Eperjeskei Közös Önkormányzati Hivatal

4646 Eperjeske, Szabadság tér 1.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Érvényes: 2022. január 03. –tól

Készítette: Dr. Gál- Lakatos Enikő

Jegyző

Jóváhagyta:

Dr. Gál- Lakatos Enikő
Jegyző

Pásztor Gábor
polgármester

Ésik Árpád
polgármester

Mészáros Lajos
polgármester

Krecz Zoltánné
Intézményvezető

Fodor Melinda
Intézményvezető

Demeter Tibor
Elnök

1. Bevezetés

Jelen Információ Biztonsági Szabályzat (továbbiakban IBSZ) célja, hogy keretet adjon az Eperjeskei Közös Önkormányzati Hivatal (továbbiakban hivatal) elektronikus információs rendszer biztonság-irányítási követelményeinek kialakítására, bevezetésre, fenntartására és folyamatos fejlesztésére. Valamint az adatvédelmi törvény, az adatbiztonság érvényesítése, az egyes szoftverekhez való hozzáférési jogok meghatározása, az ellenőrzési mechanizmusok meghatározása, a felelősségi viszonyok tisztázása, az egyes adatkezelő műveletek részletezése az adatvédelmi szabályzattal, az iratkezelési szabályzattal, illetve a vonatkozó jogszabályi előírásokkal összhangban.

Az elektronikus információs rendszer segítségével a szervezet képes arra, hogy megőrizze az információk bizalmasságát, sértetlenségét és rendelkezésre állását. Ennek érdekében meghatározza a betartandó követelményeket, valamint biztosíthatóvá válik:

- a titok és információvagyon védelmére vonatkozó előírások betartása
- a személyiségi jogok védelme
- az üzemeltetett hardver és szoftver eszközök rendeltetésszerű használatának betartása
- az informatikai eszközök karbantartása és fenntartása az üzembiztonság megtartása érdekében
- a számítógépes adatok feldolgozása és azok továbbítása során az illetéktelen hozzáférésekből és felhasználásokból eredő károk megelőzése, a hátrányos következmények minimálisra történő csökkentése
- az adatállományok tartalmi és formai épségének megőrzése
- az alkalmazott szoftverek és rendszerek sértetlenségének és rendelkezésre állásának biztosítása, dokumentációjuk nyilvántartása
- a felhasználói munkaállomásokon kezelhető adatok körének meghatározása
- az adatállományok biztonságos mentésének megvalósítása
- felelősségi viszonyok tisztázása az informatikai biztonság megőrzése érdekében
- a jogosultság és hozzáférés szabályainak dokumentált betartása

Ahhoz, hogy mindezen célok teljesüljenek, az egyes rendszerelemek teljes fennállásának ciklusa alatt – a megtervezéstől a bevezetésig, az alkalmazáson át a végleges felszámolásukig – működnie kell a védelemnek. Ezért az Informatikai Biztonsági Szabályzat a biztonsággal összefüggő szabályozásokat, ezek dokumentálását és az ellenőrzések leírását vagy ezek hivatkozásait tartalmazza.

Az IBSZ egy olyan alapvető dokumentum, mely magában foglalja:

- az informatikai biztonság meghatározását, általános célkitűzéseit és tárgykörét, valamint a biztonsági és a védelmi intézkedések fontosságát az informatikai rendszerekhez kapcsolódó adatvédelem és adatbiztonság megteremtése érdekében
- a vezetőség egyértelmű nyilatkozatát az informatikai biztonság szabályozott kialakítására, bevezetésére, illetve fenntartására
- az informatikai biztonság eleminek bevezetését, üzemeltetését és minden, a biztonsággal összefüggő egyéb folyamatra vonatkozó szabályozását
- az informatikai biztonsággal kapcsolatos feladatok, hatáskörök és felelősségek meghatározását, beleértve a jelentéstételi kötelezettséget minden biztonsági eseményről
- utalást minden olyan dokumentációra, ami támogatja a szabályzatot: (elvek, követelmények, kötelező eljárások)
    - az informatikai rendszer részletesebb biztonsági szabályzatai, eljárásrendek
    - a felhasználó számára követendő mindennapi utasítások, biztonsági szabályok

Az IBSZ-ben szereplő követelményeket, rendelkezéseket és ajánlásokat mindig a hatályos jogszabályi keretek között kell használni.

1.1. Az IBSZ szervezeti hatálya

Az IBSZ szervezeti hatálya a hivatal valamennyi olyan szervezeti egységére kiterjed, amely a hivatal elektronikus információs rendszereit használja, üzemelteti, továbbá ilyen tevékenységeket irányít és ellenőriz.

1.2. Az IBSZ személyi hatálya

Az IBSZ személyi hatálya kiterjed a hivatal munkavégzésre irányuló bármely jogviszonyban álló természetes és jogi személyre, tehát azokra, akik kapcsolatba kerülnek a hivatal elektronikus információs rendszereivel (használják, fejlesztik, telepítik, üzemeltetik, javítják stb.), így:

- a választott tisztségviselőkre (polgármester, alpolgármester, képviselők),
- a közszolgálati jogviszony alapján foglalkoztatott munkatársak,
- a munkaviszony alapján foglalkoztatott munkatársakra,
- a hivatallal szerződéses kapcsolatban álló természetes és jogi személyekre,
- más szervezetek képviseletében a hivatal munkahelyein tartózkodó személyekre.

1.3. Az IBSZ tárgyi hatálya

Az Informatikai Biztonsági Szabályzat alkalmazása kiterjed:

- a Hivatal adataival és adatainak kezelésével összefüggésben használt bármilyen adatrögzítésre, tárolásra, feldolgozásra vagy továbbításra képes elektronikus információs rendszerre és ezek működési környezetére
- ezek valamennyi dokumentációjára (fejlesztési, szervezési, műszaki, üzemeltetési, biztonsági)
- az adattárolók mentésére

1.4. Az IBSZ területi hatálya

A szabályzat területi hatálya kiterjed a közös Hivatal valamennyi telephelyére, azok intézményeire, valamint a Roma Önkormányzatokra

- Eperjeskei Közös Önkormányzati Hivatal (4646 Eperjeske, Szabadság tér 1.)
- Eperjeskei Közös Önkormányzati Hivatal Tiszamogyorósi Kirendeltsége (4645 Tiszamogyorós, Szabadság utca 33.)
- Eperjeskei Közös Önkormányzati Hivatal Benki Kirendeltsége (4643 Benk, Petőfi utca 3.)

1.5. Az IBSZ időbeni hatálya

Jelen szabályzat a kiadás napján lép hatályba.

2. A Hivatal biztonsági osztályba és biztonsági szintbe sorolása

2.1. Biztonsági osztályba sorolás

A hivatal elektronikus információs rendszereit a 41/2015. BM, technológiai végrehajtási rendelet által előírt módon, külön- külön a bizalmasság, a sértetlenség és a rendelkezésre állás fenyegetettségének vonatkozásában a hivatal ötfokú értékelési skálájának megfelelően biztonsági osztályba kell sorolni.

Az értékelési skálának összefüggésben kell lennie az adott rendszer megszervezéséhez és fenntartásához kapcsolódó költségekkel, a rendszer védelmére áldozott erőforrás-mennyiséggel és a bizalmasság, sértetlenség és rendelkezésre állás elvesztéséből eredő károkkal.

A biztonsági osztályba soroláshoz az elektronikus információs rendszerben kezelt adatokra vonatkozóan meg kell határozni a biztonsági célokra gyakorolt potenciális társadalmi-politikai hatást, és ezek jogi következményeit. Valamint a rendelkezésre állás tekintetében a közvetett anyagi kárt és a szolgáltatás kieséséből adódó károkat. Ezek segítségével a hivataltevékenysége jellegének,

nagyságrendjének és összetettségének megfelelő, kockázataival arányosan kerülnek megfogalmazásra a biztonsági célok elvesztésének hatásai.

Egy informatikai rendszer biztonsági osztályához tehát meg kell határozni a rendszerben tárolt adatokra vonatkozóan a bizalmasságra, sértetlenségre és rendelkezésre állásra gyakorolt potenciális hatását.

A biztonsági osztályba sorolást az alábbi esetekben újra el kell végezni

- jelentős változás következik be a hivatal szervezeti felépítésében
- az elektronikus információs rendszerben kezelt adatok bővülnek vagy az adatok köre változik
- változnak a hatályos információbiztonságra vonatkozó jogszabályok.

Ha nem történik lényegi változás, a biztonsági osztályba sorolást háromévente felül kell vizsgálni.

A biztonsági osztályba sorolást az IBF készíti elő az adatgazdákkal együttműködve és a jegyző hagyja jóvá.

A felhasználóknak az információ kezelése során tisztában kell lennie az adott információ védelmi igényével és ennek megfelelően kell kezelniük azt.

A hivatal elvégezte az elektronikus információ rendszereinek osztályba sorolását. A biztonsági osztályba sorolás eredményét a 2. számú melléklet tartalmazza.

2.2. Biztonsági szintekbe sorolás

Az Ibtv. 9. §-ának (1) és (2) bekezdései alapján a kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet, valamint az elektronikus információs rendszer

- fejlesztését végző,
- üzemeltetését végző,
- üzemeltetéséért felelős vagy
- információbiztonságáért felelős

szervezeti egységeket az elektronikus információs rendszerek védelmére való felkészültségük alapján a szervezettől elvárt, eltérő biztonsági szintekbe kell sorolni jogszabályban meghatározott szempontok szerint.

Az Ibtv. 9. §-ának (4) bekezdése alapján a szervezet vagy szervezeti egységek biztonsági szintjének meghatározását az elektronikus információs rendszer felhasználásának módja határozza meg.

A technológiai végrehajtási rendelet alapján **az Eperjeskei Közös Önkormányzati Hivatal elvárt biztonsági szintje 3-as.**

Mivel szakfeladatait támogató elektronikus információs rendszert használ (3-as szint), kritikus adatokat kezel – személyes adatok, adótitok - (3-as szint).

2.2.1. *Szervezeti egysége biztonsági szintbe sorolás*

A hivatal hatályban lévő Szervezeti és Működési Szabályzata alapján a hivatalban nem működnek az elektronikus információs rendszer

- fejlesztését végző,
- üzemeltetését végző,
- üzemeltetéséért felelős vagy
- információbiztonságáért felelős

szervezeti egységek, ezért azok biztonsági szintbe sorolása nem értelmezhető.

2.2.2. *A hivatal jelenlegi biztonsági szintje*

A hivatal az Ibtv. előírásainak megfelelően megvizsgálta biztonsági szintjét.

A hivatal jelenlegi biztonsági szintje: 1

3. Felelősségek, hatáskörök, elkötelezettségek az IT biztonság területén

3.1. Általános

Jelen IBSZ személyi hatálya alá tartozó valamennyi érintett felelős:

- az IBSZ munkaterületére vonatkozó előírásainak betartásáért és betartatásáért
- munkaterületén az adatbiztonság és a bizalmas adatok, információk megtartásáért, a nyilvánosságra hozatal megakadályozásáért

A hivatal minden munkatársa köteles:

- az IBSZ dokumentumában előírt ellenőrzések sikeres megvalósulását elősegíteni és támogatni,
- tudomásul venni, hogy a rendszergazda és az Informatikai Biztonsági Felelős előzetes bejelentés nélkül ellenőrizheti az informatikai biztonsághoz kapcsolódó utasításokat és a szabályzatok betartását

Az információbiztonság megvalósítását, fenntartását és ellenőrzését a hivatal a feladatok és felelősség szempontjából egymástól elhatárolt szervezeti keretek között valósítja meg.

3.2. Informatikai Biztonsági Felelős

Az Informatikai Biztonsági Felelős a kinevezésében maghatározott módon, a jegyző utasításának megfelelően látja el.

3.2.1. Feladata:

- közreműködik a hivatallal az Informatikai rendszer biztonságával összefüggő kérdésekben
- részt vesz az Informatikai rendszer biztonságával összefüggő tevékenységek jogszabályokkal történő összehangolásában, támogatásában
- az IBSZ készítésének ellenőrzése, véleményezése
- a jegyző kérésére kapcsolattartás a hatósággal

Az Informatikai Biztonsági Felelős ellenőrzési feladata:

- ellenőrzi az éves Informatikai biztonsági ellenőrzési programot
- a rendszergazdával közösen ellenőrzi az informatikai biztonsági előírások betartását; a védelmi előírások betartását; az adatvédelmi biztonsági rendszer érvényesülését; a biztonsági és behatolási védelem ellenőrzését, valamint részt vesz ezek végrehajtásában

Az Informatikai Biztonsági Felelős dokumentációs feladat:

- legalább 3 évente felülvizsgálja az IBSZ-t, a tartalmát aktualizálja a hivatal feladatai alapján
- felülvizsgálja és aktualizálja az Informatikai Biztonságpolitikát és az IBSZ-hez kapcsolódó dokumentumokat, eljárásrendeket, legalább 3 évente
- véleményezi az Informatikai rendszerhez kapcsolódó valamennyi szabályzatot, eljárásrendet és dokumentumot
- a szabályzatok módosításának szakmai elkészítéséhez jogosult igénybe venni a szervezet munkatársait

3.2.2. Felelőssége:

Az Informatikai Biztonsági Felelős felel:

- az Informatikai Biztonságpolitika és az IBSZ szakmai tartalomnak való megfelelősségéért
- az Informatikai rendszer biztonságához tartozó szabályok, eljárásrendek és dokumentumok összhangjának megteremtéséért
- a biztonsági szabályokat megsértőkkel szembeni eljárások elindításának kezdeményezéséért a jegyzőnél

3.2.3. Jogosultsága:

- az IBSZ előírásainak betartását ellenőrizni
- az Informatikai rendszer működtetésével, fejlesztésével, valamint az adatfeldolgozásokkal és adatarchiválásokkal kapcsolatos valamennyi dokumentumba betekinteni
- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezni a jegyzőnél

3.3. A rendszergazda

3.3.1. 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
- biztosítja az adat- és információvédelmi feladatok folyamatos belső ismertetését, felügyeli a képzési terv kidolgozását és oktatását

3.3.2. Felelőssége:

A rendszergazda felelős:

- az Informatikai rendszer biztonságos működtetéséért
- az Informatikai rendszer üzembiztonságáért, a rendszer kritikus részeinek és védelmi eszközeiknek folyamatos ellenőrzéséért
- az Informatikai rendszer hardver és szoftver elemeinek nyilvántartásáért, dokumentáltságáért
- az Informatikai Biztonságpolitika és az IBSZ kidolgozásáért
- az Informatikai rendszer biztonságához tartozó szabályok, eljárásrendek és dokumentumok kidolgozásáért, azok összhangjának megteremtéséért
- az informatikai biztonság tudatosításáért
- a biztonsági szabályokat megsértők szembeni eljárások elindításának kezdeményezéséért a jegyzőnél

- az Informatikai rendszerben az informatikai biztonságot érintő rendszerek megvalósulásáért, a megvalósítás menedzseléséért, felügyeletéért

3.3.3. Jogosultsága:

- az Informatika rendszer teljes körű ellenőrzése
- az Informatikai rendszer biztonságát érintő szabályzatok, eljárásrendek és utasítások véleményezése
- javaslattétel az új védelmi, biztonsági eszközök és technológiák beszerzésére, illetve bevezetésére
- az Informatikai rendszer biztonságát érintő beruházásokat véleményezése
- az előírásokkal szemben vétőkkel felelősségre vonási eljárás kezdeményezése a jegyzőnél

A rendszergazda és az Informatikai Biztonsági Felelős együttesen szabályzatgazdái az Informatikai Biztonsági Szabályzatnak, az Informatikai Biztonságpolitikának, illetve az informatikai biztonsághoz kapcsolódó egyéb eljárásrendeknek, utasításoknak, melyek összhangjáért is felelnek.

Az Informatikai Biztonsági Felelős véleményezésre előkészíti a hivatal informatikai biztonsági tervezését, figyelembe véve a hivatal feladatait az informatikai stratégia terveit a biztonsággal összefüggő célok megvalósításának érdekében.

Az Informatikai Biztonsági felelős, informatikai biztonsággal összefüggő további, jelen dokumentumban nem tisztázott feladatait és felelősségeit a 2013. évi L törvény 13. §-ban foglaltak részletezik.

4. Az informatikai rendszer általános biztonsági alapelvei

A hivatal törvény által meghatározott feladatainak elvégzéséhez adatokat gyűjt, tárol, feldolgoz és a tevékenység végrehajtásához a végrehajtók rendelkezésére bocsájtja. Az alapelvek teljesüléséhez az általa kezelt adatok, valamint informatikai rendszere tekintetében a felmerülő kockázatokkal arányos védelmet alakít ki. A védelem kialakítás alapja az információk biztonsági osztályba sorolása, az informatikai kockázatok felmérése és értékelése. Az értékelés alapján kockázatkezelést végez, és kockázatkezelési intézkedéseket hajt végre. Az intézkedések célja azoknak a biztonsági kockázatoknak a hivatal számára még elfogadható költségen történő azonosítása, kézbentartása és minimalizálása vagy megszüntetése, amelyek hatással lehetnek az informatikai rendszerek biztonságára.

Az alkalmazott informatikai rendszerek és azok üzemeltetési rendjének biztosítania kell a hivatal számára az azokban kezelt adatok bizalmasságát, sértetlenségét és rendelkezésre állását.

Az informatikai biztonsági megoldásokat úgy kell kialakítani, hogy a rendszerek mindennapi alkalmazása során akadályozza meg a működési tevékenység megszakítását és védje a kritikus működési folyamatait az informatikai rendszerek hibáinak hatásaitól, valamint szükség esetén biztosítsa a gyors újraindítás lehetőségét.

Az informatikai rendszer alkalmazására és üzemeltetésére vonatkozó szervezeti és működési rendeket, nyilvántartási és tájékoztatási szabályokat, eljárásrendeket, úgy alakítja ki, hogy a felelősségi körök és a személyes felelősségek meghatározhatóak legyenek. Valamennyi munkaterületre részletes munkaköri leírást kell készíteni, ami tartalmazza az adott munkakörre vonatkozó, az informatikai biztonsággal kapcsolatos követelményeket a felelősségek egyértelmű megjelölésével, az előírások szándékos vagy véletlen megsértéséből eredő biztonsági kockázatok mérséklése érdekében.

5. Kockázatelemzés

A kockázataranyos védelem kialakításához rendszeres és tervszerű informatikai kockázatelemzésre van szükség.

A kockázatelemzést évente el kell végezni, melynek során felül kell vizsgálni az előző évi kockázatelemzés eredményét. A kockázatelemzést soron kívül el kell végezni, hogy ha

- változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését),
- olyan körülmények következnek be, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát.

A kockázatelemzés eredményét IBF-nek dokumentálnia kell, majd meg kell ismertetnie a jegyzővel.

A nem tolerálható kockázatok kezelésére intézkedési tervet kell készíteni, melynek tartalmaznia kell a kockázat kezelésére javasolt intézkedéseket, felelős, határidő és költségvonzat megjelölésével.

A kockázatkezelési tervet az IBF-nek kell előkészítenie és a jegyző hagyja jóvá.

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.

6. Az informatikai biztonság dokumentumai

6.1. Az Informatikai Biztonsági Szabályzat

Az informatikai biztonság részletes szabályait az Informatikai Biztonsági Szabályzat tartalmazza. A Szabályzatot a jegyző teszi közé. A Szabályzat szabályzatgazdája a rendszergazda és az Informatikai Biztonsági Felelős.

Az IBSZ-t a hivatal összes munkatársával meg kell ismertetni, informatikai biztonsági oktatás formájában.A szabályok be nem tartása jogi, munkaügyi, illetve szerződésben meghatározott következményeket vonhat maga után. Az IBSZ el nem olvasása nem mentesít a felelősség alól.

A hivatalnak rendelkeznie kell az ügymeneti tevékenységet közvetlen vagy közvetve támogató informatikai rendszerre vonatkozóan a biztonságos működtetéséhez szükséges szabályokkal, eljárásrendekkel, minden olyan dokumentációval, ami a folyamatos működését biztosítja.

Az informatikai rendszerek biztonságos működéséhez szükséges előírások egységes felépítését a következő dokumentumok biztosítják.

6.1.1. Informatikai Biztonsági Szabályzat (IBSZ), Informatikai Biztonságpolitika (IBP):

Az informatikai biztonság megteremtéséhez szükséges mértékű támogatás biztosítása érdekében az informatikai biztonságpolitikát úgy kell kialakítani és karbantartani, hogy a szervezet céljaival, továbbá működési, biztonsági és informatikai politikájával, valamint valamennyi, az informatikai biztonságot érintő szabályozással összhangban legyen.

Az IBP olyan kézikönyv, mely hozzáférhető, érthető és kötelező az összes vezető és más munkavállaló számára. Ennek megismerését aláírásukkal igazolják az érintettek, mellyel az aláíró elismeri a szervezeten belüli biztonságért való felelősségét.

Az IBSZ az Informatikai Stratégiában rögzített alapelvek érvényesítésének szabályozását és az eljárásrendekre, utasításokra való hivatkozásokat tartalmazza.

6.1.2. Szabályzatok, eljárásrendek

A szabályzatok és eljárásrendek segítenek a munkavállalóknak az informatikai rendszer biztonságos használatában. A rendszergazda és az Informatikai Biztonsági Felelős által közösen elkészített szabályzatokat, eljárásrendeket a hivatal valamennyi munkatársa számára elérhetővé teszi. Az IBSZ a megfelelő helyen ezen szabályzatokra és eljárásrendekre hivatkozik.

6.1.3. Nyilvántartások

A hivatal az elektronikus információs rendszerekre, az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás bizonyos szakaszában elektronikus nyilvántartást vezet. Valamint szabványosított jegyzőkönyveket és formanyomtatványokat használ.

6.2. Összefoglaló szabályok

A szabályzatokat, eljárásrendeket és nyilvántartásokat az informatikai biztonsági kockázatok figyelembevételével kell kialakítani. Így különösen nagy hangsúlyt kell fordítani a felelősségi körök és az egyértelmű személyes felelősségek meghatározására.

Minden IBSZ-t érintő aktuális dokumentáció, nyilvántartás őrzéséről a szakterület szerint illetékes szervezeti egység gondoskodik az Egyedi Iratkezelési Szabályzatnak megfelelően.

