

A rendszerprogramokkal kapcsolatos bármely konfigurálási, hangolási műveletet csak a rendszergazda végezhet. Az alkalmazáson végzendő, annak bármely funkcióját megváltoztató művelethez – beleértve a verzióváltást és egyéb, jelentős beavatkozást igénylő hangolást is – a jegyző engedélye szükséges.

A rendszergazdának biztosítania kell, hogy a rendszerszoftver naprakész állapotban legyen, és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek az üzemeltetők számára.

Az alapszoftver módosítással egy időben a változásokat a dokumentációban is át kell vezetni.

A felhasználói adatok és alkalmazások védelme érdekében a szoftverek módosítása (frissítés, verzióváltás) folyamán az alkalmazáshoz és az adatokhoz történő illetéktelen hozzáférést és az illetéktelen próbálkozást meg kell akadályozni. Gondoskodni kell arról, hogy a telepített alkalmazások, fájlok ne károsodjanak, és a követelményeknek megfelelően működjenek.

Új hardverek üzembe állításakor a fentieket kell értelemszerűen alkalmazni.
Gondoskodni kell arról, hogy a munkaállomásokon telepített operációs rendszerek és egyéb segédprogramok naprakészek legyenek.

15.3. Kártékony kódok elleni védelem

A Hivatalnak meg kell őriznie az elektronikus információs rendszerek és az információ bizalmasságát, sértetlenségét és rendelkezésre állását a kártékony kódok és a kéretlen üzenetek
támadásaival szemben.
A kártékony kódok elleni védekezés során a következőkről kell gondoskodni:

a) Munkaállomások és kiszolgálók esetében memóriában rezidens kártékony kód elleni megoldásokat kell alkalmazni.

b) Kártékony kód elleni megoldás nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem üzemeltethető.

c) Egyéb infokommunikációs eszközök tekintetében a gyártói ajánlások és a lehetőségek figyelembe vételével törekedni kell a kártékony kódok elleni védekezésre.

d) A kártékony kód elleni alkalmazások adatbázisát automatikusan frissíteni kell.

e) A kártékony kód elleni alkalmazásnak az email-ek csatolmányát ellenőriznie kell, a futtatható állományok szűrését be kell kapcsolni.

f) A hordozható számítógépek esetében az üzemeltetőnek gondoskodnia kell a kártékony kód elleni alkalmazás adatbázisának automatikus frissítéséről, közvetlenül a hordozható számítógép bekapcsolása után.

g) A külső forrásból származó a cserélhető adathordozókat használatba vétel előtt automatikus kártékony kód ellenőrzés alá kell vetni.

h) A felhasználókat meg kell ismertetni a kártékony kód felmerülésének esetében követendő előírásokkal.

i) A kártékony kód felfedezésekor teendő intézkedéseket és a jelentési rendszert szabályozni kell. A rendszergazdának értesítenie kell az IBF-et. A további teendőket az IBF határozza meg.

j) Kártékony kód általi fertőzéskor a munkaállomást haladéktalanul le kell választani a hivatali hálózatról és így kell megtenni a szükséges vírusirtást vagy a rendszer újratelepítését.

k) A vírusfertőzésekkel és elhárításukkal kapcsolatban tett intézkedéseket dokumentálni kell.

A rendszergazda a számítógépek vírusok elleni védelmére rendszeresen frissített vírusvédelmi rendszert, és anti-spyware programot üzemeltet. Ez a védelem kiterjed a kiszolgálók, munkaállomások valamint a teljes Internet és elektronikus levélforgalom folyamatos ellenőrzésére. Új vírus megjelenése esetén még így is előfordulhat fertőzés, valamint csatolmányok, CD és DVD lemezek, cserélhető adathordozók, illetve internetről letöltött fájlok használata esetében.

Vírusvédelem nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem használható.

Dokumentumok esetében lehetőség szerint kerülni kell a makrók megnyitását, külső forrásból érkező dokumentumok esetében pedig nem szabad engedélyezni.

Ha a vírus helye nem lokalizálható, a rendszergazda jogosult a hálózat egyes funkcióit, vagy a teljes hálózat felhasználói szolgáltatásait a vírusveszély elhárításáig felfüggeszteni.

Teendők vírusfertőzés esetén:

Az IBF feladata a vírus fertőzés kivizsgálásának irányítása, a felelősség megállapítása.

A rendszergazda a feladatai:

a) a vírusvédelmi rendszer támogatójának értesítése;

b) a vírus fertőzés következtében szükséges intézkedések koordinálása;

c) a fertőzés tényének és a foganatosított intézkedéseknek a rögzítése;

d) a vírusos számítógép leválasztása a hálózatról;

e) a felhasználók értesítése a vírusról;

f) az e-mail rendszer leállítása, ha mail-ben terjedő vírusról van szó;

g) a hálózaton terjedő vírus esetén a külső kapcsolat megszakítása;

h) a vírus adatait tartalmazó vírus tudásbázis letöltése és teljes vírusellenőrzés végrehajtása;

i) a fertőzöttség lehetőségeinek feltérképezése, gondolva a hálózaton, cserélhető adathordozók által, vagy e-mail-en történő fertőzésekre;

j) a kliensek frissítése;

k) manuális vírus ellenőrzés végrehajtása azokon a munkaállomásokon, amelyek megfertőződhettek;

l) amennyiben az a hivatalon kívülre is terjedhetett, értesíteni kell az érintett szervezeteket;

m) a vírus fertőzés okának kivizsgálása a vírusvédelmi szoftver támogatójával közösen.

15.4. Automatikus frissítés

Az elektronikus információs rendszer automatikusan frissíti a kártékony kódok elleni védelmi mechanizmusokat.

15.5. Az elektronikus információs rendszer felügyelete

Az elektronikus információs rendszerek napi üzemeltetéséhez tartozik a működés felügyelete, a mentések elvégzése, illetve hiba esetén az eszközök javítását végzők bevonása.

