3.1.6.7. Fegyelmi intézkedések

3.1.6.7.1.1. Eljárásrend

Az Intézmény belső eljárási rendje szerint fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben. Az eljárást az erre kijelölt etikai bizottság folytatja le.

3.1.6.7.1.2. Jogi eszközök

Ha az elektronikus információbiztonsági szabályokat nem Az Intézmény személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti ezeket az eljárásokat.

3.1.6.8. Belső egyeztetés

Az Intézmény tervezi és egyezteti az elektronikus információs rendszer biztonságát érintő tevékenységeit, hogy csökkentse annak a nem érintett szervezeti egységeire gyakorolt hatását.

3.1.6.9. Viselkedési szabályok az interneten

Az Internet használatának kizárólagos célja a munkavégzés. A felhasználó nem jogosult magáncélra használni a web elérését.
A hálózat nem használható az alábbi módon, az alábbi tevékenységekre:
a) A hatályos magyar törvényekbe ütköző cselekmények, idecértve, de nem korlátozva azokra: mások személyiségi jogainak megsértése; tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték); a szerzői jogok megsértése; szoftver szándékos és tudatos illegális terjesztése.
b) A hálózathoz kapcsolódó más - hazai vagy nemzetközi - hálózatok szabályaiba ütköző tevékenységek, a mennyiben ezek a tevékenységek ezen hálózatokat érintik.
c) Profitszerzést célzó direkt üzleti célú tevékenység (pl. bérletöltés), reklámok terjesztése.
d) A hálózat, illetve erőforrásai normális működését megzavaró, veszélyeztető tevékenység (idegen jelszó kiderítése saját és idegen hálózatban, idegen felhasználói név használata az illető tudomása nélkül).
e) A hálózatot, illetve erőforrásait indokolatlanul vagy szándékosan túlzott mértékben, pazarló módon igénybe vevő tevékenység (pl. levélbombák, elektronikus játékok).
f) A hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, módosítása, törlése.
g) A hálózat biztonságát veszélyeztető információk, programok terjesztése.
h) Mások személyiségi jogait, vallási, etnikai, politikai vagy más jellegű érzékenységét sértő, másokat zaklató tevékenység (pl. pornográf anyagok közzététele).
i) Mások munkájának indokolatlan és túlzott mértékű zavarása vagy akadályozása (pl. kéretlen levelek).
A lokális (belső) hálózatra vonatkozó általános szabályok azonosak az internetre vonatkozó szabályokkal, kiegészítve azzal, hogy a tiltott magatartási formák előkészítése, illetve kísérlete is szankcionálható.

3.1.6.9.1.1. Információk nyilvánossága

Az Intézmény tiltja és számon kéri a szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét.

Honlap

Az Intézmény hivatalos honlapja
http://www.javorszky.hu [84.206.65.9]
A honlapot működtető portal, illetve a tartalom karbantartását a vállalat munkatársai végzik.
Az Intézménnyel kapcsolatos, nyilvános hozzáférésű elektronikus információs rendszeren bármely információ közzétételére csak és kizárólag a PR és marketing manager, illetve a főigazgató által írásban megbízott
illetve az általa kijelölt személyek jogosultak. A nyilvánosan elérhető tartalmakat az adatvédelmi tisztviselő kéthavonta ellenőrzi. Amennyiben rendellenességet talál, kezdeményezi az eltávolítását.

3.1.6.9.1.2. Tiltott tevékenységek

a) Tilos olyan tevékenységet kifejteni, amely célja mások adatainak jogosulatlan megszerzése, megváltoztatása, letörlése.

b) Tilos más felhasználók nevében tevékenykedni.

c) A felhasználó nem teheti lehetővé mások számára, hogy a nevében tevékenykedjenek. Ezért – többek között – mindent meg kell tennie a jelszavai titkosságának megőrzése érdekében, továbbá ezért, hogy a személyazonosító eszközeit (például, de nem kizárólag: VPN kulcs, azonosító kártya, mobil telefon) más ne használhassa.

d) A felhasználó köteles törekedni arra, hogy az általa pillanatnyilag használatba vett rendszerekben más személy ne fejthessen ki aktivitást.

e) Tilos más munkavégzését korlátozó tevékenységet végezni nem munka céljából kifejtett aktivitással.

f) Tilos a rendszer bármely elemének eredeti felhasználási céljától eltérő használata vagy az erre irányuló próbálkozás.

g) Tilos a hálózati forgalom figyelése, erre alkalmas szoftver telepítése.

h) Tilos Az Intézmény rendszergazdájától kapott IP címtől eltérő más IP cím jogosulatlan használata.

i) Tilos olyan anyag továbbítása, letöltése vagy közzététele az interneten, amely a magyar és uniós törvényeket sérti.

j) Tilos Az Intézmény belső informatikai rendszerén kívüli helyszínről elérni vagy megpróbálni elérni a rendszert, kivéve, ha erre az Informatikai osztály engedélyt ad.

k) Tilos külső személy számára információt adni a rendszer valamely hibájáról, sebezhető pontjáról.

3.1.6.9.1.3. Szervezettől idegen tevékenységek

Az Intézmény tiltja a közösségi oldalak használatát, magánpostafiók mellékleteinek, csatolmányainak elérését, és más, a szervezettől idegen tevékenységet.

3.1.7 Tudatosság és képzés

3.1.7.1. Kapcsolattartás

Az Intézmény kapcsolatot tart az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel az IBF-en keresztül.

3.1.7.1.1.1. Folyamatos képzés

Az Intézmény az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek folyamatos oktatásának, képzésének elősegítésére törekszik.

3.1.7.1.1.2. Naprakészség

Az Intézmény az ajánlott elektronikus információbiztonsági eljárások, technikák és technológiák naprakészen tartása érdekében minden rendelkezésére álló erőforrást igénybe vesz.

3.1.7.1.1.3. Információcsere

Az Intézmény a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megosztása érdekében kapcsolatot alakít ki és tart fenn az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és e célt szolgáló ágazati szervezetekkel, továbbá a tevékenysége körében meghatározott szakmai céllal létrejövő fórumokon.

3.1.7.2. Képzési eljárásrend

3.1.7.2.1.1. Kihirdetés

A képzési eljárásrend kihirdetési eljárása megegyezik az Informatikai Biztonsági Szabályzat kihirdetésének módjával.

3.1.7.2.1.2. Felülvizsgálat

A képzési eljárásrend felülvizsgálata és frissítésének gyakorisága azonos az Informatikai Biztonsági Szabályzat eljárásaival.

3.1.7.3. Biztonság tudatosság képzés

3.1.7.3.1. Felhasználók képzése

Az Intézmény annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára.

3.1.7.3.1.1. Új felhasználók

Az új felhasználók kezdeti képzésének részeként, a munka megkezdése előtt képzést szervez, és nyilatkozatot kér a szabályzat elfogadásáról.

3.1.7.3.1.2. Változás

Az Intézmény, amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi, haladéktalanul kiegészítő képzést szervez a felhasználóknak.

3.1.7.3.1.3. Rendszeresség

A képzéseket legalább évente meg kell tartani, és dokumentálni.

3.1.7.5. Szerepkör, vagy feladat alapú biztonsági képzés

3.1.7.5.1. Szerepkörök szerinti képzés

Az Intézmény szerepkör vagy feladat alapú biztonsági képzést nyújt az egyes szerepkörök szerinti, azért felelős személyeknek.

3.1.7.5.1.1. Előzetes felkészülés

Az Intézmény az elektronikus információs rendszerhez való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően is nyújt képzéseket.

3.1.7.5.1.2. Változás

Az Intézmény, amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi, haladéktalanul kiegészítő szakképzést szervez a felhasználóknak.

3.1.7.5.1.3. Rendszeresség

A képzéseket legalább három évente meg kell tartani, és dokumentálni.

3.1.7.6. A biztonsági képzésre vonatkozó dokumentációk

3.1.7.6.1.1. Képzések dokumentálása

Az Intézmény dokumentálja a biztonságtudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzéseket. A dokumentumok tartalmazzák:

- Az oktatás tematikáját
- Az oktatás anyagait (ppt)
- Az oktatás helyét és idejét
- A résztvevők felsorolását és aláírását
- Az oktató megnevezését, és aláírását.

3.1.7.6.1.2. A dokumentumok megőrzése

Az Intézmény a képzésen résztvevőkkel a képzés megtörténtét elismerteti, és a dokumentumokat megőrzi, legalább 5 évig.

4. Mellékletek

4.1 Alapfogalmak
4.2 Kockázatkezelési eljárásrend
4.3 Informatikai biztonság – védelmi intézkedések eljárásrendjei
4.4 Informatikai szoftverfrissítés eljárásrendje
4.5 A szerverszoba házirendje
4.6 Biztonsági osztályba sorolás

4.1 melléklet

Alapfogalmak

Számítógép (computer): Olyan elektronikus berendezés, mely információk tárolására alkalmas memóriával rendelkezik. Képes az adatok bevitelét, tárolását, feldolgozását, visszakeresését emberi közreműködés nélkül elvégezni a számítógépben korábban elhelyezett program (szoftver) működtetésével.

Felhasználó (user): A számítógépes rendszer emberekből álló környezete. Őket a számítógéptől kapható információ érdekli, nem pedig a számítógépes rendszer speciális tulajdonságai.

Hardver (hardware): A számítógépek, számítógépes rendszerek fizikai része, amelybe beletartoznak az elektromos, elektronikus összetevők (pl. áramkörök), az elektromechanikus és mágneses összetevők (pl. lemezmeghajtó), az optikai összetevők (pl. CD-ROM), és a mechanikus összetevők (pl. számítógép szerelvény).

Program (szoftver): Általános kifejezés valamely számítógép meg nem fogható, nem fizikai összetevőire. Leggyakrabban a számítógép által végrehajtott programokra és annak dokumentációjára vonatkoztatják, megkülönböztetve azok fizikai részétől, a hardvertől. A program a számítógépnek egységként átadható utasításhalmaz, amely irányítja a rendszer működését.

Állomány (fájl): Háttértáron tárolt információ. A tárolás célja, hogy az információ egy munka (job) végrehajtásához szükséges időn túl is megmaradhasson és/vagy az operatív tár (memória) kapacitásából adódó korlátozásokat túl lehessen lépni. A fájlokban programokat, adatokat, szöveget, képet, hangot stb. lehet tárolni.

Operációs rendszer (operating system): Olyan program, amely a számítógépben az egyéb programok végrehajtását vezérli, ütemezi, elosztja az erőforrásokat, biztosítja a felhasználó és a számítógép közötti kommunikációt.

Általános célú szoftver: Általános célú szoftvernek a kereskedelmi forgalomban kapható olyan programterméket nevezzük, amelyek nem valamilyen konkrét feladat megoldására készültek, hanem ilyen rendszerek működését biztosítják, vagy támogatják (operációs rendszerek, segédprogramok), illetve általános felhasználói igényeket elégítenek ki (szövegszerkesztők, táblázatkezelők).

Speciális szoftverek: Speciális szoftvernek az olyan programot, vagy programrendszert tekintjük, amelynek használatához különleges tulajdonságai miatt speciális eszközökre (rajzgép, rajzdigitalizáló, scanner stb.) és/vagy speciális hardver/szoftver ismeretekre van szükség.

Felhasználói program (application program): Olyan program, vagy programrendszer amelyet egy adott számítógépes környezetben kifejezetten egy speciális feladat elvégzésére készítettek, amely közvetlenül hozzájárul a feladat megoldásához (pl. bérszámfejtés, munkaügy), egy adott felhasználói igény kielégítéséhez.

Egy felhasználós program: Egy felhasználós program az olyan program, melyet egyidejűleg csak egy felhasználó működtethet még akkor is, ha az hálózati operációs rendszer felügyelete alatt fut.

Programvírus: Adatállományok vagy programok bemásolásával a számítógép háttértárra kerülő, és futtatása esetén az ott található programokat és adatállományokat, — vagy akár magát a számítógépet fizikailag is — károsító rosszindulatú program.

A szoftver tulajdonjogával kapcsolatos fogalmak

a) Szoftver tulajdonjoga: Az eredeti számítógépes program az azt létrehozó személy vagy vállalat szellemi tulajdona. A felhasználó tehát a szoftvertermék megvásárlásával általában nem válik a szoftver tulajdonosává. A számítógépes programokat a szerzői jogi törvény védi.

b) Szoftver licensz szerződés: Egy adott szoftver esetében a licensz szerződés határozza meg a szerzői jog tulajdonosa által megengedett szoftverhasználat feltételeit. A szoftverhez adott licensz szerződésre általában utalás történik a szoftver dokumentációjában, vagy a program indításakor megjelenő képernyőn. A szoftver ára tartalmazza a szoftver licenszét és annak elfogadása kötelezi a vevőt, hogy a szoftvert kizárólag a licensz szerződésben leírt feltételek szerint használja.

c) Jogosulatlan másolás: A szoftver licensz szerződés – amennyiben eltérően nem rendelkezik — a vevőnek a szoftverről csak egyetlen "biztonsági" másolat készítését engedélyezi arra az esetre, ha a szoftver eredeti lemeze meghibásodna, vagy megsemmisülne. A szoftver bármely további másolása jogosulatlan másolásnak minősül, és megsérti a licensz szerződést, valamint a szerzői jogi törvényt.

d) Illegális szoftverhasználat: Illegális a szoftverhasználat, ha: valaki a szoftvert, vagy annak dokumentációját — beleértve a programokat, alkalmazásokat, adatokat, kódokat és kézikönyveket — a szerzői jog tulajdonosának engedélye nélkül lemásolja, vagy terjeszti a szoftvert két vagy több gépen futtatja, kivéve ha ezt a szoftver licensz szerződése külön engedélyezi, illetve ha általában a szoftvert nem a licensz szerződésben foglalt feltételeknek megfelelően használja.

Az illegális szoftverhasználat törvénybe ütköző cselekedet, és a BTK 329/A §-a alapján bűncselekmény.

Helyi számítógép hálózat (Local Area Network): Helyi számítógép hálózatoknak tekintjük az önálló, helyi feldolgozó-képességgel és erőforráskészlettel (processzor, memória) rendelkező számítógépek összekapcsolásával létrehozott olyan hálózatot, amelyben az egyes munkaállomások (workstation) konkurens módon érhetik el a hálózat kijelölt számítógépein (fájl- vagy nyomtató szerver) tárolt adatállományokat és az egyéb erőforrásokat (nyomtatók stb.). A hálózaton belüli kapcsolatot elektromos kábelen, — újabban üvegszálon — speciális hozzáférési eljárás segítségével valósítják meg.

