NEMZETI KIBERVÉDELMI INTÉZET
Nemzeti Elektronikus Információbiztonsági Hatóság
☎+36-1-206-9320
✉: 1399 Budapest, 62. Pf.: 710/37
@: info@neih.gov.hu

NEMZETI KIBERVÉDELMI INTÉZET
NEIH

jegyző 2017.08.18.

KEVERMESI KÖZÖS ÖNKORMÁNYZATI HIVATAL
FŐOSZT.: 20 2017 AUG 18. nap
1/888-3 szám db
Ügyszám Utószám Gácsér B.

Ikt. sz.: 420/A-494-9/2016 2. sz. pld.

Gácsér Béla
jegyző
Kevermesi Közös Önkormányzati Hivatal
5744 Kevermes, Jókai utca 1.

Tárgy: *Informatikai biztonsági szabályzat nyilvántartásba vétele*

Hiv. sz.: *31391035920170803082903 1826*

HATÁROZAT

A Kevermesi Közös Önkormányzati Hivatal (székhely: 5744 Kevermes, Jókai utca 1. – a továbbiakban: Hivatal) 2017. augusztus 1-jén hatályba lépett informatikai biztonsági szabályzatát a hatósági nyilvántartásba

bejegyzem.

Döntésem ellen a kézhezvételt követő 15 napon belül fellebbezésnek van helye. A fellebbezést a Nemzeti Elektronikus Információbiztonsági Hatóságnál (a továbbiakban: Hatóság) kell benyújtani. A fellebbezés elbírálására Budapest Főváros Kormányhivatala jogosult.

Indokolás

Az információbiztonsági felelős 2017. augusztus 3-án a saját ügyfélkapujáról megküldte a Hivatal informatikai biztonsági szabályzatát.

A nyilvántartásba vételt az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 15. § (1) bekezdésének d) pontja, valamint az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről szóló 42/2015. (VII. 15.) BM rendelet 4. § (2) bekezdése indokolja. A szabályzat nyilvántartásba vételét tekintve mérlegelésnek nincs helye.

A fellebbezés lehetőségét a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (a továbbiakban: Ket.) 98. § (1) bekezdése, benyújtásának határidejét a Ket. 99. § (1) bekezdése, helyét a Ket. 102. § (1) bekezdése, az elbírálására jogosult szervet a Ket. 106. § (4) bekezdése határozza meg.

A Hatóság hatáskörét és illetékességét az Ibtv. 14. § (1) bekezdése és az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az

információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet 2. §-a állapítja meg.

Budapest, 2016. augusztus 19

P. H.

dr. Bencsik Balázs
a Hatóság vezetője

Készült: *2 pld. / 1 lap / 2 old.*
Kapja: *1. pld. NEIH irattár*
2. pld. Címzett
Készítette/Gépelte: *Szigeti Zsolt - Tel.: (1) 206-9320*
Irattári jelzés:
Azonosító:

Kevermesi Közös Önkormányzati Hivatal Informatikai Biztonsági Szabályzata

Kiadva az 1/2017.(VIII.1.) jegyzői utasítással

2017

1. Bevezetés

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

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

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

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

Az IBSZ egy olyan alapvető dokumentum, mely magában foglalja:

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

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

1.1. Az IBSZ szervezeti hatálya

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

1.2. Az IBSZ személyi hatálya

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

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

1.3. Az IBSZ tárgyi hatálya

Az Informatikai Biztonsági Szabályzat alkalmazása kiterjed:

- a KÖH tulajdonában lévő valamennyi számítástechnikai, informatikai berendezésre (ideértve az okmányirodai munkaállomásokat és az együttműködési megállapodás keretében használt lekérdező klienseket is), valamint ezek műszaki dokumentációjára is
- a rendszer- és felhasználói programokra
- az adathordozók tárolására, felhasználására
- valamint a számítástechnikai folyamatban szereplő összes dokumentációra

1.4. Az IBSZ területi hatálya

A szabályzat területi hatálya kiterjed a Kevermesi Közös Önkormányzati Hivatal valamennyi tagjára:

- Kevermesi Közös Önkormányzati Hivatal (5744 Kevermes, Jókai u. 1.)
- Kevermesi Közös Önkormányzati Hivatal Kisdombegyházi Kirendeltsége (5837 Kisdombegyház, Kossuth u. 77.)
- Kevermesi Közös Önkormányzati Hivatal Magyardombegyházi Kirendeltsége (5838 Magyardombegyház, Nagy u. 61.)

1.5. Az IBSZ időbeni hatálya

Jelen szabályzat a kiadás napján lép hatályba.

2. A KÖH biztonsági osztályba és biztonsági szintbe sorolása

2.1. Biztonsági osztályba sorolás

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

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

A biztonsági osztályba soroláshoz az elektronikus információs rendszerben kezelt adatokra vonatkozóan meg kell határozni a biztonsági célokra gyakorolt potenciális társadalmi-politikai hatást, és ezek jogi következményeit. Valamint a rendelkezésre állás tekintetében a közvetett anyagi kárt és a szolgáltatás kieséséből adódó károkat. Ezek segítségével a KÖH tevékenysége jellegének, nagyságrendjének és összetettségének megfelelő, kockázataival arányosan kerülnek megfogalmazásra a biztonsági célok elvesztésének hatásai.

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

A biztonsági osztályba sorolást mindig kockázatelemzéssel együtt kell végezni.

A biztonsági osztályba sorolást az alábbi esetekben újra el kell végezni

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

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

A biztonsági osztályba sorolást az Informatikai Biztonsági Felelős (továbbiakban IBF) készíti elő az adatgazdákkal együttműködve és a jegyző hagyja jóvá.

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

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

2.2. Biztonsági szintbe sorolás

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

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

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

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

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

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

2.2.1. Szervezeti egységek biztonsági szintbe sorolása

A KÖH hatályban lévő Szervezeti és Működési Szabályzata alapján a KÖH-ben nem működnek az elektronikus információs rendszer

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

szervezeti egységek, ezért azok biztonsági szintbe sorolása nem értelmezhető.

2.2.2. A KÖH jelenlegi biztonsági szintje

A KÖH az Ibtv. előírásainak megfelelően megvizsgálta biztonsági szintjét.