Az elektronikus információs rendszerek felügyelete az alkalmazások, az adatbázisok, a kiszolgálók és az alapszoftverek, az informatikai hálózat és a munkaállomások működésének folyamatos figyelemmel kísérését kívánja meg.

A fenti feladatok végrehajtása a rendszergazda feladata.

A rendszergazdának ismernie kell a Hivatal rendszereszközeinek, elektronikus információs rendszereinek működését és azok figyelmeztető és hibaüzeneteit. A szükséges reagálásokat tartalmazó leírást tudniuk kell alkalmazni.

A rendszergazdának rendszeresen el kell végeznie azokat a tevékenységeket, amelyek alapján meggyőződhet arról, hogy az elektronikus információs rendszer üzemszerűen működik.

Az üzembiztonság érdekében a kiszolgálók operációs rendszereinek telepítőkészleteit tartalék adathordozón is tárolni kell, valamint az operációs rendszer beállításait rendszeresen menteni kell.

Az üzemeltetési eljárások megfelelőségét az információbiztonsági felülvizsgálatok alkalmával az IBF felülvizsgálja, a szükséges módosításokat átvezetik, a jegyző pedig jóváhagyja.

15.6. A kimeneti információ kezelése és megőrzése

Az érintett szervezet az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

A kimeneti információk (pl.: nyomtatás) kezelésével és szétosztásával kapcsolatban a Hivatal

Iratkezelési Szabályzatával összhangban a következők az előírások:

a) gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről,

b) gondoskodni kell arról, hogy a kimeneti információhoz történő fizikai és logikai hozzáférészcsak az arra jogosított személyekre korlátozódik,

c) gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimenetiinformációkat,

d) biztosítani kell, hogy a megsemmisítési eljárások során az kimeneti információk tartalma

helyreállíthatatlanul megsemmisüljön.

16.Naplózás és elszámolhatóság

16.1. Naplózási eljárásrend

Biztosítani kell, hogy az alkalmazott elektronikus információs rendszerek a következő eseményeket naplózni tudják:

a) a felhasználók adminisztrációs tevékenysége:

- bejelentkezés;
- kijelentkezés;
- jelszómódosítás.

b) a rendszergazdák a rendszer bármely rétegébe történő be-és kijelentkezése;

c) a rendszergazdák tevékenysége a rendszer bármely rétegében;

d) a felhasználói jogosultságok módosítása;

e) rendszer események, esetleges hibák;

f) konfigurációs beállítások módosítása.

g) Az esemény típusának megfelelően az általános feldolgozási eseményt az eseménynaplóban, a biztonsággal összefüggő eseményeket pedig a biztonsági naplóba kell rögzíteni.

Az elektronikus információs rendszerek naplózása kialakításakor be kell vonni a rendszeradatgazdáját is, annak érdekében, hogy adatgazdai oldalról meghatározásra kerüljenek azok a többletinformációk, amelyeket az adatgazdák igényelnek.

Az önkormányzati ASP rendszer szakrendszerei naplózásának a kialakítása a működtető

feladata.

16.2. Naplózható események

Biztosítani kell, hogy az alkalmazott elektronikus információs rendszerek a következő eseményeket naplózni tudják:

- bejelentkezés
- kijelentkezés
- jelszómódosítás
- rendszergazdai műveletek
- jogosultságok módosítása
- rendszer események
- konfigurációs beállítások módosítása
- sikertelen bejelentkezések
- rendszer események (indítás, leállítás)
- biztonsági mentéssel kapcsolatos események

16.3. Naplóbejegyzések tartalma

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

A naplóbejegyzéseknek a következőket kell tartalmaznia:

a) a rendszerelem azonosítóját,

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

c) az esemény ismertetését / a funkcióazonosítót,

d) a felhasználó azonosítóját,

e) az esemény időpontját,

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

16.4. Időbélyegek

Az elektronikus információs rendszereknek a naplóbejegyzésekhez készített időbélyegeket atartományvezérlők szinkronizált órái alapján kell elkészítenie.

Az elektronikus információs rendszer a naplóbejegyzések előállításához. Időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz – úgynevezett UTC –rendelhető módon, megfelelve a Hivatal által meghatározott időmérési pontosságnak.

Az elektronikus információs rendszer meghatározott gyakorisággal összehasonlítja a belső rendszerórákat egy hiteles külső időforrással, és ha az időeltérés nagyobb, mint a meghatározott időtartam, szinkronizálja a belső rendszerórákat a hiteles külső időforrással.

16.5. A naplóinformációk védelme

Az elektronikus információs rendszereknek a jelen IBSZ-ben foglaltaknak megfelelően meg kell védenie a napló információkat és a napló eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

16.6. A naplóbejegyzések megőrzése

A Hivatal a naplóbejegyzéseket meghatározott, a jogszabályi, és a hivatalon belüli információ megőrzési követelményeknek megfelelő időtartamig megőrzi, a biztonsági események utólagos vizsgálatának biztosítása érdekében.

16.7. Naplógenerálás

Olyan elektronikus információs rendszereket kell alkalmazni, melyek

a) biztosítják a naplóbejegyzések előállítási lehetőségét a *Naplózható események* pontbanmeghatározott naplózható eseményekre;

b) lehetővé teszik meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az információs rendszer egyes elemeire;

c) naplóbejegyzéseket állít elő a *Naplózható események* pontban meghatározottak szerintieseményekre az *Naplóbejegyzések tartalma* pontban meghatározott tartalommal.

17.Rendszer és kommunikáció védelem

17.1. Rendszer és kommunikáció védelmi eljárásrend

Az elektronikus információs rendszerek és a kommunikáció védelmére vonatkozóan akövetkező eljárásrendet kell alkalmazni.