Hozzáférési jog: A könyvtárakhoz való hozzáférési jog azt jelenti, hogy a könyvtárakban levő fájlokkal mit tehet a felhasználó, vagy a felhasználók egy csoportja, ha azt egyébként külön fájl jogokkal nem szabályozták. Ezek az alábbiak:

- Rendszergazda (Supervisor) jog: Jogköre korlátlan. Megszabhatja, hogy rajta kívül ki és milyen joggal férhet hozzá az állományokhoz.
- Olvasási, (Read) jog: A fájl tartalmát megnézheti, a programot futtathatja.
- Írási, (Write) jog: A fájl tartalmát módosíthatja.

- Keresési (File Scan) jog: a könyvtár katalógusában
- Fájl és könyvtár létrehozási (Create) és törlési (Erase) jog
- Módosítási, (Modify) jog: a fájl tulajdonságainak (attribútumainak) módosítására jogosít.
- Hozzáférés engedélyezési (Acess Control) jog: Ezen jog tulajdonosa meghatározhatja, hogy kik férjenek hozzá az adott könyvtárhoz, vagy fájlhoz.

Örökölt jogok: Egy magasabb szintű (szülő) könyvtárban meglévő jogaink öröklődnek az alacsonyabb szintű könyvtárban. A tényleges jog, amellyel a felhasználó rendelkezik az a jog, melyre felhasználóként, csoporttagként szert tett az adott könyvtárban, vagy amelyet a szülő könyvtárból örökölt.

Fájl és könyvtár tulajdonságok (Attributes):

- Fájl - tulajdonságok: olvasható (RO), írható/olvasható (RW), megosztható (S), rejtett (H), rendszer (SY), végleg törölhető (P), archiválandó (A), nem törölhető (DI), nem átnevezhető (RI) stb.
- Könyvtár tulajdonságok: normál (N), rendszer (SY), rejtett (H), nem törölhető (D), nem átnevezhető (R), törölhető (P).

Hálózati vagy többfelhasználós program: A hálózati környezet lehetőségeinek kihasználására alkalmas olyan program, illetve programrendszer, amelyet előre meghatározott felhasználói jogosultság alapján több felhasználó működtethet általában közös adatállományok akár egyidejű felhasználásával.

Programdokumentáció: Egy adott program vagy programrendszer fejlesztője által a felhasználó rendelkezésére bocsátott adathordozók (mágneslemez, vagy CD-ROM), a szoftver licensz szerződés vagy felhasználási engedély és a használatához szükséges írásos anyagok (felhasználói kézikönyv, vagy programleírás).

Programtelepítés, vagy installáció: Az adott program elhelyezése adathordozóról (telepítő lemezek, CD-ROM) egy adott számítógép háttértárára — a felhasználói dokumentációban, vagy az adathordozó borítóján illetve címkéjén meghatározott, az adathordozón található telepítési eljárás vagy telepítőprogram segítségével, a licensz engedélyben előírtak betartásával — hasznos munkavégzés céljából.

4.2 melléklet

Kockázatkezelési eljárásrend

1. Kockázatelemzés

1.1 Az információbiztonsági kockázatelemzés célja, hogy

a) vizsgálja az informatikai rendszerek gyenge pontjait (sérülékenység vizsgálat);

b) feltárja az informatikai rendszerekre ható fenyegető tényezőket, veszélyforrásokat (fenyegetettség elemzés);

c) elemezze a veszélyforrások által a gyenge pontokon keresztül bekövetkező sikeres támadások bekövetkezési valószínűségét és az általuk okozott kár nagyságát (kockázatelemzés);

d) valamint kezelje a Szervezet által el nem fogadható kockázatokat (kockázatkezelés).A kockázatelemzés végrehajtása során a következő Kockázatelemzési és kockázatkezelési eljárásrendet kell alkalmazni:

1.2 Kockázatelemzések folyamata

Az IBF-nek évente el kell végeznie az informatikai rendszerek kockázatelemzését a jelen eljárásrendben foglalt módszertannak megfelelően.

A kockázatelemzés eredményét a *Kockázatelemzési jelentésben* kell dokumentálni, amelyet jóváhagyás és az érintettek számára kihirdetés céljából be kell terjeszteni az informatikai vezető és a Szervezet vezetője részére.

Jóváhagyás után az informatikai vezető irányításával és a rendszergazda közreműködésével a nem tolerálható kockázatokra *Kockázatkezelési tervet* kell készíteni, amelyet a Szervezet vezetőjének jóváhagyása után, ütemezett és dokumentált módon végre kell hajtani.

A kockázatkezelő intézkedések végrehajtása után az IBF-nek maradványkockázat elemzést szükséges végrehajtani, melynek célja, hogy kimutassa a kockázatkezelő intézkedések eredményességét és feltárja az esetlegesen megmaradó kockázatokat.

A kockázatelemzést ismételten el kell végezni, ha változás következik be az informatikai rendszerekben vagy azok környezetében (beleértve az új fenyegetések és sérülékenységek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az informatikai rendszerek biztonsági állapotát.

A kockázatelemzést legalább évente felül kell vizsgálni, újra el kell végezni figyelembe véve a változásokat.

A kockázatelemzés és a hozzá kapcsolódó dokumentumok bizalmas minősítésűek. Gondoskodni kell a dokumentumok megfelelő védelméről. A kockázatelemzési dokumentumokat kizárólag az érintettek kezelhetik, illetékteleneknek nem adhatják tovább.

Felelős: IBF

Határidő: évente

1.3 Kockázatelemzési módszertan

A Szervezetnél alkalmazott kockázatelemzési módszertan röviden a következő:

1.3.1 Kezdeti helyzetfelmérés

Az informatikai rendszer kockázatelemzésének elvégzéséhez fel kell mérni, meg kell ismerni az informatikai rendszert és a jelenlegi információbiztonsági állapotát.

A következő területeket kell a dokumentációk bekérésével, illetve szakmai interjúk lefolytatásával megismerni:

a) Adminisztratív védelmi intézkedések:
    a. a Szervezetre vonatkozó jogszabályok, szabályzatok;
    b. az informatikai rendszerre vonatkozó szabályzatok;
    c. üzemeltetési eljárások;
    d. szerződések, külső partnerek kezelése;
    e. biztonsági események kezelése.
b) Fizikai védelmi intézkedések:
    a. beléptetés;
    b. az épületben történő közlekedés;
    c. a szerverterem kialakítása;
    d. az irodák kialakítása;
    e. a tiszta asztal, üres képernyő politika alkalmazása.
c) Logikai védelmi intézkedések:
    a. szoftverfejlesztés, változáskezelés;
    b. a szervizelés, eszközcsere, selejtezés folyamata;
    c. mentési megoldások;
    d. a jogosultsági rendszer, a jogosultságigénylés folyamata;
    e. vírusok és egyéb kártevők elleni védekezés;
    f. biztonsági frissítések telepítése;
    g. naplózás, biztonsági rendszerek;
    h. a hálózat felépítése;
    i. kriptográfiai (titkosítási) megoldások.

Vagyonelemek meghatározása

Az informatikai rendszerre ható fenyegető tényezők különbözőek, attól függően, hogy a rendszer melyik összetevőjét (vagyonelemét) fenyegetik, mert az egyes vagyonelem csoportoknak eltérőek a gyenge pontjaik.

A gyenge pontok és a fenyegető tényezők megfelelő azonosítása érdekében a következő vagyonelem csoportokat kell a kockázatelemzésben vizsgálni:

a) környezeti infrastruktúra;

b) hardverek;

c) szoftverek;

d) adatok;

e) adathordozók;

f) kommunikáció;

g) dokumentációk;

h) humán erőforrások.

1.3.1.1 Gyenge pontok meghatározása

A helyzetfelmérés alapján megszerzett információk birtokában meg kell határozni az egyes vagyonelemek gyenge pontjait.

Az egyes vagyonelemek gyenge pontjait és a fenyegető tényezőket a KIB 25. számú ajánlása (25/1-3. kötet: Az Információbiztonság Irányításának Vizsgálata 1.0 verzió „gyenge pontok" és „fenyegetettségek" segédletei) alapján érdemes azonosítani.

1.3.2 Fenyegető tényezők elemzése

Az egyes vagyonelemekre ható fenyegetések, fenyegető tényezők (pl.: üzleti hírszerzés, rosszindulatú hackerek, természeti katasztrófák) mindig a gyenge pontokon keresztül fejtik ki hatásukat.

Meg kell vizsgálni, hogy a beazonosított gyenge pontokon keresztül mely fenyegető tényezők tudják kifejteni a káros hatásukat.

1.3.3 Kárérték szintek meghatározása

A bekövetkezett káresemény súlyosságának, mértékének jellemzésére a következő kárérték szintek kerültek kialakításra:

a) 1 – Kicsi;

b) 2 – Közepes;

c) 3 – Nagy.

A kárérték szintek meghatározása során azt kell figyelembe venni, hogy

a) milyen tényleges vagy erkölcsi kárt jelentene a rendszerben tárolt adatok bizalmasságának sérülése;

b) milyen következményekkel járna a rendszer ideiglenes elérhetetlensége vagy az adatok sérülése, elvesztése;

c) mennyibe kerülne a meghibásodott eszközök javítása, cseréje;

d) mennyi munkaidő ráfordítással járna a helyreállítás.

A kockázatok megállapításához az informatikai rendszer vagyonelemeire rá kell vetíteni a kárérték szinteket.

1.3.4 Bekövetkezési valószínűségek meghatározása

A következő lépésként meg kell becsülni a fenyegetések bekövetkezési valószínűségét.

A bekövetkezési valószínűséghez a következő értékeket kell használni:

a) 1 – Kicsi (pl. évente vagy több évente következhet be);

b) 2 – Közepes (pl. havonta bekövetkezhet);

c) 3 – Nagy (pl. hetente, naponta bekövetkezhet).

1.3.5 Kockázatok meghatározása

Az információbiztonsági kockázatokat a fenyegetés bekövetkezésének a valószínűsége és az okozott kárt jellemző kárérték szint szorzata fogja megadni.

A kockázatok nagyságának, értékének meghatározásához a következő kockázati mátrixot kell használni:

Kárérték	**Bekövetkezés valószínűsége**		
	1	2	3
1	1	1	2
2	1	2	
3	2		

A táblázatban a kockázatok jelentése a következő:

a) 1 – Alacsony;

b) 2 – Közepes;

c) 3 – Magas.

Nem tolerálható kockázatok meghatározása

A Szervezet azt a döntést hozta, hogy minden közepes és magas kockázatot kezelni kíván.

Ennek megfelelően a toleranciamátrix a következő:

Kárérték	Bekövetkezés valószínűsége		
	1	2	3
1	T	T	NTH
2	T	NTH	NT
3	NTH	NT	NT

A táblázatban alkalmazott jelölések értelmezése a következő:

a) T – Tolerálható;

b) NTH – Nem tolerálható, hosszú távon kockázatkezelést igényel;

c) NT – Nem tolerálható, azonnali kockázatkezelést igényel.

2. Kockázatok kezelése

A Szervezet a kockázatokat a következőképpen kezeli:

a) Megfelelő intézkedésekkel csökkenti a fenyegetés bekövetkezési gyakoriságát vagy hatását (kockázat csökkentés).

b) Elkerüli a kockázatot azáltal, hogy az érintett tevékenységet felfüggeszti (kockázat elkerülés).

c) Áthárítja a kockázatot pl. biztosítással vagy megfelelő beszállítói szerződésekkel (kockázat áthárítás).

d) Tudatosan, a következményeket felmérve elfogadja a kockázatot (kockázat elfogadás).

2.1 Kockázatcsökkentő intézkedések

A kockázatcsökkentő intézkedések az alábbi módon csoportosíthatók:

a) Megelőző jellegű intézkedések (preventív kontrollok)
A hibák, sérülékenységek, gyenge pontok, illetve ezek kihasználására való lehetőségek kiküszöbölése.

b) Korlátozó vagy javító intézkedések (korrektív kontrollok)
A veszélyek hatását csökkentő, enyhítő óvintézkedések, további tevékenységek szükségessége nélkül.

c) Észlelő és reagáló intézkedések (detektív kontrollok)
A sérülékenységek, gyenge pontok támadásának észlelése, ártalmas kihatások enyhítésére, illetve válaszreakciók kidolgozása.

3. Kockázatelemzések dokumentálása

A Szervezet a kockázatelemzés eredményét a Kockázatelemzési jelentésben, a kockázatkezelő intézkedéseket a *Kockázatkezelési tervben* dokumentálja.

3.1 Kockázatelemzési jelentés

A *Kockázatelemzés jelentés* két részből tevődik össze:

a) egy táblázatos részből, amely a módszertannak megfelelően rögzíti az elvégzett a kockázatelemzés adatait;

A táblázatos résznek tartalmaznia kell:

a) az informatikai rendszer feltárt gyenge pontjait;

b) a gyenge pontokra ható fenyegető tényezőket;

c) a fenyegető tényezők bekövetkezési valószínűségét;

d) a fenyegetés bekövetkezése esetén a kár mértékét jellemző kárértéket;

e) a valószínűség és a kárérték alapján megállapított kockázat mértékét;

f) vázlatosan a javasolt kockázatkezelő intézkedéseket;

g) a javasolt éves ütemezést a kockázatkezelő intézkedések megvalósítására.

A szöveges részben – hivatkozva a táblázatos rész kapcsolódó sorára – részletesen ki kell fejteni:

a) a felmérési állapotot: az azonosított konkrét fenyegetés, veszélyforrás részleteit;

b) a fenyegetés által jelentett kockázatot: a fenyegetés bekövetkezésének módját, a bekövetkezett káresemény és a következmények részleteit, ha a kárérték szintje nagy, a kár elhárításának becsült költségét és/vagy munkaidő ráfordítását;

c) a megállapított kockázat mértékét (alacsony, közepes, magas);

d) a kockázatkezelő intézkedésre tett javaslatot.

4. Kockázatkezelési terv

A Szervezet a nem tolerálható kockázatok kezelésére *Kockázatkezelési tervet* készít.

A tervben a *Kockázatelemzési jelentés* szöveges részéből kiindulva meg kell határozni a megvalósítandó kockázatkezelő intézkedéseket, a szükséges munkaidő ráfordítást és esetleges költségeket, valamint a felelősöket és a határidőket.