A Kevermesi Közös Önkormányzati Hivatal jelenlegi biztonsági szintje: 2

3. Felelősségek, hatáskörök, elkötelezettségek az IT biztonság területén

3.1. Általános

Jelen IBSZ személyi hatálya alá tartozó valamennyi érintett felelős:

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

A KÖH minden munkatársa köteles:

- az IBSZ dokumentumában előírt ellenőrzések sikeres megvalósulását elősegíteni és támogatni,
- tudomásul venni, hogy az üzemeltetésért felelős külsős informatikus és az IBF előzetes bejelentés nélkül ellenőrizheti az informatikai biztonsághoz kapcsolódó utasításokat és a szabályzatok betartását

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

3.2. Informatikai Biztonsági Felelős

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

3.2.1. Feladata:

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

Az Informatikai Biztonsági Felelős ellenőrzési feladata:

- az üzemeltetésért felelős külsős informatikussal közösen ellenőrzi az informatikai biztonsági előírások betartását; a védelmi előírások betartását; az adatvédelmi biztonsági rendszer érvényesülését, valamint részt vesz ezek végrehajtásában

Az Informatikai Biztonsági Felelős dokumentációs feladat:

- legalább 2 évente felülvizsgálja az IBSZ-t, a tartalmát aktualizálja a KÖH feladatai alapján
- felülvizsgálja és aktualizálja az IBSZ-hez kapcsolódó dokumentumokat, eljárásrendeket, legalább 2 évente
- véleményezi az Informatikai rendszerhez kapcsolódó valamennyi szabályzatot, eljárásrendet és dokumentumot
- a szabályzatok módosításának szakmai elkészítéséhez jogosult igénybe venni az informatikai szervezet munkatársait

3.2.2. Felelőssége:

Az Informatikai Biztonsági Felelős felel:

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

3.2.3. Jogosultsága:

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

3.3. Üzemeltetésért felelős külsős informatikus/rendszergazda

3.3.1. Feladata:

- az Informatikai rendszer IBSZ-nek megfelelő működtetése
- az Informatikai rendszer működtetéséhez szükséges valamennyi személyi és tárgyi feltétel biztosítása a biztonsági elvárások figyelembevételével
- az érzékelt vagy ismert kockázatokról az IBF-et és a jegyzőt tájékoztatni
- az informatikai biztonságot érintő minden dokumentum és utasítás elkészítésében való aktív részvétel, az elkészült dokumentumok véleményezése, kihirdetésének biztosítása
- közreműködni az Informatikai rendszer informatikai biztonságát érintő területek megvalósításában
- biztosítja a veszélyforrások körében bekövetkezett változások folyamatos követését (vírusvédelem), és kezdeményezi a szükséges intézkedések meghozatalát
- biztosítja az adat- és információvédelmi feladatok folyamatos belső ismertetését, felügyeli a képzési terv kidolgozását és oktatását

3.3.2. Felelőssége:

Az üzemeltetésért felelős külsős informatikus felelős

- az Informatikai rendszer biztonságos működtetéséért
- az Informatikai rendszer üzembiztonságáért, a rendszer kritikus részeinek és védelmi eszközeiknek folyamatos ellenőrzéséért
- az Informatikai rendszer hardver és szoftver elemeinek nyilvántartásáért, dokumentáltságáért
- az informatikai biztonság tudatosításáért
- a biztonsági szabályokat megsértők szembeni eljárások elindításának kezdeményezéséért a jegyzőnél

3.3.3. Jogosultsága:

- az Informatika rendszer teljes körű ellenőrzése
- javaslattétel az új védelmi, biztonsági eszközök és technológiák beszerzésére, illetve bevezetésére

- az előírásokkal szemben vétőkkel felelősségre vonási eljárás kezdeményezése a jegyzőnél

Az üzemeltetésért felelős külsős informatikus és az IBF együttesen szabályzatgazdái az Informatikai Biztonsági Szabályzatnak és az informatikai biztonsághoz kapcsolódó egyéb eljárásrendeknek, utasításoknak, melyek összhangjáért is felelnek.

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

4. Az informatikai rendszer általános biztonsági alapelvei

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

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

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

5. Kockázatelemzés

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

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

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

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

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

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

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

6. Az informatikai biztonság dokumentumai

6.1. Az Informatikai Biztonsági Szabályzat

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

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

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

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

6.1.1. Informatikai Biztonsági Szabályzat (IBSZ):

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

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

6.1.2. Szabályzatok, eljárásrendek

A szabályzatok és eljárásrendek segítenek a munkavállalóknak az informatikai rendszer biztonságos használatában. Az üzemeltetésért felelős külsős informatikus és az IBF által közösen elkészített szabályzatokat, eljárásrendeket a KÖH valamennyi munkatársa számára elérhetővé teszi. Az IBSZ a megfelelő helyen ezen szabályzatokra és eljárásrendekre hivatkozik.

6.1.3. Nyilvántartások

A KÖH az elektronikus információs rendszerekre vonatkozóan nyilvántartásokat vezet. Valamint az IBSZ szerinti szabványosított jegyzőkönyveket és formanyomtatványokat használ.

6.2. Összefoglaló szabályok

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

Minden IBSZ-t érintő aktuális dokumentáció, nyilvántartás őrzéséről a jegyző gondoskodik.

7. Szervezeti biztonság

7.1. Az informatikai biztonság belső szervezeti struktúrája

7.1.1. Vezetői elkötelezettség

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

A vezetői testület hatáskörébe tartozik:

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

7.1.2. Az informatikai biztonsági feladatok megosztása

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

A KÖH információbiztonsági feladatinak ellátása során a következő szerepkörök érintettek:

- a jegyző
- az Informatikai Biztonsági Felelős
- az üzemeltetésért felelős külsős informatikus/ rendszergazda
- a felhasználók

7.1.2.1. A jegyző

A jegyző feladata

- biztosítani az informatikai rendszerrel irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését
- biztosítani a KÖH-re irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését

- az informatikai rendszer biztonságáért felelős személyt nevez ki vagy bíz meg
- kiadja az Információ Biztonsági Szabályzatot

A jegyző felelős

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

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

7.1.2.2. Az Informatikai Biztonsági Felelős

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

7.1.2.3. Az üzemeltetésért felelős külsős informatikus/ rendszergazda

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

7.1.2.4. A felhasználók

A felhasználó jogosult

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

A felhasználó köteles

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

A felhasználó felelős

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

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

7.1.3. Együttműködés, kapcsolat a hatóságokkal

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

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

8. Személyi biztonság

8.1. Az alkalmazás előtt

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

8.1.1. Informatikai biztonság a felvételnél és a munkaköri leírásokban

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

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

8.2. Alkalmazás alatt

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

8.2.1. Az informatikai biztonsági tudatosság, oktatás és képzés

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

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

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

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

8.2.2. Fegyelmi eljárás

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

8.3. Alkalmazás megszűnése

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

Alkalmazás megszűnése esetén az alábbi eljárásokat mindenképpen le kell folytatni.