Az önkormányzati ASP rendszer szakrendszereinek és azok kommunikációjára vonatkozóvédelem a működtető feladata.

A Hivatal hatásköre a hivatali határvédelemig terjed.

17.2. Határok védelme

Mind a belső, mind a külső hálózati szolgáltatókhoz történő hozzáférést a következő módon kell ellenőrizni:

a) **Minden tilos, ami kifejezetten nincs megengedve!** Ez azt jelenti, hogy alaphelyzetbenmindenforgalmat tiltani kell, majd csak azt megengedni, amelyre valóban szükség van.

b) A belső hálózat irányából az internet irányába kapcsolatot csak azokra aprotokollokra/szolgáltatásokra engedélyezünk, amelyre szükség van.

c) Kifejezetten tiltani kell a belső hálózat irányából az internet irányába a levelezési (SMTP)kapcsolatokat. Levelet továbbítani csak a levelező szerveren keresztül szabad.

d) Megfelelő interfészt kell alkalmazni a Hivatal és más szervezet tulajdonában lévő, vagynyilvános hálózat között;

e) A felhasználókat jelszóval megfelelően hitelesíteni kell;

f) Ellenőrizni kell a felhasználók információszolgáltatáshoz való hozzáférését.

g) A Hivatal belső hálózatáról Internet kapcsolat kizárólag jóváhagyott tűzfalakon keresztül létesíthető.

h) Biztosítani kell, hogy a Hivatal elektronikus információs rendszerei alapértelmezés szerintne legyenek elérhetők az Internet felől. Amelyeknél az Internet felöli hozzáférés szükségesigény, ott kizárólag biztonságos és ellenőrzött kapcsolaton keresztül történhet hozzáférés.

i) Kiemelt figyelmet kell fordítani a tűzfal operációs rendszere biztonsági frissítéseinekfigyelésére és telepítésére.

j) A tűzfalat úgy kell konfigurálni, hogy az utasítsa el a port letapogatási próbálkozásokat.A felhasználóknak tilos az Internet felhasználási szabályait és biztonsági beállításait megváltoztatni, illetve megkerülni.

A felhasználónak az Internet használata során tilos:

a) a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele,

b) az Interneten elérhető nyilvános chat-és fórum oldalakon hivatali email címmel hozzászólni,

c) fájlcserélő alkalmazásokat futtatni, illetve nem hivatali munkavégzéshez szükséges letöltéseket végezni,

d) hivatali email címmel nyilvános levelezőlistákra, hírlevelekre feliratkozni.

A felhasználók kizárólag jóváhagyott szoftvereket használhatnak az Internet elérésére.

Az IBF köteles ellenőrizni, hogy a felhasználók számára biztosított az Internet elérést lehetővé

tevő szoftverek mentesek a komolyabb biztonsági hibáktól.

A Hivatal központi tűzfalát csak a belső hálózatból vagy a konzolról lehet adminisztrálni. Akülső hozzáférés nem engedélyezett.

A fentiek végrehajtása érdekében tűzfal biztonsági politikát kell készíteni, mely tartalmazza:

a) tűzfal kialakítására vonatkozó követelményeket,

b) a tűzfalon engedélyezett portokat, protokollokat és szolgáltatásokat,

c) a tűzfal adminisztrálásával kapcsolatos feladatokat és felelősségi köröket

d) a tűzfal biztonsági politikában foglaltak ellenőrzését.

17.2.1. ASP hálózati eszközök felügyelete

Az ASP rendszer eléréséhez szükséges eszközöket (NTG router, switch, szünetmentestápegység) zárt rack szekrényben kell működtetni.

A menedzselhető hálózati eszközök (switchek) konfigurálásánál a következőket kell elvégezni:

a) az eszközök hálózatba illesztéséről készüljön dokumentáció;

b) az eszköz gyári, alapértelmezett bejelentkezési azonosítói (név, password) kerüljenek megváltoztatásra;

c) a hozzáférési azonosítókat zárt borítékban, és biztonságosan zárható helyen kell tárolni;

d) a hálózati eszközöket csak a rendszergazda, valamint szerződésben a hálózati eszközök karbantartására kijelölt fél kezelheti;

e) az eszközök firmware frissítése a legutolsó stabil változatnak megfelelően történjen meg;

f) a menedzselhető eszközök legfrissebb konfigurációja legyen elmentve és zárható helyen tárolva;

g) az ASP rendszerhez csatlakozó munkaállomásokat menedzselhető hálózati eszközökre kell

kötni;

h) ezeken az eszközökön - az idegen eszközök hálózatba történő csatlakozása elleni védelem megvalósítása érdekében - be kell kapcsolni a port security megoldást.

A Hivatal belső hálózatához idegen (nem a hivatal tulajdonában lévő) infokommunikációs
eszköz nem csatlakoztatható.

17.2.2. A felhasználó hitelesítése külső összeköttetésekhez

A felhasználókat jelszóval hitelesíteni kell és ellenőrizni kell a felhasználók információszolgáltatáshoz való hozzáférését.

17.3. Kriptográfiai kulcs előállítása és kezelése

A kriptográfiai kulcsok védelmének módját a kriptográfiai eszközök biztonságos használatát garantáló szabályozásban kell kidolgozni, az adott elektronikus információs rendszer használatba vételét megelőzően.

A vonatkozó szabványoknak vagy szabványként elfogadott előírásoknak megfelelő kulcsgondozó rendszerek használhatók. A belső előírásokat kriptográfiai utasításban, illetve amegfelelő alkalmazás leírásaiban kell meghatározni.