Felelős: IBF

Határidő: évente

4.3 melléklet

Informatikai biztonságvédelmi intézkedések eljárásrendjei

1. Általános rendelkezések

1.1 Az eljárásrend célja

A védelmi intézkedések eljárásrendjeinek (továbbiakban: az eljárásrend) célja, hogy biztosítsa az Intézménynél azokat a védelmi intézkedéseket, amelyeket a 41/2015.(VII.15.) BM rendelet az Intézményre vonatkozóan előír.

1.2 Az eljárásrend szervezeti-személyi hatálya

Az eljárásrend szervezeti hatálya az Intézmény valamennyi olyan szervezeti egységére kiterjed, amely az Intézmény informatikai rendszerét használja, üzemelteti, fejleszti, továbbá ilyen tevékenységeket irányít és ellenőriz.

Az eljárásrend személyi hatálya kiterjed az Intézménnyel munkavégzésre irányuló bármely jogviszonyban álló természetes és jogi személyre, tehát azokra, akik kapcsolatba kerülnek az Intézmény elektronikus információs rendszerével (használják, fejlesztik, telepítik, üzemeltetik, javítják stb.), így:

- a munkaviszony alapján foglalkoztatott munkatársakra,
- az Intézménnyel szerződéses kapcsolatban álló természetes és jogi személyekre,
- más szervezetek képviseletében az Intézmény munkahelyein tartózkodó személyekre.

1.3 Időbeni hatály

Jelen eljárásrend a kiadás napján lép hatályba és módosításig, ill. visszavonásig érvényes.

1.4 Az eljárásrendek felülvizsgálata

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

Az eljárásrend módosítására van szükség, ha az elektronikus információs rendszer működésében vagy az elektronikus információs rendszer működését meghatározó jogszabályi környezetben jelentős változások következnek be.

Az eljárásrendet legalább évente egy alkalommal felül kell vizsgálni.

Az eljárásrend eseti módosításának, felülvizsgálatának kezdeményezése és a felülvizsgálat, valamint a módosítás elvégzése az elektronikus információs rendszerek biztonságáért felelős személy (továbbiakban: információbiztonsági felelős, rövidítve IBF) feladata. A módosítások engedélyezése és az újabb változat jóváhagyása az elnök-vezérigazgató vagy helyettesének hatásköre.

1.5 Hatásköri és illetékességi szabályok

Az eljárásrend belső használatú dokumentum: az elektronikus információs rendszer felhasználói, illetve egyéb érintettek (az Intézménnyel szerződéses kapcsolatban álló

természetes és jogi személyek, más szervezetek képviseletében az Intézmény munkahelyein tartózkodó személyek) megismerhetik és birtokolhatják, de illetéktelenekne nem adhatják tovább.

2. Rendszer kapcsolatok

2.1 Az elektronikus információs rendszer kapcsolódásainak szabályzása és dokumentálása

Szabályozni és belső engedélyhez kell kötni az elektronikus információs rendszer kapcsolódását más elektronikus információs rendszerekhez. Ezeket a kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát dokumentálni kell.

2.1.1 Belső rendszer kapcsolatok

Az elektronikus információs rendszerek összekapcsolása csak akkor lehetséges a belső rendszerek esetében, ha annak kockázatait az IBSZ szerinti Informatikai Vezető, illetve az Informatikai Biztonsági Felelős (a továbbiakban: IBF) mérlegeli, majd az Informatikai Vezető jóváhagyja.

2.1.2 Külső kapcsolódásokra vonatkozó korlátozások

Az Intézménynek a külső elektronikus információs rendszerekhez való kapcsolódásokhoz az IBSZ-ben szabályrendszert kell felállítani és alkalmazni. Ennek a szabályrendszernek az eredménye lehet az összes kapcsolat engedélyezése vagy tiltása, meghatározott kapcsolatok engedélyezése, meghatározott kapcsolatok tiltása.

2.2 Személybiztonság

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

Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem a Szervezet dolgozója, a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot is).

3. Rendszerbiztonsági terv

A Szervezetnek rendszerbiztonsági tervet kell készítenie, amely összhangban kell, hogy álljon szervezeti felépítésével

Meg kell határozni az elektronikus információs rendszer hatókörét, alapfeladatait (biztosítandó szolgáltatásait), biztonságkritikus elemeit és alapfunkcióit, valamint az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát.

Tartalmaznia kell az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait, illetve a vonatkozó

rendszerdokumentáció keretébe bele kell foglalni az elektronikus információs rendszer biztonsági követelményeit.

Ezen felül meg kell határozni a követelményeknek megfelelő aktuális, vagy tervezett védelmi intézkedéseket és intézkedés bővítéseket, illetve végrehajtani a jogszabály szerinti biztonsági feladatokat.

Gondoskodni kell arról, hogy a rendszerbiztonsági tervet (és annak változásait) a meghatározott személyi és szerepkörökben dolgozók megismerjék, de jogosulatlanok számára ne legyen megismerhető, módosítható.

A rendszerbiztonsági tervben meghatározott gyakorisággal felül kell vizsgálni az elektronikus információs rendszer rendszerbiztonsági tervét. Amennyiben az elektronikus információs rendszerben vagy annak üzemeltetési környezetében változások történnek, illetve a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén frissíteni kell a rendszerbiztonsági tervet.

3.1 Cselekvési terv

Amennyiben a Szervezet az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, úgy cselekvési tervet kell készíteni, amely dokumentálja a megállapított hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeket.

A meglévő cselekvési tervet 180 naponta frissíteni kell a biztonsági értékelések, biztonsági hatáselemzések és a folyamatos felügyelet eredményei alapján.

3.2 Személyi biztonság

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed a Szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki a Szervezet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet, függetlenül attól, hogy külsős, vagy belső munkatársról van szó. Ezeket az eljárásokat az *IBSZ. 3.1.6.1 - személybiztonsági eljárásrend* pontja taglalja.

4. Rendszer és szolgáltatás beszerzés

A rendszer és szolgáltatás beszerzésének lépéseit és követelményeit lásd az *IBSZ 3.1.3 pontjában*

4.1 A rendszer fejlesztési életciklusa

Figyelemmel kell kísérni az informatikai biztonsági helyzetet az elektronikus információs rendszereinek teljes életútján, azok minden életciklusában.

Meg kell határozni és dokumentálni az információbiztonsági szerepköröket és felelősségeket a fejlesztési életciklus egészére. Mindemellett ki kell jelölni az információbiztonsági szerepköröket betöltő, felelős személyeket.

A rendszer életciklus szakaszai a következők:

- Követelmény(ek) meghatározása
- Fejlesztés vagy beszerzés
- Megvalósítás vagy értékelés
- Üzemeltetés és fenntartás
- Kivonás (archiválás, megsemmisítés).

4.2 Funkciók, portok, protokollok, szolgáltatások

A Szervezet megköveteli, hogy a szolgáltatók dokumentáltan határozzák meg a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat.

5. Biztonságelemzési eljárásrend

Az Intézmény folyamatosan figyelemmel kíséri a felügyeleti rendszerek riasztásait, a biztonságot érintő eseményeket.

Hardver és szoftver fejlesztésekről és az infrastruktúrát működtető környezetben történt változásokról évente változásjegyzéket készít. Ilyen változásjelentés az éves informatikai biztonsági audithoz benyújtott releváns változások jegyzéke.

Munkaállomások vírus figyelmeztetéseit a víruskereső központi adminisztrációs rendszerében folyamatosan figyelemmel kíséri.

A spam szűrő szabályokat folyamatosan kiegészíti a spam filter által átengedett kéretlen levelek későbbi sikeres detektálásának érdekében.

A szünetmentes hálózat működését, állapotát folyamatosan figyelemmel kíséri, riasztások esetén a szükséges intézkedéseket megteszi.

Figyelemmel kíséri a szerverek, storage-ok, rendszerek kritikus figyelmeztetéseit és megteszi a szükséges intézkedéseket.

Az éves sérülékenység vizsgálatok által feltárt biztonsági kockázatokat megszünteti.

A biztonsági események ill. nyilvántartások alapján évente összefoglaló jelentést készít.

A szervezet az éves tanúsításokat tekinti biztonsági értékelésnek.

5.1 Biztonsági teljesítmény mérése

Az Intézmény a biztonságelemzési eljárásrendben megfogalmazott változásjelentések alapján évente felmérést készít az elektronikus információs rendszer állapotáról. Esetenként az előző évi adatok kerülnek összehasonlításra az aktuális év adataival.

A felmérés eredményét a következő tényezők befolyásolják pozitív, illetve negatív irányba:

- Hardvereszközök állapota (karbantartottság, új beszerzések)
- Szoftverkörnyezet állapota (frissítések megléte, elavult szoftverek kivezetése)

- Vírusvédelem állapota (munkaállomások vírusvédelmének naprakészsége, kártékony kódok mennyisége)
- Tűzfal állapota (Tűzfal beállításainak naprakészsége, DDoS vagy egyéb támadások átlagos darabszáma)
- Tárolók állapota (szerverek és store-ok hibajelzéseinek fajtája és mennyisége alapján)

A biztonsági teljesítményt a fenti adatokból az Informatikai vezető, illetve az IBF határozza meg.

6. Konfigurációkezelési eljárásrend

Alapkonfiguráció

Az informatikai osztály köteles összeállítani egy olyan alapkonfigurációt, mely képes futtatni azokat az programokat, melyek a munkavégzéshez szükségesek (alapkonfiguráció), e konfiguráció összeállításához javasolt alkalmazni a legnagyobb erőforrás igényű alkalmazás dokumentációja szerint meghatározott minimális hardverösszetételt.

Az alapkonfigurációt külön dokumentumokban rögzíteni kell.

Az alapkonfigurációs beállításokat évente ellenőrizni és felülvizsgálni szükséges.

6.1 Változások, tesztelés, hatásvizsgálat

Amennyiben a konfigurációban változás történik, azt a dokumentáción át kell vezetni.

Az alapkonfigurációt tartalmazó dokumentumok korábbi verzióit meg kell őrizni.

Változáskezelés hatálya alá tartozó tevékenységek:

a) kisebb verzióváltások, a gyártó által kiadott frissítések telepítése;

b) jelentős változással járó verzióváltások, új fejlesztések;

c) rendszerelemek cseréje (hardver/szoftver);

d) a rendszer működésének módosítása, jelentős beavatkozást igénylő hangolások.

A változáskezeléssel kapcsolatosan az alábbi előírásokat kell figyelembe venni:

a) A rendszer bármely funkciójának megváltoztatásához az informatikai vezető engedélye szükséges.

b) A változtatást az kezdeményezi, akinél az igényként felmerül.

d) A tervezett változtatást – a kisebb verzióváltások, a gyártó által kiadott frissítések telepítése kivételével – véleményezés céljából az IBF-nek is meg kell küldeni, aki kockázatelemzéssel megállapítja a változtatás rendszerre gyakorolt hatását.

e) A fejlesztők nem rendelkezhetnek hozzáférési jogokkal az éles informatikai rendszerhez, ezért közvetlenül változtatást sem végezhetnek a rendszeren. A változtatást a rendszer üzemeltetőjének kell elvégezni.

f) A változtatást az éles üzembe való állítás előtt az erre a célra létrehozott tesztkörnyezetben tesztelni kell (Előzetes tesztelés és megerősítés pont).

g) Az éles üzembe állítást csak a változással érintett rendszerek, adatok teljes mentését követően lehet elvégezni.

h) A változtatást munkaidőn kívül kell elvégezni, csak rendkívüli esetben végezhető munkaidőben.

i) Amennyiben a változtatáshoz a rendszer leállítása szükséges, akkor arról az informatikai üzemeltető legalább 1 munkanappal korábban köteles tájékoztatni a felhasználókat.

A változáskezelési folyamatot és a változáskezelési előírások betartását az IBF az éves ellenőrzési tervében foglaltak szerint ellenőrzi.

Az alapkonfiguráció nagyobb volumenű módosítását szükség szerint előzetes tervezésnek kell megelőznie.

Minden olyan esetben, ahol a konfiguráció módosítása hatással lehet a teljesítményre, a hibamentes működésre, az üzembiztonságra, vagy kompatibilitási problémákat vethet fel, előzetes tesztelés szükséges.

Az éles rendszer konfigurációját módosítani csak sikeres előzetes teszteket követően szabad.

6.2 Legszűkebb funkcionalitás

A rendszert úgy kell konfigurálni, hogy az csak az üzemszerű működéshez és munkavégzéshez szükséges szolgáltatásokat nyújtsa.

Ennek érdekében csak a rendszer működéséhez, üzemeltetéséhez és a munkaköri feladatok ellátásához szükséges szoftverek lehetnek telepítve, csak a szükséges szolgáltatások futhatnak és csak a szükséges kommunikációs portok lehetnek nyitva.

Ezen felül kerülendő minden nélkülözhető egyéb szoftver telepítése, szolgáltatás futtatása ill. kommunikációs port megnyitása.

Az elektronikus információs rendszer szervereinek működéséhez szükséges kommunikációs csatornákat és szervizeket dokumentálni kell, változás esetén a módosításokat a dokumentáción is át kell vezetni. Ezt a dokumentációt évente ellenőrizni kell.

6.3 Elektronikus információs rendszerelem leltár

Az információs rendszer hardver és szoftver elemeiről rendszerelem leltárt kell vezetni. Az egyes rendszerelemeket az IBSZ-ben foglaltaknak megfelelő tartalommal kell nyilvántartani. A hardver vagy szoftverváltozásokat a nyilvántartáson folyamatosan át kell vezetni.

A nyilvántartások helyességét időszakosan, szúrópróba-szerűen felül kell vizsgálni, az észlelt eltéréseket pedig korrigálni kell.

Évente, az Intézmény tárgyi eszközeinek leltározása során az információs rendszer elemeket is leltározni kell.

6.4 A szoftver használat korlátozásai

Az előfizetéses licenccel rendelkező szoftverekről (pl. Windows, Office 365, ESET Antivirus) nyilvántartást kell vezetni. Ezen szoftverek használatát szúrópróba-szerűen ellenőrizni kell. A nyilvántartást évente felül kell vizsgálni. A központi adminisztrációs felülettel rendelkező rendszereknél a felhasználók listáját ill. a felhasználás mennyiségét évente felül kell vizsgálni.

Az egyéb telepítési licenckötelés szoftverekről (pl. Total Commander, PicPic, XNView, stb.) nyilvántartást kell vezetni, amelyet telepítés vagy eltávolítás esetén aktualizálni kell.

A munkavégzéshez szükséges, nem licenszköteles segédprogramok (pl. Acrobat Reader, 7-Zip, PDFCreator, ÁNYK, e-Szignó, stb.) illetve a felhasználói bejelentkezéshez kötött rendszerek vastag kliens szoftverei a munkaállomásokra külön nyilvántartás nélkül telepíthetők.

Az informatikára karbantartásra bevitt gépeken szúrópróba-szerűen szoftverellenőrzést kell végrehajtani.

6.5 A felhasználó által telepített szoftverek

Az IBSZ „Szoftverek telepítése, módosítása, törlése" c. fejezetben foglaltaknak megfelelően a munkaállomásokra kizárólag az Informatikai osztály dolgozói jogosultak szoftvert telepíteni. A felhasználók nem rendelkezhetnek a munkaállomáson rendszergazdai jogosultsággal, ezzel technikailag is megakadályozva a felhasználói szoftvertelepítést.

7. Rendszer karbantartás eljárásrend

7.1 Rendszeres karbantartás

A folyamatos működés érdekében az elektronikus információs rendszert a gyártó ajánlása alapján rendszeresen karban kell tartani.

7.1.1 A karbantartások engedélyezése

A tervezett karbantartásokat a terület vezetőjének dokumentált formában kell engedélyeznie. Amennyiben ez az elektronikus információs rendszer leállításával jár, akkor törekedni kell arra, hogy a karbantartás az ügyfélszolgálati nyitvatartási időn kívül legyen elvégezve. Amennyiben ez nem lehetséges, a felhasználókat a karbantartás megkezdése előtt értesíteni szükséges.

7.1.2 A karbantartások dokumentálása, nyilvántartása

Az elvégzett munkákat, valamint a karbantartás tényét nyilván kell tartani. A nyilvántartásba a következő adatokat kell minimálisan rögzíteni:

a) az elvégzett karbantartás megnevezése,

b) az érintett eszközök, szoftverek, elektronikus információs rendszerek,

c) a karbantartás dátuma

7.1.3 A karbantartások ütemezése

Az elektronikus információs rendszer komponenseinek karbantartási feladatait és azok ütemezését külön dokumentumban kell szabályozni.

7.1.4 Kiszállítás

Amennyiben az adatot tartalmazó adathordozó kiszállítása válik szükségessé, akkor az {0. Adathordozók törlése} fejezetben leírtak szerint kell eljárni.

A kiszállítást az informatikai terület vezetője engedélyezi.

7.1.5 A karbantartás ellenőrzése

Az elvégzett karbantartás után az eszköz fajtájától függően funkcionális és biztonsági teszteket kell végezni. Sikertelen teszt esetén az eszköz nem helyezhető újra éles üzembe. Az eseményt jelenteni kell az informatikai terület vezetőjének, aki dönt a további intézkedésekről.

8. Adathordozók védelme

A felhasználók által használt hordozható eszközök (Pendrive, hordozható merevlemez) biztonságos tárolásáért, lopás és elvesztés elleni védelméért a felhasználó felel.

A hordozható eszközökre érzékeny, személyes, titkos adatot másolni tilos a meghajtó teljes titkosítása nélkül.

Hordozható eszközök csak a rajta található adatok végleges és biztonságos megsemmisítését követően selejtezhetők. Az adatok megsemmisítéséről jegyzőkönyvet kell felvenni.

8.1 Hozzáférés az adathordozókhoz

Az érintett szervezet az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, jogosítványuk tartalmát meghatározza.

Az elektronikus információs rendszerrel kapcsolatban csak az Intézmény tulajdonában lévő, regisztrált adathordozót lehet használni. Adathordozó igénylését az informatikai terület vezetőjéhez kell benyújtania a szervezeti egység vezetőjének.

Az eszközhasználatot, az elektronikus információs rendszerhez történő csatlakoztatása után, az Intézmény minden előzetes értesítés nélkül figyelheti, monitorozhatja.

Otthoni munkavégzés és bármilyen más célból bármilyen adatot CD-n, elektronikus levélben vagy egyéb más módon (Pl.: Pendrive) az elektronikus információs rendszerből kijuttatni csak az Adatgazda írásos engedélyével szabad. Az adatok kivitelét írásos formában kell engedélyezni.

Az Intézmény az adathordozók használatát információbiztonsági megfontolásból hardver, illetve szoftver úton korlátozhatja.

8.2 Adathordozók törlése

Az infokommunikációs eszközök újrahasznosítása, vagy mások rendelkezésre bocsátása előtt minden esetben gondoskodni kell arról, hogy az elektronikus információs rendszer adathordozóin tárolt információk visszaállíthatatlanul eltávolításra kerüljenek. Ennek érdekében

a) a rajtuk tárolt adatokat törölni kell;

b) a törlést az adattárolón lévő adatok gazdájának jóvá kell hagynia;

c) 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.

9. Azonosítás és hitelesítés

A megbízható azonosítás kulcsfontosságú, és kizárólag informatikai eszközökkel történhet. A pontos és hiteles azonosításnak a bizalmasság szempontjából nélkülözhetetlen.

Felhasználói azonosítást és hitelesítést kell alkalmazni a jogosulatlan személyek tevékenységének megakadályozása és az elszámoltathatóság megvalósítása érdekében.

Az elektronikus információs rendszerhez történő hozzáférések során a hozzáférők megfelelő szintű azonosítása és hitelesítése érdekében a jelen eljárásrendben foglaltak szerint kell eljárni.

9.1 Azonosítás és hitelesítés (belső felhasználók)

Az elektronikus információs rendszernek egyedileg kell azonosítania és hitelesítenie az Intézmény valamennyi belső felhasználóját és a belső felhasználók által végzett tevékenységeket.

Ennek érdekében az elektronikus információs rendszer rendszerdokumentációjában meghatározott névkonvenció alapján egyénre szóló felhasználói azonosítókat kell képezni, a csoportos azonosítók használata nem engedélyezett.

9.1.1 Hozzáférés privilegizált fiókokhoz

Az elektronikus információs rendszer fejlesztőjének és támogatójának, valamint az Intézmény rendszergazdáinak, azaz minden privilegizált hozzáféréssel rendelkező felhasználónak helyi hálózaton kívülről csak kétfaktoros azonosítással biztosítható hozzáférés a támogatási, hibaelhárítási, valamint üzemeltetési feladatok elvégzéséhez.

Ezen engedélyeket, illetve a technikai megvalósítását külön dokumentumban részletezni szükséges.

9.1.2 Azonosító kezelés

Az azonosítókat az informatikai terület rendszergazdái kezelik. Az azonosítókat úgy kell létrehozni, hogy az azonosítók egyértelműen hozzá legyenek rendelve a kívánt egyénhez, csoporthoz vagy eszközhöz.

A kiadott, majd megszűnt azonosítók ismételten nem használhatók fel (pl. új felhasználó nem kaphatja meg egy korábban megszűnt felhasználó azonosítóját, névazonosság esetén sem.)

Az elektronikus információs rendszer egy hónapnyi inaktivitás után tiltsa le az azonosítót.

9.1.3 A hitelesítésre szolgáló eszközök kezelése

A hitelesítésre szolgáló eszközök (továbbiakban: a jelszavak) a felhasználó számítógépes szolgáltatásokhoz való hozzáférési jogosultságának hitelesítésére szolgálnak. A jelszókezelő rendszernek hatékonyan és interaktívan kell biztosítania a megfelelő színvonalú jelszavak használatát.

A munkaállomás jelszókezelő rendszere:

a) tegye lehetővé a felhasználók számára jelszavuk kiválasztását és megváltoztatását;

b) kényszerítse ki az ideiglenes jelszavak megváltoztatását az első bejelentkezéskor;

c) kötelező megfelelő minőségű jelszavak használata, a jelszó legalább nyolc karakter hosszú legyen, és tartalmazzon a kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;

d) a jelszavakat 180 naponta meg kell változtatni;

e) a jelszavakat két napon belül nem szabad megváltoztatni;

f) tiltsa meg a korábban használt jelszavak ismételt felhasználását (utolsó 10);

g) 5 sikertelen próbálkozás után zárolja a bejelentkezést, majd előre beállított időtartam (15 perc) eltelte után engedélyezze vissza a felhasználói fiókot;

h) beíráskor ne jelenítse meg a jelszavakat a képernyőn;

i) a jelszavakat megfelelő rejtjelezéssel tárolja;

Az elektronikus információs rendszer jelszókezelő rendszere:

a) tegye lehetővé a felhasználók számára jelszavuk kiválasztását és megváltoztatását;

b) kényszerítse ki az ideiglenes jelszavak megváltoztatását az első bejelentkezéskor;

c) kényszerítse ki a megfelelő minőségű jelszavak használatát, a jelszó legalább nyolc karakter hosszú legyen, és tartalmazzon a kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;

d) a jelszavakat 180 naponta meg kell változtatni;

e) a jelszavakat két napon belül nem szabad megváltoztatni;

f) tiltsa meg a korábban használt jelszavak ismételt felhasználását (utolsó 10);

g) 3 sikertelen próbálkozás után zárolja a bejelentkezést, majd előre beállított időtartam (10 perc) eltelte után engedélyezze vissza a felhasználói fiókot;

h) beíráskor ne jelenítse meg a jelszavakat a képernyőn;

i) a jelszavakat megfelelő rejtjelezéssel tárolja;

Az elektronikus információs rendszerhez tartozó szerverek adminisztratív jelszavainak kezelése:

a) kötelező megfelelő minőségű jelszavak használata, a jelszó legalább nyolc karakter hosszú legyen, és tartalmazzon a kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;

b) a jelszavakat 180 naponta meg kell változtatni;

c) a jelszavakat két napon belül nem szabad megváltoztatni;

d) tiltsa meg a korábban használt jelszavak ismételt felhasználását (utolsó 10);

e) belíráskor ne jelenítse meg a jelszavakat a képernyőn;

f) a jelszavakat megfelelő rejtjelezéssel tárolja;

g) a jelszavakat illetéktelenek elől titokban kell tartani

h) a jelszavakat tilos mások által könnyen hozzáférhető helyen tárolni

i) a felhasználói neveket és jelszavakat zárt borítékban, páncélszekrényben el kell helyezni

A felhasználó felelősségi köre a jelszó használat során

Az elektronikus információs rendszerben a jelszavak használatának és képzésének részletes szabályai a következők:

a) Az azonosítókat a kijelölt rendszergazda hozza létre oly módon, hogy kezdeti jelszót állít be a fiók részére.

b) biztosítani kell, hogy a kezdeti jelszavak is biztonságos körülmények között kerüljenek a felhasználóknak átadásra.

c) A jelszót az első bejelentkezéskor meg kell változtatni.

d) a felhasználó a jelszavát köteles titokban tartani;

e) a jelszószabályok betartása minden felhasználónak jól felfogott érdeke. A felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el az elektronikus információs rendszerben;

f) a felhasználó nem tárolhatja jelszavait mások által hozzáférhető helyen ill. módon, így különösen tilos a jelszavakat papíron, a munkaállomás közelében tárolni (monitor, asztal, fiók, stb.);

g) ha bármilyen jel mutat arra, hogy a jelszó illetéktelen kézbe jutott, azonnal meg kell változtatni és értesíteni kell a rendszergazdát és az IBF-et;

h) nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé, pl. makróra, vagy funkció billentyűre;

i) a jelszó minél komplexebb, annál kisebb a valószínűsége, hogy nevünkben visszaélést követnek el. Ennek érdekében az alábbi szempontokat kell betartani:

j) könnyen megjegyezhető, és nehezen kitalálható legyen;

k) semmi olyasmin ne alapuljon, aminek alapján valaki kitalálhatja, ilyenek a nevek, telefonszámok, születési dátumok, stb.;

l) ne legyen a gépnévre vagy a felhasználói névre utaló;

m) ne legyen sorozat (pl.: 12345678, abcdefgh, asdfghjk)).

A fenti szabályok közül az elektronikus információs rendszer által technikailag is kikényszeríthető részét a rendszergazdának kell beállítani.

A felhasználó felelőssége, ha jelszavának neki felróható mulasztása miatti megismerése révén valaki a nevében visszaélést követ el az elektronikus információs rendszerben.

Az elektronikus információs rendszerhez történő hozzáférés során alkalmazott jelszavak idegen kézbe kerülése, illetve a jelszószabályok be nem tartása biztonsági incidensnek minősül, ezért ezekben az esetekben az Informatikai Biztonsági Szabályzatban (IBSZ) leírtak szerint kell eljárni.

Inaktivitás és munkaállomás elhagyása

A munkaállomásokat úgy kell beállítani, hogy max. 10 perc inaktivitás után automatikusan jelszavas képernyővédőre kapcsoljon.

A felhasználó köteles a felügyelet nélkül hagyott, bekapcsolt munkaállomást zárolni.

Az a felhasználó, aki 90 napig nem lép be azonosítójával a rendszerbe, felfüggesztett/inaktív státuszba kerül. Csak abban az esetben léphet be újra a rendszerbe, ha az informatikai vezető engedélyével a rendszergazda újra aktív státuszba helyezi.

9.1.4 A hitelesítésre szolgáló eszköz visszacsatolása

Az elektronikus információs rendszerben alkalmazott hitelesítésre szolgáló eszköz hibás azonosító vagy jelszó megadása esetén csak olyan hibaüzenetet adhat vissza, melyből nem szerezhető további információ sem az azonosító, sem a jelszó összetételéről.

9.1.5 Hitelesítés kriptográfiai modul esetén

Az elektronikus információs rendszer az AD-ban hitelesített felhasználókat használja a rendszerben való azonosításra, nem használ saját kriptográfiai hitelesítő modult.

9.2 Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

Az elektronikus információs rendszernek egyedileg kell azonosítania és hitelesítenie a szervezeten kívüli felhasználókat és az általuk végzett tevékenységeket.

Ennek érdekében az elektronikus információs rendszer rendszerdokumentációjában meghatározott névkonvenció alapján egyénre szóló felhasználói azonosítókat kell képezni, a csoportos azonosítók használata nem engedélyezett.

A szervezeten kívüli felhasználók tevékenységét a *{12. Rendszer és* **információ sértetlenségre vonatkozó eljárásrend**

Az elektronikus információs rendszer megfelelő működésének biztosítása érdekében gondoskodni kell a feltárt funkcionális és biztonsági hibák kijavításáról, a kártékony kódok elleni megfelelő védelemről valamint a kibertámadások elleni védekezésről.

11.1 Hibajavítás

A felhasználók az észlelt hardver és szoftver hibákat azonnal kötelesek az üzemeltető felé e-mailen, telefonon vagy személyesen jelezni.

A hibabejelentésnek tartalmaznia kell az alábbiakat:

- Esemény megnevezése (hiba leírása)
- A hibával érintett rendszerelem megnevezése
- A hiba ideje
- A hiba felfedezésekor használt alkalmazás, megnyitott állományok, adatbázisok pontos megnevezése
- Az esemény kapcsán közvetve érintett felhasználók felsorolása, behatárolása

Az informatika a hiba súlyosságának, a hiba által akadályozott tevékenység fontosságának, valamint az elvégzendő feladatok prioritásának figyelembevételével megkezdi a hatáskörébe eső hiba elhárítását.

Az Elektronikus információs rendszer olyan hibáit, amelyek egyértelműen a szoftver üzleti logikájának hibájára vezethetők vissza, a megfelelő jogosultsággal rendelkező felhasználóknak a szoftvergyártó webes igénybejelentő rendszerében kell rögzíteni. Egyéb alkalmazói szoftverek hibája esetén az adott szoftverhez rendelt bejelentési csatornákon, a kijelölt adat- ill. rendszergazdával közreműködve kell értesíteni a szoftver szállítóját.

Az Elektronikus információs rendszer hibáinak kijavításához a szoftver gyártója javítócsomagokat ad ki.

A javítócsomagok telepítését először a teszt rendszerben kell elvégezni, majd tesztelni. Éles rendszerben a telepítés csak sikeres tesztelés után végezhető el. Az éles rendszerre történő telepítést az adatgazda hagyja jóvá.

Az Elektronikus információs rendszer futtató környezetéhez, úgy, mint operációs rendszer, adatbázis szerver, stb. kiadott biztonsági és hibajavító csomagokat először a teszt rendszerre kell telepíteni és ott tesztelni. Éles rendszerben a telepítés csak sikeres tesztelés után végezhető el. Ezen javítások és frissítések telepítését a „IBSzoftverfrissítés" c. dokumentumban meghatározott módon és gyakorisággal kell elvégezni.

11.2 Kártékony kódok elleni védelem

Az elektronikus információs rendszert védeni kell a kártékony kódok ellen. Ennek érdekében mind a munkaállomásokra, mind a szerverekre vírusvédelmi rendszert kell telepíteni és azt üzemeltetni.

A vírusvédelmi rendszernek rezidens módon kell futnia, az operációs rendszer betöltésekor automatikusan el kell indulnia és már a rendszer komponensek betöltését is ellenőriznie kell.

A vírusvédelmi rendszernek ellenőriznie kell a webes és az e-mail forgalmat, továbbá ellenőrzést kell végrehajtania a helyi vagy hálózati megosztásokon található fájlokon, amikor azokat a felhasználók vagy szoftverek letöltik, megnyitják, futtatják vagy kimentik. A vírusvédelmi szoftvernek kártékony kód észlelésekor automatikusan blokkolni kell a file

letöltését, megnyitását vagy futtatását és ezzel egyidejűleg karanténba kell helyeznie és törölni kell a kártékony kódot. Az ilyen eseményeket a vírusvédelmi rendszernek naplóznia kell.

A beállítások jelszavas védelmével biztosítani kell, hogy a felhasználók a vírusvédelmi rendszert ne tudják kiiktatni ill. beállításait módosítani. A hatékony védelemhez a vírusvédelmi rendszert folyamatosan, automatikusan frissíteni kell.

11.3 Az elektronikus információs rendszer felügyelete

Az elektronikus információs rendszert védeni kell a kibertámadások ellen. Ennek érdekében a hálózat külső határain önálló behatolás-védelmi rendszert kell üzemeltetni. A behatolás-védelmi rendszeren a működést még éppen biztosító, legszigorúbb beállításokat, tűzfal szabályokat kell alkalmazni.

A behatolás-védelmi rendszer által gyűjtött naplókat rendszeresen ellenőrizni kell. Szükség esetén erősíteni kell a rendszer felügyeletét, amennyiben fokozott kockázatra utaló jelek észlelhetők.

Amennyiben lehetséges, a belső eszközökön, szervereken és munkaállomásokon szintén aktiválni kell az eszköz saját tűzfal szolgáltatását.

A határvédelmi eszközökről érkező riasztásokat a szolgáltató kapja, e-mailen tájékoztatja a Szervezetet.

11.4 Biztonsági riasztások és tájékoztatások

Az informatika az illetékes hatóságok informatikai biztonsági riasztásait, ill. az informatikai szakportálokon megjelenő biztonsági figyelmeztetéseket folyamatosan nyomon követi és a szükséges intézkedéseket megteszi.

folyamatosan nyomon követi a kormányzati eseménykezelő központ ill. a NEIH által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket, valamint az informatikai szakportálokon megjelenő biztonsági figyelmeztetéseket.

Szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki valamint megteszi a megfelelő ellenintézkedéseket és válaszlépéseket.

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

Naplózási eljárásrend/ fejezetben foglaltak szerint naplózni szükséges.

Hitelesítés szolgáltatók tanúsítványának elfogadása

Amennyiben az érintett szervezeten kívüli felhasználókat tanúsítvány felhasználásával hitelesíti az Intézmény, a hitelesítéséhez az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatja el.

10. Hozzáférés ellenőrzés

10.1 Felhasználói fiókok kezelése

Az elektronikus információs rendszerben a következőkben leírtak szerint kell a felhasználói fiókokat kezelni:

10.1.1 Fióktípusok

Az elektronikus információs rendszerhez az alábbi fő fióktípusokkal lehet hozzáférni:

a) Korlátozott felhasználó,

b) Adminisztrátor.

Az Intézmény munkatársai által használt felhasználói fiókokat a *{0. 10.1.4* Hozzáférési jogok igénylése*}* eljárásrendben leírtaknak megfelelően a rendszergazdák kezelik.

10.1.2 Szerepkörök

Az elektronikus információs rendszerben a feladatellátástól függően a következő fő szerepkörök kerültek kialakításra:

a) Behajtás, közműfejlesztés

b) Behajtás, közműfejlesztés (kiemelt szerepkör)

c) Értékesítés

d) Ügyfélszolgálat, ügyvitel

e) Tömeges számlázás

f) Pénztáros

g) Rendszer adminisztrátor

10.1.3 Tagsági feltételek

A tagsági feltételek a munkatársak szervezeti tagsága, ill. munkaköri feladatai alapján kerülnek kialakításra.

10.1.4 Hozzáférési jogok igénylése

Az elektronikus információs rendszerhez történő új hozzáférést, meglévő hozzáférési jog módosítását, illetve hozzáférési jog visszavonását a jelen fejezetben leírt eljárásrend alapján kell igényelni.

10.1.5 Új hozzáférés igénylése

Amennyiben az Intézménynél új jogosultsági igény keletkezik, az Informatikai Biztonsági adatlapok között található Jogosultságkezelési igénylőlapot kell kitölteni. Az ellenőrzött tartalmú adatlapot a munkahelyi vezető jóváhagyja, a rendszer adatgazdájával engedélyezteti, majd a rendszergazdai jogosultsággal rendelkező felelősnek eljuttatja. A kitöltött jogosultság igénylőlapnak tartalmaznia kell a felhasználó közvetlen felettese és az adatgazda aláírását, a

kért jogosultság leírását szerepkörrel vagy egyéb módon. A jogosultság kiosztása előtt meg kell győződni arról, hogy a jóváhagyó személy jogosult volt-e az engedély továbbítására.

A jogosultság beállításának megtörténtét a rendszergazda az adatlapon aláírásával igazolja.

Az aláírt adatlapok ezek után az informatikai osztályon kerülnek tárolásra.

Az IBF az említett adatlapok meglétét és a tényleges jogosultság kiadását bármikor ellenőrizheti, és véleményét írásba foglalhatja, amelyet az Intézmény a jogosultsági rendjének folyamatos javítására használ fel.

10.1.6 Hozzáférési jogok módosítása

Amennyiben egy munkavállaló jogosultságainak módosítása válik szükségessé, akkor - az új jogosultság igényléséhez hasonló módon - Jogosultságkezelési igénylőlapot kell kitölteni. Az igénylőlapon jelölni kell, hogy mely jogosultságokat kell megszüntetni, ill. a meglévő jogosultságokat milyen jogosultságokkal kell bővíteni. A jogosultság módosításának eljárásrendje egyéb tekintetben megegyezik az *(10.1.5. 10.1.5* Új hozzáférés igénylése*)* pontban leírt eljárásenddel.

10.1.7 Hozzáférési jogok visszavonása

10.1.7.1 Hozzáférési jogok visszavonása feladatkör vagy munkakör változás esetén:

A munkavállaló feladatkörének vagy munkakörének változás esetén a munkahelyi vezetőnek haladéktalanul intézkednie kell a már nem szükséges jogosultságok visszavonása iránt. Ez esetben is - az új jogosultság igényléséhez hasonló módon – a Jogosultságkezelési igénylőlapot kell kitölteni. Az igénylőlapon jelölni kell, hogy mely jogosultságokat kell megszüntetni. A jogosultságok részleges visszavonásának eljárásrendje egyéb tekintetben megegyezik az új jogosultsági igény eljárásendjével.

A munkahelyi vezetőnek haladéktalanul intézkednie kell a már nem szükséges jogosultságok visszavonása iránt. Amennyiben a hozzáférési jogok részleges visszavonására van szükség, abban az esetben a hozzáférési jog módosítása eljárásrend szerint kell eljárni.

10.1.7.2 Hozzáférési jogok visszavonása rendes felmondás esetén:

Ha az Intézmény alkalmazottjának munkaviszonya, „rendes" felmondás keretein belül megszűnik, erről a tényről a közvetlen felettesének, illetve a felmondást aláíró vezetőnek haladéktalanul tájékoztatást kell nyújtania az informatikai osztálynak. Az informatikai osztály a jelzett időponttal gondoskodik a felhasználó összes rendszerhozzáférésének adott időpontban történő megszüntetéséről vagy letiltásáról, illetve ezek kezdeményezéséről. Az eljárás megtörténtéről az informatikai osztály tájékoztatja a munkaügyi szervezeti egységet. A munkaviszonyt lezáró dokumentumok között szerepeltetni kell a jogosultságok megszűnéséről szóló tájékoztatást, ebben integráltan egy figyelmeztetést a jogosulatlan belépés, vagy annak kísérletének jogi következményeiről.

10.1.7.3 Hozzáférési jogok visszavonása rendkívüli felmondás esetén:

Amennyiben a munkavállaló munkaviszonya „rendkívüli" felmondással kerül megszüntetésre, akkor jogosultságainak megszüntetéséről haladéktalanul gondoskodni kell.

Ennek érdekében a felmondást aláíró vezetőnek haladéktalanul tájékoztatnia kell az informatikai osztályt. Az informatikai osztály tájékoztatásáért egyetemlegesen felel a felmondást szignáló személy és a munkaügyi ügyintéző. Az informatikai osztálynak haladéktalanul gondoskodnia kell az illetéktelen hozzáférés megakadályozásáról. A munkavállalónak azonnal írásos tájékoztatást kell kapnia jogosultságai megszűnéséről, és a belépési kísérletek következményeiről.

10.1.8 Felhasználói fiókok felülvizsgálata

Az Intézmény által létrehozott felhasználói fiókokat időszakosan, de legalább évente egy alkalommal felül kell vizsgálni.

A felülvizsgálat lépései:

- a jogosultak munkaviszonyának ellenőrzése
- a jogosultságok munkakörrel indokoltságának áttekintése

10.1.9 Hozzáférés ellenőrzés érvényesítése

Az elektronikus információs rendszert fel kell készíteni a jelen eljárásrendben foglalt hozzáférés ellenőrzési követelmények alapján a hozzáférések érvényre juttatására.

10.2 Sikertelen bejelentkezési kísérletek

A munkaállomásoknak a következő fiókzárolási házirendet kell alkalmaznia sikertelen bejelentkezési kísérletek esetén:

Szabály megnevezése	Beállított érték
Fiókzárolási küszöb	5 sikertelen próbálkozás
Fiókzárolás időtartama	15 perc

Az elektronikus információs rendszernek a következő fiókzárolási házirendet kell alkalmaznia sikertelen bejelentkezési kísérletek esetén:

Szabály megnevezése	Beállított érték
Fiókzárolási küszöb	3 sikertelen próbálkozás
Fiókzárolás időtartama	10 perc

A rendszerhasználat jelzése *(3.3.10.8.)*

Az elektronikus információs rendszer elindításakor – még az azonosítási és hitelesítési folyamat megkezdése előtt – tájékoztatni kell a felhasználókat a következőkről:

- a felhasználó az Intézmény elektronikus információs rendszerét használja;
- a rendszer használatot az Intézmény figyeli, rögzíti, naplózza;
- a rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással jár;

- a rendszer használatával a felhasználó elfogadja és tudomásul veszi a fentieket és a Felhasználói Informatikai Biztonsági Házirendbe foglaltakat is.

A figyelmeztető üzenetet mindaddig a képernyőn kell tartani, amíg a felhasználó közvetlen műveletet nem végez az elektronikus információs rendszerbe való bejelentkezéshez vagy további rendszer hozzáféréshez.

10.3 Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

Az elektronikus információs rendszerben nem engedélyezettek az azonosítás és hitelesítés nélkül végzett tevékenységek.

10.4 Távoli hozzáférés

Az elektronikus információs rendszerhez a következő módon engedélyezett a felhasználói távoli hozzáférés:

Az erre jogosult felhasználók a VPN kapcsolat felépítése után a saját munkahelyi számítógépükön keresztül, Távoli asztal (RDP) útján érhetik el a vízdíjszámlázási (Libra) rendszert.

Minden személy, aki az elektronikus információs rendszerhez hozzáfér, legyen az fejlesztő, támogató, az Intézmény rendszergazdája, vagy munkavállalója, a távoli elérés kizárólag kétfaktoros azonosítással biztosítható mind a támogatási, hibaelhárítási, valamint üzemeltetési és munkafolyamatok/ feladatok elvégzéséhez.

Távoli elérés kialakítását az informatikai osztályvezetőnek kell engedélyeznie, jóváhagynia. A kialakított távoli elérések (VPN kapcsolatok) technikai megvalósítását, valamint a kapcsolat felépítésére vonatkozó engedélyeket külön dokumentumban részletezni szükséges. VPN kapcsolat csak olyan partner ill. belső felhasználó számára biztosítható, aki a VPN kapcsolatok dokumentációban engedélyezettként szerepel. A VPN kapcsolatok felépítésének naplózását a rendszerekben aktiválni kell.

10.5 Vezeték nélküli hozzáférés

Az elektronikus információs rendszerhez nem engedélyezett a vezeték nélküli hozzáférés. Amennyiben a későbbiekben ez felmerül, akkor az IBF bevonásával ki kell dolgozni annak technikai megvalósítását, a felhasználás feltételeit, korlátait és az engedélyezési folyamatot.

10.6 Mobil eszközök hozzáférés ellenőrzése

Az elektronikus információs rendszerhez nem engedélyezett a mobil eszközökkel történő hozzáférés. Amennyiben a későbbiekben ez felmerül, akkor az IBF bevonásával ki kell dolgozni annak technikai megvalósítását, a felhasználás feltételeit, korlátait és az engedélyezési folyamatot.

10.7 Külső elektronikus információs rendszerek használata

Az elektronikus információs rendszerhez nem engedélyezett a külső elektronikus információs rendszerből történő felhasználói hozzáférés. Amennyiben ez a későbbiekben felmerül, akkor az IBF bevonásával ki kell dolgozni, hogy milyen feltételek és szabályok betartása mellett jogosult a felhasználó egy külső rendszerből hozzáférni az elektronikus információs rendszerhez, valamint meg kell határozni, hogy külső elektronikus információs rendszerek segítségével

hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani az Intézmény által ellenőrzött információkat.

10.8 Nyilvánosan elérhető tartalom

Az elektronikus információs rendszer nem tesz közzé nyilvánosan elérhető tartalmakat. Amennyiben a későbbiekben ez felmerül, akkor IBF bevonásával ki kell dolgozni a közzététel folyamatát, technikai megvalósítását és az engedélyezési folyamatot.

11. Rendszer és információ sértetlenségre vonatkozó eljárásrend

Az elektronikus információs rendszer megfelelő működésének biztosítása érdekében gondoskodni kell a feltárt funkcionális és biztonsági hibák kijavításáról, a kártékony kódok elleni megfelelő védelemről valamint a kibertámadások elleni védekezésről.

11.1 Hibajavítás

A felhasználók az észlelt hardver és szoftver hibákat azonnal kötelesek az üzemeltető felé e-mailen, telefonon vagy személyesen jelezni.

A hibabejelentésnek tartalmaznia kell az alábbiakat:

- Esemény megnevezése (hiba leírása)
- A hibával érintett rendszerelem megnevezése
- A hiba ideje
- A hiba felfedezésekor használt alkalmazás, megnyitott állományok, adatbázisok pontos megnevezése
- Az esemény kapcsán közvetve érintett felhasználók felsorolása, behatárolása

Az informatika a hiba súlyosságának, a hiba által akadályozott tevékenység fontosságának, valamint az elvégzendő feladatok prioritásának figyelembevételével megkezdi a hatáskörébe eső hiba elhárítását.

Az Elektronikus információs rendszer olyan hibáit, amelyek egyértelműen a szoftver üzleti logikájának hibájára vezethetők vissza, a megfelelő jogosultsággal rendelkező felhasználóknak a szoftvergyártó webes igénybejelentő rendszerében kell rögzíteni. Egyéb alkalmazói szoftverek hibája esetén az adott szoftverhez rendelt bejelentési csatornákon, a kijelölt adat- ill. rendszergazdával közreműködve kell értesíteni a szoftver szállítóját.

Az Elektronikus információs rendszer hibáinak kijavításához a szoftver gyártója javítócsomagokat ad ki.

A javítócsomagok telepítését először a teszt rendszerben kell elvégezni, majd tesztelni. Éles rendszerben a telepítés csak sikeres tesztelés után végezhető el. Az éles rendszerre történő telepítést az adatgazda hagyja jóvá.

Az Elektronikus információs rendszer futtató környezetéhez, úgy, mint operációs rendszer, adatbázis szerver, stb. kiadott biztonsági és hibajavító csomagokat először a teszt rendszerre kell telepíteni és ott tesztelni. Éles rendszerben a telepítés csak sikeres tesztelés után végezhető

el. Ezen javítások és frissítések telepítését a „IBSzoftverfrissítés" c. dokumentumban meghatározott módon és gyakorisággal kell elvégezni.

11.2 Kártékony kódok elleni védelem

Az elektronikus információs rendszert védeni kell a kártékony kódok ellen. Ennek érdekében mind a munkaállomásokra, mind a szerverekre vírusvédelmi rendszert kell telepíteni és azt üzemeltetni.

A vírusvédelmi rendszernek rezidens módon kell futnia, az operációs rendszer betöltésekor automatikusan el kell indulnia és már a rendszer komponensek betöltését is ellenőriznie kell.

A vírusvédelmi rendszernek ellenőriznie kell a webes és az e-mail forgalmat, továbbá ellenőrzést kell végrehajtania a helyi vagy hálózati megosztásokon található fájlokon, amikor azokat a felhasználók vagy szoftverek letöltik, megnyitják, futtatják vagy kimentik. A vírusvédelmi szoftvernek kártékony kód észlelésekor automatikusan blokkolni kell a file letöltését, megnyitását vagy futtatását és ezzel egyidejűleg karanténba kell helyeznie és törölni kell a kártékony kódot. Az ilyen eseményeket a vírusvédelmi rendszernek naplóznia kell.

A beállítások jelszavas védelmével biztosítani kell, hogy a felhasználók a vírusvédelmi rendszert ne tudják kiiktatni ill. beállításait módosítani. A hatékony védelemhez a vírusvédelmi rendszert folyamatosan, automatikusan frissíteni kell.

11.3 Az elektronikus információs rendszer felügyelete

Az elektronikus információs rendszert védeni kell a kibertámadások ellen. Ennek érdekében a hálózat külső határain önálló behatolás-védelmi rendszert kell üzemeltetni. A behatolás-védelmi rendszeren a működést még éppen biztosító, legszigorúbb beállításokat, tűzfal szabályokat kell alkalmazni.

A behatolás-védelmi rendszer által gyűjtött naplókat rendszeresen ellenőrizni kell. Szükség esetén erősíteni kell a rendszer felügyeletét, amennyiben fokozott kockázatra utaló jelek észlelhetők.

Amennyiben lehetséges, a belső eszközökön, szervereken és munkaállomásokon szintén aktiválni kell az eszköz saját tűzfal szolgáltatását.

A határvédelmi eszközökről érkező riasztásokat a szolgáltató kapja, e-mailen tájékoztatja a Szervezetet.

11.4 Biztonsági riasztások és tájékoztatások

Az informatika az illetékes hatóságok informatikai biztonsági riasztásait, ill. az informatikai szakportálokon megjelenő biztonsági figyelmeztetéseket folyamatosan nyomon követi és a szükséges intézkedéseket megteszi.

folyamatosan nyomon követi a kormányzati eseménykezelő központ ill. a NEIH által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket, valamint az informatikai szakportálokon megjelenő biztonsági figyelmeztetéseket.

Szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki valamint megteszi a megfelelő ellenintézkedéseket és válaszlépéseket.

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

12. Naplózási eljárásrend

Az elektronikus információs rendszereknél a következő naplózási eljárásrendet kell kialakítani.

12.1 Naplózható események

12.1.1 Elektronikus információs rendszer naplózása

Biztosítani kell, hogy az elektronikus információs rendszer a következő eseményeket naplózni tudja:

a) a felhasználók adminisztrációs tevékenysége:
   I. bejelentkezés;
   II. kijelentkezés;
   III. jelszómódosítás.
b) adatok módosítása a rendszerben;
c) a rendszergazdák a rendszer bármely rétegébe történő be-és kijelentkezése;
d) a rendszergazdák tevékenysége a rendszer bármely rétegében;
e) a felhasználói jogosultságok módosítása;
f) rendszer események, esetleges hibák;

12.1.2 Szerver operációs rendszer naplózása

Elektronikus információs rendszer szerver operációs rendszerein az operációs rendszer alábbi standard naplóinak működnie kell:

Application, Security, Setup, System

12.1.3 Munkaállomás operációs rendszer naplózása

Az Elektronikus információs rendszert használó munkaállomások operációs rendszerein az operációs rendszer alábbi standard naplóinak működnie kell:

Alkalmazás, Biztonság, Rendszer

12.1.4 Adatbázis kezelő rendszer naplózása

A medikai rendszerek adatbázis kezelő rendszerében az SQL szerver standard naplózásainak működnie kell.

A naplózási beállításokat az IBF évente felülvizsgálja annak érdekében, hogy elengedőek-e a biztonsági események kivizsgálásához.

12.2 Naplóbejegyzések tartalma

Az elektronikus információs rendszert úgy kell kialakítani, hogy a naplóbejegyzésekben gyűjtsön be elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

12.3 Napló tárkapacitás

A naplók tárkapacitását az elektronikus információs rendszer fejlesztőjének a bevonásával az előzetes kapacitástervezési folyamat során kell kialakítani.

Az operációs rendszer naplóit tároló köteten a szabad kapacitás nem csökkenhet 1GB alá.

Az elektronikus információs rendszer naplóit tartalmazó köteten a szabad kapacitás nem csökkenhet 5GB alá.

A szabad kapacitás ill. a napló tárkapacitás figyelését az elektronikus információs rendszerek felügyeleti tevékenységébe kell beépíteni.

Biztosítani kell a naplóbejegyzések felülírásának megakadályozását. Az elektronikus információs rendszer a napló felülírását az alábbi módon előzi meg:

Minden nap egy új naplófájl nyílik.

A régi naplófájl <fájlnév>-<YYYY-mm-dd>.log néven átmozgatásra kerül egy dedikált '_archive' alkönyvtárba.

Az aktuális napot megelőző két napnál régebbi átmozgatott naplófájlok betömörítésre kerülnek egy frlog-<YYYY-mm-dd>.zip nevű fájlba.

Az összes régi naplófájl megmarad, törlés nem történik."

12.4 Naplózási hiba kezelése

Az elektronikus információs rendszer naplóinak a figyelését oly módon kell kialakítani, hogy naplózási hiba esetén küldjön riasztást a rendszert üzemeltető rendszergazdáknak.

Naplózási hiba esetén a rendszergazdáknak ill. az elektronikus információs rendszer támogatójának meg kell határozni a hiba kiváltó okát, majd a hibát meg kell szüntetni.

12.5 Naplóvizsgálat és jelentéskészítés

Az elektronikus információs rendszer eseménynaplóit és biztonsági naplóit a rendszergazdának a heti üzemeltetési feladatok során át kell vizsgálni, az IBF-nek pedig legalább félévente.

A hibabejegyzéseket és a szokatlan működésre utaló jeleket meg kell vizsgálni és a hiba elhárításához szükséges lépéseket meg kell tenni.

Főbb hibaesemények kezelése:

- Számázási szoftver naplókban talált hibák: a hiba a szoftver fejlesztőjének jelentendő
- Adatbázis-kezelő alertekben adott hibák:
    - Mentéssel, tárkapacitással kapcsolatos hibákat üzemeltető kezeli,
    - A rendszergazdai hatáskörben nem kezelhető hibák a szoftver fejlesztőjének jelentendők

- Operációs rendszer naplókban talált hibákat üzemeltető kezeli, a rendszergazdai hatáskörben nem kezelhető hibákat informatikai vezetőnek jelenteni kell
- Infrastruktúrához kapcsolódó hibák: az adott infrastruktúra elem karbantartására szerződött szolgáltatónak jelentendők

A biztonsági eseményre utaló jeleket a biztonsági incidensek kezelésének megfelelő módon kell kezelni és jelenteni.

12.6 Időbélyegek

Az elektronikus információs rendszernek valamennyi naplóbejegyzését időbélyeggel kell ellátnia, melyhez a rendszerórát kell alapul vennie.

Az elektronikus információs rendszert úgy kell kialakítani, hogy hálózati időszinkron protokoll segítségével szinkronizálja a rendszerórákat az egyezményes koordinált világidőhöz.

12.7 A naplóinformációk védelme

Az elektronikus információs rendszert jelen eljárásrendben foglalt logikai védelmi intézkedések felhasználásával úgy kell kialakítani, hogy a naplóinformációk védettek legyenek a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

12.8 A naplóbejegyzések megőrzése

A naplóinformációk mentését be kell vonni az Intézmény mentési rendszerébe. A mentéseket összhangban a napló tárkapacitással úgy kell kialakítani, hogy a naplóbejegyzések nem veszhetnek el.

A naplóinformációkat biztonsági események utólagos kivizsgálása érdekében 5 évig kell megőrizni.

12.9 Naplógenerálás

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

a) biztosítania kell a naplóbejegyzések előállítási lehetőségét a *{0. 12.1* Naplózható események*}* pontban meghatározott naplózható eseményekre

b) lehetővé kell tennie az üzemeltetésért felelős rendszergazdának és szükség szerint az IBF-nek is, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az információs rendszer egyes elemeire,

c) naplóbejegyzéseket kell tudnia előállítania a *{0. 12.1* Naplózható események*}* pontban meghatározottak szerinti eseményekre az *{0. 12.2* Naplóbejegyzések tartalma*}* pontban meghatározott tartalommal.

13. Rendszer- és kommunikáció védelmi eljárásrend

13.1 Határok védelme, túlterhelés alapú támadás elleni védelem

Az Elektronikus információs rendszerhez történő kapcsolódást és az azzal folytatott kommunikációt az erre engedélyezett eszközökre és interfészekre kell korlátozni.

A rendszerhez csak a hozzáférési jogosultsággal rendelkező felhasználók munkaállomásairól, a rendszer támogatójának, valamint az Intézmény rendszergazdáinak VPN kapcsolatáról biztosítható hozzáférés. Az Elektronikus információs rendszer nem lehet hozzáférhető sem egyéb belső eszközökről sem a publikus hálózatok eszközei (internet) felől. Ennek érdekében Az Elektronikus információs rendszert elkülönített logikai hálózatban kell elhelyezni, amelyet belső és külső határvédelmi eszközzel kell védeni.

A rendszer külső határain olyan határvédelmi (tűzfal) megoldást kell alkalmazni, amely:

- alapértelmezett beállításként tilt minden külső kapcsolódást, a külön engedélyezett kapcsolatokon kívül
- figyeli, naplózza és megakadályozza a kibertámadási kísérleteket
- képes a túlterhelés alapú támadások felismerésére és hatásainak mérséklésére
- képes biztonságos VPN kommunikáció biztosítására

A rendszervédelem további eszközeként:

- blokkolni kell a belső hálózatból a veszélyesként besorolt, vagy kártékony kódot tartalmazó web oldalakhoz történő hozzáférést
- Az e-mail kommunikációban külső spam szűrő rendszert kell alkalmazni a kéretlen, adathalász és kártékony kódot tartalmazó levelek blokkolására és karanténba helyezésére.

13.2 Kriptográfiai kulcs előállítása és kezelése, védelem

A kommunikáció védelmét szolgáló kriptográfiai kulcsokat külön eszközzel kell előállítani. A kulcsokat elkülönített, biztonságos helyen kell tárolni.

VPN: A VPN kapcsolatok szerver oldali SSL kulcsai csak a VPN szervereken, a kliens oldali kulcsok csak a VPN klienseken helyezhetők el.

Vízdíjelektronikus információs rendszer: maga a rendszer SHA1 hash algoritmussal tárolja a jelszavakat. Amennyiben kétirányú jelszótárolásra van szükség, akkor a rendszernek legalább AES256-os kódolást kell használnia.

13.3 Együttműködésen alapuló számítástechnikai eszközök *(3.3.13.12.)*

Az Elektronikus információs rendszer felhasználói számára az Intézmény nem biztosít együttműködésen alapuló számítástechnikai eszközöket (kamerák, mikrofonok, stb.). Az egyéb esetekben az rendszernek meg kell gátolnia az együttműködésen alapuló számítástechnikai eszközök (kamerák, mikrofonok, stb.) távoli aktiválását, kivéve, ha az Társaság vezetése külön nem engedélyezte azt, és közvetlen jelzést ad az aktiválásáról azoknak a személyeknek, akik fizikailag jelen vannak az eszköznél.

13.4 Biztonságos név/cím feloldó szolgáltatások *(3.3.13.16-18.)*

Az Intézmény név és cím feloldó szolgáltatást üzemeltet az Intézményi információs rendszer belsőeszközeire. A név és cím feloldó szolgáltatás a belső név- és címtartományba tartozó neveket és címeket tartja nyilván és oldja fel. A külső név és címtartományra vonatkozó lekérdezéseket az engedélyezett névkiszolgálókhoz továbbítja. Az üzembiztos működéshez tartalék névkiszolgálót kell üzemeltetni.

14. Biztonsági események kezelése

Az elektronikus információs rendszerben előforduló biztonsági incidensek hatékony, gyors és a jogszabályokban előírt megfelelő szintű kezelése érdekében biztonsági incidens gyanúja esetén a jelen eljárásrendben leírtakat kell alkalmazni

14.1 Biztonsági eseménykezelési eljárásrend

Információ biztonsági eseménynek nevezzük az elektronikus információs rendszer működésében beállt olyan kedvezőtlen változást, amelynek hatására az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége, rendelkezésre állása, vagy az elektronikus információs rendszer sértetlensége vagy rendelkezésre állása sérült vagy sérülhet.

Az eseménykezelés során elsődleges cél a normál szolgáltatás lehető leggyorsabb helyreállítása és az üzleti folyamatokra gyakorolt káros hatás minimalizálása.

Az események kezelésekor a lehető leghamarabb mérséklő intézkedésnek kell születnie.

Az esemény tényét dokumentálni kell az eset későbbi kivizsgálása érdekében.

Amennyiben a rendszerhibát vélhetően külső, illetéktelen beavatkozás, vagy vírustámadás okozta, az érintett információ-feldolgozó eszközt le kell választani a hálózat(ok)ról, szükség esetén ki kell kapcsolni. Ilyen esetekben fokozottan figyelni kell a hordozható adathordozókra is. A meghibásodott eszközben használt adathordozók kizárólag a biztonsági ellenőrzést követően használhatók más számítógépekben.

Az esemény kivizsgálásának irányítása az informatikai vezető feladata. A kivizsgálás eredményeként mindent meg kell tenni az esemény előfordulási esélyének csökkentése, illetve az okozott kár mérséklése érdekében.

14.2 A biztonsági események figyelése

14.2.1 Az érintett szervezet nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági eseményeit. Az elektronikus információs rendszer naplóinak, illetve az elektronikus információs rendszer védelmét ellátó biztonsági eszközök naplóállományainak elemzésével, valamint a kialakított hibakezelési eljárások hatékony működtetésével az Intézménynek folyamatosan figyelemmel kell kísérnie az elektronikus információs rendszerben bekövetkező információbiztonsági eseményeket.

Ellenőrizendő naplók, logok:

- Tűzfal logjai

- Elektronikus információs rendszer op. rendszer logjai: Security, Setup, System, Application logok
- SQL log
- VMware alarmok
- DFM, storage riasztások
- Vírusvédelmi szoftver logjai
- Egyéb riasztások

14.3 A biztonsági események jelentése

A felhasználó köteles az általa észlelt biztonsági eseményeket azonnal jelenteni az informatikai osztály munkatársának, valamint közvetlen vezetőjének. A sürgősségre tekintettel a bejelentést elsősorban telefonon vagy személyesen kell megtenni. A hibaüzenetet (vagy az incidensre utaló jeleket) a felhasználó nem törölheti a képernyőről. A felhasználó köteles a teljes körű igazságot elmondani az előzményekről, még akkor is, ha e szabályzat megszegése az előzmények része.

A felhasználó semmiféle kísérletet nem tehet a számítógép rendszert, vagy a hálózat működését érintő hiba megszüntetésére (még akkor sem, ha kellő felhasználói ismeretekkel rendelkezik), amíg az illetékes informatikai munkatárs azt nem látta vagy a pontos hibaüzenetet, képernyőképet e-mailben el nem küldte az informatikai munkatárs részére.

Az informatikai munkatárs a hiba, incidens regisztrálása után jelenti a biztonsági eseményt az informatikai vezetőnek, valamint haladéktalanul megkezdi az incidens kivizsgálását és a szükséges intézkedéseket.

14.4 Segítségnyújtás a biztonsági események kezeléséhez

Az IBF feladata, hogy tájékoztatást és segítséget nyújtson az elektronikus információs rendszer felhasználóinak az információbiztonsági incidensek észlelése, kezelése és jelentése érdekében.

14.5 Biztonsági eseménykezelési terv

Az Intézménynek ki kell dolgoznia egy információbiztonsági eseménykezelési tervet, amely

a) iránymutatást ad az információbiztonsági események kezelési módjaira,

b) ismerteti a biztonsági eseménykezelési lehetőségek struktúráját és szervezetét,

c) átfogó megközelítést nyújt arról, hogy a biztonsági eseménykezelési lehetőségek hogyan illeszkednek az általános szervezetbe,

d) kielégíti az Intézmény feladatkörével, méretével, szervezeti felépítésével és funkcióival kapcsolatos egyedi igényeit,

e) meghatározza a bejelentés-köteles biztonsági eseményeket,

f) meghatározza és folyamatosan pontosítja a biztonsági események kiértékelésének, kategorizálásának (súlyosság, stb.) kritériumrendszerét,

g) támogatást ad a biztonsági eseménykezelési lehetőségek belső mérésére,

h) meghatározza azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenn-tartására.

Az Intézménynek gondoskodnia kell arról, hogy

a) a biztonsági eseménykezelési tervet ki kell hirdetni és tudomásul kell vetetni a biztonsági eseményeket kezelő (névvel és/vagy szerepkörrel azonosított) személyekkel és szervezeti egységekkel;

b) a biztonsági eseménykezelési tervet frissíteni kell és meghatározott gyakorisággal felül kell vizsgálni, figyelembe véve az elektronikus információs rendszer és a szervezet változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat;

c) a biztonsági eseménykezelési terv változásait megismertesse az érintettekkel;

d) a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, módosítható.

14.6 Képzés a biztonsági események kezelésére *(3.1.5.9.)*

Az információbiztonsági incidensek megfelelő kezeléséhez és jelentéséhez szükséges ismeretek átadásáról az információbiztonsági oktatások keretében gondoskodni kell.

15. Képzési eljárásrend

Az információs rendszerhez hozzáférő új munkatárs a munkát csak úgy kezdheti meg, ha írásban nyilatkozik arról, hogy az Intézmény Informatikai Biztonsági Házirendjét és az informatikai biztonságra vonatkozó eljárásrendeket, előírásokat magára nézve kötelezőnek fogadja el.

Az új munkatárs köteles az Informatikai Biztonsági Házirendet önállóan megismerni, az abban foglaltakat maradéktalanul betartani.

A vezetőknek minden szinten feladata az informatikai biztonsági követelmények betartatása, a biztonságtudatos munkavégzés megkövetelése és ellenőrzése. Az informatikai biztonsági követelmények megszegése esetén az alkalmazott fegyelmi eljárást és az alkalmazott szankciók részleteit rögzíteni kell.

Az Információ biztonságtudatosságra vonatkozó képzések alapvető célja az információs rendszerhez hozzáférő munkatársak biztonságtudatos, felelős magatartásának fenntartása ill. fejlesztése, ismereteinek bővítése, frissítése. A képzésnek része lehet az Intézménynél tapasztalt események elemzése is. Ennek érdekében időszakosan - lehetőség szerint éves gyakorisággal - szinten tartó képzéseket kell tartani.

Jogszabályi vagy technikai változások, az elektronikus információs rendszerben bekövetkezett változások, továbbá új biztonsági fenyegetések esetén soron kívüli képzést kell tartani. A soron kívüli képzés történhet e-mailben megküldött tájékoztató formájában is.

A fejlesztő képzések célja az az új biztonsági kockázatok megismerése és kezelése, ill. az esetleges technikai változásokra történő felkészülés.

A szervezetten megtartott biztonsági képzéseket dokumentálni kell. Az azon résztvevőkkel a képzés megtörténtét jelenléti ív aláírásával el kell ismertetni.

Az informatika az illetékes hatóságok informatikai biztonsági riasztásait, ill. az informatikai szakportálokon megjelenő biztonsági figyelmeztetéseket folyamatosan nyomon követi és a szükséges intézkedéseket megteszi.

16. Fizikai védelmi eljárásrend (lásd még 4.5 A szerverszoba házirendje mellékletet)

A fizikai biztonságra vonatkozó óvintézkedések az Intézményi rendszereknek helyet adó létesítmények, a rendszer erőforrások és a működést biztosító alapszolgáltatások védelmével kapcsolatban fogalmaznak meg szabályokat, annak érdekében, hogy a számítástechnikai szolgáltatások megszakadását, eszközök ellopását, a fizikai károkozást, az információk jogosulatlan felfedését, a rendszer sértetlenségének elvesztését megakadályozzák. Az elektronikus információs rendszer fizikai környezetének kialakítása, működtetése és használata során az általános biztonsági előírások szerint kell eljárni.

16.1 Fizikai belépési engedélyek

Az Intézmény összeállítja, jóváhagyja és kezeli az adatközpontnak helyet adó (központi irodaépület) létesítménybe belépésre jogosultak listáját.

A belépési jogosultságot igazoló dokumentumokat bocsát ki a belépéshez a belépni szándékozó részére.

A munkavállaló elektronikus beléptető kártyájának használatával léphet be a központi irodaépület szerverszobájába.

Rendszeresen felülvizsgálja a belépésre jogosult személyek listáját, eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépésre már nem jogosultak, intézkedik a dokumentumok visszavonásáról, érvénytelenítéséről, törléséről és megsemmisítéséről.

A nem állandó belépésre jogosult személyek adatait a Kórház az Adatvédelmi Szabályzatnak megfelelően kezeli.

A belépési engedélyek kezelésének részletes szabályozását a vagyonvédelmi szabályzat tartalmazza.

16.1 A fizikai belépés ellenőrzése

Az Intézmény ellenőrzött be- és kilépési pontokon biztosítja a fizikai belépést az arra jogosultak számára. A fizikai belépéseket naplózni kell.

Az Intézmény ellenőrzés alatt tartja a létesítményen belüli helyiségeket, kíséri a létesítménybe vendégként belépőket és figyelemmel követi a tevékenységüket.

A fizikai belépés ellenőrzésének részletes szabályozását a vagyonvédelmi szabályzat tartalmazza.

16.2 Hozzáférés az információs rendszerhez, a fizikai hozzáférések felügyelete

A fizikai belépés csak a belépésre engedélyezett személyeknek lehetséges.

Az adatközpontnak helyt adó helyiségbe csak az informatika osztály dolgozói léphetnek be.

Az informatika rendszeresen átvizsgálja a belépési naplókat, ill. soron kívül abban az esetben, ha jogosulatlan fizikai hozzáférés gyanúja merül fel.

16.3 Az adatközpont további fizikai védelmei

Az adatközpontot elegendően nagy kapacitású szünetmentes tápegységgel kell ellátni, amely biztosítja a tartalék áramellátásra történő átkapcsolás vagy a rendszerek leállításához szükséges ideig a szünetmentes áramellátást. Hosszabb áramszünetek esetére aggregátoros tartalék áramellátást kell biztosítani. Áramszünet esetére az adatközponthoz vezető ill. a menekülő útvonalakon vészvilágítást kell biztosítani.

Az adatközpontot áramszünet ellen védett, automatikus működésű tűzriasztó és tűzelfojtó berendezéssel kell ellátni. A tűzvédelmi berendezésnek tűz érzékelése esetén hangjelzéssel és a kijelölt személyeknek küldött SMS értesítéssel kell jeleznie.

Az adatközpont megfelelő üzemi hőmérsékletét folyamatosan fent kell tartani. Ennek érdekében tartalék áramforrással biztosított, redundáns klíma berendezéseket kell üzemeltetni.

Az adatközpont hőmérsékletét folyamatosan monitorozni kell. Túlmelegedés esetén a rendszernek automatikusan SMS értesítést kell küldeni a kijelölt személyeknek.

A szerverterem ideális hőmérséklete 20 és 25 Celsius-fok közé esik. Nem megengedett, hogy a hőmérséklet 10 Celsius-fok alá csökkenjen, vagy pedig 28 Celsius-fok fölé emelkedjen.

A páratartalom 40% és 50% között kell legyen.

16.4 Karbantartók

Abban az esetben, ha saját erőből a karbantartás nem végezhető el, akkor az informatikai vezető kezdeményezi külső fél (alvállalkozó) megbízását.

Karbantartási tevékenységet csak olyan külső fél végezhet, aki érvényes szerződéssel rendelkezik, a titoktartási nyilatkozatot aláírta és megismerte az Intézmény vonatkozó információbiztonsági előírásait.

A karbantartást végző külső felekről nyilvántartás kell vezetni, melynek minimálisan a következőket tartalmaznia:

a) szervezet megnevezése,

b) szerződésszám,

c) szerződés időtartama,

d) szerződéses kapcsolattartó neve, elérhetősége,

e) karbantartás végzők neve, elérhetősége

f) szerződés tárgya, hatálya (mely rendszerelemre terjed ki).

Külsős karbantartó munkavégzése esetén az informatikai vezetőnek ki kell jelölnie azokat a személyeket, akik folyamatosan felügyelik a karbantartást.