8.3.1. Az eszközök visszaadása

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

Ilyen eszköznek tekintjük:

- szoftverek
- hivatali és egyéb munkavégzéshez biztosított dokumentumok
- informatikai eszközök
- elektronikus és optikai adathordozók

8.3.2. Hozzáférési jogok visszavonása

Alapvető biztonsági követelmény, hogy a munkaviszony megszűnésekor, szerződő fél megállapodásának lejártakor vagy ezek megváltozásakor minden informatikai rendszert érintő hozzáférési jogosultságot vissza kell vonni.

Gondoskodni kell arról, hogy a távozó munkatárs a munkaviszony megszűnése után a KÖH adatival dolgozó külső szervezetek informatikai rendszeréhez se férhessen hozzá.

8.4. Az internet használat és az elektronikus levelezés szabályai

8.4.1. A web böngészés szabályai

A KÖH minden munkavállalója számára olyan munkaeszközt biztosít, ami internetelléréssel rendelkezik.

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

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

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

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

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

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

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

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

Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, kiiktatása. Ebbe a körbe tartoznak a vírusellenőrző és internet böngésző kontrollok is.

Tilos internetes vagy más jellegű szolgáltatást nyújtó külső féllel hálózati kapcsolat kialakítása.

Tilos az elektronikus információs rendszerek használata a KÖH értékeivel összhangban nem álló célokra, vagyis pl. szexuális jellegű fájlok fogadására, küldésére, fenyegetésre vagy megfélemlítésre, megkülönböztetésre, gyűlölködésre, fegyverekkel és illegális drogokkal való kereskedésre, erőszakra, internetes- illetve szerencsejátékokra, bármilyen kereskedelmi, illetve jogellenes tevékenységre.

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

A munkával összefüggésbe nem hozható oldalak elérhetőségét a jegyző jogosult korlátozni.

8.4.2. Az elektronikus levelezés használata

A KÖH által biztosított elektronikus levél cím és az elektronikus levelezési szolgáltatás kizárólag munkavégzés céljára használható. Az elektronikus levelezés használatának elveit és szabályait valamennyi, a KÖH által biztosított postafiók esetében be kell tartani.

8.4.2.1. Alapelvek

- A levelek nem tartalmazhatnak a hatályos magyar jogszabályokba ütköző tartalmat.
- A levelek nem sérthetik mások becsületét, emberi jogait, faji, nemzetiségi hovatartozását, vallási, politikai világnézetét.
- A levelek nem ronthatják a KÖH hírnevét, megítélését, nem terjeszthetnek róla szándékosan valótlan információkat.

- A levelezés nem veszélyeztetheti a hálózati infrastruktúra működését.
- A KÖH levelező rendszere magáncélú haszonszerzésre nem használható.
- Más személy levelezési címét használni szigorúan tilos. Kivétel ez alól a meghatalmazással rendelkező munkatársak.
- A postafiókkal rendelkező felhasználók kötelesek minden munkanap bejelentkezni a levelező rendszerbe, és bejövő üzeneteiket ellenőrizni.
- Az elektronikus levelek és csatolmányok védelmi előírásai megegyeznek az egyéb dokumentumok védelmének előírásaival.
- Elektronikus levél önmagában nem használható kötelezettség vállalására, illetve annak visszaigazolására.

8.4.2.2. Szabályok

- Tilos kéretlen leveleket, hirdetéseket kiküldeni.
- Tilos a KÖH elektronikus postafiókját levelezési láncok küldésére használni.
- Tilos a levelek fejlécének megváltoztatása, hamis levelek kiküldése.
- Tilos a levelezési címet olyan szolgáltatásnál regisztrálni, ami nem a KÖH feladat ellátási köréből adódik. Ha a KÖH feladat ellátásából adódóan kell email címet bármilyen platformon regisztrálni, úgy célszerű külön, csak erre a feladatra szolgáló különleges email címet igényelni.
- Ismeretlen feladótól érkezett, különös témájú, csatolt fájlt tartalmazó leveleket körültekintéssel kell kezelni, szükség esetén az üzemeltetésért felelős külsős informatikus segítségét kell kérni, a gyanús levelet a rendszerből el kell távolítani.
- Nagyméretű fájlokat tilos sok címzettnek elküldeni, mert az túlzott mértékben leterheli a hálózat forgalmát, illetve megbéníthatja azt. Nagyméretű fájlok esetében más adatátadó, adathordozó eszköz igénybevételével kell eljuttatni az információt.
- Az alábbi információk nyílt továbbítása elektronikus levélben szigorúan tilos:
    - nem a nyilvánosságnak szánt üzleti és pénzügyi információk

- a KÖH informatikai vagy biztonsági rendszerére vonatkozó bármilyen adat (pl.: jelszavak, felhasználó nevek, IP címek)
- nem a nyilvánosság számára készült belső eljárásrendek (pl.: jelen szabályzat)

- A KÖH tevékenységével kapcsolatos levelet csak a címzett kifejezett kérésére szabad ingyenes internetes levelezési címre küldeni.
- Amennyiben valaki hiba folytán olyan elektronikus üzenetet kap, melynek szándékolt címzettje nyilvánvalóan nem Ő, köteles azt – amennyiben egyértelműen meghatározható – az eredeti címzettnek továbbítani, erről a feladót értesíteni. Amennyiben az eredeti címzett nem határozható meg, úgy köteles a feladót a téves kézbesítésről értesíteni és a levelet postafiókjából törölni.