Az önkormányzati ASP rendszerhez történő csatlakozás során használandó E-személyi kezelését a következő szolgáltatói dokumentumok szabályozzák:

a) Általános szerződési feltételek a PKI szolgáltatásokhoz (ÁSZF-PKI) v1.6

b) Szolgáltatási szabályzat a személyazonosító igazolványokhoz kibocsátott minősítetttanúsítványokhoz (HSZSZ-ESZIG) v1.3

c) Hitelesítési rend a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz (HR-ESZIG) v1.3

d) Időbélyegzés Szolgáltatási Rend (ISZR) v1.2Szolgáltatási szabályzat a minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz(HSZSZ-M) v1.6

17.4. Kriptográfiai védelem

A Hivatalnak az elektronikus információs rendszereiben az adatok sértetlenségének és bizalmasságának védelmére szabványos, a vonatkozó jogszabályokban biztonságosnak minősített kriptográfiai műveleteket kell alkalmaznia.

A Hivatal elektronikus információs rendszereiben csak olyan kriptográfiai megoldások alkalmazhatók, amelyek:

a) a vonatkozó szabványoknak vagy szabványként elfogadott előírásoknak megfelelő kriptográfiai algoritmusokat és protokollokat használnak;

b) alkalmazását az IBF jóváhagyta.

17.5. Együttműködésen alapuló számítástechnikai eszközök

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

17.6. A folyamatok elkülönítése

Az elektronikus információs rendszer elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.

IV. ASP specifikus irányelvek

A 257/2016. (VIII. 31.) Korm. rendelet 2. melléklete tartalmazza az önkormányzati ASP rendszer szakrendszereinek használatához szükséges felhasználói (önkormányzati) munkaállomásokkal szembeni minimumkövetelményekhez tartozó megfelelés elvárását. Ez alapján ki lehet alakítani azt az informatikai infrastruktúra környezetet, amellyel biztosított az ASP rendszerhez történő csatlakozás a következők alapján.

Az informatikai környezet fő komponensei:

- Munkaállomások beüzemelése
- Nyomtatók üzembe állítása
- Hálózati eszközök beüzemelése, hálózat kiépítése
- Vírusvédelmi rendszer beüzemelése
- Tűzfal beüzemelése
- Internetkapcsolat üzembe állítása

18.Az infrastruktúra felállításának főbb feladatai

- Tenant létrehozása a Keretrendszerben (ASP. KERET), Tenant adminisztrátor felvétele a Keretrendszerben (ASP.KERET).
- Adatbázisok létrehozása a Gazdálkodási (ASP. GAZD) és szakrendszerben.
- Tenant felhasználók felvétele és szerepkörök összerendelése a Keretrendszerben (ASP. KERET).
- Tanúsítványok elkészítése és hozzárendelése.
- Tanúsítványok kiosztása önkormányzati felhasználók között.

19.IT biztonsági feltételek megteremtése

- Önkormányzati biztonsági szint meghatározása.
- A meghatározott biztonsági szinthez kapcsolódó védelmi intézkedések biztosítása.
- Információbiztonsági szabályozások kialakítása, szükség szerinti módosítása, jóváhagyása, kihirdetése.

- Biztonsági auditra való felkészülés.
- ASP-vel kapcsolatos audit tevékenység csak a Hatóság írásbeli engedélyével végezhető el. Erről az önkormányzat tájékoztatást ad a Magyar Államkincstár részére.
- ASP rendszeren külsős Fél, szervezet nem végezhet sérülékenységi vizsgálatot a Hatóság írásbeli engedélye nélkül. Ezen vizsgálati tényről az önkormányzat tájékoztatást ad a Magyar Államkincstár részére.

20.Fizikai biztonság megteremtése ASP-ben

A fizikai biztonság meghatározásánál az ASP-t futtató objektum tekintetében, amennyiben a hivatal teheti, szükséges biztonsági zónákat kijelölni, melyet minden esetben az hivatali szervezet határoz meg saját eljárásrendjében, az alábbi javaslatok figyelembevételével:

- Az épület földrajzi elhelyezkedését. Lehetőleg a bejutás ellenőrzött legyen.
- Az épület építészeti, épületgépészeti adottságait.
- Ügyfélforgalom mértékét.
- ASP felhasználóknak nyújtott szolgáltatásokat.
- Az információk osztályozását, minősítését.

21.Őrzés, védelem

A törekedni kell az élő erős őrzés megvalósítására. Ha megvan a lehetőség, akkor szabályzatban szükséges rögzíteni az őrszolgálat működési rendjét, az incidenskezelés folyamatát.

Az hivatalok ASP-t is futtató helységeibe a bejutás ellenőrzötten kell, hogy megtörténjen, az ellenőrzésről lehetőség szerint beléptető rendszer gondoskodik.

Lehetőséghez képest legyen kialakítva az objektum védelme beléptető, behatolás védelmi, tűzjelző és video-megfigyelő rendszerrel. A biztonsági rendszerek adatai legyenek archiválva, akár több hónapra visszamenőleg megőrizve a hazai jogszabályokat figyelembe véve.

Földszinti ablakokon lehetőség szerint vasrács védjen az illetéktelen behatolástól. Az informatikai biztonsági felelős rendszeresen (pl. félévente) ellenőrzést hajtson végre, az eredményt jegyzőkönyvbe rögzítse. A jegyzőkönyvet az ASP Szolgáltatási szerződésben megjelölt fél kérésére, illetve a Hatóság felszólítására betekintésre adja át.