6.3. Felülvizsgálat és értékelés

A rendszergazda gondoskodik arról, hogy a szabályzatok felülvizsgálata minden, az informatikai rendszer szempontjából jelentős változást követően megtörténjen.

Ezen kívül időszakos vizsgálatokat kell beütemezni, melynek idejét a kockázatelemzés alapján, a kockázat mértékének jelentős változása határozza meg.

Rendszeres és eseti vizsgálatokat az alábbi esetekben kell végezni:

- az irányelvek biztonsági hatékonysága nagymértékben csökken
- az ellenőrző és biztonsági eszközök hatékonysága nincs egyensúlyban a költséghatékonysággal
- szervezeti vagy működési környezetet érintő műszaki változások esetén
- jogszabályi háttér változásakor

7. Szervezeti biztonság

7.1. Az informatikai biztonság belső szervezeti struktúrája

7.1.1. Vezetői elkötelezettség

Az informatikai biztonság olyan felelősség, amelyen a vezetés minden tagja osztozik. Ezért elengedhetetlen, hogy a vezetés minden tagja a kellő elkötelezettséggel és a szükséges erőforrások rendelkezésre bocsátásával támogassa az informatikai biztonságot.

A vezetői testület hatáskörébe tartozik:

- javaslattétel az informatikai biztonsági célok megfogalmazásához és azok szervezeti integrációjához
- az informatikai biztonsági irányelvek és feladatok vizsgálata és jóváhagyása, a megvalósításához szükséges humán és anyagi erőforrások biztosítása
- az informatikai biztonsági események nyomon követése, az intézkedések hatékonyságának felülvizsgálata
- az informatikai biztonság fokozását szolgáló kezdeményezések, fejlesztések jóváhagyása
- az Informatikai Biztonsági Felelős személyének kijelölése, szükség esetén külső közreműködők igénybevétele
- az informatikai biztonság tudatosság fenntartása a szervezetnél

7.1.2. Az informatikai biztonsági feladatok megosztása

A szabályzatnak vagy a szabályzatban hivatkozott egyéb eljárásrendeknek egyértelműen meg kell határozniuk a biztonsági folyamatok felelőseit.

Pontosan meg kell határozni minden olyan területet, amelyért az egyes vezetők felelnek, különösen az alábbiakat:

- egyértelműen be kell azonosítani minden egyes önálló rendszerhez hozzárendelt eszközt, folyamatot és felelőst
- a felelősségköröket és jogosultságokat tisztán, és pontosan kell meghatározni és írásba kell foglalni
- az egyes folyamatok, eszközök és rendszerek felelőseit egyértelműen meg kell adni, a változásokat nyomon kell követni

Az IBSZ általános iránymutatással szolgál a hivatalban a biztonsági szerepek és felelősségek kiosztására.

A védelmi intézkedések betartása az egyes szervezeti egységek vezetőinek is a feladata. Az egyes vagyontárgyakért az azt használó személy, csoportos használat esetén a felhasználó terület vezetője a felelős.

A hivatal információbiztonsági feladatainak ellátása során a következő szerepkörök érintettek:

- a jegyző
- az Informatikai Biztonsági Felelős
- a rendszergazda
- az adatgazdák
- a felhasználók

7.1.2.1. A jegyző

A jegyző feladata

- biztosítani az informatikai rendszerrel irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését
- biztosítani a hivatalra irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését
- az informatikai rendszer biztonságáért felelős személyt nevez ki vagy bíz meg
- kiadja az Információ Biztonsági Szabályzatot
- gondoskodik az informatikai rendszerek védelmi feladatinak és felelősségi köreinek oktatásáról, biztonságtudatossági képzésről, a biztonsági ismeretek szinten tartásáról
- a rendszeres biztonsági kockázatelemzések, ellenőrzések és auditok lefolytatása révén meggyőződni arról, hogy a hivatal informatikai rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak
- minden szükséges és rendelkezésre álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről
- ha az informatikai rendszereket érintően bármilyen témában külsős közreműködőt vesz igénybe, gondoskodnia kell arról, hogy az IBSZ-ben foglaltak szerződéses kötelemként teljesüljenek

A jegyző felelős

- az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért
- a hivatalban az Ibtv. által előírt biztonsági szintnek és biztonsági osztályoknak megfelelő információ biztonsági intézkedések megvalósulásáért, illetve a végrehajtásához szükséges erőforrások biztosításáért
- megteszi az informatikai rendszer védelmében felmerülő egyéb szükséges intézkedéseket

A jegyző köteles együttműködni a jogszabályban meghatározott hatóságokkal. Ennek során az Információ Biztonsági Felelős személyéről tájékoztatást nyújt, a hivatal IBSZ-ét tájékoztatás céljából megküldi, biztosítja a hatóságok részére az ellenőrzés lefolytatásához és a biztonsági incidensek kivizsgáláshoz szükséges feltételeket.

7.1.2.2. Az Informatikai Biztonsági Felelős

Az Informatikai Biztonsági Felelős felelősségét, feladatait és jogosultságát a jelen szabályzat 3.2. pontja tartalmazza.

7.1.2.3. A rendszergazda

A rendszergazda feladatait, felelősségét és jogosultságait a jelen szabályzat 3.3. pontja tartalmazza.

7.1.2.4. Az adatgazdák

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

Az adatgazdák feladata

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

Az adatgazdák felelősek

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

7.1.2.5. A felhasználók

A felhasználó jogosult

- a számára munkavégzés céljából biztosított információs rendszerek és infokommunikációs eszközök üzemszerű használatára
- a munkájához szükséges adatállományok elérésére, jogosultsági szintjének megfelelően
- biztonság tudatossági képzésen való részvételre
- meghibásodás, üzemzavar esetén az elhárítás igénylésére

A felhasználó köteles

- védeni az információt azok keletkezésének, feldolgozásának, szétosztásának, tárolásának és selejtezésének teljes folyamata során
- az általa észlelt vagy tudomására jutott biztonsági incidensekről azonnali hatállyal értesíteni a felettesét
- a biztonsági incidensek kivizsgálásakor együttműködni
- bizalmasan kezelni valamennyi felhasználói azonosítóját és jelszavát, vagy egyéb olyan tokent, kulcsot, ami a hivatal informatikai rendszereihez biztosít hozzáférést

A felhasználó felelős

- jelen IBSZ megismeréséért és abban foglaltak betartásáért
- a birtokában lévő, vagy tudomására jutott információk bizalmas kezeléséért
- a számára átadott azonosítók és jelszavak, vagy egyéb fizikai azonosító eszközök védelméért és át nem ruházásáért
- a hivatal informatikai rendszerinek üzemszerű használatáért
- a személyi használtra átvett eszközök megfelelő fizikai védelméért

A felhasználó számára büntetőjogi, illetve munkajogi felelősségre vonás terhe mellett TILOS illetéktelenül más felhasználó jogosultságának használata, a hivatal hálózatának monitorozása, felderítése, jelszavak kipróbálás, illetve illetéktelen hozzáférések megkísérlése.

7.1.3. Együttműködés, kapcsolat a hatóságokkal

A jogszabályoknak megfelelően a hivatalnak kapcsolatot kell tartania különböző hatóságokkal, szabályozó testületekkel, továbbá informatikai szolgáltatókkal, közművekkel. A megfelelő kapcsolat kiépítéséért a jegyző, illetve az általa megbízott munkatársak a felelősek.

Az együttműködés során korlátozni kell a biztonsággal kapcsolatos információk kijutását, megelőzendő, hogy a hivatal bizalmas információi illetéktelen kezekbe kerülhessenek.

7.2. Külső személyek által történő hozzáférések

A hivatal informatikai eszközeit csak a hivatal feladatából eredő indokolt esetben, és ellenőrizhető módon szabad külső személyek számára hozzáférhetővé tenni. A hozzáférés engedélyezése előtt azonosítani kell a biztonsági kockázatokat, az ellenőrzés és a felügyelet követelményeit fel kell mérni.

A külső szervezettel vagy személlyel kötött szerződésben az alkalmazandó védelmi intézkedésekről előre meg kell egyezni. Tisztázni kell a hozzáférés feltételeit, meg kell határozni a külső szervezet résztvevőit.

7.2.1. A hozzáférések típusai

Külső személyek hozzáférési fajtái a következők:

- fizikai hozzáférések (a hivatal épületéhez, irodákhoz, informatikai eszközökhöz)
- logikai hozzáférések (a hivatal adatbázisaihoz, informatikai rendszereihez)

7.2.2. A hozzáférések engedélyezési feltételei

A hivatal számára szolgáltatást nyújtó személyek tevékenységük végzéséhez fizikai és/vagy logikai hozzáférést kapnak.

Ilyen szolgáltatást nyújtó személyek az alábbiak lehetnek:

- hardver- és szoftvertámogató személyzet
- társszervezetek, amelyek információt cserélhetnek, információs rendszerekhez vagy adatbázis részekhez férhetnek hozzá

Amennyiben külső személynek hozzáférési lehetőséget kell biztosítani, azt csak és kizárólag az engedélyezési eljárás után lehet megtenni. A hozzáférést mindaddig ki kell zárni, amíg a szükséges

ellenőrzés nem valósult meg, és a szerződésben nem határozták meg a hozzáférés feltételeit. A szerződés elválaszthatatlan részét kell, hogy képezze a Titoktartási nyilatkozat.

A szerződésekben, szükség esetén az alábbiakat kell figyelembe venni:

- az informatikai biztonság fő szabályait
- az információs vagyon bizalmasságának, sértetlenségének és rendelkezésre állásának meghatározását, illetve a védelem érdekében meghatározott eljárásokat
- az információk másolásának és nyilvánosságra hozatalának feltételeit
- a szolgáltatás elvárt szintjének és a szolgáltatási időszaknak a meghatározását
- a felek felelősségének meghatározását
- a szellemi tulajdon védelmére és másolására vonatkozó jogokat és kötelezettségeket
- a teljesítések ellenőrizhetőségét, monitorozását és jelentések készítését
- a felmerülő problémák kezelését
- a hardver- és szoftvertelepítésből és karbantartásokból eredő felelősséget
- világos és egyértelmű jelentéskészítési struktúrát és rendszert
- a változáskezelések egyértelmű és meghatározott folyamatát
- óvintézkedések meghatározását a kártékony kódok ellen
- biztonsági események kivizsgálására és jelentésére vonatkozó intézkedések meghatározását
- az alvállalkozók bevonására vonatkozó szabályokat

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 hozzáférési jogosultság lejárat időpontjának minden esetben szerepelnie kell a hozzáférési engedélyben.

7.2.3. Helyszíni tevékenységet végző külső személyek

Azon külső személyek, akik szerződéses vagy egyéb jogviszony alapján helyszíni tevékenységet végeznek, ugyancsak biztonsági kockázatot jelentenek.

A helyszínre települő külső személyek az alábbiak lehetnek:

- hardver és szoftver karbantartó és támogató személyzet
- takarító, karbantartó, ellátó és biztonsági személyzet, valamint hasonló erőforrás-kihelyezést támogató szolgáltatások

- eseti, alkalmi munkatársak, konzultánsok
- ellenőrző szervezetek munkatársai

A külső személyek által történő hozzáférések esetén még a munka megkezdése előtt egyértelműen meg kell határozni a munkavégzés célját, helyét, idejét, módját, fel kell mérni a hozzáférés engedélyezésének kockázatát.

A harmadik féllel az összes feltétel és körülmény mellett meg kell ismertetni az IBSZ-ben foglaltak rá vonatkozó részeit.

8. Személyi biztonság

8.1. Az alkalmazás előtt

A biztonsági követelményeket a munkaerő-felvételnél, a szerződésekben, valamint az egyén foglalkoztatása során egyaránt érvényesíteni kell.

8.1.1. Informatikai biztonság a felvételnél és a munkaköri leírásokban

Valamennyi munkaterületre részletes munkaköri leírást kell készíteni. A munkaköri leírásnak tartalmaznia kell az adott munkaterületre vonatkozó, a biztonsággal kapcsolatos követelményeket is a felelősség egyértelmű megjelölésével.

Annak érdekében, hogy egyértelműek és tisztázhatóak legyenek a követelmények és ne legyenek átfedések a munkakörök és feladatok tekintetében részletes, és mindenre kiterjedő munkaköri leírást kell alkalmazni. A munkaköri leírásban meghatározott munkaköröknek és feladatoknak a hivatal szervezeti felépítéséhez kell alkalmazkodnia, valamint megbízottak szerződéseiben kell a vonatkozó követelményeket megjeleníteni.

8.1.2. A személyzeti politika

A munkatársak esetében ellenőrzést kell végezni a felvételi eljárás során. Az átvizsgálás menetének kialakításakor figyelembe kell venni az összes ide tartozó titoktartási, személyes adatvédelmi és alkalmazáson alapuló mindenkor hatályos jogszabályokat.

Informatikai biztonsági szempontból az alábbi ellenőrzéseket kell megtenni a belépő munkavállalóval kapcsolatban:

- üzleti és személyi referenciák megléte
- önéletrajz pontossága
- hatóság által kibocsátott azonosító irat
- erkölcsi bizonyítvány megléte
- nyílt közösségi hálók információi
- összeférhetetlenségre vonatkozó információk megállapítása

Az ellenőrző eljárást a szerződő felekre is ki kell terjeszteni. A felek között fennálló szerződésben rögzíteni kell a szerződő fél felelősségét a munkatársak ellenőrzésére vonatkozóan, különös tekintettel a kapcsolattartókra.

A jelölteket tájékoztatni kell az ellenőrzés tényéről.

8.1.3. A foglalkoztatás feltételei

A hivatal munkavállalóinak foglalkoztatásuk előtt az általános és a munkakörre vonatkozó speciális biztonsági előírásokat meg kell ismerniük és aláírásukkal annak elfogadását igazolniuk. A foglalkoztatás kikötései tükrözzék a szervezet biztonságpolitikáját.

8.2. Alkalmazás alatt

Az alkalmazás alatt folyamatosan gondoskodni kell arról, hogy a felhasználók tudatában legyenek az informatikai biztonság fenyegetéseivel, és motiválva legyenek a hivatal informatikai védelmi szabályzatainak és intézkedéseinek betartására.

8.2.1. A vezetőség felelősségei

A vezetőség felelőssége, hogy megkövetelje az alkalmazottaktól, a szerződő felektől és a harmadik féltől, hogy a meghatározott szervezeti szabályokat és eljárásokat a biztonsági intézkedésekkel összhangban alkalmazzák.

Az alkalmazottakban, a szerződő felekben és a harmadik félben tudatossá kell tenni a biztonság iránti felelősségüket.

8.2.2. Az informatikai biztonsági tudatosság, oktatás és képzés

A hivatal valamennyi munkatársát, és ha szükséges, a harmadik fél felhasználóit is, megfelelő képzésben kell részesíteni a hivatal biztonsági szabályairól és eljárásairól.

A hivatal elektronikus információs rendszereit csak olyan személyek használhatják, akik megfelelő számítástechnikai, informatikai ismeretekkel rendelkeznek.

Rendszeres belső oktatásokkal gondoskodni kell arról, hogy a felhasználókban tudatosodjanak az alapvető információbiztonsági fogalmak, illetve ismerjék meg a munkájuk során felmerülő információbiztonsági fenyegetettségeket. Gondoskodni kell arról is, hogy a napi feladatok végzése során a felhasználók kellőképpen felkészültek legyenek a jelen IBSZ-ben foglaltak betartására.

A képzés foglalja magába a biztonsági követelményeket, a jogi felelősséget, az üzleti óvintézkedéseket, valamint az informatikai eszközök helyes használatát.

Az oktatáson való részvétel az informatikai rendszerrel kapcsolatba kerülő valamennyi személy számára kötelező, az oktatáson történő megjelenést a résztvevők aláírásukkal kötelesek tanúsítani.

A kiemelt jogosultságokkal rendelkező munkatársak részére külön oktatást kell tartani.

Az információbiztonsági oktatások és továbbképzések tematikájának kidolgozása, a szükséges szakirodalom és tájékoztató anyagok biztosítása, valamint a képzés megtartása az IBF feladata.

A jegyzőnek, a rendszergazdának és az Információ Biztonsági Felelősnek külön jogszabályban előírt továbbképzésen kell részt venniük.

8.2.3. Fegyelmi eljárás

A hivatal biztonsági szabályzatait és eljárásait megsértő alkalmazottakkal szemben a közszolgálati tisztviselőkkel szembeni fegyelmi eljárásról szóló 31/2012. (III.7.) Korm. rendeletet alapján fegyelmi eljárást kell indítani. A fegyelmi eljárás a jogszabályok és hivatal belső szabályai szerint történik.

8.3. Alkalmazás megszűnése vagy megváltozása

Ugyanazon szintű biztonsági intézkedések vonatkoznak a munkaviszony szervezeten belüli megváltozására, mint a munkaviszony megszüntetésére. Ennek magyarázata, hogy az egyes szervezeti egységek eltérő adatállományt és eltérő adatfeldolgozó eszközöket használhatnak, ezért eltérő jogosultsággal, hozzáféréssel kell rendelkezniük. Annak érdekében, hogy az átfedéseket, összeférhetetlenségeket elkerüljük szükséges a változások esetében is ugyanolyan gondossággal eljárni, mint amikor az adott munkavállaló elhagyja a hivatalt.

A munkajogviszony megszűnésére vagy változására vonatkozó intézkedéseket időben meg kell tenni, annak érdekében, hogy mire az adott munkavállaló elhagyja a hivatalt, vagy megkezdi munkáját az új munkakörében, addigra minden szükséges biztonsági intézkedés az új helyzetre vonatkozóan megvalósuljon.

Alkalmazás megszűnése vagy megváltozása esetén az alábbi eljárásokat mindenképpen le kell folytatni.

8.3.1. Az eszközök visszaadása

Minden munkavállalónak vagy szerződő félnek a szerződése vagy megállapodása lejárásával a munkavégzéshez kapott eszközöket vissza kell szolgáltatnia a hivatal részére.

9. Az eszközök biztonsági besorolása és ellenőrzése

A vagyontárgyak kezelése a hivatal biztonsági intézkedéseinek célja. A védelem biztosítása érdekében minden vagyontárgyat leltárba kell venni (szabályzat létrehozásakor, valamint új beszerzés esetén), és minden vagyontárgynak megnevezett felelős gazdát kell kijelölni.

A hivatal vagyonleltára informatikai biztonsági szempontból az alábbiakat tartalmazza:

- információ-vagyon: az adatok, az adatbázisok, szoftver-kezelési kézikönyvek, oktatási, üzemeltetési, biztonsági segédletek és nyilvántartások
- szoftver-vagyon: rendszerszoftverek, alkalmazói szoftverek, fejlesztő-eszközök és szolgáltatások
- fizikai-vagyon: hardver (számítógépek, perifériák, mobil számítástechnikai eszközök), kommunikációs eszközök (telefonok, telefaxok, modemek, hálózati csatoló eszközök), adathordozók és egyéb műszaki berendezések (szünetmentes tápegység, légkondicionáló berendezés)

9.1. A vagyoni felelősségre vonhatóság

A hivatalnak képesnek kell lennie eszközeit, vagyontárgyait egyértelműen azonosítani. Meg kell határozni, hogy hol találhatóak, kinek a felelősségi körébe tartoznak, és osztályozni kell bizalmasság, sértetlenség és rendelkezésre állás fenntartásában játszott szerepüknek megfelelően.

Valamennyinek meg kell nevezni a felelősét, az alkalmazott védelmi intézkedésekre vonatkozóan is. A védelmi intézkedések megvalósításának felelősségét át lehet ruházni, de a felelősségre vonhatóság akkor is a megnevezett felelősnél marad.

9.2. Eszköz és vagyonleltár

A hivatal a vagyonleltár segítségével képes azonosítani vagyonát, és megállapítani a vagyontárgyai értékét és fontosságát. A kockázatkezelés fontos része a vagyonleltár, ezért a hivatal minden olyan jelentős vagyontárgyáról leltárt kell felállítani és aktualitását fenntartani, amely valamelyik informatikai rendszerrel kapcsolatos.

Egyértelműen azonosítani kell valamennyi vagyontárgyat és nyilvántartást kell vezetni róla.

Az informatikai biztonságot érintő vagyontárgyak nyilvántartása jelen IBSZ 3. számú mellékletét képezi.

Az informatikai eszköz-nyilvántartás a következőket tartalmazza:

- a vagyontárgy fizikai elhelyezkedését: szervezeti egység
- az eszköz nevét
- leltári számát

A szoftver-nyilvántartásnak tételesen fel kell sorolnia – amennyiben a licenszszerződés nem tiltja – a rendelkezésre álló szoftver licenszeket az alábbi adatok feltüntetésével:

- tételazonosító sorszám
- a szoftver gyártója
- a szoftver neve
- a szoftver leírása
- a licensztípusa
- a szoftver típusa
- a dokumentációt, illetve az eredeti adathordozót birtokló szervezeti egység megnevezése
- amennyiben releváns, az adatgazdát

9.3. A vagyontárgyak gazdája

Az adatfeldolgozási eszközökhöz kapcsolódó minden információnak és vagyontárgynak van felelős gazdája. Amennyiben egy elemhez nem rendelhető egyén, a felhasználó szervezeti egységhez, mint csoporthoz kell rendelni. A felelősség ezekben az esetekben a felhasználó szervezeti egység vezetőjéé.

9.4. Az eszközök megfelelő használata

Az informatikai eszközök használatának módját szabályozni kell, melyet minden alkalmazottnak és szerződő félnek, valamint harmadik félnek be kell tartania.

A felhasználó:

- köteles az eszközöket és szoftvereket rendeltetésüknek megfelelően használni
- köteles a tőle elvárható gondossággal eljárni az eszközök használata során
- az eszközöket védeni köteles rongálás vagy károkozás ellen
- a rábízott eszközöket nem adhatja kölcsön harmadik személynek, kockáztatva az eszköz épségét és a rajta lévő adatok biztonságát és sértetlenségét

- bármilyen hiba vagy sérülés észlelése esetén azonnal jelentenie kell a felettesének
- a használatába adott eszközökön csak a munkavégzéshez szükséges feladatokat végezheti
- tilos az eszközök személyes haszonszerzés, illetve nem a hivatal érdekében történő használata
- a hivatal információ feldolgozó eszközeit a hivatal helyiségeiből csak külön engedéllyel szabad kivinni

9.5. Az adatok biztonsági osztályozása

Az informatikai eszközök megfelelő védelmének érdekében szükséges az informatikai eszközök védelmi szintjének meghatározása. A számítástechnikai rendszerek, illetve adatok biztonsági osztályának tükröznie kell a védelem szükségességét, prioritásait és mértékét.