8.4.2.3. Az elektronikus levelezés ellenőrzése

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

Az informatikai biztonságot ellátó személyeknek munkájuk során szükségük lehet a levelek tartalmának vizsgálatára, ez azonban csak alapos indokkal, dokumentáltan, a jegyző írásbeli engedélyével történhet. Minden olyan esetben, amikor ezt valamilyen különleges eset (pl.: fegyelmi eljárás, vagy vétség megállapítása) nem indokolja, a postafiók használóját előzetesen értesíteni kell a vizsgálatról.

9. Az elektronikus információs rendszerek nyilvántartása

9.1. Célja

Az elektronikus információs rendszerek nyilvántartásának célja:

- szoftvergazdálkodás optimalizálása
- a KÖH szoftver- és hardvervagyonának nyilvántartása
- a KÖH működéséhez szükséges informatikai feltételek biztosítása, az optimalizált eszközhasználat segítségével

9.2. Felelősök

A KÖH elektronikus információs rendszerinek nyilvántartását az üzemeltetésért felelős külsős informatikus végzi. A nyilvántartás karbantartásáért szintén az üzemeltetésért felelős külsős informatikus felel. Felülvizsgálatát, ellenőrzését az Informatikai Biztonsági Felelős végzi.

9.3. A nyilvántartásban tárolt adatok

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

- szoftver neve, azonosítója
- szoftver gyártója, kapcsolattartója (amennyiben releváns)
- licencek száma (amennyiben azok a KÖH kezelésében vannak)

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

9.4. A szoftverekben, rendszerekben tárolt adatok köre

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

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

A nyilvántartásnak az alábbiakat kell tartalmaznia:

- szoftver neve

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

10. Biztonságtervezés

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

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

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

10.1. Rendszerbiztonsági terv

Új elektronikus információs rendszerek bevezetése előtt el kell készíteni az elektronikus információs rendszerek rendszerbiztonsági tervét, mely a következőket tartalmazza:

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

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

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

11. Fizikai környezet és biztonság

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

11.1. Biztonsági zónák

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

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

11.1.1. Az irodák, a helyiségek és az eszközök biztonsága

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

A KÖH-nek az irodák védelmét az alábbiak szerint kell szabályozni:

- a kulcsokat nem szabad nyilvános, idegenek számára is könnyen hozzáférhető helyen tárolni
- a dokumentumok tárolása védett területen történjen
- azokban az időszakokban, amikor a helyiségek felügyelet nélkül maradnak, az ajtókat és ablakokat zárva kell tartani

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

11.1.2. Védelem a külső és környezeti fenyegetettségek ellen

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

11.2. A berendezések fizikai védelme

11.2.1. A berendezések karbantartása

Az informatikai eszközökön javítást, módosítást, illetve új eszközök telepítését csak az üzemeltetésért felelős külsős informatikus, vagy az IBF által engedélyezett és ellenőrzött külső vállalkozó végezhet.

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

11.2.2. A berendezések biztonságos tárolása és újrafelhasználása

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

Az érzékeny információt tartalmazó tárolóeszközöket vagy meg kell fizikailag semmisíteni, vagy biztonságosan felül kell írni (biztonsági törlést végző alkalmazás pl.: Shredder, AlienVault, stb) az egyszerű, szokásos törlési művelet alkalmazása helyett.

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

11.2.3. Az eszközök selejtezése, elvitele

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

12. Általános rendszer és szolgáltatás védelmi intézkedések

12.1. Védelem rosszindulatú programok ellen

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

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

A rosszindulatú kódok a bizalmasság, a sértetlenség és a rendelkezésre állás elvesztéséhez is vezethetnek.

12.1.1. A rosszindulatú programokat ellenőrző eszközök

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

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

A KÖH a vírusvédelmi feladatokat az ESET NOD szoftver és az AVG free szoftver segítségével látja el. Az üzemeltetésért felelős külsős informatikus köteles minden KÖH-i számítógépen a szoftvert telepíteni és a megfelelő konfigurálásáról gondoskodni.

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

A felhasználónak tilos kikapcsolnia ezt a védelmet.

12.1.1.1. A vírusvédelmi programot az irányelvekben meghatározott időpontban és gyakorisággal frissíteni kell, automatikus frissítési funkció beállításával.A vírusvédelmi rendszer kialakítása és működtetése

A KÖH a rosszindulatú kódok alábbi fajtáját határozza meg:

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

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

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

12.1.2. Teendők vírusfertőzés esetén

Vírus támadás, vagy egyéb incidens esetén az azt észlelő személynek haladéktalanul tájékoztatnia kell az üzemeltetésért felelős külsős informatikust a fertőzésről vagy annak gyanújáról.

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

12.2. Az adathordozók biztonságos kezelése

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

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

A KÖH-ben csak a KÖH tulajdonában lévő, regisztrált adathordozót lehet használni. Adathordozó igénylését az üzemeltetésért felelős külsős informatikushoz kell benyújtania az illetékes vezetőnek.

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

12.2.1. Hordozható adathordozók kezelése

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

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

12.2.1.1. Az adathordozók tárolása

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

12.2.1.2. A tárolók környezeti paramétereire vonatkozó előírások

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

Ezért az alábbi szabályokat kell betartani a tárolás során:

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

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

12.2.1.3. Az elöregedésből fakadó adatvesztés elleni megelőző intézkedések

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

12.2.1.4. A másodpéldányok biztonságos tárolására vonatkozó előírások

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

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

12.2.1.5. Az adathordozók kivitele

Számítástechnikai eszközöket, adathordozókat, programokat kizárólag a jegyző engedélyével szabad kivinni a KÖH-ből.

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

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

12.2.2. *Az adathordozók újrahasznosítása, selejtezése*

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

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

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

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

12.2.3. *Adatkezelési eljárások*

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

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

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

12.2.4. *Adathordozók szállítása*

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

A számítástechnikai adathordozók szállítására vonatkozóan az alábbi intézkedéseket kell megtenni:

- a szállítást lehetőleg a KÖH munkatársa végezze, külső szállítócég csak szerződéses viszony esetében végezhet szállítást; ilyenkor a szerződésben ki kell térni a szükséges biztonsági intézkedésekre

- az adathordózókat védeni kell a fizikai sérülésektől, ennek érdekében a gyártó által jóváhagyott módon kell a szállítást megvalósítani
- a kockázattal arányosan, az értékes információkat hordozó adathordozókat olyan speciális csomagolással kell ellátni, mely láthatóvá teszi a felbontást, vagy az arra tett kísérletet

12.3. Biztonsági megfigyelőrendszer használata

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

12.3.1. Biztonsági események naplózása

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

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

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

12.3.2. A rendszerhasználat megfigyelése

Az informatikai rendszerekben történő, felhasználók által elvégzett tevékenységeket rögzíteni, naplózni kell.

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

12.3.3. *Naplózási információk védelme*

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

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

A naplóbejegyzéseknek az alábbi adatokat kell tartalmaznia:

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

12.3.4. *Naplózási infrastruktúra*

12.3.4.1. Naplóforrások beállítása

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

12.3.4.2. Log tárolás

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

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

12.3.4.3. Logok megsemmisítése, logrotálás

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

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

13. Hozzáférés ellenőrzés

13.1. A hozzáférés ellenőrzés követelményei

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

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

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

13.1.1. A hozzáférés ellenőrzésének szabályai

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

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

13.1.1.1. Külső fél hozzáférés ellenőrzése

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

13.2. A felhasználó hozzáférés ellenőrzése

A felhasználók csak jóváhagyott hozzáférés-védelmi megoldásokat alkalmazhatnak.

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

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

Az eljárásoknak ki kell terjednie a felhasználók szervezetben betöltött egész életciklusára a belépéstől, a munkakör változáson át a szervezet elhagyásáig.

13.2.1. A felhasználók regisztrációja

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

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

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

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

13.2.2. Jogosultságok kezelése

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

A KÖH az alábbi felhasználói jogosultságukat különbözteti meg:

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

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

13.2.3. Felhasználói jelszavak kezelése

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

- a felhasználóval meg kell ismertetni a jelszóhasználat szabályait (jelszóhossz, egyediség, bonyolultság)
- a felhasználóknak ideiglenes jelszavat kell biztosítani, melyet az első belépés után kötelezően meg kell változtatniuk
- a felhasználók jelszavaikat csak a biztonsági intézkedések maximális betartása mellett tárolhatják, függetlenül az információhordozó formai megjelenésétől
- az informatikai rendszerekben szigorúan tilos rejtjelezetlen formában tárolni a jelszavakat

13.2.4. Hozzáférési jogosultságok visszavonása vagy korlátozása

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

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

A hozzáféréseket csak a rendszergazda módosíthatja, szüntetheti meg, vagy vonhatja vissza.

13.3. A felhasználó felelősségei

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

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

13.3.1. Jelszóhasználat

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

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

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

13.3.1.1. A felhasználói jelszavakkal szemben támasztott követelmények

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

- minimális jelszóhossz: 7 karakter
- központi jelszómegadás utáni első bejelentkezéskor kötelező jelszócsere
- jelszó maximális élethossza: 1 év (egyes szakrendszerek esetében ez eltérhet)
- jelszó zárolása: 5 kísérlet után
- jelszóképzés szabályai: kisbetűt, nagybetűt és számot is kell tartalmaznia, valamint nem lehet része a felhasználónév

13.3.2. Felügyelet nélküli berendezésekre vonatkozó felhasználói felelősségek

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

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

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

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

13.3.3. „Tiszta íróasztal, tiszta képernyő" irányelvek

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

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

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

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

Az informatikai rendszerekben tárolt bizalmas adatok nyomtatása nem történhet felügyelet nélkül. A KÖH-nek olyan intézkedéseket kell hozni, melyek megakadályozzák az illetéktelen nyomtatást, vagy a nyomtatás során keletkezett papír alapú anyag illetéktelen kézbe kerülését. Annak betartásáért a jegyző felel.

13.4. Azonosítás és hitelesítés

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

Az informatikai rendszer, és az abban tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának védelme érdekében minden lehetséges eszközt fel kell használni annak érdekében, hogy megakadályozzuk az illetéktelen hozzáféréseket a számítástechnikai erőforrásokhoz.

Ezeknek a következőket kell tenniük:

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

13.4.1. Biztonságos hitelesítési, bejelentkezési eljárások

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

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

Biztonságos bejelentkezési eljárásnak az alábbiakat tekintjük:

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

13.4.2. A felhasználó azonosítás, hitelesítése

A KÖH informatikai rendszerének minden felhasználóját egyedi módon azonosítani kell. Ez az egyedi azonosító a felhasználó kizárólagos azonosítására szolgál, ennek értelmében nem módosítható, másnak át nem adható. Az egyedi azonosító a felhasználó KÖH-ből való távozása után sem törölhető az esetleges visszakeresések érdekében. Ha egy felhasználó valamilyen oknál fog rövidebb vagy hosszabb ideig elhagyja a szervezetet, úgy visszatértekor számára biztosítani kell a korábbi azonosítójának használatát.

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

A felhasználói azonosítók kiadása az üzemeltetésért felelős külsős informatikus feladata. Új azonosító kiadása csak a jegyző engedélyével lehetséges.

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

13.5. A mobil informatikai tevékenység, a távmunka

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

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

13.5.1. A mobil informatikai tevékenység

Alapvető biztonsági cél, hogy a KÖH-ben megfelelő biztonsági intézkedéseket alkalmazzanak a mobil számítástechnikai berendezések védelmére.

Mobil számítástechnikai eszköznek az alábbiak számítanak:

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

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

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

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

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

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

A mobil hálózatok vezeték nélküli összeköttetését a kockázatok figyelembe vételével csak az üzemeltetésért felelős informatikus engedélyezheti.

13.5.2. A távmunka

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

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

14. Az informatikai rendszerek informatikai biztonsági követelményei

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

Az alkalmazásokra vonatkozó biztonsági intézkedéseket dokumentálni kell.

14.1. A bemenő adatok hitelesítése

Az alkalmazások bemenő adatait hitelesíteni, ellenőrizni kell.

Az ellenőrzés eszközei:

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

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

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

14.2. Az adatfeldolgozás ellenőrzése

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

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

14.2.1. Veszélyeztetett területek

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

14.2.2. Vezérlő és ellenőrző eljárások

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

A megfelelő biztonsági intézkedések meghozatala az üzemeltetésért felelős külsős informatikus feladata. A biztonsági intézkedések meglétének ellenőrzését az Informatikai Biztonsági Felelős végzi.

14.3. Az üzenetek hitelesítése

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

14.4. A kimenő adatok hitelesítése

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

A kimenő adatok védelmi eljárásai:

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

14.5. Kriptográfiai eszközök

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

14.5.1. *A kriptográfiai eszközök alkalmazásának irányelvei*

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

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

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

14.5.1.1. Titkosítás

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

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

14.5.1.2. Digitális és elektronikus aláírás

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

Az elektronikus aláírás olyan kriptográfiai eljárás, melynek segítségével akár a kézzel írott aláírással egyenértékű bizonyító erejű dokumentum hozható létre a hatályos jogszabályoknak megfelelően, különösen az elektronikus aláírásról szóló 2001. évi XXXV. törvény szerint.

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

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

14.5.2. Kulcskezelés

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

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

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

14.6. Informatikai biztonság a bevezetési és karbantartási folyamatokban

Az alkalmazásokat három különböző életciklusba sorolhatjuk:

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

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

14.6.1. Változáskezelés

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

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

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

A változtatások során az alábbi szabályokat kell betartani:

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

14.6.2. Az operációs rendszer megváltoztatásával kapcsolatos ellenőrzések

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

A cserét minden esetben szabályozotton, előzetes vizsgálatok, kockázatelemzések megtételével kell megvalósítani, biztosítva az ügymenet folytonosságot. A javítócsomagokat kizárólag a rendszergazda vezetheti át a rendszeren, a felhasználóknak semmiképpen nem engedélyezhető a munkaállomásokon való telepítése.

14.6.3. A szoftvercsomagok frissítésének korlátozása

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

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

14.6.4. A rendszerinformációk kiszivárgásának megakadályozása

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

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

14.6.5. A szoftverfejlesztés kihelyezése

A KÖH nem végez szoftverfejlesztést.

14.7. A műszaki sérülékenységek kezelése

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

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

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

14.7.1. A műszaki sérülékenységek ellenőrzése

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

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

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

15. Ügymenet-folytonosság

15.1. Az ügymenet-folytonosság informatikai biztonsági szempontjai

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

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

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

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

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

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

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

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

Meg kell fontolni a kritikus adatvagyonra történő biztosításkötést.

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

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

A KÖH-nek rendelkeznie kell működésfolytonossági tervvel, melynek intézkedéseit és szabályait pontosan dokumentálni szükséges.

15.1.2. Az ügymenet-folytonossági hatásvizsgálatok és a kockázatok elemzése

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

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

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

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

15.1.3. Az ügymenet-folytonossági terv kidolgozása

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

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

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

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

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

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

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

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

15.1.4.1. A tervek tesztelése

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

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

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

15.1.4.1.2. A tervek karbantartása és újraértékelése

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

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

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

15.2. Ügymenet-folytonosság fázisa és tartalma

15.2.1. Rendkívüli helyzetek osztályozása, minősítése

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

15.2.1.1. Katasztrófa

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

Ilyen katasztrófák az alábbiak lehetnek:

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

15.2.1.2. Krízis

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

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

- megoldás
- kompromisszum
- összeomlás

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

15.2.1.3. Részleges leállás

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

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

A részleges leállás fő okai:

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

15.2.1.4. Incidens

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

Az incidensek lehetnek véletlen események vagy szándékos károkozás eredményei is.

A KÖH a leggyakrabban előforduló típusokként az alábbiakat különbözteti meg:

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

15.2.2. Az ügymenet-folytonosság fázisai

15.2.2.1. Azonnali reakció fázis

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

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

A fázis feladatai:

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

15.2.2.2. Átmeneti fázis

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

Ezen információk az alábbiak lehetnek:

- a nem várt eseménnyel érintett kulcsfontosságú folyamatok ismerete
- az érintett folyamatok és az ezeket működtető rendszerek függőségei
- az ezeket a folyamatokat támogató erőforrások listája
- a minimális szolgáltatás fenntartásához szükséges alternatív lehetőségek és az ezek kiszolgálását támogató erőforrások
- az érintett folyamatok helyreállításának és stabilizálásának tervei

15.2.2.3. Helyreállítási fázis

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

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

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

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

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

15.3. Eljárás a rendkívüli helyzetek elhárítására

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

15.3.2. Esemény osztályozása

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

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

15.3.2.1. Kivétel

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

15.3.3. 3-as és 4-es szintű események kezelése

A rendszergazda a 3-as és 4-es szintű eseményeket saját hatáskörben oldja meg. Amennyiben olyan incidens történt, mely további informatikai segítségnyújtást nem igényel a rendszergazda jelzi azt a szervezeti csoport vezetőjének, a rendszer automatikusan naplózza az eseményt.

Informatikai segítségnyújtás esetén a rendszergazda az eseményre tekintettel elvégzi a hibaelhárítást, biztosítja az ügymenet normál módú működését. Ezzel le is zárult a 3-as és 4-es szintű események kezelése.

15.3.4. 1-es és 2-es szintű események kezelése

15.3.4.1. Értesítés

1-es és 2-es szintű események esetében azonnal értesíteni kell az üzemeltetésben és a rendkívüli események elhárításában érintett személyeket. Az érintett személyek: az üzemeltetésért felelős informatikus, az Informatikai Biztonsági Felelős és a jegyző, ez szükség szerint kibővül a katasztrófa elhárításban résztvevő szervekkel.

Ezzel egy időben azonnal meg kell kezdeni az emberi élet és eszközök mentését.

15.3.4.2. Helyzetelemzés, katasztrófahelyzet kihirdetése

Az üzemeltetésben és a rendkívüli események elhárításában résztvevő személyek felmérik a helyzetet, megvizsgálják az informatikai rendszerek állapotát, döntenek a további intézkedésekről az ügymenet-folytonossági tervnek megfelelően.

A bekövetkezett esemény helyzetértékelése alapján kihirdetésre kerül az informatikai katasztrófa, vagy krízis, melyről valamennyi érintett tájékoztatást kap. Ezzel egyidejűleg megkezdődik a visszaállítás folyamata a mentés-visszaállítási terv alapján.

15.3.4.3. Az informatikai rendszerek visszaállítása

A lehető legrövidebb időben belül meg kell tenni a kritikus informatikai rendszerek visszaállításához szükséges lépéseket. A kritikus rendszerek újraindítása érdekében a szükséges és rendelkezésre álló tartalék rendszereket és erőforrásokat is be kell vonni. A kritikus informatikai rendszerek listáját az informatikai eszközök adtabázisa tartalmazza.

A visszaállítás során az elsődleges prioritással bíró rendszerek bekapcsolása és működőképességének tesztelése is megtörténik. Sikeres tesztet követően meg kell vizsgálni, hogy a további kiesett rendszerek normál üzembe való visszaállításai is megtörténhetnek-e.

15.3.4.4. Teljes helyreállítás

A lehető legtöbb rendszer visszaállítása után következik a helyreállítás fázisa, amikor a kritikus ügyviteli folyamatokhoz szükséges rendszerek az eredeti, vagy az eredetivel azonos erőforrást biztosító eszközök beállításával stabilizálásra kerülnek.

A folyamatnak akkor van vége, amikor az egész informatikai rendszer az eredetivel legalább azonos módon működőképes.

15.3.4.5. Kárelemzés

A helyreállítás után történik a károk felmérése, melyre szükség esetén külön csoport alakul. Az eseményről jelentést kell készíteni.

A jelentésnek az alábbiakat kell tartalmaznia:

- esemény időpontja
- esemény megnevezése
- esemény minősítése (szint meghatározása)
- esemény részletes leírása
- eseményben résztvevő személyek neve
- eseményben érintett informatikai rendszerek felsorolása
- visszaállítás időpontja
- tesztelés eredménye
- normál üzemmódra történő helyreállás időpontja
- keletkezett károk leírása

A károk felmérése és elemzése után az üzemeltetésért felelős informatikus és az Informatikai Biztonsági Felelős értékeli a helyzetet és meghozza a döntést a kockázatelemzés illetve kockázatkezelési eljárásra vonatkozóan.

16. Szabályozási környezet

16.1. Megfelelés a hatályos jogszabályi környezetnek

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

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

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

16.1.1. A vonatkozó hatályos jogszabályok, szabványok és eljárások

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

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

A melléklet naprakészségéért a jegyző felel.

16.1.2. A szellemi tulajdonjogok védelme

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

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

A követelmények megszegésének elkerülésére az alábbi intézkedések kerüljenek bevezetésre:

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

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

16.1.3. A szervezet adatainak biztonsága

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

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

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

16.1.4. A személyes adatok védelme

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

16.1.5. A védelmi eszközökkel elkövethető visszaélések megelőzése

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

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

16.1.6. A kriptográfiai eszközök kezelésének szabályozása

Minősített adatok esetében a rejtjelezést csak a 2009. évi CLV. és a 2011. évi CXVII. törvény szerint szabad végezni. Érdemes jogi tanácsot kérni, mielőtt rejtjelezett információt vagy kriptográfiai eszközöket más országba továbbítunk.

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

A KÖH-nek gondoskodnia kell arról, hogy a rendszerek megfeleljenek a biztonságpolitikájának, szabályzatainak és a szabványoknak.

Az informatikai rendszerek biztonságát időről időre felül kell vizsgálni.

16.2.1. Az informatikai biztonsági előírásoknak való megfelelés

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

Ennek keretében vizsgálni kell:

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

A KÖH elvárja az informatikai rendszerek tulajdonosaitól, hogy eltűrjék és segítsék a rendszerek átvizsgálását.

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

A biztonsági megfelelősséget a következő esetekben kell vizsgálni:

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

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

Az informatikai rendszert védő biztosítékokat a következő módon lehet ellenőrizni:

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

16.2.2. A műszaki követelményeknek való megfelelés

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

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

A felülvizsgálatok végrehajtásáért az üzemeltetésért felelős informatikus felel.

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

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

16.3. Az informatikai rendszerek biztonsági ellenőrzésének szempontjai

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

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

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

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

16.3.1. Rendszer-auditálási óvintézkedések

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

Az alábbiakat kell megvalósítani:

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

16.3.2. Rendszer-auditálási eszközök védelme

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

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

17. Záró rendelkezések

Jelen dokumentum 2017. augusztus 1-én lép hatályba.

.....

Gácsér Béla

jegyző

KEVERMESI KÖZÖS ÖNKORMÁNYZATI HIVATAL * JEGYZŐJE *

1. számú melléklet

Vonatkozó hatályos jogszabályok, szabványok és ajánlások

Jogszabályok:

- Az informatikai biztonsággal kiemelten foglalkozó jogszabályok:
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 187/2015. (VII.13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat – és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
- 41/2015. (VII.15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról
- 1139/2013. (III.21.) kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

A titokvédelemmel kapcsolatos jogszabályok:

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

A személyes adatok kezelésével és védelmével kapcsolatos jogszabályok:

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

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

Az elektronikus aláírásról, az elektronikus szolgáltatásokról szóló jogszabályok:

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

Szabványok és ajánlások:

- Magyar Informatikai Biztonsági Ajánlások - MIBIK és MIBÉTS
- ISO/IEC 13335-1:2004 Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management
- ISO/IEC 20000-1:2005 Information technology - Service management - Part 1: Specification
- ISO/IEC 20000-2:2005 Information technology - Service management - Part 2: Code of

practice

- ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements
- ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management
- ISO/IEC 13335-1:2004 Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management
- ISO/IEC TR 13335-2:1997 Information technology - Guidelines for the management of IT Security - Part 2: Managing and planning IT Security
- ISO/IEC TR 13335-3:1998 Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security
- ISO/IEC TR 13335-4:2000 Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards
- ISO/IEC TR 13335-5:2001 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security
- Az Európai Unió Tanácsának Biztonsági Szabályzata (kiadva az Európai Unió Tanácsának 2001/264/EK számú határozatával).
- SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANISATION (NATO) - C-M(2002)49 /AC/35-D/2000 Directive on Personnel Security, AC/35-D/2001 Directive on Physical Security, AC/35-D/2002 Directive on Security of Information, AC/35-D/2003 Directive on Industrial Security, AC/35-D/2004 Primary Directive on INFOSEC, AC/35-D/2005 INFOSEC Management Directive for Communications and information Systems/
- ISACA ajánlások: COBIT (Control Objectives for Information and Related Technology), COBIT MAPPING - Mapping of ISO/IEC 17799:2000 With COBIT, COBIT SECURITY BASELINE

,

2. számú melléklet

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

Az informatikai rendszer megnevezése	Az informatikai rendszer leírása	Adatgazda	Rendszerben kezelt adatok	Tárolt adatok köre		Az informatikai rendszer telepítésének helye		Bizalmasság	Sértetlenség	Rendelkezésre állás	Biztonsági osztály
				Önkormányzati	Állami	Saját szerveren/helyben	Külső szolgáltató/interneten keresztül				
CGR	önkormányzati pénzügy-számviteli integrált rendszer, amely az ASP bevezetése után a korábbi évek gazdálkodási adatinak kinyerésére szolgál	**jegyző**	pénzügyi, számviteli adatok	x			x	2	2	2	2
DMSONE Professional	iktató program	jegyző	iktatás	x		x		2	2	1	2
E-iktat	iktató program	jegyző	iktatás	x		x		2	2	1	2
Országos Szociális Információs Rendszer	PTR: pénzügyi és természetbeni ellátások rendszere, MÜKENG: szociális szolgáltatások működési engedélyezése	jegyző	szociális adatok	x			x	2	2	1	2
KIRA	MÁK központosított illetményszámfejtési	jegyző	béradatok	x			x	2	2	2	2

	rendszer										
KIR	köznevelési információs rendszer	jegyző	oktatási adatok	x			x	2	2	1	2
TÉR	közszolgálati teljesítményértékelési rendszer	jegyző	teljesítmény adatok	x			x	2	2	1	2
TVP (Probono)	Közigazgatási és továbbképzési vizsgaportál	jegyző	továbbképzések	x			x	2	2	1	2
ASP adó szakrendszer	helyi adók kezelése	jegyző	önkormányzati adók	x			x	4	4	4	4
ASP gazdálkodási szakrendszer	önkormányzati pénzügyi-gazdálkodási, költségvetési szakrendszer	jegyző	könyvelés, számlázás	x			x	3	3	3	3
ASP keretrendszer	felhasználók felvétele, jogosultságok kiadása az ASP-ben	jegyző	keretrendszer	x			x	4	4	4	4

3. számú melléklet

A KÖH informatikai eszköznyilvántartása

Kevermesi Közös Önkormányzati Hivatal

Informatikai eszköz megnevezése	Informatikai eszköz azonosítója	Telepített operációs rendszer	Egyéb szoftverek
számítógép konfiguráció	01. (Admin-PC)	Windows 7 HP	Office 2007, ÁNYK, e-Szignó 3.2, Nero 8 micro, ESET ENDPOINT AV 5.0.
számítógép konfiguráció	02. (Marika)	Windows XP Pro	Office XP Sandard, ESET NOD 32 4.0
számítógép konfiguráció	03. (Jegyző-PC)	Windows 10 Pro	Libre Office 5, e-Szignó 3.2.7.17., ESET NOD32 AV9
számítógép konfiguráció	04. (Polgármester-PC)	Windows 10 Home	Libre Office 4.2, ESET NOD 32 AV8
számítógép konfiguráció	05. (Admin-PC1)	Windows 10 Home	DMS One Pro Kliens, Hercules 1.1, Office 2007, ESET NOD 32 AV9
számítógép konfiguráció	06. (Polgármester)	Windows XP Pro	Office 2007 Professional, ESET NOD 32 AV4
számítógép konfiguráció	07. (M014618)	Ubuntu 10.04.1 LTS	Open Office
számítógép konfiguráció	08. (Anyakonyv_1)	Windows 7 Home	Office 2007 Enterprise, ESET NOD 32 AV4

számítógép konfiguráció	09. (Penzugy_utalos)	Windows 10	Libre Office 4, ESET NOD 32 AV8
számítógép konfiguráció	10. (Penzugy_levelezos)	Windows 10	Libre Office 4, ESET NOD 32 AV9
számítógép konfiguráció	11. (Adougy_gep)	Windows 10	Önkadó, Libre Office 5. Office 2007, ESET NOD 32 AV9
számítógép konfiguráció	12. (Penzugy_2)	Windows 10	Libre Office 4, Office 2007, CGR Tervezés Számvitel, CGR Főkönyv, CGR Pénzügy, ÁNYK, ESET NOD 32 AV8
számítógép konfiguráció	13. (Fokonyv)	Windows 8.1	Libre Office, CGR Főkönyv, CGR Pénzügy, ÁNYK, ESET NOD 32 AV8
számítógép konfiguráció	14. (Muszak-PC)	Windows 10	Office 2007, KER-INFO Nyilvántartó, PTI-KER-INFO 2016, TUR-INFO Nyilvántartó, ESET NOD 32 AV9
laptop	15. (Felhasznalo-HP)	Windows 7	Office 2010, KER-INFO Nyilvántartó, Kompozer, Libre Office, ESET Endpoint AV
számítógép konfiguráció	16. (User-PC)	Windows 7	CGR Pénzügy, CGR Analitika, KIRA, Open Office 3.3, ESET AV7

Kevermesi Közös Önkormányzati Hivatal

Kisdombegyházi Kirendeltség

Informatikai eszköz megnevezése	Informatikai eszköz azonosítója	Telepített operációs rendszer	Egyéb szoftverek
számítógép konfiguráció	USER-PC	Windows 7	Office, CGR, AVG free
számítógép konfiguráció	IRODA2-PC	Windows 7	Office, AVG free, ASP
számítógép konfiguráció	Iroda8	Windows 7	Office, TEA, CGR, AVG free, ASP
számítógép konfiguráció	JUDIT	Windows 7	Office, AVG free,ASP
számítógép konfiguráció	Polg-87C8C28ABA	Windows XP	Office, AVG free
számítógép konfiguráció	ADÓ	Windows 10	Office, Önkadó, AVG free, ASP
számítógép konfiguráció	Szerver	Windows 7	Office, KIRA, ÁNYK, AVG free,ASP
számítógép konfiguráció	Gazdálkodás	Windows 10	Office 2010, AVG free,E-iktat, ASP

Kevermesi Közös Önkormányzati Hivatal

Magyardombegyházi Kirendeltség

Informatikai eszköz megnevezése	Informatikai eszköz azonosítója	Telepített operációs rendszer	Egyéb szoftverek
laptop	Ovi laptop	Windows 7	Office 2007, AVG
számítógép konfiguráció	ADO	Windows 10	Office, AVG free, Önkado, ASP
számítógép konfiguráció	Gazdálkodás	Windows 10	Office, AVG free, ASP
számítógép konfiguráció	Gazdálkodás2	Windows 7	Office 2007, AVG free, ASP