A fizikai biztonságnak meg kell felelnie a jogszabályi elvárásoknak, s ezáltal a Hivatal:

- a létesítménybe történő fizikai belépés ellenőrzésén túl külön engedélyhez köti a fizikai belépést az elektronikus információs rendszereknek helyt adó helyiségekbe is,
- jogosultságok kiosztásával ellenőrzi az elektronikus információs rendszer kimeneti eszközeihez való fizikai hozzáférést annak érdekében, hogy jogosulatlan személyek ne féljenek azokhoz hozzá,
- ellenőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt fizikai hozzáféréseket annak érdekében, hogy észlelje a fizikai biztonsági eseményt és reagáljon arra rendszeresen átvizsgálja a fizikai hozzáférésekről készült naplókat; azonnal átvizsgálja a fizikai hozzáférésekről készült naplókat, ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak; összehangolja a biztonsági események kezelését, valamint a napló átvizsgálások eredményét. Az érintett szervezet felügyeli a fizikai behatolás riasztásokat és a felügyeleti berendezéseket. Az érintett szervezet a létesítménybe való fizikai belépések ellenőrzésén felül külön felügyeli az elektronikus információs rendszer egy vagy több elemét tartalmazó helyiségekbe történő fizikai belépéseket,
- meghatározott ideig megőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt látogatói belépésekről szóló információkat; azonnal átvizsgálja a látogatói belépésekről készített információkat és felvételeket, ha a rendelkezésre álló információk jogosulatlan belépésre utalnak,
- automatizált mechanizmusokat alkalmaz a látogatói belépésekről készített információk és felvételek kezeléséhez, átvizsgálásához,
- védi az elektronikus információs rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben,
- az elsődleges áramforrás kiesése esetére, a tevékenységhez méretezett, rövid ideig működőképes szünetmentes áramellátást biztosít az elektronikus információs rendszer szabályos leállításához,
- az elsődleges áramforrás kiesése esetén biztosítja a hosszú távú tartalék áramellátást az elektronikus információs rendszer minimálisan elvárt működési képességének és előre definiált minimálisan elvárt működési idejének fenntartására,

- lehetőséget biztosít az elektronikus információs rendszer vagy egyedi rendszerelemek áramellátásának kikapcsolására vészhelyzetben; gondoskodik a vészkikapcsoló berendezések biztonságos és könnyű megközelíthetőségéről; megakadályozza a jogosulatlan vészkikapcsolást,
- az érintett szervezet az elektronikus információs rendszer védelmére olyan tűzjelző berendezést vagy rendszert alkalmaz, amely tűz esetén automatikusan működésbe lép,
- automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer közelében megjelenő folyadékszivárgás észlelésére és az érintett szervezet által kijelölt személyek riasztására,
- engedélyezi, továbbá figyeli és ellenőrzi a létesítménybe bevitt, onnan kivitt információs rendszerelemeket, és nyilvántartást vezet ezekről,
- védi az elektronikus információs rendszert a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzárószelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek,
- úgy helyezi el az elektronikus információs rendszer elemeit, hogy a legkisebb mértékűre csökkentse a szervezet által meghatározott fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét,
- védi az információt tartalmazó karbantartási eszközt a jogosulatlan elszállítással szemben azzal, hogy ellenőrzi, az eszköz nem tartalmaz-e információt; ha az eszköz tartalmaz információt, azt törli vagy megsemmisíti; az eszközt a létesítményen belül őrzi az ezért felelős személyekkel engedélyezteti az eszköz elszállítását a létesítményből (nem releváns),
- megköveteli a hozzáférési jogosultság igazolását az elektronikus információs rendszeren karbantartást végzőktől,
- a megfelelő biztonsági engedéllyel nem rendelkező karbantartó személyek alkalmazása során az ilyen karbantartó személyeket megfelelő hozzáférési jogosultságú, műszakilag képzett belső személyekkel felügyelete alatt tartja az elektronikus információs rendszeren végzett karbantartási és diagnosztikai tevékenységek során.

22.Humán erőforrás az ASP-ben

Az ASP rendszereket használó hivatal szervezeti egység vezetőjének a felelőssége, hogy meghatározza az egyes, ASP szakrendszer munkakörökhöz tartozó felelősségeket és feladatokat.

Alkalmasság vizsgálat:

- A hivatal humánpolitikai szervezet vezetőjének vagy a jegyzőnek a felelőssége, hogy foglalkoztatás előtt a betöltendő ASP rendszerhez kapcsolódó munkakör kockázataival arányos mértékű megfelelőségi vizsgálatot végezzen el a foglalkoztatni kívánt munkatárs vonatkozásában.
- A kockázattal arányos mértékben mérlegelni kell a foglalkoztatni kívánt személy egyéni tulajdonságait is (pl. megbízhatóság, felelősségtudat, elkötelezettség, terhelhetőség, koncentrálóképesség stb.).
- Meg kell győződni arról, hogy a foglalkoztatni kívánt személy rendelkezik a munka elvégzéséhez szükséges végzettséggel, tapasztalatokkal.
- Az informatikai biztonsági szakterület vezetőjének vagy a rendszergazda támogatásával a jegyző felelőssége, hogy az informatika külsős felek által, a szerződött feladatok végrehajtására kijelölt személyek a munkavégzés kockázataival arányos mértékben átvilágításra kerüljenek.
- A humánpolitikai szakterület vezetőjének vagy a jegyzőnek a felelőssége, hogy a foglalkoztatás alkalmával az hivatal munkaköri leírásban rögzítse a kockázatokkal arányosan a titoktartás követelményeit (ASP titoktartási nyilatkozat, mely korábban megküldésre került) és a foglalkoztatás egyéb kikötéseit.
- A hivatal jogi szakterület vezetőjének vagy a jegyzőnek felelőssége, hogy a szerződő felek a szerződésben rögzítsék a kockázatokkal arányosan a titoktartás követelményeit és az együttműködés egyéb kikötéseit.

23.Oktatás, képzés az ASP-ben

Az önkormányzati munkatársaknak ASP oktatáson kell részt venni, amely alapján a rendszert az elvárásoknak megfelelően, önállóan is használni tudják. Az informatikai biztonsági képzés az Informatikai Biztonsági Felelős feladata, mely rögzítésre került a hatályos Informatikai

Biztonsági Szabályzatban. Az oktatás folyamatát a képzési eljárásrendnek kell szabályoznia. A Hatóság és a Magyar Államkincstár jogosult a képzési dokumentációk megtekintésére.