9.5.1. Az osztályozás irányelvei

Az informatikai rendszerben az adatok kezelése a mindenkor hatályos jogszabályoknak megfelelően kell, hogy történjen.

A 2013. évi L. törvény alapján az informatikai rendszereket biztonsági szintekbe kell sorolni, mely figyelembe veszi a rendszerek, illetve az általuk kezelt és tárolt adatok bizalmasságát, sértetlenségét és rendelkezésre állását.

9.5.2. Az adatok minősítése, címkézése és kezelése

A hivatalban a jogosultságok alapján, az elfogadott osztályozási sémával összhangban megfelelő eljárást kell kialakítani, mely meghatározza az információ minősítésének, címkézésének és kezelésének módját.

Ezeknek az eljárásoknak fizikai és elektronikus formátumokban le kell fedniük az egész információvagyont.

Az adatfeldolgozás egyes tevékenységeinél alkalmazható adatkezelési eljárásokat a következőképpen kell meghatározni:

- másolás
- tárolás
- archiválás
- továbbítás (postai úton, faxon, elektronikus levelezéssel)
- megsemmisítés

Az informatikai rendszerben megvalósított adat- és információvédelmet az IBSZ-szel összhangban kell meghatározni.

Az informatikai rendszerben az adatvédelem érdekében előírás:

- az informatikai rendszer eszközeinek a biztonsági osztályuknak megfelelő védelem
- erős felhasználó azonosítás és hitelesítés
- a felhasználók számon kérhetőségét biztosító biztonsági beállítások
- jogosultság és eseménynaplók működtetése

10. Az elektronikus információs rendszerek nyilvántartása

10.1. 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

10.2. Felelősök

A hivatal elektronikus információs rendszerinek nyilvántartását Sajtos Lajos végzi. A nyilvántartás karbantartásáért szintén ő felel. Felülvizsgálatát, ellenőrzését az Informatikai Biztonsági Felelős végzi.

10.3. A nyilvántartásban tárolt adatok

A nyilvántartásban kötelezően a szoftverekről, alkalmazásokról az alábbi adatokat kell tárolni:

- szoftver neve, azonosítója
- szoftver gyártója, kapcsolattartója (amennyiben releváns)
- szoftver verzió száma
- szoftver sorozatszáma
- licenc típusa
- licencek száma
- aktiválási dátum
- szoftver telepítésének helye

A pontos és folyamatosan karbantartott leltár a sérülékenységek feltárásában, illetve elkerülésében is fontos szerepet játszik.

10.4. A szoftverekben, rendszerekben tárolt adatok köre

A hivatal külön nyilvántartást vezet a rendszereiben, szoftvereiben tárolt adatokról, információkról.

A tárolt adatok körének meghatározása a rendszerek biztonsági osztályának, minősítésének elengedhetetlen feltétele. A biztonsági osztály, a minősítés tükrözi a védelem szükségességét, prioritását és mértékét. A nyilvántartás az alapja a kockázatkezelés során a megfelelő biztonsági intézkedések meghozatalának.

A nyilvántartásnak az alábbiakat kell tartalmaznia:

- szoftver neve
- szoftver telepítési helye
- a szoftverben tárolt adatok adatgazdája
- a szoftverben tárolt adatok köre az alábbiak szerint: önkormányzati, államigazgatási
- a szoftverben tárolt adatok biztonsági szintjének meghatározása bizalmasság, sértetlenség és rendelkezésre állás szempontjából

11. Biztonságtervezés

A hivatal az informatikai biztonság megteremtése érdekében szabályozza a biztonsági intézkedéseket. A biztonsági intézkedéseknek, illetve döntések meghozatalának ki kell terjednie az informatikai rendszer minden életszakaszára. Ennek értelmében egy-egy új alkalmazás bevezetésére, a meglévők változtatásaira vagy éppen üzemeltetésére is.

Biztonságtervezési szempontból a hivatal az alábbi időszakokat definiálja az információs rendszerek életciklusának tekintetében:

- követelmények meghatározása
- beszerzés
- megvalósítás vagy értékelés
- üzemeltetés és fenntartás
- kivonás (archiválás, megsemmisítés)

11.1. Rendszerbiztonsági terv

El kell készíteni az elektronikus információs rendszerek rendszerbiztonsági tervét, mely a következőket tartalmazza:

- az elektronikus információs rendszer hatóköre, alap feladatai (biztosítandó szolgáltatásai), biztonságkritikus elemei és alap funkciói
- az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztálya
- az elektronikus információs rendszer működési körülményei és más elektronikus információs rendszerrel való kapcsolatai

Az elektronikus információs rendszer biztonsági követelményeit a vonatkozó rendszerdokumentációban kell rögzíteni.

Meg kell határozni a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedésbővítéseket, illetve végre kell hajtani a jogszabály szerinti biztonsági feladatokat.

A rendszerbiztonsági tervet meg kell ismertetni a hivatal érintett munkatársaival.

Az elektronikus információs rendszerek rendszerbiztonsági tervét kétévente felül kell vizsgálni.

Soron kívül felül kell vizsgálni a rendszerbiztonsági terveket az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások, illetve a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén.

Az elektronikus információs rendszerek rendszerbiztonsági tervét az érintettek bevonásával az IBF készíti el.

A rendszerbiztonsági tervek bizalmasnak minősülnek, ezért azok megismerésére az IBF, a rendszergazda, a jegyző, valamint a jegyző által írásban kijelölt személyek jogosultak.

11.2. Az internet használat és az elektronikus levelezés szabályai

11.2.1. A web böngészés szabályai

A hivatal minden munkavállalója számára olyan munkaeszközt biztosít, ami internetelléréssel rendelkezik. Az internetelérést védi a zavarásoktól, illetéktelen hozzáférésektől és a sérülésektől.

A világháló használata a munka támogatására engedélyezett. Magán célra történő böngészés csak ésszerű keretek között, a minőségi munkát nem akadályozva lehetséges.

A nem munkavégzést szolgáló hálózati sávszélesség foglalása (pl. nagyméretű állományok letöltése), és adatok kiszolgálón történő tárolása esetén a felhasználó figyelmeztetésben részesül. Ismételt előfordulás esetén a rendszergazda jelentést tesz az IBF-nek, aki eljár az ügyben a jegyző felé.

A felhasználók kellő felelősséggel és hozzáértéssel használják az internetet. Lehetőség szerint csak ismert és biztonságos oldalakat látogassanak, az ismeretlen és nem megbízható oldalakat igyekezzenek kerülni.

Alapesetben tiltani kell a felugró ablakok automatikus megjelenését a böngészőben. Amennyiben a felhasználó által, munkavégzéshez használt alkalmazások megkívánják az előre ugró ablakok megnyitását, úgy ezen webhelyeket kivételként fel kell venni, és engedélyezni szükséges azok automatikus megjelenését. A kivételek rögzítése a rendszergazda feladata.

A Java alkalmazások és Active-X vezérlők automatikus futtatását le kell tiltani, azokat lehetőleg csak akkor szabad engedélyezni, ha megbízható forrásból származnak, illetve ha a várható működés ellenőrizhető.

Az internetről jogvédett anyagokat csak a jogtulajdonos beleegyezésével és a felhasználására vonatkozó szabályok betartásával lehet letölteni vagy használni. A hivatal tiltja a hang és mozgókép állomány, valamint végrehajtható kódot tartalmazó programfájl letöltését, torrent kliensek használatát.

File letöltéseket az informatikai rendszer csak olyan esetben engedélyez, amikor az a megfelelő védelmi és biztonsági (vírus) ellenőrzéseken átesett. A hibás, sérült vagy kétes eredetű file-ok letöltése tilos. Különleges esetekben a rendszergazda segítségével és a megfelelő biztonsági intézkedések alkalmazásával engedélyezhető a szűrésen fennakadt file-ok letöltése.

Azonnali üzenetküldésre alkalmas, külön telepítést igénylő alkalmazások (pl.: Skype, Yahoo messenger stb.) nem használható. Ettől eltérni a jegyző külön engedélyével és az Informatikai Biztonsági Felelős jóváhagyásával, csak határozott időre lehet. Az azonnali üzenetküldésre alkalmas alkalmazások telepítését minden esetben a rendszergazda végzi, és az engedélyben meghatározott idő lejártával törölni kell az alkalmazást a felhasználó gépéről.

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 informatikai biztonsági feladatokat ellátó személyeknek munkájuk során szükségük lehet a felhasználók internet használati adataira, illetve a látogatott oldalak (böngészési előzmények) vizsgálatára. Az ellenőrzést előzetes bejelentés nélkül is meg lehet tartani, azonban minden esetben dokumentálni kell a folyamatot, a dokumentációba az érintett felhasználó az ellenőrzés lezárása után betekinthet.

A munkával összefüggésbe nem hozható oldalak elérhetőségét az informatikai üzemeltetés jogosult korlátozni.

- Tilos a levelezési címet olyan szolgáltatásnál regisztrálni, ami nem a hivatal feladat ellátási köréből adódik. Ha a hivatal feladat ellátásából adódóan kell email címet bármilyen platformon regisztrálni, úgy célszerű külön, csak erre a feladatra szolgáló különleges email címet használni.

- Ismeretlen feladótól érkezett, különös témájú, csatolt fájlt tartalmazó leveleket körültekintéssel kell kezelni, szükség esetén a rendszergazda segítségét kell kérni, a gyanús levelet a rendszerből el kell távolítani.

- Nagyméretű fájlokat tilos sok címzettnek elküldeni, mert az túlzott mértékben leterheli a hálózat forgalmát, illetve megbéníthatja azt. Nagyméretű fájlok esetében más adatátadó, adathordozó eszköz igénybevételével kell eljuttatni az információt.

- Az alábbi információk nyílt továbbítása elektronikus levélben szigorúan tilos:

    - nem a nyilvánosságnak szánt üzleti és pénzügyi információk

    - a hivatal informatikai vagy biztonsági rendszerére vonatkozó bármilyen adat (pl.: jelszavak, felhasználó nevek, IP címek)

    - nem a nyilvánosság számára készült belső eljárásrendek

- A hivatal tevékenységével kapcsolatos levelet csak a címzett kifejezett kérésére szabad ingyenes internetes levelezési címre küldeni.

- Amennyiben valaki hiba folytán olyan elektronikus üzenetet kap, melynek szándékolt címzettje nyilvánvalóan nem Ő, köteles azt – amennyiben egyértelműen meghatározható – az eredeti címzettnek továbbítani, erről a feladót értesíteni. Amennyiben az eredeti címzett nem határozható meg, úgy köteles a feladót a téves kézbesítésről értesíteni és a levelet postafiókjából törölni.

11.2.2.3. Az elektronikus levelezés ellenőrzése

Az elektronikus levelek tartalmának biztonságára vonatkozóan a hivatal garanciát nem vállal, ezért a felhasználónak minden esetben körültekintően kell eljárnia a használat során.

Az informatikai biztonságot ellátó személyeknek munkájuk során szükségük lehet a levelek tartalmának vizsgálatára, ez azonban csak alapos indokkal, dokumentáltan, a jegyző írásbeli engedélyével történhet. Minden olyan esetben, amikor ezt valamilyen különleges eset (pl.: fegyelmi

eljárás, vagy vétség megállapítása) nem indokolja, a postafiók használóját előzetesen értesíteni kell a vizsgálatról.

12. Fizikai környezet és biztonság

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 rendszereket 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 gondoskodni kell

12.1. Biztonsági zónák

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

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.

12.1.1. 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.

12.1.2. Beléptetési intézkedések

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.

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 háromhavonta, és eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése már nem indokolt.

12.1.3. 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 számítógépterem/szerverterem 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.

12.1.4. Védelem a külső és környezeti fenyegetettségek ellen

Kockázatokkal arányosan kell biztosítani a védelmet a tűz, árvíz, földrengés, robbanás vagy más természeti, vagy emberi jellegű károkozás ellen. A biztonságos zónákat úgy kell kialakítani, hogy veszélyes vagy éghető anyagok kellő távolságban legyenek, a tartalékberendezések és a tartalék adathordozókat biztonságos távolságban kell elhelyezni a működésfolytonosság biztosításának érdekében.

12.1.5. Munkavégzés a biztonsági zónákban

A biztonságos zónákban való munkavégzés estén kiegészítő intézkedésekre és útmutatókra van szükség.

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.

12.2. 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.

12.2.1. 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. Minden alkalmazottnak a „Tiszta asztal tiszta képernyő" elve alapján kell eljárnia.

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.

A berendezéseket meg kell védeni a tápáramellátás, és más közmű szolgáltatások meghibásodásától. Ennek érdekében olyan villamos tápáramellátást kell alkalmazni, amelyik megfelel a

berendezésgyártó specifikációjának. A tartalék tápáramellátást biztosító szünetmentes egységen túl aggregátoros betáplálási lehetőséget is biztosítani kell.

A fenti intézkedések megvalósításához szükséges erőforrások biztosításáért a jegyző, a kialakításért és megvalósításáért a rendszergazda a felelős.

12.2.2. 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 a föld alatt vagy egyéb módon védve ajánlatos elvezetni az adatfeldolgozó rendszerekhez csatlakozó kábeleket a jogosulatlan lehallgatás és károkozás elkerülésének érdekében.

A kábelezés biztonságáért a rendszergazda felel.

12.2.3. A berendezések karbantartása

Az informatikai eszközökön javítását, módosítását, illetve új eszközök telepítését csak a rendszergazdák, vagy az Informatikai Biztonsági Felelős által engedélyezett és ellenőrzött külsős, szerződött vállalkozó végezhet.

Adathordozók esetében, ha a javítás külső helyszínen történik, az adattartalmat törölni, az el- és visszaszállítást pedig dokumentálni kell. Ez alól kivételt képez az adatvisszaállítás céljából elszállított eszköz.

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.

12.2.4. A telephelyen kívüli berendezések védelme

A biztonság érdekében a jegyzőnek kell felhatalmazást adnia minden olyan berendezés használatára, amelyen a hivatal számára „házon-kívül" végeznek adatfeldolgozást. Ezekre a berendezésekre vonatkozó biztonsági intézkedések biztonsági foka egyezzen meg a hasonló munkavégzésre szolgáló „házon-belüli" berendezések biztonsági védelmével.

Minden munkatársnak az elvárható gondossággal kell eljárnia telephelyen kívüli berendezés használatakor.

Ennek felügyeletéért a szervezeti egység vezetője, ellenőrzéséért az Informatikai Biztonsági Felelős a felelős.

12.2.5. 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 (biztonsági törlést végző alkalmazás pl.: Shredder, AlienVault, stb) az egyszerű, szokásos törlési művelet alkalmazása helyett.

Az érzékeny információt tartalmazó, de sérült tárolóeszközök tartalmának kritikussága alapján kell meghatározni, hogy az adott eszköz megsemmisítésre vagy javításra kerüljön.

12.2.6. Az eszközök selejtezése, elvitele

A hivatal vagyonleltárába tartozó valamennyi eszközre vonatkozóan a hivatal belső szabályozásának megfelelő irányelveket kell alkalmazni.

12.2.6.1. Az informatikai eszközök kivitele, szervizbe küldése

Írásos engedély nélkül (állandó vagy eseti) berendezést, informatikai eszközt vagy szoftvert házon kívülre vinni nem szabad.

Az elszállításról szállítólevelet kell kitölteni, melyben fel kell tüntetni a kivitt eszköz típusát, gyári számát.

A vagyontárgyakat illetéktelenül nem lehet eltávolítani, ennek ellenőrzésére helyszíni szemléket kell tartani. A helyszíni szemle lehetőségéről mindenkit tájékoztatni kell, ami lehet időszakos vagy váratlan. Váratlan helyszíni szemlét csak a hatályos jogszabályok betartásával lehet végezni.

13. Számítógépes hálózati szolgáltatások és az üzemeltetés menedzsmentje

Az IBSZ-ben megfogalmazott előírások és a biztonsági intézkedések célja az adatfeldolgozó eszközök helyes és folyamatos működésének biztosítása.

Az összes adatfeldolgozó eszköz üzemeltetési eljárásait és az üzemeltetéssel járó felelősségi köröket előre definiálni kell, és folyamatosan felül kell vizsgálni. Az üzemeltetési eljárásokat úgy kell létrehozni, hogy maximálisan támogassák a feladatok és felelősségek elhatárolását. A jól definiált feladatelhatárolódás lehetővé teszi, hogy minden munkavállaló csak a munkájához szükséges információkhoz férjen hozzá.

13.1. Az üzemeltetési eljárások és felelősségek

13.1.1. Az üzemeltetési eljárások dokumentációja

Az üzemeltetési eljárásrendeknek, megjelenési formájuktól függetlenül az alábbiakról kell rendelkeznie.

- az adott részelem adatkezeléséről, feldolgozásáról és tárolásáról
- az ütemezés követelményeiről, beleértve az összefüggéseket más rendszerekkel
- a munkaidőn kívüli munkavégzésről
- minden rendszerelemre vonatkozó hibaesetekről és a rendellenes működésre vonatkozó eljárásokról
- az adott részelem során használt hardver és szoftver karbantartási eljárásokról
- a munkavégzés során jelentkező kivételes állapotok kezeléséről
- a rendszer újraindításának eljárásáról, a hibás működés utáni rendszerviszaállítás szabályairól

Az adott munkafolyamatra, rendszerelemre vonatkozó üzemeltetési eljárások dokumentációját az adott rendszerelem üzemeltetési helyén hozzáférhetővé kell tenni.

Az informatikai rendszer eszközei üzemeltetésének és rendelkezésre állásának biztosítása a rendszergazda feladata.

Az informatika rendszer vagy valamely eleme leállásairól, meghibásodásairól hibanaplót kell vezetni.

13.1.2. Változáskezelés

Az adatfeldolgozó eszközöket és rendszereket érintő változásokat ellenőrizni kell.

A jelentős változások lehetséges hatásait fel kell mérni, a változásokat azonosítani és rögzíteni kell. Az informatikai rendszerben bármely változás csak ellenőrzött módon vezethető be. Biztosítani kell, hogy a tervezett változások mind jóváhagyottak legyenek. A változások jóváhagyásának felelőse a rendszergazda.

A változások minden részletes adatát minden érintett személlyel, jogosultságának megfelelő mértékben közölni kell.

13.1.3. A feladatkörök elhatárolása

A jegyzőnek biztosítani kell a feladatok vagy felelősségi körök végrehajtásának és irányításának a szétválasztását annak érdekében, hogy az információ jogosulatlan módosítására vagy visszaélésre vezető alkalmak esélyét csökkentse.

Ha fennáll az összejátszás veszélye, akkor olyan védelmi intézkedéseket kell tenni, hogy két vagy három személy vegyen részt az adott tevékenységben, hogy ezzel csökkenjen az összejátszás lehetősége.

Az egyes feladatot ellátó személyek között minimum kettesével, de ha lehetőség van rá hármasával kell a feladatokat és felelősségeket kiosztani a helyettesítés megoldására.

13.1.4. A fejlesztési, teszt és üzemeltetési feladatok szétválasztása

A fejlesztő, tesztelő és az üzemeltetési eszközök szétválasztásával lehet elérni a vonatkozó szerepkörök elkülönítését.

A fejlesztő, tesztelő és éles üzemi szoftvert, ahol csak lehetséges és szükséges, különböző számítógép rendszereken kell futtatni. Amennyiben a logikai szétválasztási szint biztosítja a tesztelői és éles környezet közötti átjárhatatlanságot, úgy nem szükséges a fejlesztői és üzemeltetési környezet fizikai szétválasztása.

Logikai szétválasztás egyik eszköze a teszt környezetbe és az éles rendszerbe való bejelentkezési eljárás eltérő használata. A fejlesztő személyzetnek az éles környezetben csak megfelelő engedélyezési eljárás után lehet hozzáférést biztosítani. A jogosultság lejárta után a hozzáférést le kell tiltani.

13.2. Harmadik fél által nyújtott szolgáltatásának irányítása

13.2.1. Szolgáltatás színvonala, szolgáltatásnyújtás

A harmadik féltől igénybevett szolgáltatás során alapvető biztonsági szempont, hogy a szolgáltatási szerződésekben meghatározott biztonsági intézkedések, a szolgáltatás színvonala folyamatosan fenntartható lehessen. A szerződéskötés előtt fel kell mérni a kockázatot, és kellő óvintézkedéseket kell bevezetni, melyekről a szerződő felet is tájékoztatni kell.

A hivatalnak gondoskodnia kell arról, hogy mindig legyenek vésztervei a szolgáltatás átmeneti vagy végleges leállására vonatkozóan. A kockázatokkal arányosan ajánlatos a szolgáltatási szerződésekben kikötni a vészhelyzet esetén alkalmazandó intézkedéseket, a bevonható helyettesítő szolgáltatások körét.

13.2.2. Harmadik fél által nyújtott szolgáltatás monitorozása és felülvizsgálata

A harmadik fél által nyújtott szolgáltatási szerződésekben meg kell határozni a hivatal ellenőrzési jogkörét. A szolgáltatások színvonalát, a jelentéseket és feljegyzéseket ellenőrizni kell, időszakosan, de legalább évente felül kell vizsgálni. A felülvizsgálatért az Informatikai Biztonsági Felelős felel.

A szolgáltatások ellenőrzése során az alábbiakra kell kitérni:

- szolgáltatás színvonalának ellenőrzésére, a megállapodások betartásának felügyeletére
- a szolgáltatási jelentések átvizsgálására
- az információbiztonsági incidensek feljegyzéseire, a biztonsági dokumentumok megfelelőségére
- az üzemeltetési problémák, meghibásodások nyomon követésére

13.2.3. Harmadik fél által nyújtott szolgáltatás változáskezelése

A szolgáltatás nyújtásában bekövetkező változásokat, illetve a szolgáltatással kapcsolatos végbemenő változásokat kezelni kell. A változáskezelés elősegíti az esetleges üzemeltetési, szolgáltatási hibák gyors behatárolását.

A harmadik fél által nyújtott szolgáltatások változáskezelésébe szükség esetén, és a kockázatokkal arányosan a következőket kell bevonni:

- minden új alkalmazás és rendszer fejlesztését
- a hivatal szabályzatainak és eljárásrendjeinek módosítását, frissítését

- az informatikai biztonsági incidensek megoldására és a biztonság fejlesztésére meghozott intézkedéseket
- hálózatok bővítése, módosítása

13.3. Az informatikai rendszerek tervezése és átvétele

Informatikai rendszerek tervezése során a hivatalnak minimalizálni kell a meghibásodások és a túlterhelések kockázatát. Ennek kulcseleme a kapacitástervezés, melynek segítségével megbecsülhető a hivatal informatikai rendszerének hardver és tárigénye. Az átvétel és használatba vétel előtt meg kell állapítani, dokumentálni kell és bevizsgálni az új rendszerek üzemeltetési követelményeit.

13.3.1. Kapacitástervezés

A rendszer kapacitásának folyamatos figyelemmel kíséréséért a rendszergazda felel. A kapacitástervezés célja, hogy időben biztosíthassuk a kellő feldolgozási teljesítmény és tároló hely, rendelkezésre állását a munkafolyamatok támogatásához.

A rendszergazda a korábbi és várható trendek figyelembevételével elkészíti a jövőre vonatkozó kapacitás bővítések terveit.

Az informatikai rendszer új elemeinek beszerzése előtt meg kell határozni a kívánt berendezésre vonatkozó biztonsági követelményeket, és a beszerzésre vonatkozó döntés előtt vizsgálni kell a követelmények teljesülését.

13.3.2. A rendszer átvétele

Az új informatikai rendszerek, a korszerűsítések és az új változatok, verziók átvételi követelményeit előre definiálni kell. A rendszervizsgálatokat még az átvétel előtt el kell végezni. A rendszergazda és az Informatikai Biztonsági Felelős együttesen gondoskodik az új rendszerek átvételi követelményeinek egyértelmű és egyeztetett meghatározásáról, dokumentálásról. Az új rendszer átvételére csak a dokumentált rendszerkövetelmények megléte esetén kerüljön sor.

Átvétel előtt a biztonság érdekében a következőket mindenképpen ellenőrizni kell:

- a hibajavító és újraindító eljárásokat
- a rutin üzemeltetési eljárásokat
- a megállapodás szerinti biztonsági intézkedések megvalósulását

- az üzletmenet folytonosságára gyakorolt hatását, az üzletmenet folytonosságának érdekében a hozzáféréseket
- az új rendszer hatásait a már meglévőkre
- az új rendszer üzemeltetésének és használatának betanítását adott munkavállaló számára

13.4. Védelem rosszindulatú programok ellen

A hivatalnak minden óvintézkedést meg kell tennie annak érdekében, hogy az informatikai rendszerben a rosszindulatú programok bejutását megakadályozza. A munkaállomásokon és a kiszolgáló gépeken is szükséges az óvintézkedések megtétele a számítógépvírusok bejutásának megelőzésére és észlelésére.

A felhasználóknak tudatában kell lenniük, hogy milyen módon tudnak rosszindulatú kódokat a rendszerbe juttatni, hogy kellő odafigyeléssel és elvárható óvatossággal kezeljék az ilyen interfészek használatát.

A rosszindulatú kódok a bizalmasság, a sértetlenség és a rendelkezésre állás elvesztéséhez is vezethetnek. Ezért a felhasználók és rendszergazdák részére az eljárások gyakorlati útmutatását kell kidolgozni a rosszindulatú kód behurcolási lehetőségének minimalizálására.

13.4.1. A rosszindulatú programokat ellenőrző eszközök

A rosszindulatú szoftver elleni védelem érdekében észlelő és megelőző óvintézkedéseket kell hozni.

Az informatikai rendszer kliensalkalmazásinak állandó biztonsági kockázatokkal szembeni védelmét azok a kliensoldali alkalmazások biztosítják, amelyek egyesítik a vírusok elleni védelem, a kártékony programok elleni küzdelem és a személyi védelmi megoldások elemeit.

A hivatal a vírusvédelmi feladatokat szoftver segítségével látja el. A rendszergazda köteles minden hivatali számítógépenvírusvédelmi szoftvert telepíteni és a megfelelő konfigurálásáról gondoskodni.

A védelmi rendszer biztosítja azt, hogy a munkavégzés során használt informatikai, elektronikai eszközök, valamint az internet használat során előforduló támadások észlelése és elhárítása megtörténjen. A vírusvédelmi programnak rezidens módban kell futnia, azaz adott eszköz elindításával együtt maga a védelmi rendszer is aktiválásra kerül és állandó háttérvédelmet biztosít. A 100%-os felügyeleti időnek köszönhetően felismeri a támadási kísérletet és arra reagálva azonnal elvégzi a szükséges biztonsági intézkedéseket, melyről értesíti a felhasználót.

A felhasználónak tilos kikapcsolnia ezt a védelmet.

A vírusvédelmi programot az irányelvekben meghatározott időpontban és gyakorisággal frissíteni kell.

13.4.1.1. A vírusvédelmi rendszer kialakítása és működtetése

A hivatal a rosszindulatú kódok alábbi fajtáját határozza meg:

- vírusok (bootvírusok, fájlvírusok, makróvírusok)
- férgek
- trójai vírusok

A rosszindulatú kódokat a rendszerbe külső csatlakozásokon és hordozható lemezeken, adattárolókon behozott állományokon és szoftvereken keresztül lehet behozni. A hivatal az alábbi hordozókat tekinti a rosszindulatú kódok elsődleges veszélyforrásainak:

- pendrive-ok
- egyéb kivihető, mobil adathordozók
- elektronikus levelek
- hálózatok
- távoli hozzáférések
- letöltések

13.4.2. Mobil kód elleni intézkedések

A mobil kód egy szoftver, mely általában az internetről letölthető és a helyi munkaállomásokon végrehajtandó állományokat tartalmaz. A mobil kód számos szoftverszolgáltatással társul, ezért biztonsági szempontból kulcsfontosságú, hogy ne tartalmazzon rosszindulatú kódot.

A hivatalban a mobil kódok alkalmazása, futtatása csak külön engedéllyel lehetséges. Azokon az eszközökön, amiken mégis engedélyezni kell a mobil kódok futtatását, ott az alkalmazott szoftverkonfigurációnak kellő védelmet kell biztosítani a rosszindulatú kódokkal szemben.

13.4.3. Teendők vírusfertőzés esetén

Vírustámadás, vagy egyéb incidens esetén az azt észlelő személynek haladéktalanul tájékoztatnia kell a rendszergazdát a fertőzésről vagy annak gyanújáról.

A fertőzött eszközt le kell állítani és azonnal el kell távolítani a hálózatból. A javítást, hibakeresést, vírusirtást csak és kizárólag a hálózatból leválasztott állapotban lehet megkezdeni.

13.5. Mentés

Az információ és az adatfeldolgozó szoftverek épségének és rendelkezésre állásnak biztosítása érdekében az adatokat rendszeresen menteni kell. Az adatmentések lényege a teljes, veszteségmentes visszaállíthatóság, ezért a mentési médiák visszaállíthatóságát legalább évente egyszer ellenőrizni kell.

13.5.1. Adatmentések

Az ügymenet adatainak és szoftverek biztonsági mentésének folyamatos időszakos elkészítése, és ellenőrzése alapvető biztonsági követelmény. Ugyanakkor tartalék mentési eszközöket kell biztosítani arra az esetre, ha a mentési rendszer valamelyik eleme hibásodna meg.

A mentések elsődlegesen disk alapú adathordozóra, egy kizárólag erre a célra rendszeresített tárterületre történnek.

A mentések gyakorisága

- hetente teljes biztonsági mentés
- naponta inkrementális mentés

A mentések időzítését a hivatali munkaidőn kívülre kell beállítani. A teljes mentéseket minimum egy évig meg kell őrizni.

A mentési rend részletes szabályait a Mentési Szabályzat tartalmazz.

13.6. Hálózatmenedzsment

A hálózatmenedzsment célja a hálózaton áthaladó információ és a támogató infrastruktúra védelme. Különösen nagy körültekintést és odafigyelést igényel a hálózatbiztonság kérdése a nyilvános hálózatokon átmenő adatok esetében.

13.6.1. Hálózatbiztonsági intézkedések

A hivatal fizikailag független, illetve virtuális hálózatainak esetében az egyes hálózatok tekintetében egységes biztonsági szabályrendszert kell alkalmazni.

A hálózaton továbbított adatok felfedésének kockázatával, azok minősítésének megfelelően arányos védelmet kell biztosítani. A kockázatok azonosítása és a megfelelő intézkedések meghozatala az Informatikai Biztonsági Felelős feladata.

A hivatal kommunikációs rendszerit úgy kell kialakítani, hogy biztosítsák az adatátvitel bizalmasságát, sértetlenségét és rendelkezésre állását.

A nyilvános hálózatokon keresztül továbbított érzékeny adatok, illetve a kapcsolt rendszerek védelmére ellenőrző eszközöket, intézkedéseket kell alkalmazni. Ehhez pontosan definiálni kell a hálózat határait.

A hálózati eseményeket naplózni kell, a naplófájlokat meghatározott időközönként, de legalább évente ellenőrizni kell.

Minden informatikai rendszerhez csatlakozott vagy attól függetlenül használt munkaállomásról pontos és naprakész nyilvántartás kell vezetni.

Az informatikai rendszerben a felhasználók számára a hozzáférést szabályozni kell. Minden felhasználónak joga van saját felhasználói fiókhoz és a munkavégzéshez szükséges web szolgáltatáshoz.

13.6.2. A hálózat használatának szabályai

A hivatal hálózata nem használható az alábbi tevékenységekre:

- a mindenkor hatályos jogszabályokba ütköző cselekmények előkészítésére vagy végrehajtására, így különösen mások személyiségi jogainak megsértésére, tiltott haszonszerzésre irányuló tevékenységre, szerzői jogok megsértésére
- profitszerzést célzó, üzleti célú tevékenységre, reklámra
- a rendeltetésszerű működést és biztonságot megzavaró, veszélyeztető tevékenységre, vagy ilyen információknak és programoknak a terjesztésére
- a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférésre, azok illetéktelen használatára
- a hálózat erőforrásainak, a hálózaton elérhető adatok illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenységre
- másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységét bántó, zaklató tevékenységre

13.6.3. Hálózati szolgáltatások biztonsága

Minden hálózati szolgáltatás esetén fel kell mérni a szolgáltatás biztonsági jellemzőit, irányítási követelményeit, és ezeket a biztonsági követelményeket bele kell venni a szolgáltatási szerződésekbe.

A hálózati szolgáltatási szerződésekben ki kell kötni a biztonsági intézkedések folyamatos betartását, és azok ellenőrizhetőségét.

A biztonsággal összefüggő paraméterek és minősített adatok csak és kizárólag kriptográfiai protokoll alkalmazásával továbbíthatók.

A nyilvános és magánhálózatokon elérhető szolgáltatásokat igénybevevő szervezeti egységeknek gondoskodniuk kell arról, hogy el legyenek látva valamennyi igénybevett szolgáltatás biztonsági jellemzőinek egyértelmű leírásával. A szükséges biztonsági beállítások elvégzése a rendszergazda feladata.

13.7. Az adathordozók biztonságos kezelése

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 szervezeti egység vezetőjének.

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

13.7.1. Hordozható adathordozók kezelése

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

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

13.7.1.1. Az adathordozók tárolása

Az adathordozókat jól zárható, könnyen tisztítható helyiségben, szekrényben vagy fiókban kell elhelyezni úgy, hogy a tárolás és/vagy a szállítás során a sérülés, a károsodás veszélye kizárható vagy minimális szintre csökkenthető legyen. Az adathordozót használónak kizárólagos joga van az adott eszközhöz való hozzáféréshez, ezért biztosítani kell számára a mindenkori hozzáférését.

13.7.1.2. A tárolók környezeti paramétereire vonatkozó előírások

Az adathordozók mobilitásuk és fokozott fontosságuk miatt más veszélynek vannak kitéve a fizikai biztonságukkal kapcsolatos fenyegetettségekkel szemben.

Ezért az alábbi szabályokat kell betartani a tárolás során:

- minden esetben figyelembe kell venni az eszköz gyártójának az üzemeltetésre vonatkozó előírásait
- óvni kell a fröccsenő víztől, illetve a levegő magas portartalmától
- óvni kell az erős mágneses, vagy elektromágneses tértől
- bizonyos eszközök számára biztosítani kell a gyári specifikációban előírt betáplálást
- óvni kell az erős fizikai behatásoktól

A fentiek betartásáért az adott adathordozó használója, azaz a felhasználó felel.

13.7.1.3. Az elöregedésből fakadó adatvesztés elleni megelőző intézkedések

Az adathordozók elöregedéséből adódó adatvesztések elkerülésének érdekében szükséges az eszközökön tárolt adatok rendszeres átírása, ellenőrzése.

13.7.1.4. A másodpéldányok biztonságos tárolására vonatkozó előírások

Minden adathordozóról, annak minősítése után másolati példányt kell készíteni. A másolati példány készítésért az adat előállítója felel. A hivatal informatikai rendszerének működési struktúrájából adódóan a megfelelő helyen tárolt adatokról, dokumentumokról automatikus mentés, ezáltal másolat keletkezik. Az egyedi helyeken tárolt adatok esetében szükséges a kézi duplikáció.

A manuálisan készített másolati példányokat az eredeti példánytól nemcsak logikailag, hanem fizikailag is elkülönítve kell tárolni. A tárolásra vonatkozó előírások megegyeznek az eredeti példány tárolási követelményeivel.

13.7.1.5. Az adathordozók kivitele

Számítástechnikai eszközöket, adathordozókat, programokat kizárólag a jegyző engedélyével szabad kivinni a hivatalból.

A kivitelre kerülő eszközökön tárolt adatok illetéktelenek általi elérhetetlenségére fokozottan ügyelni kell.

Meghibásodott eszköz cseréje esetén adathordozó csak úgy vihető ki, ha arról minden adat visszavonhatatlan módon törlésre került.

13.7.2. Az adathordozók újrahasznosítása, selejtezése

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.

13.7.3. Adatkezelési eljárások

Az adatkezelési eljárásoknak igazodniuk kell a hivatal összes előírásához, szabályzatához.

Az adathordozókat azonosíthatóságuk miatt címkézni kell. Az illetéktelen személyeket ki kell szűrni, hozzáférésüket meg kell akadályozni. Ellenőrizni kell az adatok elosztását, minősítésüknek, osztályozásuknak megfelelően korlátozni kell a hozzáféréseket. Az adatok minősítésében vagy kezelésében bekövetkezett változásokat naplózni kell.

Az észlelt eltéréseket haladéktalanul ki kell vizsgálni, az eredményt jegyzőkönyvben rögzíteni kell.

13.7.4. A rendszerdokumentációk biztonsága

A rendszerdokumentációk különböző biztonságilag érzékeny adatot tartalmazhatnak.

Annak érdekében, hogy a rendszerinformációkat megóvjuk a jogosulatlan hozzáférésektől a következő védelmi intézkedéseket kell betartani:

- a rendszerdokumentációt biztonságosan kell tárolni
- korlátozni kell a dokumentációhoz való hozzáféréseket
- a rendszerdokumentációknak naprakésznek lennie, ezért gondoskodni kell a változások bevezetéséről

13.8. Adatok és programok cseréje

Az adatok és programok cseréje nemcsak a hivatalon belül, hanem harmadik fél számára is történhet. Ezért különösen fontos az adatok és programok átadásának ellenőrzése.

13.8.1. Az adatcserére vonatkozó szabályzatok és eljárások

Az adatcserére vonatkozó szabályzatok és eljárásrendek meghatározáskor különös figyelmet kell fordítani a bizalmasság, a sértetlenség és rendelkezésre állás fenntartására.

Az adatok védelmének érdekében az alábbi irányelveket kell követni:

- bizalmas beszélgetések nem történhetnek nyilvános helyen, nyitott irodákban, vagy vékony falú helyiségekben
- a telefonon vagy telefaxon való bizalmas adatközlést kerülni kell
- telefonbeszélgetés során szem előtt kell tartani a lehallgatás lehetőségét (mind a készüléken, mind a közvetlen környezetre vonatkozóan)
- hordozható adathordozóra csak a megfelelő, és a kockázatokkal arányos biztonsági intézkedések betartásával kerülhetnek érzékeny információk
- az információ biztonságos felhasználásának érdekében biztosítani kell a szükséges ismereteket, az ilyen eszközök használatára vonatkozó irányelveket, eljárásokat
- a hivatal más szervezettel adat- és programcserét kizárólag írásbeli szerződés alapján bonyolíthat, melyben utalni kell az érzékeny információk kezelésére

13.8.2. Adathordozók szállítása

Az adat a fizikai szállítás során fokozottan ki van téve az illetéktelen hozzáféréseknek és visszaéléseknek.

A számítástechnikai adathordozók szállítására vonatkozóan az alábbi intézkedéseket kell megtenni:

- ki- és beszállítás során átadás-átvételi elismervény szükséges
- a szállítást lehetőleg a hivatal munkatársa végezze, külső szállítócég csak szerződéses viszony esetében végezhet szállítást; ilyenkor a szerződésben ki kell térni a szükséges biztonsági intézkedésekre
- az adathordózókat védeni kell a fizikai sérülésektől, ennek érdekében a gyártó által jóváhagyott módon kell a szállítást megvalósítani
- a kockázattal arányosan, az értékes információkat hordozó adathordozókat olyan speciális csomagolással kell ellátni, mely láthatóvá teszi a felbontást, vagy az arra tett kísérletet

13.9. Az elektronikus levelezés biztonsága

13.9.1. Biztonsági kockázatok

A hivatal fontosnak tartja a munkatársai hatékony belső és külső kommunikációját ezért elektronikus levelezési lehetőséget biztosít. Az elektronikus üzenetküldésnek azonban a papír alapú adatközléstől jelentősen eltérő biztonsági kockázata van, melyek csökkentésére biztonsági intézkedéseket alkalmaz.

A biztonsági intézkedések az alábbi kockázatokra adnak előírást:

- üzenet sérülékenysége, jogosulatlan hozzáférés
- helytelen címzés, téves elirányítás
- távoli felhasználók hozzáférését a hivatal levelezőrendszeréhez
- bizalmas adatok továbbításának lehetősége
- a levél átvételének bizonyítása
- nem hitelesíthető, kétes forrásból származó üzenetek megnyitása, vírusfertőzött üzenetek

13.9.2. Az elektronikus információs rendszerek

Az elektronikus információs rendszerek lehetőséget adnak az információk szabad áramlására, elosztására. Az információ megjelenésének sokszínűsége (papír alapú, számítógép, mobil eszköz, telefon, fax) miatt meglehetősen bonyolult feladat az ilyen átfogó rendszerek védelme.

Alapvető biztonsági követelmény, hogy a hivatal a vele összekapcsolt valamennyi elektronikus információs rendszeren keresztül forgalmazott adatot a kockázatoknak megfelelővédelemmel biztosítsa.

Az ilyen rendszerek használata során biztonsági szempontból figyelembe kell venni az alábbiakat:

- a szervezet egy vagy több egysége használja a rendszert
- csak belső használatú a rendszer, vagy külső felhasználó számára is szükséges hozzáférés biztosítása
- tartalmaz-e érzékeny információkat, minősített dokumentumokat
- hogyan valósul meg a rendszerben tárolt adatok mentése

13.10. Az elektronikus közszolgáltatás

Törvény, kormányrendelet, önkormányzati rendelet eltérő rendelkezése hiányában a hivatal az ügyfelei számára lehetővé teszi, hogy a közigazgatási hatósági ügyeiket elektronikus úton is intézhetik. Az elektronikus út lehetővé tételével a hivatal célja az ügyfelek és az ügyintézők munkájának könnyítése, ugyanakkor elégséges biztonság nyújtás a tévedésekkel, szándékos hamisításokkal szemben.

13.10.1. Az elektronikus közszolgáltatással szembeni általános követelmények

A hivatal az elektronikus ügyintézés, illetve szolgáltatás teljesítéséhez csak olyan informatikai rendszert vehet igénybe, amely biztosítja a hivatal és az ügyfelek közötti biztonságos kapcsolatot, az adatvédelmi szabályoknak megfelelő adatkezelést és a hiteles dokumentumcserét.

Az elektronikus ügyintézéshez kapcsolódóan biztosítani kell:

- a szolgáltatás ügyfélbarát jellegét
- az akadálymentes használatát
- elektronikus útmutatót, oktatási segédanyagot
- naprakésznek és tartalmilag pontosnak kell lennie

Az ügyfél és a hivatal között ügyintézésre az elektronikus űrlapkitöltő alkalmazás szolgál, mely a kitöltött űrlapot az ASP központba küldi. A központ pedig továbbítja a megfelelő szakrendszerbe.

13.10.2. Az ügyek intézéséhez szükséges azonosítás

A hivatal által meghatározott eljárástípusokban az elektronikus kapcsolattartás lehetősége biztosított, ezért a 85/2012. (IV.21.) Kormányrendelet 16. §-ban foglaltaknak megfelelően köteles az eljárási cselekmény azonosítási biztonsági szintje szerint biztosítani.

Ezek alapján megkülönböztetjük az alábbi azonosításokat:

- anonim ügyintézés
- pszeudonim azonosítás
- névhez kötött azonosítás

Elektronikus aláírás alapján valamely adat akkor tekinthető igazoltnak, ha az aláírás legalább fokozott biztonságú elektronikus aláírás, mely megfelel a jogszabályban meghatározott követelményeknek.

A közigazgatási eljárások során a felhasználható elektronikus űrlapok és dokumentumok azonosítással egybekötött benyújtására a Kormányzati Portál által biztosított Ügyfélkapun keresztül történő hitelesítés segítségével nyújt lehetőséget a hivatal.

Az ügyfél az ügyfélkapu létesítését a regisztrációs feladat ellátására jogosult szerveknél kezdeményezheti (névhez kötött azonosítás). Az ügyfélkapunál használt jelszó alapján történő azonosítás alacsony biztonsági fokozatú azonosítás.

13.10.3. Dokumentumhitelesítés

Elektronikus ügyintézés, kapcsolattartás keretében csak hitelesített elektronikus dokumentum használható.

Az elektronikus dokumentum hitelesítése történhet:

- fokozott biztonságú elektronikus aláírással, jogszabályban meghatározott módon
- az azonosításra visszavezetett dokumentumhitelesítés szabályai szerint
- az iratérvényességi nyilvántartásban történő elhelyezéssel
- a hivatal zárt informatikai rendszerében történő felhasználás esetén

Elektronikusan aláírt dokumentum esetén a hivatal köteles az aláírás, szükség esetén az időbélyegző, valamint az azokhoz kapcsolódó tanúsítvány érvényességének ellenőrzésére.

13.11. Biztonsági megfigyelőrendszer használata

Annak érdekében, hogy kiszűrhetők, illetve megakadályozhatók legyenek az illetéktelen hozzáférések, a tiltott tevékenységeket figyelemmel kell kísérni, a hozzáférési irányelvektől való eltéréseket rögzíteni kell, hogy adott esetben bizonyítékként szolgáljanak, segítséget nyújtsanak a biztonsági események kivizsgálásához.

13.11.1. Biztonsági események naplózása

A kivételes és biztonságot fenyegető eseményeket eseménynaplóba kell bejegyezni és azt meg kell őrizni.

A naplózási rendet úgy kell kialakítani, hogy abból utólag megállapíthatóak legyenek az informatikai rendszer biztonságát érintő fontosabb események. Ezáltal ellenőrizni lehet a hozzáférések jogosultságát, meg lehet állapítani a felelősséget, valamint az illetéktelen hozzáférés kísérletét, megtörténtét.

A naplózási rendszernek alkalmasnak kell lennie mindegyik felhasználó vagy felhasználói csoport által végzett művelet szelektív regisztrálására.

13.11.2. A rendszerhasználat megfigyelése

Az informatikai rendszerekben történő, felhasználók által elvégzett tevékenységeket rögzíteni, naplózni kell. Az üzemeltetéséről üzemeltetési naplót kell vezetni, melyet az Informatikai Biztonsági Felelősnekévente ellenőriznie kell.

Az eredményeket felül kell vizsgálni, melynek gyakorisága az adott informatikai rendszer kockázati tényezőitől függ.

A naplóellenőrzés foglalja magába azokat a fenyegetettségeket, veszélyeket, amelyekkel a rendszerek szembenéznek. Ugyanakkor gyakran ezek a rendszernaplók tartalmaznak nagy mennyiségben nem biztonsági jellegű információt is. Célszerű ezért olyan segédprogramok használata, ami kiszűri a biztonsági megfigyelés számára lényeges eseményeket.

13.11.3. Naplózási információk védelme

A naplóbejegyzések utólagos módosíthatóságát, törlését meg kell akadályozni. Ennek érdekében a naplófájlok hozzáférését megfelelő biztonsági intézkedésekkel korlátozni kell, illetve szükség esetén további titkosítási intézkedéseket kell hozni.

Alapvető biztonsági intézkedés, hogy a rendszernaplók archiválásra kerüljenek, annak érdekében, hogy az abban tárolt információk a későbbiekben is hozzáférhetők és felhasználhatók legyenek. A rendszernaplókat központilag kell gyűjteni, az elemzésük megkönnyítése érdekében.

A naplóbejegyzéseknek az alábbi adatokat kell tartalmaznia:

- esemény dátuma
- a rendszer megfelelő összetevője
- az esemény keletkezésének helye
- az esemény típusa
- a felhasználó azonosítója
- az esemény kimenetele (sikeres vagy hiba)

13.11.4. Naplózási infrastruktúra

13.11.4.1. Naplóforrások beállítása

A naplóforrásokat úgy kell beállítani, hogy a bejegyzések mindig a megfelelő tartalommal, a megfelelő helyen keletkezzenek és a szükséges ideig legyenek megtartva.

13.11.4.2. Log tárolás

A hivatal a logok tárolásának az alábbi lehetséges eseteit különbözteti meg:

- *nincs tárolás*: nem tárolja azokat a logokat, melyeknek nincs vagy nem nagy az értékük a biztonság szempontjából
- *rendszerszintű tárolás*: a kliens eszközökön történik csak a tárolás, a bejegyzések csak a rendszergazdának szolgálnak információval, azokat nem érdemes a központi tárba továbbítani
- *rendszer és infrastruktúra szintű tárolás*: azok az események, melyek elég érdekesek ahhoz, hogy mind a keletkezési helyén, mind a központi tárban megőrizzék, mindkét helyen tárolásra kerülnek
- *infrastruktúra szintű tárolás*: azokat a naplóállományokat, amik fontosak a biztonság szempontjából, és elengedhetetlen a meglétük, központi helyen kell tárolni

13.11.4.3. Logok megsemmisítése, logrotálás

A hivatal a rendszerszinten tárolt naplóállományok tekintetében az alábbi tárolási paramétereket határozza meg:

- biztonság eseménynapló:
    - maximális mérete: 50 MB
    - tárolási méret túllépése esetén írja felül az eseményeket (legrégebbi esemény először)
    - minden esemény másolása központi tárolóba
- rendszer eseménynapló:
    - maximális méret: 50 MB
    - tárolási méret túllépése esetén írja felül az eseményeket (legrégebbi esemény először)

14. Hozzáférés ellenőrzés

14.1. A hozzáférés ellenőrzés követelményei

A felhasználó részére az informatikai rendszerbe belépést csak akkor lehet engedélyezni, ha valamilyen módon azonosítja magát. Ennek érdekében minden felhasználó vagy felhasználó csoport számára világosan meghatározott hozzáférés ellenőrzési szabálynak kell lennie. Általánosan elfogadott elv, hogy csak a szükséges jogokat szabad kiadni.

A rendszerben azonosítani kell a felhasználókat az illetéktelen hozzáférés megakadályozása érdekében. Erre azonosítási és hitelesítési szabályokat kell alkalmazni. A hozzáférési-védelmi eljárásoknak biztosítania kell, hogy a felhasználók a szervezeti funkciójuknak megfelelő jogosultságokhoz (adatokhoz, rendszerekhez) férhessenek hozzá.

A szervezeti és biztonsági követelmények változásával mindenkor összhangban kell lennie a felhasználói hozzáféréseknek, ezért fontos a rendszeres ellenőrzés.

A felhasználói hitelesítések folyamatát naplózni kell, mely tartalmazza a sikeres és sikertelen belépési kísérleteket. A hitelesítési folyamat során keletkező naplók kezelési szabályai megegyeznek az egyéb informatikai rendszerek és a biztonsági események naplózási előírásaival, melyeket a 13.11. pont tartalmazza.

14.1.1. 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).

14.1.1.1. Külső fél hozzáférés ellenőrzése

Külső fél hozzáférésének ellenőrzése azonos követelményeknek megfelelően kell történjen. Külső fél csak egyedi jegyzői engedély alapján kaphat hozzáférést, a hozzáférés feltételeit az engedélyben vagy egyedi szerződésben minden esetben rögzíteni kell.

14.2. A felhasználó hozzáférés ellenőrzése

A felhasználók csak jóváhagyott hozzáférés-védelmi megoldásokat alkalmazhatnak.

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

- A meghatározott jogosultságok alkalmazásával minimalizálható legyen a rosszindulatú vagy egyéb jogosulatlan hozzáférés kockázata.
- Az elektronikus információs rendszerrel kapcsolatba kerülő személyeknek a munkájuk ellátásához szükséges minimális jogosultságokat kell biztosítani, a munkavégzésük időtartamára.
- Az azonos tevékenységet ellátó felhasználók jogosultságai szerepkörök szintjén legyenek kialakítva, és a felhasználók a kialakított szerepkörökbe kerüljenek besorolásra.
- Az összeférhetetlenségi szabályokat figyelembe kell venni.
- Az elektronikus információs rendszerben alkalmazott hozzáférési jogosultságokat adminisztrálni kell.
- Törekedni kell arra, hogy a jogosultságok automatizált módon kerüljenek nyilvántartásba, szükség esetén papír alapon kell a nyilvántartást vezetni.
- Minden egyes elektronikus információs rendszerhez, csak a megfelelő adminisztrálást követően lehet felhasználói jogosultságot adni, módosítani, és felfüggeszteni, illetve visszavonni.
- Az éles elektronikus információs rendszerekben a fejlesztők hozzáférési jogosultságokkal nem rendelkezhetnek.

Az eljárásoknak ki kell terjednie a felhasználók szervezetben betöltött egész életciklusára a belépéstől, a munkakör változáson át a szervezet elhagyásáig. Egyértelműen rögzíteni kell a belépéskor szükséges engedélyezési dokumentumok, folyamatok menetét. A változásokat dokumentálni kell, a kilépésekkor azonnal vissza kell vonni a hozzáféréseket.

A felhasználói hozzáféréseket az adott szervezeti egység vezetője igényli. Szintén a szervezeti egység vezetőjének felelőssége a jogosultságok megvonásának, visszavételének kérvényezése.

14.2.1. A felhasználók regisztrációja

A felhasználókat az informatikai rendszerekben egyedi, jellemző, ellenőrizhető és hitelesítésre alkalmas módon kell azonosítani. Az egyedi felhasználói azonosítót a hozzáférés szabályozására, az adatok és az információk védelmére, valamint a hitelesítés támogatására kell felhasználni.

Az ismétlődő felhasználói azonosítókelkerülése érdekében automatikusan nem ismételhető módon kerülnek kiosztásra a felhasználói azonosítók. A kiosztott azonosítókról nyilvántartást kell vezetni, a nyilvántartást rendszeresen ellenőrizni kell. A nyilvántartásból felhasználói azonosítót törölni nem, csak inaktívvá tenni lehet. A hivatalt elhagyó munkatárs felhasználói azonosítását inaktívvá kell tenni, jogosultságait törölni kell.

A felhasználóknak azonosítójuk kiosztása előtt tájékoztatást, oktatást kell tartani a felhasználási szabályokról. Az előírások megismeréséről nyilatkozatot kell tennie.

Helyettesítéseket lehetőség szerint úgy kell megoldani, hogy a helyettesített munkavállalóval megegyező, vagy ahhoz nagymértékben, de legalább a fontosabb feladatok ellátásához szükséges jogosultságokkal rendelkezzen a helyettesítő munkavállaló.

14.2.2. Jogosultságok kezelése

A jogosultságok kiosztását ellenőrzött módon kell megvalósítani. Azonosítani kell a hivatalban lévő jogosultságokat, ezek alapján ki kell alakítani különböző jogokat, jogosultság csoportokat. A felhasználók hozzáférési jogosultságait, a munkához szükséges minimum jogok alapján kell megadni.

A hivatal az alábbi felhasználói jogosultságukat különbözteti meg:

- olvasási jog
- létrehozási jog (adott objektumon újabb komponenst tud létrehozni)
- módosítási jog
- törlési jog
- írás jog (adott objektumra menteni tud)
- telepítési jog
- jogok szerkesztése jog (a hivatalban csak a rendszergazda rendelkezik ezen joggal)

A rendszergazdai és adminisztrátori előjogokat külön kell kezelni a felhasználói jogoktól. Az azonosítójuknak eltérő, jól elkülöníthető formátummal kell rendelkeznie. A rendszergazdai, adminisztrátori előjogokat csak a rendszergazda engedélyezheti

14.2.3. Felhasználói jelszavak kezelése

Az informatikai rendszerekben a felhasználók azonosságukat jelszóval igazolják. A jelszavak generálása és biztonsági szintje az egyes rendszerekben jelentősen eltérhetnek. Annak érdekében, hogy az adott informatikai rendszer biztonsági szintjének megfelelő legyen a jelszó erőssége az alábbi intézkedéseket kell megvalósítani:

- a felhasználóval meg kell ismertetni a jelszóhasználat szabályait (jelszóhossz, egyediség, bonyolultság)
- a felhasználóknak ideiglenes jelszavat kell biztosítani, melyet az első belépés után kötelezően meg kell változtatniuk
- a felhasználók jelszavaikat csak a biztonsági intézkedések maximális betartása mellett tárolhatják, függetlenül az információhordozó formai megjelenésétől
- az informatikai rendszerekben szigorúan tilos rejtjelezetlen formában tárolni a jelszavakat
- az adminisztrátori jogokhoz kapcsolódó azonosítók, jelszavak, rejtjelezőkulcsok biztonsági másolatát lezárt, lepecsételt borítékban zárható lemez- vagy páncélszekrényben kell tárolni; ezeket rendszeresen ellenőrizni kell; felelőse az Informatikai Biztonsági Felelős

14.2.4. A felhasználói hozzáférési jogosultságok ellenőrzése

A felhasználói hozzáféréseket és azonosítókat rendszeresen ellenőrizni kell, hogy a tényleges hozzáférésük jogosultsága megfelel-e a szerepkörüknek.

A felhasználók hozzáférési jogait legalább évente, vagy az informatikai rendszerekben bekövetkezett jelentős változások esetén felül kell vizsgálni.

Az ellenőrzést az Informatikai Biztonsági Felelős kezdeményezi, és az által meghatalmazott rendszergazda a szervezeti egység vezetőjével közösen végzi.

14.2.5. Hozzáférési jogosultságok visszavonása vagy korlátozása

A hozzáférési jogosultság kiosztási szintjeit felül kell vizsgálni az alábbi esetekben:

- szervezeti struktúra változás
- munkakör módosulás
- munkavállalói kilépés
- ideiglenes hozzáférési jogosultság lejárta
- felhasználói igény esetén

A hozzáféréseket csak a rendszergazda módosíthatja, szüntetheti meg, vagy vonhatja vissza a szervezeti egység vezetőjének kérésére és jóváhagyásával.

14.3. A felhasználó felelősségei

A felhasználó az informatikai rendszerrel, vagy annak biztonsági intézkedéseivel kapcsolatban a biztonságtudatosság képzés keretében kapjon teljes körű tájékoztatást feladatáról, felelősségéről.

Az előírások megértéséről, elfogadásáról felhasználóval a képzés befejezésével nyilatkozatot kell aláíratni.

14.3.1. Jelszóhasználat

A felhasználó a jelszóval igazolja az informatikai rendszerekhez való hozzáférésének jogosultságát, ezért elengedhetetlen, hogy az általa használt jelszavakkal az alábbi biztonsági intézkedések betartásával megfelelően bánjon.

- jelszavait bizalmasan kell kezelnie: titokban kell tartania, harmadik fél számára ki nem adhatja
- jelszavak papírra való rögzítését lehetőleg kerülje, amennyiben mégis írott formában kívánja tárolni, úgy gondoskodjon a biztonságos tárolásáról, mások által hozzá nem férhető módon
- „erős" jelszavat válasszon a felhasználó, ami nem tartalmaz semmilyen személyre utaló információt; lehetőleg legyen benne kis és nagybetű, valamint szám
- a jelszavakat rendszeresen, vagy amikor a szoftver a jelszócserét megköveteli, változtassa meg
- első bejelentkezés alkalmával meg kell változtatni a jelszavát, nem használhat alapértelmezett jelszavat, akkor sem, ha a jelszó minősége, „erőssége" maximálisan kielégítő lenne

A biztonságos jelszóhasználatot a biztonság tudatossági képzés keretében oktatni kell. Fel kell hívni a felhasználó figyelmét, hogy amennyiben más személy az ő azonosítójával és jelszavával lép be az informatikai rendszerekbe, úgy a rendszer automatikusan a felhasználó terhére rója a végrehajtott műveleteket. Felhasználót ilyen esetekben is személyes felelősség terheli.

14.3.1.1. A felhasználói jelszavakkal szemben támasztott követelmények

A hivatal a felhasználók által használt jelszavakra vonatkozóan az alábbi követelményeket határozza meg:

- minimális jelszóhossz: 8 karakter
- központi jelszómegadás utáni első bejelentkezéskor kötelező jelszócsere
- jelszó maximális élethossza: 1 év (egyes szakrendszerek esetében ez eltérhet)
- jelszó zárolása: 5 kísérlet után
- jelszóképzés szabályai: kisbetűt, nagybetűt, számot vagy speciális karaktert is kell tartalmaznia, valamint nem lehet része a felhasználónév

14.3.2. *Felügyelet nélküli berendezésekre vonatkozó felhasználói felelősségek*

A felhasználóknak gondoskodniuk kell a felügyelet nélkül hagyott eszközök megbízható védelméről. Az irodákban lévő munkaállomások különösen nagy kockázatnak vannak kitéve az illetéktelen hozzáférésekkel szemben, ezért a felhasználónak az alábbiak betartásával gondoskodnia kell az általa használt berendezések biztonságáról abban az esetben is, ha nem tartózkodnak irodájukban.

A felhasználók az aktív munkafolyamatokat mindenképpen zárják le, lépjenek ki az adott informatikai rendszerből, szoftverből vagy alkalmazásból, minimum zárolják a képernyőt mielőtt őrizetlenül hagynák az eszközt.

A munkaállomások blokkolásánál a jelszóval védett kombinált képernyővédő funkciót kell alkalmazni. A képernyővédő funkció feloldása csak a sikeres jelszó megadása után legyen lehetséges.

A munkaállomásokat nem elég leállítani vagy áramtalanítani, minden esetben ki kell jelentkeznie a felhasználónak.

14.3.3. *„Tiszta íróasztal, tiszta képernyő" irányelvek*

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. A hivatalnak olyan intézkedéseket kell hozni, melyek megakadályozzák az illetéktelen nyomtatást, vagy a nyomtatás során keletkezett papír alapú anyag illetéktelen kézbe kerülését. Annak betartásáért az adott szervezeti egység vezetője felel.

14.4. A hálózatokhoz való hozzáférés

A hálózatokhoz való hozzáférés szabályozásának és ellenőrzésének célja megakadályozni a hivatal hálózataihoz való illetéktelen hozzáférést.

14.4.1. A hálózati szolgáltatások használatának irányelvei

A hivatalnak biztosítania kell, hogy az informatikai rendszereken belül a felhasználók csak azokhoz a szolgáltatásokhoz, programokhoz, alkalmazásokhoz férhessenek hozzá, melyre az engedélyük kifejezetten vonatkozik.

Ennek érdekében meg kell határozni

- az engedélyezett hálózatok elérési kritériumait
- azokat a személyeket, eszközöket, alkalmazásokat, melyek valamilyen kapcsolatba kerülnek a hálózatokkal
- az ellenőrzési eljárásokat

A hálózatok, hálózati szolgáltatások használati irányelveinek összhangban kell lennie az informatikai biztonsági irányelvekkel.

A felhasználók hálózathoz való hozzáférését, a munkájukat nem akadályozó módon, de korlátozni kell. Az alkalmazásokban a felhasználói jogosultságok egyedi vagy szerepkörhöz kötött módon kell megkülönböztetni, a jogosultságokról nyilvántartást kell vezetni.

Egy hálózathoz jogosultságot csak az a felhasználó kaphat, akinek a munkavégzéshez szükséges az adott szolgáltatás elérése, és rendelkezik az adott szolgáltatás használatához szükséges szakmai és információbiztonsági tudással, valamint arra az adott szervezeti egység vezetője írásos engedélyt adott. Ilyen írásos engedélynek számít a hozzáférés igénylés.

A hálózatot monitorozni kell, annak érdekében, hogy biztosítsuk annak folyamatos rendelkezésre állását. Valamint ellenőrizni kell a felhasználói végpont és a számítóközpont közötti útvonalat. Amennyiben lehetséges kötelezően előírt útvonalat kell használni az informatikai rendszerek eléréséhez. Ennek érdekében az útvonal különböző pontjain a megfelelő ellenőrzéseket kell megvalósítani.

14.4.2. Felhasználói azonosítás-hitelesítés távoli kapcsolatnál

A hivatal hálózatához kívülről csak engedélyezett és szabályozott módon történhet a kapcsolódás. Ennek tükrében az egyéb, külső hozzáférések VPN-enkeresztül valósulhatnak meg. VPN kapcsolat kialakítása, kiadása csak jegyzői engedéllyel lehetséges.

14.4.3. A hálózati eszközök, munkaállomások azonosítása és hitelesítése

Az informatikai rendszerekhez távolról való összes csatlakozást azonosítani és hitelesíteni kell. Automatikus csatlakozást a hivatal a belső hálózatához nem engedélyez. Különleges esetekben, a kockázatokat mérlegelve az Informatikai Biztonsági Felelős engedélyével, és a szükséges biztonsági intézkedések megvalósulásával történhet eszközök csatlakozása a hálózathoz.

14.4.4. A távdiagnosztikai portok védelme

A hivatal által használt rendszerek rendelkezhetnek távoli diagnosztikai eszközzel, melyet az adott rendszer karbantartásáért felelős műszaki szakemberek használnak. Kellő védelem hiányában ezek a pontok lehetőséget adhatnak az illetéktelen hozzáféréshez. Ennek megakadályozására olyan védelmi intézkedéseket kell hozni, melyek biztosítják a jogosulatlan hozzáférést.

A külső félnek hozzáférést ilyen portokhoz csak külön megállapodás keretében szabad biztosítani. A kockázati szempontból kritikus eszközök esetében csak különösen indokolt esetben, és csak a jegyző engedélyével lehet a hozzáférést megadni.

14.4.5. A hálózatok biztonsági szegmensei

A hivatal hálózata átlépi a hagyományos értelemben vett intézményi, társasági határokat, ami fokozhatja az azon keresztül elérhető információs rendszerekhez való illetéktelen hozzáférések kockázatát.

A hivatal hálózatainak biztonsági ellenőrzéseire alkalmas módszer a hálózat logikai struktúrákra, tartományokra való szétosztása, mely mindegyikét egy meghatározott biztonsági háló védi.

A hálózatok elkülönítésének kritériumait a hozzáférés ellenőrzésre vonatkozó irányelvek és a hozzáférési igények alapján kell kialakítani. A kialakításnak a kockázatok mértékével arányosnak kell lennie.

14.5. Azonosítás és hitelesítés

A hivatal az azonosítási és hitelesítési eljárásrendjét az általános biztonsági program részeként alakítja ki, a kritikus informatikai rendszerek tekintetében külön szabályozást is alkalmazhat, melyet az adott informatikai rendszer dokumentációjában rögzít.

Az informatikai rendszer, és az abban tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának védelme érdekében minden lehetséges eszközt fel kell használni annak

érdekében, hogy megakadályozzuk az illetéktelen hozzáféréseket a számítástechnikai erőforrásokhoz.

Ezeknek a következőket kell tenniük:

- azonosítás és hitelesítés: felhasználó személyének, terminál vagy hely azonosítása, hitelesítése
- sikeres és eredménytelen hozzáférések rögzítése
- minőségi jelszavak használata: megfelelő jelszókezelő rendszer használata
- rendszergazdai jogosultságok elválasztása

14.5.1. Biztonságos hitelesítési, bejelentkezési eljárások

Valamennyi munkaállomáshoz a belépési eljárást úgy kel kialakítani, hogy a jogosulatlan hozzáférés lehetőségét a minimálisra csökkentse. Ahol szükséges, ott automatikus azonosítást kell alkalmazni. Ilyen eset, ha egy munkát vagy tranzakciót csak egy adott terminálról lehet elvégezni.

Biztosítani kell, hogy csak a központilag nyilvántartott munkaállomásokról valósulhasson meg belépés, ennek érdekében célszerű egységes munkaállomás névhasználatot bevezetni.

Biztonságos bejelentkezési eljárásnak az alábbiakat tekintjük:

- biztosított, hogy csak a sikeres bejelentkezés után jelenik meg a rendszerre vonatkozó adat
- bejelentkezés csak akkor valósulhat meg, ha a belépéshez szükséges valamennyi adat megadására sor került
- sikertelen bejelentkezés esetén nem utalhat a rendszer a belépéshez szükséges hibás adatokra
- korlátozva van a sikertelen próbálkozások száma
- minősített esetben le kell tiltani a felhasználót, ha a próbálkozások száma elérte a legmagasabb értéket, letiltott felhasználó újra engedélyezéséhez az adott szervezeti egység vezetőjének írásos kérelme kell
- a rendszer naplózza az előző sikeres belépést, és az azóta végzett sikertelen próbálkozások részletes adatait

14.5.2. A felhasználó azonosítás, hitelesítése

A hivatal informatikai rendszerének minden felhasználóját egyedi módon azonosítani kell. Ez az egyedi azonosító a felhasználó kizárólagos azonosítására szolgál, ennek értelmében nem módosítható, másnak át nem adható. Az egyedi azonosító a felhasználó hivatalból való távozása után

sem törölhető az esetleges visszakeresések érdekében. Ha egy felhasználó valamilyen oknál fog rövidebb vagy hosszabb ideig elhagyja a hivatalt, úgy visszatértekor számára biztosítani kell a korábbi azonosítójának használatát.

A felhasználó szervezetben betöltött szerepének változása esetén sem kap új azonosítót. Ilyen helyzetekben az azonosítóhoz rendelt jogosultságokat és hozzáféréseket kell felülvizsgálni és szükség szerint módosítani.

A felhasználói azonosítók kiadása a rendszergazda feladata. Új azonosító kiadása csak az adott szervezeti egység vezetőjének engedélyével lehetséges.

Alapértelmezetten a felhasználók helyi hozzáférését az azonosítás és hitelesítés keretében egylépcsős jelszóval kell ellenőrizni. Szükséges esetekben, ha ezt az érintett rendszer, vagy az abban tárolt adatok köre megkívánja többtényezős hitelesítés is történhet. Többtényezős hitelesítés esetén a tudás alapú azonosítás mellet birtoklás alapú azonosító eszközöket használ a hivatal (pl.: kártyaolvasó).

14.5.3. Jelszómenedzsment rendszer

A jelszavak rendszerszintű kezelését az adott operációs rendszer vagy alkalmazási rendszer beépített jelszókezelői rendszere végzi.

A jelszavakra vonatkozó előírásokat a 14.3.1.1-es pont tartalmazza.

14.5.4. A rendszer segédprogramjainak használata

Biztonsági cél, hogy mindazon operációs rendszerelemek és segédprogramok használata korlátozva és szigorúan ellenőrizve legyen, melyek képesek a rendszer- és alkalmazásvezérlések hatástalanítására.

Csak nagyon ritka, speciális esetekben az Informatikai Biztonsági Felelős engedélyezheti a segédprogramok használatát.

14.5.5. Kapcsolati időkorlátozás

Nagy kockázatú alkalmazások esetén célszerű megfontolni az összeköttetési idő korlátozását. Kapcsolati időkorlátozásra az Informatikai Biztonsági Felelős ad javaslatot, melyet a jegyző hagy jóvá.

A hivatal összeköttetési időkorlátot az alkalmazás hozzáféréséhez az újrahitelesítés módszerével alkalmazza.

14.6. Alkalmazásszintű hozzáférések vezérlése

A felhasználói rendszereken belül az illetéktelen hozzáférések megakadályozására biztonsági eszközöket kell alkalmazni. A logikai hozzáféréseket a programokhoz és adatokhoz minden esetben az engedéllyel rendelkező felhasználókra kell korlátozni.

Az alkalmazások ellenőrizzék az adatokhoz, a rendszer funkcióihoz való hozzáféréseket. Nyújtsanak védelmet az illetéktelen hozzáférésekkel szemben valamennyi segédprogram, rendszerprogram, vagy rosszindulatú program számára, melyek képesek a rendszer vagy alkalmazási vezérlések hatástalanítására. A védelmet úgy kell megszervezni, hogy ne befolyásolja más rendszerek biztonságát, melyek az adott rendszerrel közös informatikai erőforrásokat használnak.

14.6.1. Érzékeny adatokat kezelő rendszer elkülönítése

Különösen érzékeny adatokat a hivatalban csak azok kezelhetnek, akiket erre külön feljogosít a munkáltatói jogkört gyakorló személy. Az érzékeny adatokat kezelő felhasználónak rendelkeznie kell a megfelelő jogosultságot biztosító azonosítóval, a hitelesítést lehetővé tévő jelszóval, indokolt esetben egyéb azonosításra alkalmas eszközzel.

A különösen érzékeny adatokat szükség szerint elkülönített informatikai eszközön kell kezelni.

Azok az alkalmazások, melyek érzékenyek a lehetséges veszélyekre, különleges kezelést igényelnek. Az, hogy egy alkalmazás mennyire érzékeny kiderül az alkalmazás tulajdonosának dokumentációjából. Az érzékenységnek három fokozatát különböztetjük meg:

- az alkalmazást egy célirányos számítógépen kell futtatni, hogy biztosítani tudjuk a sértetlenséget
- az alkalmazás csak megbízható alkalmazási rendszerek erőforrásain osztozhat
- az alkalmazás semmiféle korlátozást nem kíván

14.7. A mobil informatikai tevékenység, a távmunka

Mind a mobil informatikai eszközön, mind a távoli hozzáféréssel végzett munka esetén is meg kell teremteni a biztonságot. Mindezt úgy, hogy a meghozott intézkedések összhangban legyenek a speciális munkavégzés kockázataival.

A mobil informatikai tevékenység és távmunka szabályozását a jegyzőnek kell jóváhagynia. A pontos biztonsági előírásokat a megbízási szerződésbe bele kell foglalni.

14.7.1. A mobil informatikai tevékenység

Alapvető biztonsági cél, hogy a hivatalban megfelelő biztonsági intézkedéseket alkalmazzanak a mobil számítástechnikai berendezések védelmére.

Mobil számítástechnikai eszköznek az alábbiak számítanak:

- laptop
- memóriakártya
- külső winchester
- okos telefon
- pendrive

A mobil számítástechnikai berendezések védelme érdekében különösen nagy gondot kell fordítani arra, hogy a működési információ ne legyen veszélyeztetve. A mobil eszközzel végzett munka kockázatával arányosan kell alkalmazni a fizikai védelemre, a hozzáférés-védelemre, a kriptográfiai technikákra, a mentésekre és a vírusvédelemre vonatkozó követelményeket.

Nyilvános helyeken, konferencia termekben és más védelem nélküli tereken fokozottan ügyelni kell a jogosulatlan személyek általi betekintés kockázatára. Ugyanúgy álljanak rendelkezésre a rosszindulatú szoftverek elleni eljárások, és azok frissítései.

Megfelelő védelemmel kell ellátni a mobil eszközöket arra az esetre is, amikor hálózatba kapcsolva használjuk. Külső, nyilvános hálózatra történő kapcsolódás csak akkor jöhessen létre, ha sikeres volt az azonosítási és hitelesítési mechanizmus.

A mobil számítástechnikai eszközöket fizikailag is védeni kell a lopás, sérülés ellen, különösen az eszköz szállításakor. Egyedi módon kell biztosítani ezen eszközök védelmét a lopás vagy elvesztés esetére, figyelembe véve a hivatal jogi és biztosítási követelményeit.

Kényes üzemeltetési információkat tartalmazó mobil eszközt nem szabad felügyelet nélkül hagyni. Azokat lehetőség szerint el kell zárni, vagy különleges zárat kell alkalmazni a berendezés biztosítására.

A mobil hálózatok vezeték nélküli összeköttetését a kockázatok figyelembe vételével csak az IBF engedélyezheti.

14.7.2. A távmunka

A hivatal jelenleg nem foglalkoztat távmunkában munkavállalót. Amennyiben a jövőben mégis várható távmunka végzése, akkor gondoskodnia kell a távmunka végzéséhez szükséges szabályzatok és üzemeltetési tervek elkészítéséről.

Távmunka esetén is gondoskodni kell a biztonsági követelmények és előírások betartásáról, a megfelelő és rendszeres ellenőrzésről.

15. Az informatikai rendszerek tervezése és karbantartása

15.1. Az informatikai rendszerek informatikai biztonsági követelményei

Az informatikai rendszerek integrált biztonságának kialakítása a biztonságpolitika által meghatározott szempontok szerint kell, hogy történjen.

A biztonság alapvető feltételeinek egyike az alkalmazást vagy szolgáltatást támogató folyamat megtervezése és megvalósítása. Ahhoz, hogy egy informatikai rendszer megfelelően működjön szükség van a biztonsági követelmények meghatározására még a megvalósítás előtt.

15.1.1. A biztonsági követelmények elemzése és meghatározása

Az informatikai beruházások előkészítési és tervezési fázisában már ki kell alakítani a biztonsági szempontokat. Ennek megfelelően minden rendszerelem dokumentáltságára nagy hangsúlyt kell fordítani, hogy a bevezetés után a hivatal is képes legyen az adott rendszer rendszerhasználati szintű üzemeltetésére.

A tervezés szakaszában meg kell vizsgálni az új informatikai rendszerben kezelendő adatokat, a megbízható működéshez szükséges védelmi intézkedéseket meg kell fogalmazni.

Meg kell állapítani az informatikai rendszer várható biztonsági osztályát, annak érdekében, hogy a fizikai és logikai védelmi rendszer kialakítása, a megvalósításhoz szükséges feltételek megteremtése a biztonsági előírásoknak megfelelően történjen.

Új rendszer bevezetése előtt fel kell mérni az összes költséget, beleértve a biztonsági intézkedések költségét is. A költségeket össze kell hasonlítani a lehetséges kockázatokkal. Amennyiben a lehetséges kockázatok és a költségek nagysága nincs arányban a bevezetést érdemes átgondolni.

Az informatikai rendszerek éles üzembe helyezését megelőzően, amennyiben biztonsági szempontból indokolt, tesztkörnyezetben célszerű a szállítói tesztelésektől független, dokumentált tesztelésnek alávetni.

A tesztelés céljára kialakított rendszerben nem használhatóak éles, bizalmas adatok. Ha az éles adatok betöltése elengedhetetlen, akkor a tesztelést oly módon kell végrehajtani, ami megfelel a benne kezelt adatok kezelésére vonatkozó adat- és titokvédelmi követelményeknek.

A hivatal nem tárol forráskódokat.

15.2. Az alkalmazási rendszerek biztonsága

A felhasználói rendszerek kiválasztása során lehetőség szerint figyelembe kell venni, hogy a bevezetni kívánt rendszer rendelkezik e a megfelelő ellenőrző eszközökkel és eseménynaplókkal. Az érzékeny adatok feldolgozását végző vagy ilyen adatokat kezelő rendszereknél fokozottabb ellenőrzés szükséges. Az ellenőrző eszközöknek az adott alkalmazás biztonsági követelményeinek és kockázatelemzésének megfelelőnek kell lennie.

Az alkalmazásokra vonatkozó biztonsági intézkedéseket dokumentálni kell.

15.2.1. A bemenő adatok hitelesítése

Az alkalmazások bemenő adatait hitelesíteni, ellenőrizni kell.

Az ellenőrzés eszközei:

- időszakos adatállomány vizsgálat
- a nyomtatott input dokumentumok ellenőrzése
- adatbevitel során az ismételt adatbevitel megakadályozása
- az alkalmazásokhoz történő hozzáférés naplózása

Az adatok pontosságának, helyességének és hitelességének ellenőrzéséért az adatgazda felel.

Az informatikai rendszeren belül is alkalmazni kell különböző ellenőrzéseket. A feldolgozó rendszer lehetőleg beépítetten ellenőrizze a bevitt adatokat.

15.2.2. Az adatfeldolgozás ellenőrzése

A felvitt adatoknak is szavatolni kell a helyességét, pontosságát a feldolgozás egész ideje alatt. Az adatok sérülésének elkerülése érdekében az alábbi intézkedéseket kell bevezetni:

- az adatfeldolgozás rendszerébe ellenőrzési, hitelesítési pontokat kell beépíteni
- korlátozásokat kell bevezetni
- szükség esetén korrekciós programokat kell alkalmazni

15.2.2.1. Veszélyeztetett területek

A helyesen bevitt adatok is sérülhetnek, akár a feldolgozás hibái, akár szándékos tevékenységek következményeként. Az ilyen meghibásodások elkerülésének érdekében érvényesítő ellenőrzéseket célszerű bevezetni. Alapvető elvárás, hogy a korlátozások megvalósítása valóban minimalizálja a sértetlenség elvesztéséhez vezető feldolgozási hibák kockázatát.

15.2.2.2. Vezérlő és ellenőrző eljárások

A biztonsági intézkedések mértéke attól függ, hogy milyen az alkalmazás természete, azaz milyen hatással lehet a folyamatokra a hibás adat.

A megfelelő biztonsági intézkedések meghozatala a rendszergazda feladata. A biztonsági intézkedések meglétének ellenőrzését az Informatikai Biztonsági Felelős végzi.

15.2.3. Az üzenetek hitelesítése

Az üzenethitelesítő kódok az üzenet hitelességét garantálják, ami magába foglalja az üzenet adatintegritását, azaz változatlanságát és az üzenet eredetét is igazolja. Ilyen kód használatával ellenőrizni tudjuk, hogy a kapott üzenet megegyezik-e az elküldöttel, valamint az üzenetet ténylegesen az a személy küldte, akitől várjuk.

15.2.4. A kimenő adatok hitelesítése

Az adatfeldolgozó rendszerek kimeneti adatainak hitelességét ellenőrizni kell annak érdekében, hogy biztosítsuk a tárolt adatok helyes feldolgozását és a követelményeknek való megfelelőségét.

A kimenő adatok védelmi eljárásai:

- integritásellenőrzés
- adattartalom meglétének, értékének ellenőrzése
- a megfelelő minősítés meglétének ellenőrzése
- a kimenő adatokkal dolgozó munkatársak feladatainak és felelősségeinek pontos meghatározása

15.3. Kriptográfiai eszközök

Az informatikai rendszerben kezelt adatokat a minősítésükkel és kockázatukkal arányosan rejtjelező eszközökkel és technikákkal kell védeni.

15.3.1. A kriptográfiai eszközök alkalmazásának irányelvei

A kriptográfiai eszközök alkalmazására vonatkozó döntés egy hosszú és körültekintő folyamat része, mely folyamat során részletesen ki kell vizsgálni, hogy mik legyenek a felmerülő kockázatok és a szükséges óvintézkedések megvalósításának feltételei.

A kriptográfiai eszközök kiválasztása során az alábbi szempontokat kell figyelembe venni.

- Adatátviteli rendszer esetén:
    - a rendszer által kezelt védett adatok típusa, körének nagysága
    - átviteli közeg sávszélessége, minősége
    - visszafejtési időkorlát
    - felhasználói kör összetétele
- Adattároló egység esetén:
    - a rendszer által kezelt védett adatok típusa, körének nagysága

15.3.1.1. Titkosítás

Informatikai biztonsági okokból az adatokat titkosítással, kriptográfiai rendszerekkel, technikákkal kell védeni minden olyan esetben, amikor fennáll az adatok illetéktelen személyhez való kerülésének, sértetlenségének fenyegetettsége.

Az alkalmazandó kriptográfiai technológiának a kockázatokkal arányosnak kell lennie. A 3-as vagy magasabb besorolású adat nem továbbítható nyilvános csatornán keresztül, csak titkosított formában.

15.3.1.2. Digitális és elektronikus aláírás

A digitális aláírás az elektronikus kommunikációban használt titkosítási eljárás. Célja, nem magának az adatnak a titkosítása, hanem annak igazolása, hogy hiteles forrásból származik az üzenet és azt más nem módosíthatta.

Az elektronikus aláírás olyan kriptográfiai eljárás, melynek segítségével akár a kézzel írott aláírással egyenértékű bizonyító erejű dokumentum hozható létre a hatályos jogszabályoknak megfelelően, különösen az elektronikus aláírásról szóló 2004. évi LV. törvény szerint.

Az elektronikus és a digitális aláírás közti különbség, hogy az elektronikus aláírás a technológia mellett a jogi fogalmat is megjelöli.

A hivatal a külső szervezetekkel való kapcsolattartás során, valamint az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvénynek megfelelően használ elektronikus aláírást.

15.3.2. Kulcskezelés

A kulcskezelés szabályait ki kell alakítani minden elektronikus aláírással, titkosítással rendelkező rendszerben.

A hivatal csak más szervezet által kiadott kulcsot használ, melynek megfelelőségére a szolgáltatási szerződésben meghatározott intézkedések, valamint felelősségi körök a garancia.

A kulcskezelési eljárások a kriptográfiai rendszereket biztosító külső szolgáltatóival kötött szerződések részét képezik. A hivatal minden esetben a külső szolgáltató szabványai alapján jár el. A kulcskezelés során csak olyan szolgáltatóval köt szerződést, akik rendelkeznek a jogszabályokban előírt elvárásokkal, és ezt minden kétséget kizáróan bizonyítani is tudják.

15.4. A rendszerfájlok védelme

Gondoskodni kell arról, hogy a hivatal által használt valamennyi szoftver nyilvántartásba vétele megtörténjen, annak érdekében, hogy ellenőrizni és dokumentálni lehessen a védendő rendszerállományokat.

15.4.1. Az operációs rendszer ellenőrzése

Az informatikai rendszer, valamint a rendszerben futó programok forráskódjait és azok módosítását folyamatosan ellenőrizni kell. Minden szoftver telepítését dokumentáltan, ellenőrzötten kell végrehajtani.

Az integritás védelmében a következő intézkedéseket kell meghozni:

- a programkönyvtárak frissítését a rendszergazda vagy annak megbízottja végzi
- ha lehetséges, az üzemeltető rendszer csak futtatható kódot tartalmazzon
- végrehajtható kódot éles, üzemeltetési rendszeren csak akkor szabad futtatni, ha rendelkezésre állnak a sikeres tesztelés dokumentumai
- a szoftver korábbi változatait a tartalékolás mértékében célszerű megtartani
- amennyiben a szoftverek rendelkeznek saját naplózási rendszerrel, akkor azt be kell kapcsolni, melyeket rendszeresen ellenőrizni kell
- az éles rendszer nem tartalmazhat félkész, befejezetlen forráskódokat

A vásárolt szoftvereket a szállító javaslatai és iránymutatási alapján kell frissíteni. A módosításokat az új változat biztonsági kockázatának ismerete és az ennek megfelelő intézkedések megvalósulása mellett szabad csak átvezetni. Érdemes olyan szoftverjavításokat alkalmazni, amelyek segítenek a biztonsági rések eltávolításában.

15.4.2. A rendszer teszt adatainak védelme

A teszt adatokat védelem és ellenőrzés alatt kell tartani. Lehetőség szerint a teszt és éles rendszereket egymástól el kell választani, eltérő környezetben kell futtatni.

A teszt adatbázisok is többnyire olyan adatokat igényelnek, melyek közel állnak az éles rendszer adataihoz. Ezért szükséges a teszt rendszerek üzemeltetése során is a megfelelő védelem biztosítása.

A következő óvintézkedések betartása elengedhetetlen:

- az éles rendszerekhez hasonló hozzáférési eljárásokat kell alkalmazni
- személyes adatokat tartalmazó üzemeltetési adatbázis használata tilos
- üzemeltetési információt ajánlatos a tesztelés, vizsgálat után visszaállíthatatlanul törölni

15.4.3. A program forráskönyvtárhoz való hozzáférésének ellenőrzése

A hivatal nem kezel és nem tárol forráskódokat. Amennyiben mégis szükséges lenne, az alkalmazások forráskódjának kezelésére a következő fontosabb intézkedések betartását kell biztosítani.

- a forrásprogramok könyvtárait nem szabad éles rendszerekben tartani
- a rendszergazdának kell kijelölnie azokat a személyeket, akik hozzáférést kaphatnak a forrásprogramok könyvtáraihoz, ezen hozzáférések egy-egy személyre vonatkozóan nem lehetnek teljes körűek
- a forráskönyvtár minden változásáról eseménynaplót kell vezetni
- programozó munkatárs a forrásprogramok átdolgozása után csak a rendszergazda engedélyével frissíthet
- a forrásprogramok korábbi változatait archiválni kell

15.5. Informatikai biztonság a bevezetési és karbantartási folyamatokban

Az alkalmazásokat három különböző életciklusba sorolhatjuk:

- bevezetés/tesztelés alatt álló
- éles üzemeltetésű/karbantartott
- archiválandó/használatból kivont

Az informatikai rendszerek valamennyi életszakaszában fenn kell tartani a biztonságát, melyhez szükség van a támogatási környezet ellenőrzésére.

15.5.1. Változáskezelés

Az informatikai rendszerek – akár infrastruktúra, akár alkalmazások esetén - bármely életciklusa során bekövetkező változásokat követni és ellenőrizni kell.

A változások kezelését úgy kell kialakítani, hogy az informatikai rendszer tervezett, illetve végrehajtott változásait az Információ Biztonságért Felelős személy nyomon követhesse, azt ellenőrzései során felhasználhassa.

A kockázatkezelési módszereket úgy kell alkalmazni, hogy a változtatások ellenőrzése folyamatos és kellően szabályozott legyen.

A változtatások során az alábbi szabályokat kell betartani:

- meg kell határozni a változtatást végrehajtó személyek körét
- a módosításhoz szükséges valamennyi szoftver, adatbázis és hardver azonosítását el kell végezni
- előzetes kockázatelemzést kell készíteni
- biztosítani kell, hogy a hivatal működési folyamatai ne sérüljenek a változtatás alatt
- a kapcsolódó dokumentációkat aktualizálni kell a módosításoknak megfelelően

15.5.2. Az operációs rendszer megváltoztatásával kapcsolatos ellenőrzések

Az operációs rendszereket időről-időre felül kell vizsgálni, szükség esetén le kell cserélni annak érdekében, hogy az új alkalmazások is megfelelő, modern környezetben futhassanak.

A cserét minden esetben szabályozotton, előzetes vizsgálatok, kockázatelemzések megtételével kell megvalósítani, biztosítva az ügymenet folytonosságot. A javítócsomagokat kizárólag a rendszergazda

vezetheti át a rendszeren, a felhasználóknak semmiképpen nem engedélyezhető a munkaállomásokon való telepítése.

15.5.3. A szoftvercsomagok frissítésének korlátozása

A hivatal az informatikai rendszereire csak és kizárólag jogtiszta szoftvereket telepít. A munkavállalói csak jogtiszta szoftvereket használhatnak.

Ha a szerződés másként nem rendelkezik a szoftverek tekintetében a szerzői jog alapján kell eljárni. Amennyire lehetséges, az eladó által szolgáltatott szoftvercsomagokat módosítás nélkül kell alkalmazni. Ha változtatások szükségesek, az eredeti szoftvert meg kell tartani és a módosításokat egy másolaton kell végrehajtani. Minden egyes változtatást teljes egészében dokumentálni kell, úgy, hogy szükség esetén ismét alkalmazni lehessen a szoftver jövőbeni javított kiadásaihoz.

15.5.4. A rendszerinformációk kiszivárgásának megakadályozása

A rendszerinformációk kiszivárgását minden lehetséges eszközzel meg kell akadályozni. A megelőzés érdekében az alábbi intézkedéseket kell alkalmazni:

- programot csak megbízható forrásból szabad beszerezni
- csak levizsgált terméket használjunk
- ellenőrizzük a telepített kód minden hozzáférését és módosítását
- csak a megfelelő engedélyezési eljáráson (átvizsgáláson) átesett munkatársak, szerződő partnerek dolgozhassanak a hivatal informatikai rendszerein
- az erőforrások számítógéprendszerekben való alkalmazását figyelemmel kell kísérni

15.5.5. A szoftverfejlesztés kihelyezése

A hivatal nem végez szoftverfejlesztést. Egyedi szoftverek fejlesztése kihelyezett tevékenységként, szerződéses keretek között valósul meg.

A kihelyezett szoftverfejlesztések esetében az alábbi szempontokat kell figyelembe venni:

- licencszerződéseket, a szoftver tulajdonjogát és a szellemi tulajdonjogokat
- a végzett munka minőségének és pontosságának tanúsítását
- a harmadik fél hibája esetére vonatkozó lépéseket
- a szoftverminőség szerződéses követelményeit
- a telepítés előtt elvégzendő vizsgálatokat

A szoftverfejlesztések dokumentációja olyan részletes legyen, hogy a hivatal a fejlesztett elemeket a fejlesztő nélkül is képes legyen biztonságosan üzemeltetni, egyedi esetekben utána gyártani, pótolni.

15.6. A műszaki sérülékenységek kezelése

A rendszereket ért támadások megakadályozása érdekében fel kell térképezni a használt informatikai eszközöket és szoftvereket. A biztonsági intézkedések célja a közzétett sérülékenységek kihasználásából származó veszélyforrások csökkentése.

Biztosítani kell, hogy a hivatal az informatikai eszközeit érintő új biztonsági rések megjelenése esetén, a kockázatok felmérése után, a kockázatokkal arányosan és gyorsan tudjon reagálni.

Minősített esetben, ha a kockázat nem vállalható, meg kell fontolni a veszélyeztetett informatikai szolgáltatás leállítását, legalább addig, amíg fel nem készítik a rendszert a veszélyforrás kiküszöbölésére.

15.6.1. A műszaki sérülékenységek ellenőrzése

Egy naprakész és pontos vagyonleltár az előfeltétele a műszaki sérülékenység eredményes kezelésének.

Egy jól működő kezelési folyamatrendszer kialakításához az alábbi intézkedéseket kell alkalmazni:

- a hivatal határozza meg a műszaki sebezhetőség kezelésével kapcsolatos feladatokat és felelősségeket
- a hivatal biztosítsa az információforrások jegyzékét
- a reagálási határidő minél rövidebb legyen
- a javításokat az erre a célra létrehozott tesztkörnyezetben ellenőrizze, hogy ne okozzanak felesleges kockázatokat
- a frissítések kezeléséért a rendszergazda felel

16. Az informatikai biztonsági incidensek kezelése

Az informatikai rendszervédelmi intézkedéseit úgy kell megvalósítani, hogy a biztonsági események megelőzhetőek legyenek, de ha mégis bekövetkeznek, akkor hatásukat folyamatosan nyomon kell követni, az általuk okozott kárt minimalizálni kell.

A működési zavarok következményeit mérsékelni kell, a lehető leghamarabb vissza kell állni a normál üzemmódra. Az esemény során szerzett tapasztalatokat fel kell jegyezni.

Mindazon biztonsági eseményeket, melyek a folyamatos éles működést megzavarják, a napi munkát, feldolgozást akadályozzák, haladéktalanul jelezni kell vagy a szervezeti egység vezetőjének, vagy a rendszergazdának. A rendszergazda köteles az Informatikai Biztonsági Felelősnek jelentést tenni a biztonsági eseményről.

A kockázatelemzéshez és eredményességének növeléséhez információkra van szükség a biztonsági eseményekről. Az információkat az egyes szervezeti egységek informatikai esemény elemzési sémája szerint kell gyűjteni és elemezni. A gyűjtött információkat hozzáférhetővé kell tenni a kockázatelemzés, valamint más biztonsághoz kapcsolódó tevékenység számára.

A munkavállalókkal a biztonság tudatosság képzés keretében meg kell ismertetni az események kezelésére vonatkozó lépéseket, annak érdekében, hogy a biztonsági események bekövetkeztekor a felhasználó a tőle elvárható módon reagáljon.

Az események kivizsgálására szükség esetén létre kell hozni úgynevezett Informatikai Biztonsági Eseménykezelő Csoportot (IBCS). Az IBCS állhat belső vagy külső, szerződött résztvevőkből is.

Az IBCS felállítását az Informatikai Biztonsági Felelős kezdeményezi.

A hivatalnak felkészültnek kell lennie a biztonsági események bekövetkezésére. Ezért az alábbi követelményeket fogalmazza meg:

- felkészülés: előre dokumentált megelőző intézkedések, eseménykezelési útmutatók, és eljárások megléte szükséges
- bejelentés: minden munkavállalónak tisztában kell lennie a biztonsági események bejelentésére vonatkozó eljárásrenddel, felelősségi körrel
- értékelés: a biztonsági esemény súlyosságának meghatározása
- irányítás: az esemény során alkalmazandó eljárások koordinálása a károk csökkentése érdekében
- helyreállítás: eljárások és felelősségek meghatározása a normál üzemmód visszaállításához

- áttekintő vizsgálat: az eseményt követő tevékenységek, illetve következmények elemzése, ide értve a jogi következményeket is

16.1. Biztonsági események és sérülékenységek jelentése

16.1.1. A biztonsági események kezelése

A biztonsági eseményeket, a szoftverek rendellenes működéseit és a felfedezett gyenge pontokat, amilyen gyorsan csak lehet, jelenteni kell a megfelelő vezetői csatornákon keresztül.

A hivatal munkavállalóinak tudatában kell lenniük azzal, hogy a biztonsági eseményeket, a biztonsági sérülékenységeket, a hibásan működő szoftvereket, vagy bármely olyan eseményt, melyből arra következtetnek, hogy az informatikai rendszer sérülését eredményezheti, haladéktalanul jelenteniük kell.

A rendszergazda a lehető leghamarabb vizsgálja ki a biztonsági eseményt. Az eredményről az Informatikai Biztonsági Felelőst is tájékoztatni kell. Valamint emberi mulasztás, vagy kötelezettségszegés gyanúja esetén a munkáltató jogokat gyakorló személyt is értesíteni kell a további intézkedések érdekében.

16.1.2. Sérülékenységek jelentése

A hivatal munkavállalóitól meg kell követelni, hogy jelentsék az általuk használt rendszerek vagy szolgáltatások minden felismert vagy feltételezett biztonsági sérülékenységét. A felhasználók a feltételezett gyengeségeket semmilyen körülmények között se próbálják maguk megszüntetni.

A felhasználó teendői rendszer, illetve alkalmazáshiba esetén:

- figyeljen a képernyőn megjelenő üzenetekre, azokat figyelmesen olvassa el mielőtt bezárná, ha bármilyen hibás működésre gyanakszik ne zárja be az üzenetet, haladéktalanul értesítse a rendszergazdát
- vírustámadás gyanúja esetén fejezzen be minden munkafolyamatot és jelentse a rendszergazdának, aki azonnal távolítsa el az eszközt a hálózatból a továbbfertőzés megakadályozásának érdekében

16.2. Az informatikai biztonsági eseménykezelés

16.2.1. Eljárások és felelősségi körök

A váratlan események kezelésének felelősségeit és eljárásait úgy kell rögzíteni, hogy a biztonsági eseményekre gyorsan, hatékonyan és rendben meg lehessen tenni a válaszlépéseket.

Az események kezelésére az alábbi intézkedéseket kell meghozni:

- véletlen biztonsági események minden lehetséges fajtáját lefedő eljárásokat kell bevezetni
- tartalékolási tervvel a lehető leggyorsabban vissza kell állítani a rendszereket és szolgáltatásokat
- átvizsgálási naplókat és egyéb bizonyítékokat össze kell gyűjteni és meg kell őrizni a későbbi elemzések, valamint a lehetséges kötelezettségszegések bizonyításának érdekében
- a visszatérések, valamint a rendszerhibák javítását dokumentálni és ellenőrizni kell

16.2.2. Okulás az informatikai biztonsági eseményekből

Az eseményeket típus, terjedelem, okozott kár, helyreállítási költségek, illetve a felügyeleti rendszer működési zavara szerint értékelni kell. Az eredmények alapján, amennyiben szükséges, kezdeményezni kell a biztonsági intézkedések felülvizsgálatát, a szabályzatok korszerűsítését.

16.2.3. Bizonyítékok gyűjtése és védelme

16.2.3.1. A bizonyítékokra vonatkozó szabályok

Fegyelmi vagy jogorvoslati eljárás kezdeményezése előtt kellő bizonyítékkal kell rendelkezni.

Amikor a káros tevékenység a polgári vagy büntető törvénykönyvet érinti, akkor a benyújtott bizonyítékok feleljenek meg a hatályos jogszabályokban vagy az illetékes bíróság eljárási szabályaiban rögzített követelményeknek.

Ezek a szabályok:

- a bizonyíték elfogadhatósága
- a bizonyíték súlya: minősége és teljessége
- a bizonyíték keletkezésének körülményei

16.2.3.2. A bizonyítékok elfogadhatósága

A bizonyítékok elfogadhatóságához szükséges, hogy a hivatal informatikai rendszerei feleljenek meg az elfogadható bizonyítékok előállítására vonatkozó szabályoknak vagy eljárásrendeknek.

16.2.3.3. A bizonyítékok minősége és teljessége

A bizonyítékok minőségének és teljességének biztosításához bizonyítéknaplóra van szükség.

Bizonyítéknapló készítéséhez az alábbiak megléte, betartása szükséges:

- papíron rögzített dokumentumok: az eredetit biztonságos helyen kell tárolni, rögzíteni kell, hogy ki, hol és mikor találta meg, és a megtalálást kik tudják tanúsítani
- számítógép-adathordozón rögzített információ: a hordozható adathordozók, valamint a merevlemezen és a központi tárolón talált bizonyítékok másolatát meg kell őrizni

17. Ügymenet-folytonosság

17.1. Az ügymenet-folytonosság informatikai biztonsági szempontjai

A hivatal számára létfontosságú biztonsági cél, hogy fenntartsa ügymenetét, megakadályozza a működési tevékenységeinek megszakítását, és védje a kritikus működési folyamatait az információs rendszerek hibáinak hatásától, valamint biztosítsa a lehető leggyorsabb újraindítását.

Az ügymenet-folytonosság megteremtésének érdekében azonosítani kell a kritikus működési folyamatokat, melynek eredményeként működésfolytonossági intézkedéseket kell bevezetni. Figyelembe kell venni a személyzettel, nyersanyaggal, munkaeszközzel és szolgáltatással való folyamatos ellátás igényét. Az üzemzavarokat, eszközhibákat, szolgáltatás-kieséseket pedig hatáselemzéseknek kell alávetni.

A működésfolytonosság irányítása tárja fel és mérsékelje a sajátos kockázatokat, kiegészítve az átfogó kockázatkezelést. Korlátozza a biztonsági események káros hatását, és biztosítsa, hogy a szükséges információk könnyen rendelkezésre álljanak.

17.1.1. Az informatikai biztonsági szempontok érvényesítése az ügymenet-folytonosság irányításában

A kritikus üzleti és informatikai folyamatok érdekében mérsékelni kell a különböző rendellenességek és a biztonsági rendszer meghibásodása által okozott fennakadásokat.

A meghibásodások, fennakadások következményeit elemezni kell. Az ügymenet-folytonosságnak ki kell, hogy térjen a kockázatok azonosítására és csökkentésére alkalmas ellenőrző eszközök bevezetésére, a kárt okozó események következményeinek korlátozására. A lényeges tevékenységek mielőbbi újraindításáról gondoskodni kell.

A hivatalt érintő kockázatokat meg kell becsülni, amit valószínűsége, időbeli hatása, illetve az okozott kár mértéke alapján rangsorolni kell.

A biztonsági események nagyságát és hatását a hivatalra, az informatikai eszközökre és az ügymenet-folytonosságra nézve abból a szempontból is meg kell vizsgálni, hogy milyen kieséseket okozhatnak, és ezeket a kieséseket milyen eszközökkel lehet csökkenteni.

Meg kell fontolni a kritikus adatvagyonra történő biztosításkötést.

Szükséges kiegészítő, megelőző és mérséklő intézkedések bevezetése, elegendő pénzügyi, szervezeti, műszaki és környezeti források azonosítása, azért, hogy a meghatározott biztonsági követelmények megvalósulhassanak.

A személyzet, az adatfeldolgozó eszközök és egyéb vagyontárgyak védelméről is gondoskodni kell.

A hivatalnak rendelkeznie kell működésfolytonossági tervvel, melynek intézkedéseit és szabályait pontosan dokumentálni szükséges.

17.1.2. Az ügymenet-folytonossági hatásvizsgálatok és a kockázatok elemzése

Az ügymenet-folytonosság akkor lesz megfelelő, amikor az informatikai rendszer kiesés kockázatának szintje a hivatal számára még elviselhető. A tűréshatárt az ügymenet kritikus rendszereinek egy meghatározott (maximális) kiesési ideje határozza meg.

Az Ügymenet-folytonossági terv részletesen meghatározza a kívánt ügymenet-folytonosság fenntartásához szükséges feltételeket, szervezeti és szervezési lépéseket, valamint szabályozza a megvalósítás módját.

A biztonsági cél, hogy azonosítsák azokat a biztonsági eseményeket, amelyek az ügymenet megszakadását okozhatják, valamint elemezzék ezek kockázatait.

A működésfolytonosság kockázatának felmérését a működési források és folyamatok tulajdonosainak teljes körű bevonásával végezzék. A felmérés azonosítsa, számszerűsítse és sorolja be elsőbbség szempontjából a kockázatokat a hivatalra vonatkozó kritériumok és célok szerint, beleértve a kritikus erőforrásokat, a megszakadás hatásait, a megengedhető kiesési időket és a helyreállítási elsőbbségeket.

17.1.3. Az ügymenet-folytonossági terv kidolgozása

Az ügymenet-folytonossági terv tartalmazza, hogy a támogató folyamatok és eszközök sérülése vagy kiesése esetén hogyan lehet a szervezet működését fenntartani.

Az ügymenet-folytonossági terv célja, hogy a hivatal ügyviteli folyamatait támogató informatikai erőforrások üzemidőben a lehető legjobb időkihasználással és a legszélesebb funkcionalitással működjenek annak érdekében, hogy a biztonsági események által okozott közvetlen és közvetett károk minimálisak legyenek.

Az ügymenet-folytonossági tervnek részletesen meg kell határoznia a kívánt ügymenet-folytonosság fenntartásához szükséges megelőző, helyettesítő, illetve visszaállító intézkedések megvalósításához szükséges feltételeket, a szervezeti és szervezési lépéseket és a megvalósítás módját.

A tervezés lényeges eleme a kiesési kockázatok elemzése, melynek során mérlegelni kell az okozott kár nagyságát és az üzemzavari események bekövetkezésének gyakoriságát.

A terveknek le kell fedniük a lehetséges esetek minél teljesebb körét:

- különböző hosszúságú kiesések
- különböző eszközök és létesítmények elvesztése
- a helyszínekhez való fizikai hozzáférés teljes elvesztése
- a rendeltetésszerű működéshez való visszatérés igénye

A helyreállítási terveknek le kell írniuk, hogy miként kell visszaállítani a váratlan eseménnyel érintett informatikai rendszereket.

17.1.4. Az ügymenet-folytonossági tervek vizsgálata, karbantartása és újraértékelése

17.1.4.1. A tervek tesztelése

A tervek tesztelésére azért van szükség, mert a tesztelés során felfedezhetjük az elavult hivatkozásokat, a hiányosan dokumentált személyzeti vagy berendezési változásokat, és más eltéréseket. A vizsgálatot célszerű rendszeresen elvégezni, hogy a terv naprakész és hatékony maradjon.

A vizsgálat ütemtervének azt is meg kell mutatnia, hogy mikor és hogyan vizsgálják a terv adott elemét. A módszeres technikák közül érdemes minél szélesebb körben választani, hogy elég biztosítékot szerezzünk a tervek a valós életben várható működéséről.

A teszt értékelése során az ügymenet-folytonossági terveket módosítani, aktualizálni kell, és be kell illeszteni a szabályozási környezetbe.

17.1.4.1.2. A tervek karbantartása és újraértékelése

Az ügymenet-folytonossági tervet rendszeresen, de minimum évente felül kell vizsgálni, és aktualizálni kell, hogy hatékonysága megmaradjon.

Az ügymenet-folytonossági tervet soron kívül felül kell vizsgálni

a.) az elektronikus információs rendszer vagy a működtetési környezet jelentős változása

b.) az ügymenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémák esetén

A felülvizsgálat során az alábbi területek kockázatváltozásait is át kell tekinteni:

- személyzet
- címek és telefonszámok
- üzleti stratégia
- elhelyezés, eszközök, erőforrások
- jogszabályi környezet
- szállítók, szolgáltatók, kulcsfontosságú ügyfelek
- akár az új, akár a visszavont folyamatok
- üzemeltetés és pénzügyek

17.2. Ügymenet-folytonosság fázisa és tartalma

17.2.1. Rendkívüli helyzetek osztályozása, minősítése

Ahhoz, hogy azonnal és megfelelően reagálni lehessen az ügymenet-folytonosságát veszélyeztető fenyegetésekre meg kell határozni az adott fenyegetettség típusát. A hivatal négy típusba csoportosítja ezen fenyegetettségeket.

17.2.1.1. Katasztrófa

A hivatal jelen dokumentumban katasztrófának tekinti a váratlan, hirtelen bekövetkező, egyszeri és elkülönült eseményeket, amely a hivatal épületében, gépeiben, informatikai eszközeiben, informatikai rendszerében alapvető változást okoz, mely változás a lényeges elemben történt módosulás miatt helyreállíthatatlan, teljes összeomlást eredményez.

Ilyen katasztrófák az alábbiak lehetnek:

- természeti katasztrófa
- tűz vagy víz okozta károk
- rendkívüli méretű elemi csapás

17.2.1.2. Krízis

A krízis, a hivatal életében, és informatikai rendszereiben bekövetkező olyan fordulópont, válságos helyzet, mely kimenetelét megfelelő akciótervekkel, biztonsági intézkedésekkel vissza lehet fordítani, meg lehet oldani.

Attól függően, hogy milyen gyors és hatékony a felismerés és a beavatkozás a kritikus helyzetek kimenetelei az alábbiak lehetnek:

- megoldás
- kompromisszum
- összeomlás

Mind a katasztrófa, mind a krízis lényeges eleme, hogy a hivatal és/vagy az informatikai rendszer egészét érinti a válságos helyzet.

17.2.1.3. Részleges leállás

Részleges leállásnak azt tekintjük, amikor egy vagy több, de nem az egész hivatalt vagy informatikai rendszert érintő szolgáltatás átmeneti meghibásodás miatt nem, vagy csak korlátozottan működik, érhető el.

A hivatal ügymenet-folytonosságában ugyan fennakadást okoz a részleges leállás, de kárérték tekintetében ez a fennakadás nem jelentős, viszonylag hamar helyreállítható és nem jár nagyobb bizalmasság vesztéssel.

A részleges leállás fő okai:

- tervezett leállás: a szolgáltatás kiesése előre meghatározott okból (pl.: karbantartás, frissítés) következik be
- áramellátás ingadozik
- emberi mulasztás történt
- kibertámadás érte az informatikai rendszert

17.2.1.4. Incidens

Az incidens a hivatal ügymenet-folytonossága és az informatikai rendszer működése szempontjából olyan nem kívánt vagy nem várt egyedi információbiztonsági esemény, mozzanat, mely nagy valószínűséggel veszélyezteti és fenyegeti az információbiztonságot.

Az incidensek lehetnek véletlen események vagy szándékos károkozás eredményei is.

A hivatal a leggyakrabban előforduló típusokként az alábbiakat különbözteti meg:

- emberi hibák (pl.: informatikai eszköz, szoftver nem megfelelő használata)
- szabályzatnak vagy irányelvnek való nemmegfelelés
- a fizikai biztonsági rendelkezések megsértése
- nem ellenőrzött rendszerbeli változások
- hozzáférési sértések
- a bizalmasság és sértetlenség megsértése
- rosszindulatú kód

17.2.2. Az ügymenet-folytonosság fázisai

17.2.2.1. Azonnali reakció fázis

Az azonnali reakció fázisán közvetlenül az előre nem várt esemény bekövetkezése utáni időszakot értjük.

A krízis bekövetkezte után a legfontosabb feladat annak felmérése, hogy mekkora a bekövetkezett esemény által okozott kár vagy sérülés mértéke. Ennek érdekében az ügymenet-folytonossági tervben meghatározott cselekvések közül aktiválni kell azon folyamatokat, melyek feltárják az eseményre vonatkozó adatokat.

A fázis feladatai:

- értesíteni a lehetséges érintetteket
- kárfelmérés
- problémakezelés
- folyamatos kommunikáció
- helyreállítás megszervezése

17.2.2.2. Átmeneti fázis

Az azonnali fázisban meghatározott feladatok elvégzése után már rendelkezésre állnak azok az információk, melyek szükségesek a nem várt esemény bekövetkezése előtti állapot helyreállításához.

Ezen információk az alábbiak lehetnek:

- a nem várt eseménnyel érintett kulcsfontosságú folyamatok ismerete
- az érintett folyamatok és az ezeket működtető rendszerek függőségei
- az ezeket a folyamatokat támogató erőforrások listája

- a minimális szolgáltatás fenntartásához szükséges alternatív lehetőségek és az ezek kiszolgálását támogató erőforrások
- az érintett folyamatok helyreállításának és stabilizálásának tervei

17.2.2.3. Helyreállítási fázis

A helyreállítási fázis során megtörténik az incidens előtti állapotra való visszaállás.

A helyreállítás fázisa változó intervallumú lehet. Annak időtartama a nem várt esemény jellegétől függ.

Attól függően, hogy az átmeneti fázisban milyen cselekvési terv került elfogadásra a helyreállítást illetően megkülönböztetünk korlátozott vagy eredeti szolgáltatási színvonalra történő helyreállítást.

A korlátozott szolgáltatási színvonalú helyreállítás során az incidens kezelés csak a minimális működéshez elengedhetetlen erőforrásokat és feltételeket állítja vissza, vagy teremti meg azokat.

Az eredeti szolgáltatási színvonalú helyreállítás esetén a nem várt esemény bekövetkezése előtti állapot teljes körűen biztosított, a szolgáltatás kiesést leszámítva egyéb kár nem keletkezett, az ügymenet további beavatkozás nélkül folytatódhat.

17.3. Eljárás a rendkívüli helyzetek elhárítására

Az esemény bekövetkezésekor a 17.2.2-es pontban meghatározott fázisokra építve az alábbi feladatokat kell végrehajtani.

17.3.2. Esemény osztályozása

Azonnali reakcióként értékelni kell a kialakult helyzetet, és ennek megfelelően osztályozni és minősíteni kell azt. Az osztályozáshoz és minősítéshez minden esetben értesíteni kell a rendszergazdát. Az esemény besorolását ő végzi.

Az események osztályozása a 17.2.1-es pont alapján történik. Így megkülönböztetünk katasztrófát (1. szint), krízist (2. szint), részleges leállást (3. szint) és incidenst (4. szint).

17.3.2.1. Kivétel

Az esemény-osztályozás felesleges abban az esetben, amikor a katasztrófa nemcsak az informatikai rendszert érinti, hanem a hivatal összes szegmensét. Ilyen esetben az üzemeltetésben és rendkívüli események elhárításában érintett személyek kezdik meg a helyzetelemzést, és végzik a visszaállítást a katasztrófa elhárítási terv alapján.

18. Szabályozási környezet

18.1. Megfelelés a hatályos jogszabályi környezetnek

Az informatikai rendszerek tervezésére, fejlesztésére, üzembe helyezésére, működtetésére, használatára és kezelésére különböző törvények, jogszabályok, szabványok, ajánlások, valamint az egyes szerződésekben rögzített biztonsági követelmények vonatkoznak. Ezek szervezeti szintű érvényesülése érdekében lekell fektetni a hivatal informatikai rendszerére vonatkozó biztonsági kritériumokat.

El kell kerülni bármely jogszabályi, szabályozói vagy szerződéses kötelezettségnek, valamint bármely biztonsági követelménynek a megszegését.

A fentieknek megfelelően a hivatal a szabályait, eljárásrendjeit a hatályos jogszabályok, szabványok, ajánlások hazai gyakorlatának és a nemzetközi előírásoknak a figyelembevételével készíti el.

18.1.1. A vonatkozó hatályos jogszabályok, szabványok és eljárások

Az informatikai rendszerekre vonatkozó jogszabályi, szabályozói vagy szerződéses követelményeket és ezek teljesítésére hozott intézkedéseket részletesen, a felelősségi köröket pedig egyénekre lebontva kell meghatározni és dokumentálni.

A vonatkozó jogszabályokat, szabványokat és ajánlásokat az 1. számú melléklet tartalmazza.

A melléklet naprakészségéért a jegyző felel.

18.1.2. A szellemi tulajdonjogok védelme

A hivatal az Adatvédelmi Szabályzat előírásainak megfelelően kezeli a szervezettől idegen szellemi tulajdonban álló termékek jogszerű használatának ellenőrzési módját, különös tekintettel a szerzői és tervezői jogokra, valamint a védjegyekre.

A jogszabályi, szabályozói vagy szerződéses követelmények korlátozhatják a hivatal tulajdonát képező anyagok másolását.

A követelmények megszegésének elkerülésére az alábbi intézkedések kerüljenek bevezetésre:

- olyan eljárásrend kiadása, mely meghatározza, hogy mi számít a szoftverek jogszerű használatának

- a munkatársakban tudatosítani kell a szerzői jogok, a beszerzések szabályszerűségét, valamint az ezek megszegéséből adódó fegyelmi eljárás lehetőségét
- a szoftverekre is kiterjedő vagyonleltárt kell vezetni
- a licencek és szoftverek tulajdonlásáról szóló dokumentumokat biztonságos módon meg kell őrizni
- biztosítani kell, hogy a szoftvert csak a megengedett licencek számában vegyék igénybe a felhasználók
- kizárólag jogtiszta szoftvereket szabad telepíteni
- a nyilvános hálózatról szerzett szoftverek és adatok felhasználási követelményeit be kell tartani

18.1.3. A szervezet adatainak biztonsága

A hivatal fontos dokumentumait, adatait védeni kell lopás, hamisítás és sérülés ellen. Egyes dokumentumokat jogszabály alapján vagy üzleti érdekből kiemelt biztonságban kell őrizni.

Az egyes adatokat, a rá vonatkozó jogszabályban meghatározott ideig meg kell őrizni.

A dokumentumok megőrzésére és kezelésére vonatkozó előírásokat a hivatal Egyedi Iratkezelési Szabályzata tartalmazza.

18.1.4. A személyes adatok védelme

A személyes adatok védelmére vonatkozó jogszabályi előírások intézkedési kötelezettségeket rónak azokra az adatkezelőkre, akik személyes adatot kezelnek. Az adatvédelmi jogszabályoknak való megfelelés kellő irányítási struktúrát és ellenőrzést igényel. A hivatal az adatok védelmének érdekében előírja az Adatvédelmi Szabályzatában foglaltak szigorú betartását.

18.1.5. A védelmi eszközökkel elkövethető visszaélések megelőzése

A hivatal adatfeldolgozó eszközeit ügyviteli célra hozták létre, melyeket a vezetőségnek elérhetővé kell tennie az illetékes munkavállalók számára. Ezen eszközök bármilyen, az ügyviteli céloknak ellentmondó vagy felhatalmazás nélküli használatát tiltani kell.

Az információs rendszer vagy adat megsértése bűncselekmény. A hivatal munkatársait és a harmadik félhez tartozó felhasználót ezért tájékoztatni kell arról, hogy semmilyen más hozzáférés nincs engedélyezve, csak amire konkrét felhatalmazást kapott.

18.1.6. A kriptográfiai eszközök kezelésének szabályozása

Minősített adatok esetében a rejtjelezést csak a 161/2010. (V.6.) Korm. rendelet szerint szabad végezni. Érdemes jogi tanácsot kérni, mielőtt rejtjelezett információt vagy kriptográfiai eszközöket más országba továbbítunk.

18.2. Az informatikai biztonsági szabályzatnak, szabványoknak és műszaki követelményeknek való megfelelés

A hivatalnak gondoskodnia kell arról, hogy a rendszerek megfeleljenek a biztonságpolitikájának, szabályzatainak és a szabványoknak.

Az informatikai rendszerek biztonságát időről időre felül kell vizsgálni.

18.2.1. Az informatikai biztonsági előírásoknak való megfelelés

A szakmai vezetők felelősséggel tartoznak a hatáskörükbe tartozó biztonsági eljárások helyes végrehajtásáért. Az ügymenet minden területét időről időre felül kell vizsgálni, hogy megfelelnek-e a biztonsági szabályoknak.

Ennek keretében vizsgálni kell:

- az informatikai rendszereket
- az informatikai rendszerek szállítóit
- az adatgazdákat és az adatfeldolgozó eszközök tulajdonosait
- az informatikai rendszerek felhasználóit
- a teljes vezetőséget

A hivatal elvárja az informatikai rendszerek tulajdonosaitól, hogy eltűrjék és segítség a rendszerek átvizsgálását.

Az átvizsgálás azt mutatja ki, hogy az informatikai rendszerek és szolgáltatások megfelelnek-e az informatikai biztonságpolitikában és az IBSZ-ben lefektetett követelményeknek.

A biztonsági megfelelősséget a következő esetekben kell vizsgálni:

- új informatikai rendszerek vagy szolgáltatások bevezetésekor
- meglévő informatikai rendszerek és szolgáltatások esetében meghatározott időszakonként
- ha változás történt a biztonságpolitikában

Biztonsági átvizsgálást külső vagy belső személyzet, valamint a NEIH egyaránt végezhet.

Az informatikai rendszert védő biztosítékokat a következő módon lehet ellenőrizni:

- rendszeres vizsgálatokkal és tesztekkel
- a működési teljesítmény ellenőrzésével valós biztonsági események bekövetkezésekor
- szúrópróba jellegű vizsgálatokkal

18.2.2. A műszaki követelményeknek való megfelelés

A műszaki megfelelősség-ellenőrzés foglalja magába az üzemeltetési rendszer vizsgálatát, mellyel szavatolni lehet a hardver és szoftver óvintézkedések megvalósításának helyességét, pontosságát.

Az informatikai rendszert időről időre ellenőrizni kell sérülékenységének megállapítása, a biztonsági előírások megvalósulásának tekintetében.

A felülvizsgálatok végrehajtásáért a rendszergazda felel.

Az ellenőrzéseknek ki kell terjednie a hivatal működési folyamatinak ellátásához szükséges számítógépekre, egyéb informatikai eszközökre, szoftverekre, valamint a tartalék berendezésekre és az adatátviteli hálózatra.

Bármely műszaki megfelelősség-ellenőrzés elvégezhető, amennyiben csak az illetékes, erre felhatalmazott személyek végzik vagy felügyelik azt.

18.3. Az informatikai rendszerek biztonsági ellenőrzésének szempontjai

Az ellenőrzés egy folyamatos tevékenység, mely azt vizsgálja, hogy a rendszer és felhasználói, valamint a környezet fenntartja-e az informatikai biztonsági tervben meghatározott biztonsági szintet.

Az informatikai biztonsági ellenőrzés rendszerességét fent kell tartani, annak érdekében, hogy időben felismerhessük és rangsorolhassuk az új kockázatokat. Ilyenkor ellenőrizni kell az eszközöket és értéküket, sérülékenységeiket, biztosítékaikat, valamint az eszközökre irányuló fenyegetéseket.

A biztosítékok teljesítményét és hatékonyságát is rendszeresen ellenőrizni kell. Az ellenőrzési folyamatot írásba kell foglalni.

A rendellenességeket ki kell vizsgálni, és a megállapításokat jelenteni kell.

18.3.1. Rendszer-auditálási óvintézkedések

Az üzemelő rendszer auditálását gondosan meg kell tervezni, és annak feltételeit egyeztetni kell az érintettekkel, hogy minimalizálni lehessen az üzemkiesés kockázatát.

Az alábbiakat kell megvalósítani:

- a szoftverek és adatok ellenőrzése a „csak olvasás" jellegű hozzáféréssel ellenőrizhetők
- a „csak olvasás" jellegűtől eltérő hozzáférést csak akkor szabad engedélyezni, ha a hozzáférés más módon nem oldható meg, ebben az esetben a vizsgálatot végző személy mellett a rendszergazda vagy a vizsgált terület részéről felügyelet szükséges
- az ellenőrzéshez az erőforrásokat pontosan azonosítani kell, és a szükséges fizikai/logikai hozzáféréseket biztosítani kell
- a vizsgálati tevékenység nyomon követéséhez minden egyes hozzáférést figyelni, és naplózni kell
- az audit során feltárt tényeket, eltéréseket, felelősségeket dokumentálni kell

18.3.2. Rendszer-auditálási eszközök védelme

Az auditáláshoz szükséges programokat és adatállományokat védeni kell az illetéktelen hozzáférésektől, annak érdekében, hogy kizárjuk a lehetséges visszaéléseket.

Ha az auditot harmadik fél végzi, a szolgáltatási szerződésben le kell fektetni a titoktartásra és a tudomására jutott információk kezelésére vonatkozó előírásokat.

19. Záró rendelkezések

Jelen dokumentum 2022. január 3. napján lép hatályba.

1. számú melléklet

Vonatkozó hatályos jogszabályok, szabványok és ajánlások

Jogszabályok:

- Az informatikai biztonsággal kiemelten foglalkozó jogszabályok:
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 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
- 41/2015. (VII.15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 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
- 1139/2013. (III.21.) kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

A titokvédelemmel kapcsolatos jogszabályok:

- 2009. évi CLV. törvény a minősített adat védelméről
- 161/2010. (V. 6.) kormányrendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól
- 180/2004. (V. 26.) kormányrendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről
- 21/1996. (VIII. 31.) BM rendelet a belügyminiszter irányítása alatt álló titkos információgyűjtésre feljogosított szervek adatkezelésének egyes szabályairól

A személyes adatok kezelésével és védelmével kapcsolatos jogszabályok:

- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

- 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról
- 1996. évi XX. törvény a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról
- 1995. évi CXIX. törvény a kutatás és a közvetlen üzletszerzés célját szolgáló név és lakcímadatok kezeléséről
- 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről
- 1995. évi LXVI. törvény a közokiratokról, a közlevéltárakról és a magánlevéltári anyag védelméről

Az elektronikus aláírásról, az elektronikus szolgáltatásokról szóló jogszabályok:

- 2001. évi XXXV. törvény az elektronikus aláírásról
- 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól
- 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
- 335/2005. (XII. 29.) kormányrendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről
- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
- 41/2016. (X.13.) BM rendelet a minősített elektronikus aláírást és a minősített elektronikus bélyegzőt létrehozó eszközök megfelelőségét tanúsító szervezetekről és a kijelölésükre vonatkozó szabályokról
- 34/2004. (XI. 19.) IM rendelet az elektronikus dokumentumok közjegyzői archiválásának szabályairól és az elektronikus levéltárról

Szabványok és ajánlások:

- Magyar Informatikai Biztonsági Ajánlások - MIBIK és MIBÉTS
- ISO/IEC 13335-1:2004 Informationtechnology - Securitytechniques - Management of information and communicationstechnologysecurity - Part 1: Concepts and modelsforinformation and communicationstechnologysecurity management
- ISO/IEC 20000-1:2005 Informationtechnology - Service management - Part 1: Specification
- ISO/IEC 20000-2:2005 Informationtechnology - Service management - Part 2: Code of practice

- ISO/IEC 27001:2005 Informationtechnology - Securitytechniques - Informationsecurity management systems - Requirements
- ISO/IEC 27002:2005 Informationtechnology - Securitytechniques - Code of practiceforinformationsecurity management
- ISO/IEC 13335-1:2004 Informationtechnology - Securitytechniques - Management of information and communicationstechnologysecurity - Part 1: Concepts and modelsforinformation and communicationstechnologysecurity management
- ISO/IEC TR 13335-2:1997 Informationtechnology - Guidelinesforthe management of IT Security - Part 2: Managing and planning IT Security
- ISO/IEC TR 13335-3:1998 Informationtechnology - Guidelinesforthe management of IT Security - Part 3: Techniquesforthe management of IT Security
- ISO/IEC TR 13335-4:2000 Informationtechnology - Guidelinesforthe management of IT Security - Part 4: Selection of safeguards
- ISO/IEC TR 13335-5:2001 Informationtechnology - Guidelinesforthe management of IT Security - Part 5: Management guidanceonnetworksecurity
- Az Európai Unió Tanácsának Biztonsági Szabályzata (kiadva az Európai Unió Tanácsának 2001/264/EK számú határozatával).
- SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANISATION (NATO) - C-M(2002)49 /AC/35-D/2000 DirectiveonPersonnelSecurity, AC/35-D/2001 DirectiveonPhysicalSecurity, AC/35-D/2002 DirectiveonSecurity of Information, AC/35-D/2003 DirectiveonIndustrialSecurity, AC/35-D/2004 PrimaryDirectiveon INFOSEC, AC/35-D/2005 INFOSEC Management DirectiveforCommunications and information Systems/
- ISACA ajánlások: COBIT (ControlObjectivesforInformation and RelatedTechnology), COBIT MAPPING - Mapping of ISO/IEC 17799:2000 With COBIT, COBIT SECURITY BASELINE ,

2. számú melléklet

A hivatal informatikai rendszereinek és az azokban kezelt adatok biztonsági osztályba sorolása

Az informatikai rendszer megnevezése	Az informatikai rendszer leírása	Adatgazda	Rendszerben kezelt adatok	Tárolt adatok köre		Az informatikai rendszer telepítésének helye		Bizalmasság	Sértetlenség	Rendelkezésre állás	Biztonsági osztály
				Önkormány-zati	Állami	Saját szerveren/helyben	Külső szolgáltató/interneten keresztül				
ASP (asp.lgov.hu)	keretrendszer	Jegyző	keretrendszer				x	4	4	4	4
ASP (asp.lgov.hu) Gazdasági szakrendszer	gazdasági szakrendszer	Jegyző	könyvelés, számlázás	x			x	3	3	3	3
ASP (asp.lgov.hu) Adó szakrendszer	adó szakrendszer	Jegyző	önkormányzati adók	x	x		x	4	4	4	4
ASP (asp.lgov.hu) Elektronikus ügyintézés	elektronikus ügyintézési rendszer	Jegyző	vegyes ügyintézési adatok	x			x	3	3	2	3
ASP (asp.lgov.hu) Oktatási rendszer	oktatási rendszer	Jegyző	tananyagok	x			x	2	2	1	2
ASP (asp.lgov.hu) Hagyaték	hagyatéki ügyek nyilvántartása	Jegyző	hagyatéki adatok	x			x	2	2	1	2
ASP (asp.lgov.hu) Iktatás	iktató rendszer	Jegyző	iktatási adatok	x			x	2	2	2	2
ASP (asp.lgov.hu) Ingatlanvagyon	vagyonkataszter	Jegyző	kataszteri adatok	x			x	2	2	2	2
ASP (asp.lgov.hu) Ipar-kereskedelem	ipar-kereskedelmi rendszer	Jegyző	cégadatok	x			x	2	2	1	2

3. számú melléklet

A hivatal informatikai eszköznyilvántartása

Szervezeti egység megnevezése	Informatikai eszköz megnevezése	Informatikai eszköz azonosítója	Telepített operációs rendszer	Egyéb szoftverek
			Windows 10	Microsoft Office

Megismerési nyilatkozat

Az Eperjeskei Közös Önkormányzati Hivatal Informatikai biztonsági szabályzatban foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

Név	Beosztás	Aláírás	Megismerés dátuma
Pásztor Gábor	Eperjeske Község Önkormányzata - polgármester		2022.01.03.
Iván Barna Zsolt	Eperjeske Község Önkormányzata - alpolgármester		2022. 01. 03
dr. Gál-Lakatos Enikő	jegyző		2022.01.03.
Sajtosné Juhász Tamara	pénzügyi ügyintéző		2022. 01. 03.
Siposné Fodor Ágnes	pénzügyi ügyintéző		2022.01.03.
Krecz Zoltánné	Eperjeskei Kastélykert Óvoda és Konyha - intézményvezető		2022.01.03.
Móré Zsuzsanna Marianna	Eperjeskei Kastélykert Óvoda és Konyha - óvodapedagógus		2022. 01.03
Pásztor Gáborné	Eperjeskei Kastélykert Óvoda és Konyha - élelmezésvezető		2022.01.03
Demeter Tibor	Eperjeske Község Roma Nemzetiségi Önkormányzata - elnök		2022.0103
Demeterné Vadász Mária	Eperjeske Község Roma Nemzetiségi Önkormányzata - elnökhelyettes		2022.01.03.
Ésik Árpád	Tiszamogyorós Község Önkormányzata - polgármester		2022.01.03.
László Béla	Tiszamogyorós Község Önkormányzata - alpolgármester		2022.01.03

Fodor Melinda	Tiszamogyorósi Tündérkert Óvoda és Konyha - intézményvezető	2022.01.03.	Fodor Melinda
Szabó Attiláné	Tiszamogyorósi Tündérkert Óvoda és Konyha - óvodapedagógus	2022.01.03.	Szabó Attiláné
Mészáros Lajos	Benk Község Önkormányzata - polgármester		2022.01.03.
Halász Bertalan Zoltán	Benk Község Önkormányzata - alpolgármester	Halász Zoltán 2022	2022.01.03