17. Mentési/archiválási eljárásrend

17.1 A mentendő / archiválandó rendszerek és alkalmazások meghatározása

17.1.1 Rendszernyilvántartás elkészítése

Az Intézmény számára elengedhetetlen, hogy tudja, milyen informatikai infrastruktúrát tart fenn és milyen rendszereket üzemeltet. Ezért a használt szolgáltatásokhoz informatikai rendszer nyilvántartást kell készíteni. A rendszernyilvántartást az infrastruktúra-szolgáltatást nyújtó rendszerek esetében is ki kell tölteni (pl. Active Directory, DNS stb), de önálló adatgazdai szerepkört nem kell hozzárendelni.

A nyilvántartást elektronikus formában kell tárolni.

17.1.2 Mentendő/archiválandó rendszerek meghatározása

Az informatikai infrastruktúra az alábbi fő rendszer-elemekből áll:

- A rendszer géptermi elhelyezésének és működtetésének szükséges alapvető elemei:
    - zárt, klimatizált elsődleges és tartalék gépterem (adatközpont)
    - a rendezett fizikai elhelyezést biztosító állvány (rack)
    - elektromos táp és kommunikációs hálózati kábelezés
    - szünetmentes áramforrások (UPS)
- Az alkalmazások feldolgozását, kiszolgálását végző gépek, szerverek
- Közös, hálózaton elérhető adattároló eszköz (NetApp A200)
- A szerverek logikai felosztását, hatékony kihasználtságát lehetővé tevő szerver-virtualizáció szoftver
- Adatmentő alrendszer (szerver, szalagtár, szoftverek) – a tartalék gépteremben

17.1.2 Mentés/archiválás feltételeinek meghatározása

Minden mentendő rendszerre vonatkozóan meg kell határozni, hogy

- milyen gyakran kell menteni,
- mikor kell menteni,
- mennyi ideig kell gyorsan elérhető (on-line / kvázi on-line) tárban tárolni,

17.2 Mentés/archiválás menetének meghatározása

A mentéssel megbízott személy a rendszergazda, távolléte esetén az informatikai vezető, vagy az általa kijelölt személy veszi át a szerepét.

Ha a mentés feltételei rendelkezésre állnak, a mentési tevékenységgel megbízott felelős feladata a mentés menetének meghatározása és annak biztosítása.

17.3 A mentésért felelős személy feladatai:

- mentések ütemezése

- mentési job-ok beállítása (honnan - hova és mit mentsen)
- mentési média ellenőrzése és rendelkezésre állás biztosítása
- mentés folyamatának ellenőrzése
- mentés eredményének ellenőrzése

17.4 A mentés menete és műszaki paraméterei

17.4.1 Mentési naplók

A mentési naplók az alkalmazott mentési rendszer formátumában elégségesek. A mentési naplók tárolási helye az alkalmazott rendszer naplójában van.

A naplók ellenőrzése: a mentési naplókat hetente ellenőrizni kell, és az esetlegesen talált rendellenességek kezeléséhez felelőst és határidőt kell rendelni.

A naplókat megőrzési ideje: min 1 év

17.4.2 Mentési média (szalagos) címkézése

A médiák címkézését az alkalmazott rendszer automatikusan elvégzi.

17.4.3 Adathordozók darabszáma

Folyamatosan figyelemmel kell kísérni a mentendő adatmennyiség változását, és ennek megfelelően kezdeményezni új adathordozók beszerzését. Minden médiatípus esetén legalább 10% tartalékot szükséges tartani.

17.4.4 Adathordozók élettartama

A használt mentési médiák (szalag) használati idejét a gyártó által megadott élettartam figyelembevételével, 10%-os biztonsági tartalékkal kell meghatározni.

Az élettartamot figyelembe kell venni mind a többszöri felhasználásnál, mind pedig a hosszú távon megőrzendő adatok tárolásánál.

Az élettartamok figyelését a mentésért felelős munkatársnak kell elvégezniük. Amennyiben egy média élettartama meghaladta a használati időt, a mentésért felelős munkatársnak kezdeményeznie a média selejtezését, és az új média beszerzését.

17.4.5 Az adathordozók selejtezése

Az adatok hosszú távú tárolása és elérhetősége érdekében az adathordozók élettartamát folyamatosan ellenőrizni kell.

A már fel nem használható (elöregedett, megsérült) adathordozókat selejtezni kell. A selejtezést a mentésért felelős munkatárs kezdeményezheti.

A selejtezés során az alábbi követelményeket kell betartani:

- a selejtezésről jegyzőkönyv felvétele kötelező.
- a kritikus adatok tárolására használt adathordozó selejtezését úgy kell elvégezni, hogy utána arról semmilyen adat, vagy adatrészlet ne lehessen visszaállítható (demagnetizálás, hevítés, darálás, pépesítés),

- selejtezett adathordozó kommunális szemétbe nem kerülhet.
- törekedni kell a környezetvédelmi szempontok érvényesítésére.

17.4.6 Az adathordozók tárolása

A felhasznált szalagos adathordozókat egy külső helyszínen (Ligetváros, iroda páncélja) kell tárolni. A mentésekhez, illetve archívumokhoz csak az informatikai vezető, illetve távollétében az általa kijelölt munkatárs férhet hozzá. A mentési média külső helyszínre/ről történő ki- és beszállításakor fokozott figyelemmel kell lenni, a média biztonságáért a szállításával megbízott személy felel.

17.5 Visszatöltési eljárások

A visszatöltési eljárások dokumentálása:

A visszatöltést akár részleges, akár teljes visszatöltés történik a meghatározott adatgazda(k) kezdeményezheti írásban, vagy e-mailben. A visszatöltést csak a mentésért felelős kollégák végezhetnek.

A visszatöltési teszteket kell végezni az alábbi esetekben:

- a mentési infrastruktúrát érintő változások esetén,
- rendszeresen, de legalább évente, a teljes mentési dokumentáció felülvizsgálatakor.

Visszaállítási teendőkkel kapcsolatos feladatok és dokumentációi

A visszaállítási teendőkkel kapcsolatos feladatokat, alkalmazás katalógusban megjelölt rendszer

újraindítási eljárásának megfelelően kell végrehajtani. Ezen eljárásokat a rendszer dokumentációja tartalmazza.

4.4 melléklet

Informatikai szoftverfrissítés eljárásrendje

1. Az eljárásrend célja

Jelen eljárásrend célja, hogy meghatározza az operációs rendszerek és egyéb alkalmazások biztonsági, illetve feature frissítéseinek telepítési módját.

2. Felhasználó oldali szoftver frissítések telepítése

2.1 Asztali operációs rendszerek

Asztali operációs rendszerek esetében automatikusra kell állítani a biztonsági frissítések telepítését. Ezzel biztosítva felhasználói oldalról az IT környezet biztonságát.

2.2 Asztali segédalkalmazások

A különböző segédalkalmazások (Java JRE, Adobe Reader, stb.), esetében is az automatikus, lehetőleg felhasználói beavatkozást nem igénylő frissítési mechanizmust kell használni a felhasználók számítógépein.

2.3 Ki a felelős a telepítésért

Amennyiben az automatikus telepítésre nincs mód, úgy a telepítéseket manuálisan hajtja végre az Informatikai csoport. Az Informatikai Biztonsági Felelős félévente, szúrópróbaszerű ellenőrzéseket hajt végre és amennyiben hiányosságokat talál, tájékoztatja a szolgáltatót, akiknek egy héten belül pótolnia kell az elmaradt telepítéseket.

3. Szerver oldali szoftver frissítések telepítése

3.1 Teszt rendszerek operációs rendszer frissítési fázisai

Biztonsági kategóriába sorolt frissítések telepítése automatikusan történik teszt rendszerek esetében.

Feature kategóriába sorolt frissítések telepítése manuálisan történik havonta egyszer, az Informatika csoport által.

3.2 Teszt rendszerek alkalmazásainak frissítési fázisai

A fejlesztők által kiadott frissítési csomagok telepítését minden esetben manuálisan végzi el az Informatika csoport. A telepített frissítéseket vagy a fejlesztő által előírt módon vagy a feature list alapján kell letesztelni. A rendszergazdai teszt után a felhasználóknak is tesztelniük kell a frissítéseket.

3.3 Ki a felelős a telepítésért

A telepítéseket manuálisan hajtja végre az Informatikai csoport, kivéve a szerverek esetében, mert itt az üzemeltetéssel megbízott cég a felelős. Az Informatikai Biztonsági Felelős havonta, szúrópróbaszerű ellenőrzéseket hajt végre és amennyiben hiányosságokat talál, tájékoztatja a szolgáltatót, akiknek egy héten belül pótolnia kell az elmaradt telepítéseket.

3.4 Éles rendszerek operációs rendszer frissítési fázisai

Biztonsági kategóriába sorolt frissítések telepítése manuálisan történik, 2 héttel azután, hogy a teszt rendszerre telepítve lettek a frissítések.

Feature kategóriába sorolt frissítések telepítése manuálisan történik havonta egyszer, az Informatikai csoport által. Itt is 2 hetes ráhagyással, a teszt rendszerhez képest.

3.5 Éles rendszerek alkalmazásainak frissítési fázisai

A fejlesztők által kiadott frissítési csomagok telepítését minden esetben manuálisan végzi el az informatikus, amennyiben a teszt rendszerben sikeresen lezajlott a teszt és mind a rendszergazda, mind az adatgazda jóváhagyja azok telepítését az éles rendszerre.

3.6 Ki a felelős a telepítésért

A telepítéseket manuálisan hajtja végre az Informatikai csoport. Az Informatikai Biztonsági Felelős havonta, szúrópróbaszerű ellenőrzéseket hajt végre és amennyiben hiányosságokat talál, tájékoztatja a szolgáltatót, akiknek egy héten belül pótolnia kell az elmaradt telepítéseket.

4.5 melléklet

A szerverszoba házirendje

1. Összefoglaló

E dokumentumban összefoglaljuk mindazokat a kritikus pontokat, amelyek minimálisan megkövetelték az Intézmény szerverszoba környezetében.

2. Hatálya

Ez a dokumentum kiterjed minden olyan munkatárs szerverszobában végzett munkájára - legyen az belső vagy külső munkatárs-, akinek állandó belépője van a szerverszobába. Ezen személyek felelősek az általuk beengedett, belépővel nem rendelkező (klímaszerelők, telefon szerelők, villanyszerelő, stb.) személyek munkájával kapcsolatban is.

3. Szerverterem

3.1 Behatolásvédelem

A szerverterem behatolásvédelmének biztosítására a következő szempontokat kell érvényesíteni:

- Belépést regisztráló rendszer kialakítása
- Riasztórendszer alkalmazása

3.2 Tűzvédelem

Tűzvédelem biztosításának érdekében az alábbi szempontok figyelembevétele szükséges:

- Automata tűzriasztó rendszer alkalmazása
- Kézi tűzoltó berendezések alkalmazása

3.3 Klimatizálás

A szerverterem üzemi hőmérsékletének szabályozásának érdekében az alábbi szempontok figyelembevétele szükséges:

- A szerverteremben klíma-berendezéseket kell üzemeltetni, a megfelelő üzemi hőmérséklet szabályozására.
- A klíma berendezések darabszámát, típusát, teljesítményét úgy kell tervezni, hogy még egy klímaberendezés meghibásodása esetén is biztosítani tudják a megfelelő szabályozást.
- A klíma-berendezések automatikus újraindítását biztosítani kell az esetleges áramszünet megszűnése esetén.
- A szerverteremben a hőmérséklet és páratartalom ellenőrzésére thermometer-t kell alkalmazni. A hőmérsékletet és a páratartalmat napi két alkalommal szemrevételezéssel ellenőrizni szükséges.
    - szerverterem hőmérséklete 15 – 25 Celsius fok között optimális
    - páratartalom maximum 50% lehet

3.3 Eszközök dokumentálása

- Minden eszközt felirattal kell ellátni, amely tartalmazza az eszköz nevét és IP címét.
- A feliratokat havonta ellenőrizni kell (esetleges tartalmakat aktualizálni)
- Minden Rack-en el kell helyezni egy listát a benne található eszközökről

3.4 Rendtartás

- Ne hagyjunk semmilyen adminisztratív információt szabadon a szerver szobában
- A helyiség rendbentartásáról folyamatosan gondoskodni kell.
- Szerelők nem hagyhatnak maguk után szemetet, üres dobozt, szerelési anyagokat stb.
- Installálás után minden segédeszközt el kell távolítani a szobából (dobozok, CDk, kábelek, kinyomtatott anyagok)
- A kiszerelt hardver-elemeket, telepítő CD-ket, kábeleket a helyiségben lévő zárt szekrényben helyezzük el. Ha ez nem lehetséges, akkor az informatikai iroda zárt szekrényében.
- A szerverteremben élelmiszert bevinni és ott tárolni tilos!

3.5 Mentési adathordozók

- A mentéshez szükséges adathordozókat tilos a szerverszobában tárolni! Ezeknek az erre kialakított páncélszekrényben a helyc.

3.6 Belépés

- Vendégek, a szerver szobába nem jogosult emberek csakis kíséret mellett tartózkodhatnak.
- A belépések nyilvántartását az erre szolgáló belépési naplóban kell vezetni. A szerverszobába belépéskor mind a vendégnek mind a kísérőnek rögzítenie kell a belépés időpontját

3.7 Informatikai eszközök ki- és beszállítása

- Informatikai eszközök ki- és beszállítása csak dokumentált formában megengedett (szállítólevél, átadás/átvételi bizonylat)
- Adathordozó szállítása esetén a szállítást végző köteles kellő gondossággal eljárni az adathordozók és adatok biztonságának megőrzése érdekében.
- Informatikai eszközt selejtezési céllal elszállítani, vagy harmadik fél számára elérhetővé tenni kizárólag az informatikai vezető előzetes engedélyével lehetséges.
- A selejtezést végző és átadó munkatárs is köteles meggyőződni arról, hogy adathordozó, vagy papír alapú dokumentum nem maradt az eszközben.

4. Házirend felülvizsgálata

Jelen házirendet a kiadást követően hathavonta felül kell vizsgálni.

4.6 melléklet

Biztonsági osztályba sorolás

e-Medsol – ovi4602_eMedSolution.xlsx táblában,

CT-Ecostat – ovi4602_ct-EcoSTAT.xlsx táblában,

DMSone – ovi4602_DMSone.xlsx táblában,

Főnix – ovi4602_Főnix.xlsx. táblában,

Gyurika – ovi4602_Gyurika.xlsx. táblában,

Jdolber – ovi4602_Jdolber.xlsx. táblában