24.ASP jogosultság kezelés

A szerződésben meghatározott tenant adminisztrátorok rendszerbe történő „felvitelét" az ASP Központ végzi el az önkormányzat által megküldött adatlap alapján.

- A privilegizált joggal rendelkező felhasználók a munkatársaik részére további jogosultságot osztanak. Ezt a tevékenységet az önkormányzati jegyző felelősségi és hatáskörébe tartozóan tudják elvégezni.
- Egy önkormányzati fióknál (tenantnál) minimum egy felhasználó karbantartónak szükséges „lenni", ezt a rendszer figyeli (pl.: nem lehet zárolni, vagy elvenni tőle a jogot, ha csak egyedüli felhasználó karbantartó a tenantnál).
- A rendszer használata során elvárt, hogy a privilegizált joggal rendelkező munkatársak a privilegizált jog használatát munkavégzésükhöz csak indokolt esetben használják.
- A privilegizált joghoz tartozó bejelentkezési azonosítót zárt borítékban, biztonságosan zárható helyen kell tárolni.

A tenant adminisztrátor feladatai:

- új felhasználók (userek) rögzítése,
- meglévő felhasználók adatainak módosítása,
- felhasználók zárolása (szükség szerint),
- felhasználói jogosultságok (szerepkörök) kiosztása,
- felhasználói jogosultságok módosítása, megvonása,
- helyettesítések beállítása, eltávolítása,
- felhasználói csoportok létrehozása, módosítása, törlése (ugyanazon szerepkörök kiosztása több felhasználónak),
- üzleti napló megtekintése (a rendszerben történő változásokat lehet lekérdezni, követni).

25.Az ASP rendszerbe történő belépés, authentikáció

Az ASP elsődleges autentikációs eszköze az eSZIG. A használatához javasolt kártyaolvasók hatóság által bevizsgált és elfogadott eszközök.

Az ASP eSZIG-gel történő azonosítás során személyes adathoz az ASP rendszer nem fér hozzá. Belépéskor ugyanis az e-személyi érvényességét közvetlenül a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatalának (a továbbiakban: KEKKH) szervere ellenőrzi. A KEKKH szervere az ASP rendszernek egy ún. hash-kódot (RID) ad vissza, mely azonos okmány esetén mindig ugyanaz, de ez a kód nem fejthető vissza személyes adattá. Az ASP rendszer ehhez az anonim hash-kódhoz rendeli a felhasználót.

Az elektronikus személyigazolvánnyal történő authentikáció során a következő szabályzókra kell megkülönböztetett módon figyelni:

- Minden ASP rendszert használó munkatársnak rendelkeznie kell eSZIG-el.
- Az eSZIG használatához szükséges a kártyaolvasó számítógépre történő telepítése.
- Az ASP rendszerbe történő sikeres beléptetés érdekében a Keretrendszerbe rögzített felhasználói fiók és az eSZIG összerendelése szükséges.
- A személyi igazolvány kártyát csak a tulajdonosa használhatja, azt ASP rendszer authentikációs folyamat céljából másnak átadni tilos.
- A hivatal vezetőjének a Jegyzőnek gondoskodnia kell arról, hogy a kérdéses kártya hiánya esetén az ASP rendszerbe történő ideiglenes bejelentkezés lehetősége biztosított legyen. Az ehhez tartozó szabályrendszer kialakítása elengedhetetlen.

26.ASP rendszer kliens oldali biztonsága

Az ASP kapcsán kiemelten kell kezelni a csatlakozó önkormányzatokkal kapcsolatos biztonsági kockázatokat. A csatlakozó önkormányzatok a saját infrastruktúrájukat fogják használni az alkalmazások igénybevétele során, így a kliens rendszerek biztonsága nagymértékben befolyásolja a teljes ASP rendszer biztonságát.

Fontos az ASP rendszerbe olyan kikerülhetetlen biztonsági megoldásokat beépíteni, ami szűkíti a felhasználók biztonságra kockázatos tevékenységének lehetőségét.

Az csatlakozó önkormányzatok tekintetében a lehetséges fenyegetettségek, sebezhetőségek, valamint ezek megelőzésére alkalmazható intézkedések az alábbiak:

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
ASP rendszer önkormányzati, végponti állomásai	Érzékeny adatok ellopása, adatfájlok törlése, ellopása, módosítása.	Hozzáférés védelem beállítása.
	Rosszindulatú program (vírus, trójai faló, stb.) bejuttatása a rendszerbe.	Vírusvédelmi rendszer alkalmazása.
	Vírus, trójai faló, féreg aktiválódása, pl. e-mail csatolmány megnyitásakor.	Vírusvédelmi rendszer alkalmazása.
	Végrehajtható programok, script-ek (Java Applet, JavaScript, VB Script, CGI, stb.) letöltése, pl. az állomás DoS támadásra való felhasználására a felhasználó tudtán kívül.	Böngésző biztonsági beállítása
	Web és alkalmazásba csomagolt ActiveX objektumok, amelyek a programozó szándékától függően a legkülönbözőbb károkat (gépleállítás, konfiguráció feltérképezés, monitor/billentyűzet elvétel, stb.) okozhatják.	Böngésző biztonsági beállítása
	Ismeretlen forrásból érkező e-mail-ek és azok csatolmányainak megnyitása.	Vírusvédelmi rendszer alkalmazása, felhasználó oktatása.
	Az Internet böngészőkben meglévő biztonsági „lyukak" megszüntetésére szolgáló javító programok letöltésének elmulasztása. A biztonsági „lyukak" kihasználásával elérhetők a végponti felhasználó érzékeny adatai (jelszó, az állomás konfigurációja, fájl nevek, fájl struktúra, a	Legújabb verziók, frissítések telepítése.

	meglátogatott weblapok címei, stb.).	
	A munkaállomásra letöltött adatlapok (kérdőív, adatszolgáltató formanyomtatvány, stb.) programhibái. A szolgáltatott adatok rejtjelezés nélküli elküldése.	Csak megbízható forrásból származó program használata.
	Vírusvédelmi program frissítésének elmulasztása.	Rendszeres, automatikus frissítés.
	Az igénybevett szolgáltatás letagadása.	Naplózás.
	A munkaállomás ellopása.	Követelményrendszer szerinti hozzáférés-védelem és rejtjelezés alkalmazása.
	Mobil eszköz ellopása	Az előírt fizikai védelmi eszközök alkalmazása. Követelményrendszer szerinti hozzáférés-védelem és rejtjelezés alkalmazása.
Internet	A felhasználó login adatainak (felhasználói-azonosító, jelszó) lehallgatása, ezek segítségével a felhasználó megszemélyesítése.	Rejtjelezett adatátviteli csatorna használata.
	Érzékeny adatok lehallgatása.	Rejtjelezett adatátviteli csatorna használata.
	Adatok lehallgatás és továbbítása megváltoztatott tartalommal elleni védelme.	Hozzáférés-vezérlés kialakítása. Rejtjelezett adatátviteli csatorna. Egyszer használatos jelszó.

	E-mail-ek, elektronikus dokumentumok eltérítése.	Hozzáférés-vezérlés kialakítása.
Tűzfal	Tűzfal-biztonságpolitika hiánya vagy hiányos volta.	Tűzfal-biztonságpolitika elkészítése, vagy aktualizálása.
	Ad hoc vagy nem a biztonságpolitikának megfelelő biztonsági beállítás, vagy üzemeltetés.	Biztonsági beállítások rendszeres ellenőrzése, naplózás, riasztás.
	Portok letapogatása.	Tűzfal biztonsági beállítása.
	IP cím megszemélyesítés, a támadó a védett hálózaton működő számítógép (pl. szerver) IP címét megszerezve egy belső munkaállomást „szimulálva" a tűzfalon keresztül fér hozzá a szerveren levő adatállományokhoz.	Megfelelő hálózati biztonságpolitika, architektúra terv kialakítása.
	Visszaélés, forrás útvonalválasztással. A támadó a védett belső hálózat felépítésének ismeretében a saját gépében meghatározott útvonallal és belső IP címmel belső gépet „játszik el" és fér hozzá az útvonal végén levő belső géphez.	Megfelelő hálózati biztonságpolitika, architektúra terv kialakítása. Hálózati végpont IP címhez, MAC címhez kötése.
	Szerver típus specifikus biztonsági lyukak az operációs rendszerben. Az aktuális javító- és szerviz csomagok telepítésének elmulasztása.	Operációs rendszerek biztonsági frissítéseinek folyamatos figyelése, végrehajtása.
	A tűzfal távoli, pl. Interneten keresztül történő adminisztrálása.	Tűzfal adminisztrálása csak védett hálózatból, vagy konzolról.

	Vírusvédelmi programok frissítésének elmulasztása.	Vírusvédelmi rendszer folyamatos frissítése.
	Hiányos biztonsági naplózás. A biztonsági naplók értékelésének elmulasztása vagy rendszertelensége.	Minden jelentős biztonsági esemény naplózása, naplózott események folyamatos értékelése.
	Hiányos fizikai biztonság.	Követelményrendszer szerinti fizikai biztonság kialakítása.

27.ASP munkaállomásokra vonatkozó biztonsági elvárások

Az ASP rendszerhez csatlakozó eszközök karbantartásáról, változáskövetéséről gondoskodni kell a következők figyelembevételével:

- A folyamatot változáskövetési eljárásrendbe szükséges megfogalmazni.
- A munkaállomásokon legyen telepítve vírusvédelmi program, a legfrissebb vírus definíciós adatállománnyal. A végpontvédelem tartalmazzon e-mail (csatolmány) védelmet is.
- A munkaállomáson legyen megoldott a böngésző megfelelő biztonsági beállítása.
- A munkaállomások programfrissítése kötelező, különös tekintettel a legfrissebben kiadott security patch komponensekre.
- A telepítő programok, a licensz azonosítók zárható helyen legyenek tárolva.

A munkaállomások elhelyezésénél gondot kell fordítani:

- A készülékek olyan módon legyenek a hivatalban elhelyezve, hogy azokat az ügyfelek ne tudják elérni.
- A monitor kijelzési képét az ügyfelek ne tudják elolvasni.
- Ideiglenesen magára hagyott készülékek zárolása, képernyővédő aktiválása legyen megoldott.
- Munkaidő végén a munkaállomások kikapcsolása történjen meg.

Az ASP központhoz csatlakoztatott infrastruktúra elemekre értelmezve javasolt:

- a naplóinformációnak a védelme,
- hiba esetén a naplóbejegyzések elemzése,
- a rendszer hozzáférés ellenőrzése.

28.További biztonsági követelmények

- Az ASP Központtól kapott szoftveres tanúsítvány és annak jelszava nem adható át az ASP Központ által nem feljogosított személynek.
- Az önkormányzati ASP rendszerben csak a „257/2016. (VIII. 31.) Korm. rendelet az önkormányzati ASP rendszerről" jogszabályban említett szereplők végeznek, illetve végeztetnek központilag fejlesztői, üzemeltetői, működtetői tevékenységet. Bárminemű fejlesztői tevékenységet az ASP Központ vezetője engedélyez írásban.
- Az önkormányzati ASP rendszerben tesztelést végezni csak az idézett Korm. rendeletben meghatározott felek jogosultak.
- Azokon az eszközökön, amelyeken önkormányzati ASP rendszer van használatban, vagy adat továbbítódik rá, tilos olyan alkalmazást használni, amely az eszközt az ASP Központon kívüli harmadik féllel köti össze, és amellyel lehetőség van távoli támogatásra, vezérlésre, távoli hozzáférésre, képernyő átvételére stb.
- A tenant adminisztrátornak törekednie kell a legkisebb jogosultság kiosztásához a felhasználók körében. A jogosultságok kiosztásánál javasolt figyelembe venni a szervezeti és működési szabályzatot, amely nem kerülhet ellentmondásba jelen szabályzattal.

  Az ASP Központ egy esetleges biztonsági incidens során a tenant adminisztrátoroknak privilégiumokkal járó jogosultság-kiosztását számon kérheti. Biztonsági audit során, ha az indokoltnál magasabb hozzáférés állapítható meg egyes felhasználók esetében, annak oka jegyzőkönyvben kell, hogy szerepeljen. Általánosságban megállapítható, hogy a gondatlanságból bekövetkezett biztonsági események kapcsána jogosultságok kiosztója is felelőssé tehető.

  Biztonsági incidensek esetén a jelen szabályzat szerint kell eljárni (dokumentálás, eljárások, ellenőrzés, utóvizsgálat stb.), azonban az önkormányzati ASP-t ért incidensek észlelését jelenteni kell az ASP Központ felé is a Kormányzati

Eseménykezelő Központ mellett (utóbbi esetén az észlelés nem feltétlenül jelentkezik a Hivataloknál, de kizárni sem lehet). A jelentés nem tartalmazhat olyan szenzitív adatot (pl. személyes adatot), elemeket, amelyet harmadik fél nem ismerhet meg. Az incidens nem feltétlenül a kliens oldali eszközön jelentkezett, még ha azt az ASP rendszer felhasználója úgy véli, emiatt fontos az eszkalálás. Ennek bejelentési felülete a hibabejelentő rendszer. Az ASP Központ a bejelentéseket fogadja, továbbítja az illetékes terület felé és a jogszabály szerinti lépéseket megteszi. A Hivatalnak további kötelezettségei is vannak biztonsági incidensek kapcsán (pl. Kormányzati Eseménykezelő Központtal történő kapcsolatfelvétel), melyet a jogszabályok részleteznek.

- Ha az önkormányzati ASP-t üzemeltetői, működtetői oldalon éri biztonsági incidens, az ASP Központnak kötelessége értesítést elhelyeznie a Tájékoztatási Portál nyilvánosság elől elzárt felületén, megjelenítve a lehetséges elhárítási határidőt, illetve a keretrendszer elérhetősége esetén, a keretrendszer felületén is megjeleníteni ezeket az információkat. Ebben az esetben az üzemeltető szervezet veszi fel a kapcsolatot a jogszabályban megjelölt Hatósággal.
- A Korm. rendelet szerinti üzemeltető és működtető felek a Hatóság kérésére, utasítására is leállíthatják az önkormányzati ASP rendszert, vagy annak bizonyos elemeit (pl. kibertámadás esetén). Ebben az esetben az ASP Központ tájékoztatása addig nem fog megtörténni, amíg az incidens kiváltója, okozója, felderítése akadályokba ütközhet, azaz a Hatóság írásbeli engedélyezéséig.

V. Kapcsolódó jogszabályok

a) 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről

b) 2012. évi I. törvény a munka törvénykönyvéről

c) 2012. évi C. törvény a Büntető Törvénykönyvről

d) 2013. évi V. törvény a Polgári Törvénykönyvről

e) 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (továbbiakban: Ibtv.)

f) 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól

g) 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

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

i) 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

j) 257/2016. (VIII. 31.) Korm. rendeletet,az önkormányzati ASP rendszerről

VI. Alapfogalmak

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

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

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

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

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

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

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

8. *bizalmasság*: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

9. *biztonsági esemény*: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

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

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

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

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

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

15. *elektronikus információs rendszer biztonsága*: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

33. *létfontosságú információs rendszerelem*: az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt

létfontosságú rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené;

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

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

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

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

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

39. *sértetlenség*: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

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

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

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

43. *Hivatal*: az adatkezelést vagy adatfeldolgozást végző jogi személy,

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

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

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

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

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

VII. Mellékletek

Oktatási napló

Oktatás dátuma: ..... év ..... hó ..... nap

Oktatás típusa: .....

(lehet éves tervezett, vagy változás kapcsán felmerülő rendkívüli)

Részvételre kötelezettek: .....

(pl. Új dolgozók név szerint, vagy a jelenléti ív szerinti dolgozók)

Az oktatás tematikája:

Kelt: ....., ... év. ..... hó ..... nap

Titoktartási nyilatkozat

Alulírott, mint Létavértesi Közös Önkormányzati Hivatal és annak szervezeti egységei által nyújtott IT szolgáltatások felhasználója kijelentem, hogy a Hivatal informatikai rendszereinek használata során a tudomásomra jutott információkat, adatokat időbeli korlátozás nélkül

a) üzleti titokként kezelem,

b) azokat jogosulatlan személy részére nem szolgáltatom ki, illetve nem teszem egyéb módon hozzáférhetővé,

c) azokat csak a munkakörömben foglalt feladatok teljesítéséhez, az ehhez szükséges mértékben használom fel, és csak az annak megismerésére jogosult számára teszem hozzáférhetővé,

d) azzal egyéb módon nem élek vissza.

Az IT rendszerekben tárolt, általam megismert személyes adatokra a fentieket megfelelően alkalmazva, azok tekintetében titoktartási kötelezettséget vállalok.

A nyilatkozatot adó adatai:

Név:

Lakcím:

Dátum:

Aláírás:

A nyilatkozatot átvevő adatai:

Név:

Szervezeti egység:

Dátum:

Aláírás: