INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

Kunszentmiklósi
Polgármesteri Hivatal
6090 Kunszentmiklós,
Kálvin tér12.

Készítette: Muhr László, Dénes György	Jóváhagyta: Kelemen Henrietta
Beosztás: Információbiztonsági felelős	Beosztás: Jegyző
Dátum:2018.05.15	Dátum:2018.05.15
Aláírás:	Aláírás:

Dokumentumváltozások története

Verzió	Dátum	Változás leírása	Módosította
verzió 1.	2018.05.15	végleges átadott verzió	Muhr László és Dénes György

Tartalom

1 BEVEZETÉS

1.1 A szabályzat célja, felépítése

Az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) célja a biztonsági követelményrendszer meghatározása egy kétszintű IBSZ létrehozásával.

1.1.1 A kétszintű IBSZ belső szabályozási környezete

Kunszentmiklósi Polgármesteri Hivatal IBSZ-e mint jegyzői utasítás lép hatályba és az alábbi informatikai szabályozásokkal együtt fedi le a Hivatal információbiztonsági szabályozását.

1.1.1.1 Információbiztonsági szabályozások

- Informatikai biztonsági politika
- Informatikai biztonsági stratégia
- Informatikai stratégia
- Kockázatkezelési és Elemzési eljárás
  - Kockázatkezelési és elemzési Eljárás 1. és 2. melléklet
  - Cselekvési terv
- Informatikai Biztonsági Szabályzat
- Informatikai Biztonsági Szabályzat 1mellélet Fogalomtár
- Informatikai Biztonsági Szabályzat 2mellélet Felelősök feladatai
  - Fizikai és Környezeti Biztonsági Utasítás
  - Informatikai Üzemeltetési Utasítás
    - Hozzáféréskezelési és hálózati biztonság / Jogosultsági utasítás
    - Vírusvédelemi utasítás
    - Változáskezelési utasítás
    - Mentési, archiválási utasítás
  - Működés folytonosság és Katasztrófaelhárítási terv
  - Felhasználói utasítás
  - Információbiztonsági kézikönyv

1.1.1.2 Hivatali szabályozások

Szabályzatok:
• Leltár jegyzékek, • Iratkezelési szabályzat • Gazdálkodási szabályzat • Pénzkezelési szabályzat • SZMSZ

1.1.2 Hivatali szintű IBSZ

- Az Informatikai Biztonsági Szabályzat keretdokumentumként az általános és minden rendszerre érvényes részletesebb szabályokat tartalmazzák:
- a Hivatal vezetésének egyértelmű nyilatkozatáról az informatikai biztonság szabályozott kialakításáról, illetve fenntartásáról,
- az informatikai biztonság alapvető fogalmairól,
- az informatikai biztonsággal kapcsolatos feladatról és hatáskörökről, és felelősségekről,
- a biztonsági események jelentésének rendjéről,
- elvekről, követelményekről, kötelező eljárásokról és szabványokról,
- a biztonsági irányelvekről, amelyek meghatározza az informatikai infrastruktúra teljes életciklusát,
- és a tervezésnél, beszerzésénél, fejlesztésénél, üzemeltetésénél és selejtezésénél alkalmazandó általános biztonsági elvárásokról.

1.1.3 Rendszer szintű IBSZ

A rendszer szintű IBSZ külön dokumentumokban részletezi az IBSZ által megfogalmazott szabályok szerinti:

- eljárásokat, biztonsági utasításokat, mely leírja a biztonsági intézkedéseket, azok dokumentálásának és ellenőrzésének feladatait, a végrehajtás felelősét és a végrehajtás gyakoriságát vagy idejét;
- végrehajtási eljárásrendek, melyek részletesen leírják az biztonsági utasításban meghatározott feladatok végrehajtásának, ellenőrzésének módját, felelőseit, gyakoriságát, eszközeit, és technikai lépéseit és ezek folyamatát.

1.2 Fogalomtár

A Szabályzatban használt fogalmak magyarázatát az 1. számú melléklet tartalmazza.

2 HIVATALI BIZTONSÁG

2.1 Az informatikai biztonság belső Hivatali struktúrája

2.1.1 Vezetői elkötelezettség

Cél:

A Hivatal létrehoz egy vezetői fórumot, amely szavatolja, hogy a biztonsági kezdeményezéseket a vezetés jól érzékelhető támogatása kíséri. Ez a fórum a szükséges erőforrások rendelkezésre bocsátásával támogassa az informatikai biztonságot. Ennek a testületnek olyan emberekből kell állnia, akiknek megvan a követelmények azonosításához, politikák kialakításához, biztonsági programok írásba foglalásához, a munka értékeléséhez és az informatikai biztonsági vezető irányításához szükséges képessége, és szolgáltatások nyújtásában, valamint felhasználásában vesznek részt.

Szabályok:

Az informatikai biztonsági fórum hatáskörébe tartozik:

- javaslattétel az informatikai vezető testület számára a stratégiai tervezéshez, az informatikai biztonsági célok megfogalmazásához és azok Hivatali integrációjához;
- az informatikai biztonsági irányelvek és feladatok vizsgálata és jóváhagyása, a megvalósításhoz szükséges humán és anyagi erőforrások biztosítása;
- az informatikai biztonsági intézkedések teljes körű bevezetésének koordinációja és biztosítása Hivatali szinten;
- a bevezetett informatikai biztonsági intézkedések, irányelvek hatékonyságának folyamatos felülvizsgálata;
- az információs erőforrások súlyos veszélyeztetettségében történő jelentős változások nyomon követése;
- az informatikai biztonsági események nyomon követése;
- az informatikai biztonság fokozását szolgáló jelentős kezdeményezések jóváhagyása;
- az informatikai biztonsági vezető személyének kijelölése, feladat és hatáskörének meghatározása;
- az informatikai biztonságtudatosság fenntartása oktatás keretében.

2.1.2 Az informatikai biztonság és a Hivatali struktúra összehangolása

Cél:

Az informatikai biztonság Hivatali struktúrájának összehangolása magában foglalja a vezetők, felhasználók, adminisztrátorok, rendszerfejlesztők, auditorok és a biztonsági munkatársak együttműködését, valamint szakértői jártasságot olyan területeken, mint biztosítás, jogi kérdések, emberi erőforrás, vagy kockázatelemzés. Fontos, hogy a Hivatalen belül a feladat, felelősség és hatáskörök az egyes Hivatali egységek, illetve személyek között jól elkülönüljenek, ezáltal elősegítsék a Hivatal céljainak elérését, az ütköző feladatok csökkentését és a letagadhatatlanságot.

Szabályok:

Ennek érdekében a Hivatal összhangban az Adatvédelmi és adatbiztonsági Szabályzat az információ biztonsághoz kapcsolódóan az alábbi hatásköröket hozza létre: az informatikai biztonság területén is.

- **Informatikai biztonsági fórum:** mely döntésképes a különböző szakterületeket átfogó kérdésekben, és jóváhagyja az informatikai biztonsággal kapcsolatos irányelveket és szabályozásokat.
- **Biztonsági vezető**: a Hivatal jegyzője aki a Hivatal általános és teljes körű biztonságáért felelős.
- **Informatikai biztonsági vezető**: aki a Hivatalben előforduló minden informatikai biztonsághoz kapcsolódó kérdésért felelős, és a biztonsági vezető közvetlen alárendeltje.
- **Információbiztonsági felelős:** aki a 2013. évi L. törvény és a 41/2015. (VII. 15.) BM rendelet szerint végzi el feladatait a Hivatalnál.
- **Belső adatvédelmi felelősök és adatgazdák:** a személyes adatok védelmének biztosításáért a Hivatal ágazatvezetői és az irodavezetői személyesen felelnek az irányításuk alá tartozó Hivatali egységnél az Adatvédelmi és adatbiztonsági szabályzat figyelembe vételével.
- **Felhasználók:** a Hivatal dolgozói és az önkormányzat megválasztott képviselői
- **Informatikai rendszerüzemeltetők:** Külső és belső IT üzemeltetésért felelős személyek és cégek.

2.1.3 Az informatikai biztonság felelősségeinek kiosztása

Cél:

Egyértelműen ki kell jelölni az egyes biztonsági folyamatok felelőseit. Pontosan meg kell határozni minden olyan területet, amelyért az egyes vezetők felelnek. Ennek keretében:

- pontosan azonosítani kell, és egyértelműen meg kell határozni az egyes rendszerekhez tartozó minden eszközt és folyamatot;
- az egyes eszközökért és folyamatokért felelős vezető személyében meg kell egyezni, és a vonatkozó felelősséget dokumentálni kell;
- tisztán és pontosan meg kell határozni a hatásköröket (jogosultsági szinteket), és ezt írásba kell foglalni.
-

Szabályok:

Az Informatikai Biztonsági Szabályzat 2. melléklete részletezi az egyes biztonsági folyamatok felelőseinek feladatit és kötelezettségeit, hatásköreit és jogosultsági szintjeit.

2.1.4 Az adatfeldolgozás engedélyezési eljárásai

Cél:

Az adatfeldolgozás csak akkor engedélyezhető, ha az – legalább – az adatkörök biztonsági osztályba sorolásának megfelelő adatfeldolgozó eszközökön és a Hivatal Adatvédelmi és adatbiztonsági szabályzat figyelembe vételével történik.

Szabályok:

A Jegyző új adatfeldolgozó eszközökre és eljárásokra vonatkozó jóváhagyását csak abban az esetben adhatja meg, ha azok megfelelnek a biztonsági követelményeknek. Az új adatfeldolgozási eszközökre és lehetőségekre vonatkozó engedélyezési eljárásokat kell létrehozni és azokat az IBSZ:

- Felhasználói
- Jogosultság és hozzáférési,
- Hitelesítési és Hálózatbiztonsági
- Változáskezelés
- Üzemeltetési
- Kockázatelemzési

Utasításában rögzíteni kell.

Szabályok új eszközök és rendszerek bevezetése során:

Ellenőrzéssel kell meggyőződni a hardverek, szoftverek és más rendszerösszetevők kompatibilitásáról a bevezetés előtt;

- a minősített, vagy magas kockázatot jelentő adatokat feldolgozó rendszer használata a biztonsági vezető engedélyezi,
- az új rendszert az Információbiztonsági Felelős kötelezően kockázatelemzési eljárásnak veti alá, amely alapján a védelmi intézkedéseket a rendszer bevezetését megelőzően vagy azzal együtt be kell vezetni,
- a minősített, vagy magas kockázatot jelentő adatokat feldolgozó rendszerek használatát a rendszergazdának a biztonsági vezetővel és Információbiztonsági Felelőssel egyeztetve szabályoznia kell;
- az adatfeldolgozás megkezdése előtt minden felhasználónak meg kell ismernie a rendszer használatának biztonsági szabályait, és ezek megértését aláírásával igazolnia kell.

Szabályok személyi használatú eszközök bevezetésére:

Biztonsági kockázatokat hordozó:

- informatikai eszközök,
- adatfeldolgozásra alkalmas mobileszközök,
- otthoni munkavégzés és a távmunkára is használt notebookok, pendriveok
- nagy háttértárral rendelkező mobiltelefonok,
- PDAk,
- és digitális fényképezőgépek,

bevezetése és engedélyezése előtt azokat biztonsági vizsgálatnak kell megelőznie az Informatikai rendszerüzemeltetők és az Információbiztonsági felelős által és a határvédelmi és használati szabályokat be kell vezetni. Az ilyen eszközök használatának biztonsági kockázatait fel kell mérni a Hivatal összes

működési területére vonatkozólag, és ahol szükséges, ott korlátozni kell a használatukat, tiltani a területre történő bevitelüket.

2.1.5 Titoktartási nyilatkozatok

A titoktartási nyilatkozat célja, hogy jogszerű eszközökkel védje a bizalmas információt. A Hivatal Titoktartási nyilatkozatot minden olyan személlyel köteles aláíratni, aki munkája folytán a Hivatal minősített adataihoz hozzáférhet.

A titoktartási nyilatkozatok, megállapodások alapvető tartalmi követelményei a következők:

- a megvédendő információ meghatározása,
- a megállapodás időtartamának meghatározása, ideértve a határozatlan időtartamot is,
- a kívánt intézkedések előírása a megállapodás lejárta utáni időszakra,
- az aláíró jogi felelősségének ismertetése,
- feleljen meg a hatályos jogszabályi rendelkezéseknek,
- rendelkezzen az aláíró jogairól és kötelezettségeiről a bizalmas információk használatára vonatkozólag,
- tartalmazza az aláíró jelentési kötelezettségét a véletlenül bekövetkező jogosulatlan felfedésre és kiszivárogtatásra vonatkozólag,
- definiálja a minősített adatokat érintő, a megállapodás megszűnésére vonatkozó feltételeket, valamint a megállapodás megsértése esetén teendő lépéseket.

A munkatársak az ilyen megállapodást alkalmazásuk alapfeltételeként írják alá. Alkalmi munkaerőnek és a külső személynek, akikről a meglévő, a titoktartási megállapodást is tartalmazó szerződés nem rendelkezik, külön titoktartási megállapodást kell aláírniuk, még mielőtt az adatokhoz vagy az informatikai eszközökhöz hozzáférést nyernének.

A titoktartási megállapodást felül kell vizsgálni, amikor az alkalmazási feltételek megváltoznak, különösen akkor, amikor egy munkavállaló arra készül, hogy elhagyja a Hivatalt, vagy ha a szerződés lejártának időpontja várható.

Felelősség:

A titoktartási nyilatkozat tartalmi követelményeit a védendő információ minősítésének megfelelően a Hivatal Titoktartási nyilatkozata alapján a Jegyző köteles meghatározni. A Hivatal a védendő információ minősítésének, használatának megfelelően a titoktartási nyilatkozatok, megállapodások különböző formáit használhatja.

2.1.6 Együttműködés külső szervezetekkel, hatóságokkal

Felelősség:

A Hivatal Információbiztonsági Felelőse köteles kapcsolatot tartani a Nemzeti Elektronikus Információbiztonsági Hatósággal (a továbbiakban: NEIH), illetve a Kormányzati Eseménykezelő Központtal (Gov CERT), és kezelni az általuk küldött riasztásokat és a Hivatal informatikai üzemeltetésével közösen a megfelelő védelmi intézkedéseket megtenni.

2.1.7 Az informatikai biztonság független felülvizsgálata

Felelősség:

Az informatikai biztonsági politikában, az informatikai biztonsági stratégiában, valamint az informatikai biztonsági szabályzatban rögzítettek megvalósulását az informatikai biztonsági vezető utasításai szerint az Információbiztonsági Felelős ellenőrzi évente egy vizsgálat keretében. Ez az általános ellenőrzési jogkör nem mentesíti a szakterületek (projektek vagy rendszerek) vezetőit az alól, hogy az informatikai biztonság megvalósulását a beosztottaik munkavégzése közben folyamatosan ellenőrizzék.

2.2 Előírások a külső személyek szolgáltatók vagy felek hozzáféréseire

Cél:

A Hivatal informatikai eszközeit csak a Hivatal profiljával indokolható esetben és ellenőrzötten szabad külső személyek számára hozzáférhetővé tenni.

Szabályozás:

A külső személlyel kötött szerződésben az elvárt védelmi intézkedésekre ki kell térni. A külső személynek adott hozzáférés további résztvevőket is magával hozhat: az ilyen érintettek hozzáférési feltételeit is szabályozni kell.

A Hivatal olyan rendszereiben, amelyek külső személyek számára is hozzáférhetők, a hozzáféréseket minden esetben ellenőrizni kell. Az ellenőrzésért a Hivatal részéről felelősként, kapcsolattartóként meghatározott Hivatali egység vezetője, ennek hiányában a szerződő Hivatal vezetője, illetve az általa kijelölt személy felel. A megállapodás előtt a biztonsági kockázatokat fel kell mérni; ennek alapján az ellenőrzés, a felügyelet és az adminisztráció követelményeit rögzíteni kell a szerződésben. A felmérésért a szerződést – szakterületi oldalról – előkészítő személy a felelős.

Külső személyek hozzáféréséhez további résztvevők közreműködésére is szükség lehet. A hozzáférésről szóló szerződésekben rendelkezni kell arról, hogy más jogosult közreműködők milyen feltételekkel férhetnek hozzá az egyes eszközökhöz, különös tekintettel az egyedi jelleggel hozzáférést igénylőkre (tanulók, konzultánsok, stb.), valamint a takarító, karbantartó személyzetre.

Felelősség:

A fenti szabályok betartása az ilyen szerződések létrejöttének, valamint az adatfeldolgozás kiszervezésének elengedhetetlen feltétele. Ennek ellenőrzése és a szerződések megkötése a Hivatal jegyzőjének a hatásköre.

Külső szolgáltatók, harmadik felek igénybe vételével az informatikai biztonsággal kapcsolatos felelősség nem hárítható át, az a feladatért felelős szervezet első számú vezetőjét a Jegyzőt terheli.

Minden harmadik féllel kötött megállapodás esetében elvárásként kell megfogalmazni a jelen Szabályzatban foglaltak betartását. Ennek teljesítése érdekében informatikai tárgyú szerződést a Hivatal kizárólag az Informatikai rendszerüzemeltetők véleményezése után köthet.

A folyamatban lévő megállapodások (pl. üzemeltetési, karbantartási szerződések) és az új szerződések információbiztonsági, titoktartási vonatkozásait, azok tartalmát és formáját az Informatikus ellenőrzi, és legalább évenként felülvizsgálja.

2.2.1 A külső személyek hozzáféréseinek kockázatainak kezelése

2.2.1.1 A hozzáférések típusai

A külső személyek hozzáférései különös jelentőséggel bírnak. A következő hozzáféréstípusokat különböztetjük meg:

- fizikai hozzáférés (pl. irodákhoz, számítógéptermekhez, irattároló szekrényekhez);
- logikai hozzáférés (pl. adatbázisokhoz, informatikai rendszerekhez).

2.2.1.2 A hozzáférések engedélyezési feltételei

Cél:

A Hivatal a külső felhasználói mint például:

- képviselő testület tagjai
- stb.

számára szolgáltatásokat nyújt, tevékenységük végzéséhez meghatározott és engedélyezett fizikai és/vagy logikai hozzáféréseket biztosít:

Szabályozás:

Az informatikai biztonsági vezető elsősorban a Hivatal figyelembevételével dönt az engedély megadásáról, a kiadott engedély másolatát átadja a kérelmezőnek és az informatikai vezetőnek. A hozzáférést mindaddig ki kell zárni, amíg a szükséges ellenőrzést el nem végezték, és a szerződésben vagy jegyzői utasításban meg nem határozták a hozzáférés feltételeit. A szerződés vagy képviselő esetén jegyzői engedély elválaszthatatlan része a titoktartási nyilatkozat.

A lejárat időpontját minden esetben fel kell tüntetni a hozzáférési engedélyben.

A külső partnerek hordozható számítógépein tárolt – a munkavégzés során megszerzett és a Hivatallal kapcsolatos – adatokat a munkavégzés befejezése után visszaállíthatatlanul törölni kell, amelyet a felelősnek kötelessége ellenőrizni.

Védelmi szempontból nagyon fontos, hogy a biztonsági szolgálat tagja, vagy az a személy, aki a külső felet várja, győződjön meg annak személyi azonosságáról. A felek szerződésben állapodnak meg a beengedhető külső munkavégzők vagy képviselő személyében.

Felelősség:

Amennyiben külső személyeknek hozzáférési lehetőséget kell biztosítani, azt csak és kizárólag engedélyeztetési eljárás után lehet megtenni. A hozzáférési engedélyt minden esetben a Jegyző engedélyezheti.

2.2.1.3 Helyszíni tevékenységet végző külső személyek

Cél:

A helyszíni tevékenységet végző külső személyek munkájából eredő biztonsági kockázatok csökkentése:

Szabályozás:

Szerződéses vagy egyéb jogviszony alapján helyszíni tevékenységet végző külső személyek biztonsági

kockázatot jelentenek. A biztonsági kockázatok csökkentése érdekében:

- a külső személlyel kötött szerződésekben ki kell kötni a Hivatal ellenőrzési jogosultságát;
- az informatikai biztonsági szabályzat egyértelműen határozza meg a külső személyek hozzáférési lehetőségeit;
- az informatikai rendszerekhez, az abban kezelt adatokhoz külső személyek hozzáférését mindaddig ki kell zárni, amíg a megfelelő (és szerződésben is rögzített) ellenőrzést el nem végezték;
- a külső személyek helyszíni tevékenységének informatikai biztonsági ellenőrzése során a munkahelyi vezetőnek közre kell működnie;
- még a munka megkezdése előtt kötelező megvizsgálni a külső személyek várható helyszíni tevékenységét;
- meg kell határozni az együttműködés jogszabályi feltételeit, valamint a megállapodás be nem tartásának következményeit.

Felelősség:

Amennyiben külső személyeknek hozzáférési lehetőséget kell biztosítani, azt csak és kizárólag engedélyeztetési eljárás után lehet megtenni. A hozzáférési engedélyt minden esetben csak az érintett ágazati egység vezetője kérheti, és a Jegyző engedélyezheti (képviselők esetén csak a jegyző).

2.2.1.4 A külső személyek hozzáféréseinek engedélyezése

Külső személyek hozzáféréséhez a munka megkezdése előtt egyértelműen meg kell határozni a munkavégzés célját, helyét, idejét, módját, fel kell mérni az alkalmazás kockázatait.

E vizsgálat során a Hivatal vegye figyelembe a következőket:

- a külső fél által hozzáférhető adatfeldolgozó eszközökkel kapcsolatos kockázatokat;
- a hozzáférés típusát és annak kockázatait,
- a Hivatal és a külső fél hálózatának összekapcsolásából eredő veszélyforrásokat (pl. átmeneti, tartós engedélyhez kötött, vagy adott időszakokra engedélyezett belső hálózati csatlakozás, vagy távoli hozzáférés);
- a hozzáférést és a helyszínéből eredő veszélyforrásokat: Hivatalen belüli vagy Hivatalen kívüli a hozzáférés, milyen fizikai biztonsági zónákba jut be a külső személy, ott milyen információkhoz férhet hozzá (pl. asztalon lévő szerződések, titkok, riasztórendszerkódok, adatfeldolgozó eszközök, adathordozók, egyéb – szemmel látható – védelmi eljárások);
- a külső hozzáféréskor elérhető információ esetleges kikerülésének kockázatait, az adott információ érzékenysége, értéke, minősítése szerint;
- a Hivatali információ kezelésébe bevont külső fél személyi kockázatait;
- a külső személy pontatlan hitelesítéséből eredő kockázatokat: hogyan lehet az adott személy azonosságát ellenőrizni, milyen gyakran kell ezt megtenni;
- intézkedéseket olyan információ megvédésére, amelyet nem szándékoznak hozzáférhetővé tenni külső felek számára;

- az adattárolás formáinak, feldolgozásának, közlésének, elosztásának és cseréjének a kockázatait;
- a külső fél általi hozzáférések rendelkezésre állásának kockázatait: milyen hivatali vagy egyéb kárt okozhat, ha a hozzáférés nem történhet meg, vagy a hálózati hozzáférés nem érhető el, vagy hibás adatokat szolgáltat;
- az esetleges biztonsági események és lehetséges károk kockázatait: hogyan korlátozható a külső fél hozzáférése biztonsági esemény bekövetkezésekor, vannake ilyen esetre belső eseménykezelő eljárások;
- a különféle szerződések hibáiból eredő kockázatokat: megfelelneke a titoktartási nyilatkozatok és egyéb megállapodások a hatályos jogszabályoknak.

2.2.2 Ügyfélkapcsolatok informatikai biztonsága

Cél:

Az ügyfélkapcsolatok informatikai biztonságával kapcsolatos intézkedések célja, hogy megakadályozza az üzletmenet folytán keletkező minősített adatok kiszivárgását.

Szabályozás:

A Hivatal ügyfelei az esetek többségében bebocsájtást nyernek a Hivatal objektumaiba, az ügyfélfogadás során kényes információk birtokába juthatnak, belátást nyerhetnek bizonyos minősített adatokba vagy esetleg védelmi eljárásokba, bejuthatnak védett helyiségekbe ellophatnak megsemmisíthetnek iratokat.

A Hivatal dolgozói az:

- Adatvédelmi és adatbiztonsági Szabályzat
- Iratkezelési Szabályzat
- alapján adhatnak ki bármilyen adatot vagy információt az ügyfelek részére.

A Hivatal a vagyonvédelmi őrzést és személy beléptető rendszert alkalmaz, és az ügyfeleket a megfelelő szabályok betartása mellett fogadja és kíséri az épületben: a:

- Közös elektronikus megfigyelő rendszer
- Biztonsági szolgálat működése és biztonsági zónák

szabályzatok alapján tartózkodhat.

Felelősség:

Az ügyfelek jogosulatlan adatszerzéséért a Jegyző és az Ágazatok vezetői a felelősek. Az ügyfelek jogosulatlan helyen történő tartózkodásáért a Biztonsági szolgálat vezetője a felelős.

2.2.3 Informatikai biztonsági követelmények a harmadik személlyel külső felekkel kötött szerződésekben

Harmadik (külső) személyeknek vagy a Hivatal informatikai rendszereihez való hozzáférése kizárólag olyan írásbeli szerződésen alapulhat, melynek az összes – biztonsággal kapcsolatos – előírása igazodik a Hivatal biztonsági előírásaihoz és elfogadott szabványaihoz.

A szerződésekben ügyelni kell arra, hogy minden azonosított kockázatot és biztonsági követelményt bevegyenek a megállapodásokba Ahol szükséges a szerződésekben, a kívánt intézkedéseket és eljárásokat

egy Biztonságkezelési terv című mellékletben érdemes szerepeltetni.

Harmadik személy számára – a velük kötött szerződésben részletezettek szerint – az adatok elektronikus, papíralapú, mágneses, vagy bármely más típusú adathordozón történő átadásátvétele csak az adat minősítéséhez, biztonsági osztályba sorolásához és kezeléséhez rendelt engedélyezési eljárásnak megfelelően szabályozott és dokumentált formában történhet, az adott szerződés elválaszthatatlan mellékletét képező adatvédelmi és titoktartási nyilatkozatokkal összhangban. Az átadásátvétel csak az ügyvitelre, az adat és titokvédelemre vonatkozó szabályokban meghatározott előírások szerint történhet.

A Hivatalnak rendelkeznie kell olyan eljárásokkal, melyekkel időben felderíthetők a biztonsági események (előfordulte adatvesztés vagy módosítás), illetve korlátozható a Hivatali adatok másolása és közzététele.

A kötelező eseti és rendszeres adatszolgáltatások, továbbá a bíróságok vagy más hatóságok eljárásai során, illetve a hivatalból eljáró ügyvéd, közjegyző eljárása esetén a szerződéstől és a titokvédelmi nyilatkozattól el kell tekinteni, de az adatátadás jogszerűségét vizsgálni kell, az átadás tényét pedig dokumentálni. Ezekről minden esetben a Hivatal jegyzője dönt.

A Hivatalnak a következő biztonsági kérdések közül az adott szerződés esetén relevánsakat kell figyelembe venniük a harmadik féllel kötött szerződések kapcsán:

- vagyontárgyak védelme, beleértve az információ megjelenésének összes formáját, az ügyfelek által hozzáférhető területek, adatfeldolgozó eszközök folyamatos megfigyelését,
- az információ és vagyontárgyak visszaküldése vagy megsemmisítése a megállapodás lejártával vagy a megállapodás szerinti időpontban,
- a Hivatal adatainak védelme a rosszindulatú szoftverek ellen,
- a rendszer bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása,
- korlátozások az információ másolására vagy felfedésére vonatkozóan, valamint titoktartási megállapodások használata,
- az ügyfél hozzáférésének különböző indokai, feltételei,
- hozzáféréssel kapcsolatos biztonsági intézkedések, beleértve a megengedett hozzáférési módokat, az egyedi azonosítók és a hitelesítési folyamatok ellenőrzését,
- nyilvántartási kötelezettséget azokról a személyekről, akik a rendszer használatára és vagy adminisztrálására jogosultak,
- a nem engedélyezett kommunikációs csatornák zárva tartása, valamint gyors lehetőség a hozzáférési jogok visszavonására vagy a rendszerek közötti kapcsolat megszakítására,
- a téves információ jelentésének és a biztonsági események kivizsgálásának rendje,
- a szolgáltatás minőségének biztonsági kérdései (a szolgáltatás elfogadható vagy elfogadhatatlan szintje),
- a Hivatal vagyontárgyaira vonatkozó bármely tevékenység figyelemmel kísérésének és megvonásának joga,
- továbbviteli folyamat kialakítása a problémamegoldásra,
- a szolgáltatás folytonossági követelményei, beleértve a rendelkezésre állást szolgáló intézkedéseket,

összhangban a Hivatal működési prioritásaival,

- megállapodás feleinek saját felelőssége,
- jogszabály szerinti felelősségi körök rögzítése szellemi tulajdonjog és szerzői jog megállapítása titoktartási nyilatkozatok,
- alvállalkozókra vonatkozó biztonsági intézkedések,
- feltételek az együttműködési megállapodások újratárgyalására vagy befejezésére,
- legyen vészhelyzeti terv arra az esetre, ha bármelyik fél be kívánja fejezni az együttműködést,
- a megállapodásban jelzett időpont előtt; legyen lehetőség a megállapodás újratárgyalása,
- ha a Hivatal biztonsági követelményei változnak; legyen mindig pontosan dokumentált a vagyontárgyak jegyzéke, illetve a rájuk vonatkozó jogok.

2.3 Kiszervezés

2.3.1 Előírások a kiszervezési szerződésekben

Cél:

Az informatikai biztonságot akkor is fenn kell tartani, ha a Hivatal az adatfeldolgozást más Hivataltól szolgáltatásként veszi igénybe a jövőben.

Szabályozás:

Mivel jelenleg nincs kiszervezett feladat a Hivatalnak, ezért a jövőbeni kiszervezés esetén az érintett informatikai rendszereket, hálózatokat, környezeteket, az azokat érintő kockázatokat, valamint az alkalmazott biztonsági eszközöket, eljárásokat és felelősségi köröket a két fél között létrejött szerződésben rögzíteni kell.

A szerződés tartalmazza a felelősség kérdését, az átmeneti időszak tervezését, erre az időszakra vonatkozó katasztrófatervet, valamint a biztonsági eseményekre vonatkozó információk gyűjtésének és kezelésének folytonosságát.

Kiszervezés csak írásbeli szerződéssel lehetséges, amelyben az informatikai biztonsági politikát érvényesíteni kell. A szerződésben rá kell térni arra, hogy:

- a résztvevő felek tisztában vannak az informatikai biztonsági felelősségükkel,
- hogyan fogják a jogi előírásokat (pl. a személyes adatok védelmét) kielégíteni,
- hogyan fogják fenntartani és vizsgálni az adatok bizalmasságát és sértetlenségét,
- milyen fizikai és logikai védelmi intézkedésekkel fogják szabályozni a jogosult felhasználók a hozzáférését a Hivatal érzékeny hivatali adataihoz,
- hogyan fogják biztosítani a szolgáltatások rendelkezésre állását rendkívüli helyzetekben (pl. természeti csapások esetében),
- milyen fizikai védelmet fognak nyújtani a kiszervezéssel érintett berendezések esetében,
- ki, mikor, milyen feltételek mellett végezhet, illetve végezzen biztonsági vizsgálatot, ellenőrzést.

Kiszervezés esetén legalább a következő védelmi intézkedéseket kell előírni:

- Ha a vállalkozó saját telephelyén végzi az informatikai fejlesztést adatfeldolgozást, adata archiválást, vagy más információ feldolgozással kapcsolatos jövőbeni tevékenységet, a Hivatal részéről csak rejtjelezve továbbíthatók a fejlesztés tárgyát képező programok és adatok a fejlesztő számára. Az éles üzemű rendszerekhez a vállalkozó nem férhet hozzá.
- Programokat, adatokat a felhasználás céljának, időbeli és egyéb korlátainak megjelölésével, a felelősöknek mindkét részről történő kijelölésével, a személyi és fizikai biztonsági követelmények egyértelmű írásbeli rögzítésével, kizárólag átadásátvételi jegyzőkönyv alapján szabad átadni. A jegyzőkönyvnek tartalmaznia kell:
    - programátadás esetén
    - a program megnevezését, készítőjét,
    - a program funkcióját,
    - a program könyvtárstruktúráját,
    - a programot alkotó fájlok felsorolását,
    - a verzióinformációkat;
    - fájlátadás esetén
    - teljes fájlnevet (nevet, kiterjesztést),
    - a fájl méretét,
    - a módosítás dátumát,
    - a fájl típusát;
    - adatátadás esetén
- ha az adat nem tartozik a fájl fogalmába, akkor a papíralapú iratkezelésre vonatkozó szabályok az iránymutatóak amelyeket a Hivatal Adatvédelmi és adatbiztonsági Szabályzat és az Iratkezelési Szabályzat tartalmaz.

Az anyagokat tartalmazó adathordozókat a következő lényeges szabályok szerint kell kezelni:

- Az adathordozók azonosíthatók, ellenőrizhetők legyenek, rajtuk a minősítési és az azonosítási jeleket vagy jelöléseket olvashatóan, letörölhetetlenül, eltávolíthatatlanul kell feltüntetni.
- A harmadik személy az előző bekezdésben felsorolt minősítésekkel, jelölésekkel kapcsolatos kezelési szabályokat a teljes munkafolyamat során köteles betartani, ellenkező esetben a teljesítése nem fogadható el. Az adathordozók csak a biztonsági ellenőrzések végeztével vehetők használatba a Hivatal rendszerein.

Külső fejlesztő részére tesztelésre éles üzemi adatok csak kivételesen, indokolt esetben és az informatikai biztonsági vezető előzetes engedélyével adhatók át, éles üzemi tesztek viszont csak a Hivatal saját rendszerein végezhetők. Tesztrendszerben csak az eredeti adatra vissza nem következtethető adat fordulhat elő.

E szabályok betartásának, a szabályok szerinti tevékenység dokumentálásának ellenőrzésére a Hivatal felelősévé vagy kapcsolattartójává kijelölt Hivatali egység, valamint az informatikai biztonsági Hivatali

egység kijelölt munkatársai jogosultak, illetve kötelezettek.

Ha a vállalkozó a saját telephelyén működő fejlesztőrendszeren vagy adatfeldolgozó adatarchiválási rendszeren dolgozik, akkor a következő főbb biztonsági szabályok az irányadók:

- A tevékenységet a Hivatal folyamatosan felügyeli; az informatikai biztonsági szabályzat betartását dokumentálja és ellenőrzi.
- Belépési vagy hozzáférési jogosultságot az általános jogosultsági szinten túlmenően csak külön engedély alapján, a tevékenysége elvégzéséhez szükséges időre kapjon.
- Távoli hozzáférésekkel történő fejlesztés adatarchiválás csak indokolt esetben folyhat (pl. amikor az előző pontokban meghatározott fejlesztési mód alapos indok miatt nem valósítható meg).
- Távoli hozzáféréssel történő fejlesztés csak az érintett szakmai vezető kezdeményezésére, valamint az Informatikai és a biztonsági vezető előzetes írásbeli engedélyével történhet. Az erre irányuló javaslatot a fejlesztő és megrendelője köteles megindokolni.
- Fejlesztési célú távoli hozzáférés csak az engedélyben megadott végpontról és csak a Hivatal ellenőrzése alatt álló védelmi rendszerrel támogatva történhet.

2.4 Előírások az eszközbeszerzések lizing, tartós bérleti vagy IT szolgáltatói árajánlatok hoz

Cél:

Az informatikai biztonságot akkor is fenn kell tartani, ha a Hivatal IT eszközöket, szolgáltatsokat szerez be állít rendszerbe vagy szerződésben vesz igénybe vagy eszközöket lizingel a jövőben.

Szabályozás:

Mivel jelenleg nincs a Hivatalnak ilyen feladat, ezért a jövőbeni kiszervezés esetén az érintett informatikai rendszereket, hálózatokat, környezeteket, az azokat érintő kockázatokat, valamint az alkalmazott biztonsági eszközöket, eljárásokat és felelősségi köröket a két fél között létrejött szerződésben rögzíteni kell.

Eszközbeszerzések:

A beszerzések esetén az árajánlatok megkérésekor az alábbiakat kell figyelembe venni.

- Kért eszközök összehasonlíthatósága az ajánlatokban.
- Szolgáltatások
  - szállítás
  - képzés
  - üzemeltetés
- Garancia
  - hossza
  - tartalma
  - ügyintézés módja
  - gyorsasága
  - helye

- Határidőtartás
- Ár és fizetési feltételek
- Referenciák azonosak-e a hivatal IT-infrastruktúrájával
- Panaszkezelési hajlandóság
-

Szolgáltatások:

A beszerzések esetén az árajánlatok megkérésekor az alábbiakat kell figyelembe venni.

- Kért szolgáltatások összehasonlíthatósága az ajánlatokban.
- Szolgáltatások
  - embernapban lebontott ütemterv
- Garancia
  - hossza
  - tartalma
  - ügyintézés módja
- Határidőtartás
- Ár és fizetési feltételek
- Referenciák azonosak-e a hivatal méretével
- Panaszkezelési hajlandóság

3 ESZKÖZBIZTONSÁG

Cél:

A vagyontárgyak kezelésével kapcsolatos biztonsági intézkedések célja a Hivatal vagyontárgyainak megfelelő és folyamatos védelme. A védelem kulcsténye zője, hogy minden vagyontárgyat vegyenek leltárba, és minden vagyontárgynak legyen egy megnevezett felelős gazdája.

Szabályozás:

A Hivatal biztonságának kialakítása során az egyik legfontosabb adatbázis a Hivatal vagyonleltára, amely informatikai biztonsági szempontból a következőket tartalmazza:

1. adatvagyon: az adatok, adatbázisok, szoftverkezelési kézikönyvek, oktatási, üzemviteli, üzemeltetési, biztonsági segédletek és nyilvántartások.

2. szoftvervagyon: rendszerszoftverek, alkalmazói szoftverek, fejlesztőeszközök és szolgáltatások.

3. fizikai vagyon: hardver (számítógépek, perifériák, mobil számítástechnikai eszközök), kommunikációs eszközök (telefonok, faxok, modemek, hálózati csatoló eszközök, telefonalközpontok), adathordozók és egyéb műszaki berendezések (szünetmentes tápegység, légkondicionáló berendezés, villámhárító stb.).

3.1 Számadási kötelezettségek az eszközökkel kapcsolatban

Cél:

A Hivatal vagyontárgyait leltárba kell venni annak megjelölésével, hogy hol találhatók, kinek a felelősségi körébe tartoznak, és osztályozni kell azokat a biztonsági célkitűzések (bizalmasság, sértetlenség és rendelkezésre állás) fenntartásában játszott szerepük szerint. Mindnek legyen megnevezett felelőse, és az alkalmazott védelmi intézkedések karbantartásának felelőssége is legyen kiosztva.

Szabályozás:

A Hivatal:

- leltározási és értékelési szabályzatot,
- letár jegyzéket,
- eszköz átadásátvételi jegyzőkönyvi részt tartalmazó munakkör átadás-átvételi jegyzőkönyvet

készít és folyamatosan karbantart.

A Hivatal a Leltározási és értékelési szabályzatban az alábbi védelmi intézkedések hozza az az informatikai működéssel kapcsolatos eszközeinek megvédése érdekében. A védelmi intézkedések megvalósítását át lehet ruházni, de a vele járó felelősséget nem.

- Ki kell jelölni a leltárilag nyilvántartott eszközök felelősét.
- Megfelelő személyekre (leltárfelelősökre) kell bízni a szükséges ellenőrző eszközök fenntartását. A leltárfelelősöket a szakterületek (Hivatali egységek) vezetői nevezik ki.
- A Hivatali egységeknél kijelölt leltárfelelősök munkaköri leírásában rögzíteni kell a készletleltárral kapcsolatos tevékenységüket, illetve a felelősségüket.
- A munkavállaló beiktatásakor munakkör átadás-átvételi jegyzőkönyvt kell kitöltetni, amelyen szerepel a munkaeszköz átadásátvétele, és aláírással nyilatkoztatni kell az eszközökre vonatkozó számadási kötelezettségéről, illetve a felelősség és a vele járó szankciók tudomásul vételéről.
- A számadási kötelezettségeket a leltározási és értékelési szabályzat előírásai alapján kell ellenőrizni.
- Minden évben egy alkalommal a jelentős vagyontárgyakról, amelyek valamelyik informatikai rendszerrel kapcsolatosak leltárellenőrzést el kell végezni.
- munkaviszony megszűntekor: a munkavállaló által leadott eszközöket össze kell vetni az átadásátvételi jegyzőkönyvvel – megfelelés esetén igazolást kell kiadni a számadási kötelezettségek teljesítéséről, eltérés esetén pedig jegyzőkönyvet kell felvenni, és haladéktalanul értesíteni kell a munkáltatót a felelősségre vonási eljárás megindítása érdekében;
- más Hivatali egységbe, más munkavégzési helyiségbe való átlépéskor, az előző pontban részletezettek megtartásával;
- ha okafogyottá válik az eszköz használata – leadás esetén is ellenőrizni kell az átadásátvételi jegyzőkönyvvel való egyezést;

3.2 Eszköz és vagyonleltár

Cél:

A Hivatalnak szüksége van arra, hogy feltérképezze a vagyonát, illetve megállapítsa vagyontárgyai értékét és fontosságát, mert ez a kockázatokkal arányos védelem egyik fő tényezője.

Szabályozás:

A Hivatalban az informatikai eszközök leltárját fel kell állítani a Leltározási és értékelési szabályzat alapján, és karbantartani minden olyan jelentős vagyontárgyról, amely valamelyik informatikai rendszerrel kapcsolatos. Egyértelműen azonosítani kell valamennyi vagyontárgyat, megállapítani és írásba foglalni annak felelősét és biztonsági osztályát, valamint pillanatnyi elhelyezését (ez azért fontos, hogy elveszés vagy megrongálódás esetén vissza lehessen állítani). Minden, a készletleltár határain belül talált eszközt azonosítani kell. Bármilyen, a készletleltárból akármely okból kizárt eszközt hozzá kell rendelni egy másik vizsgálathoz, hogy biztosíthassuk, hogy nem kerülik el a figyelmünket, és nem feledkezünk meg róluk. A pontos eszközleltár a sérülékenységek kezelésének is fontos dokumentuma.

3.3 A vagyontárgyak gazdája

Cél:

A vagyontárgyakkal kapcsolatos személyi felelősség a hivatali biztonság alappillére. Alapvető biztonsági követelmény, hogy az adatfeldolgozási eszközökhöz kapcsolódó minden információnak és vagyontárgynak legyen felelős gazdája.

A vagyontárgy gazdája felelős:

- az adatfeldolgozó eszközhöz kapcsolódó információ és vagyontárgy megfelelő minősítéséért;
- a hozzáférési jogok kiosztásáért és azok időszakos, hozzáféréskezelési szabályzat alapján történő átvizsgálásáért.
- Gazda szerepet lehet kijelölni
- a működési folyamatra;
- a tevékenységek meghatározott csoportjára;
- egy alkalmazásra;
- egy meghatározott adatcsoportra.

3.4 Az eszközök (vagyontárgyak) megfelelő használata

Cél:

Az adatfeldolgozó eszközök megfelelő, szabályozott és dokumentált használata.

Szabályozás:

Minden alkalmazottnak, szerződő félnek és harmadik félnek be kell tartania az adatfeldolgozó eszközök elfogadható használatára vonatkozó szabályokat, beleértve:

- az elektronikus levelezésre és az internetes böngészésre vonatkozó szabályokat,
- a mobil berendezések Hivatal helységein belüli és kívüli használatára vonatkozó szabályokat,
- Az alkalmazottaknak, szerződő feleknek, akik a Hivatal adatfeldolgozó eszközeit használják, ismerniük kell az eszközök hasznára vonatkozó biztonsági korlátozásokat.

3.5 Az adatok biztonsági osztályozása

Cél:

A biztonsági osztályozás célja az informatikai vagyontárgyak szükséges védelmi szintjének előírása. Az informatikai eszközök megfelelő védelméről való gondoskodás magában foglalja, hogy az adatok minősítésének tükröznie kell a védelem szükségességét, prioritásait és mértékét.

Szabályozás:

A Hivatal az Információbiztonsági fenntartása érdekében a 41/2015. (VII. 15.) BM rendelet szerint hozta létre kockázatkezelési eljárás rendjét, amely az **IBSZ Kockázatkezelési és Elemzési eljárásban és a Cselekvési tervben szabályoz.**

A Hivatal a következő okokból bekövetkező károkat veszi figyelembe az adatok biztonsága érdekében:

- jogszabályok és egyéb szabályozások megsértése;
- az alaptevékenységek akadályozása;
- szavahihetőség, jó hírnév elvesztése;
- személyes információkkal kapcsolatos titoksértés;
- személyi biztonság veszélyeztetése;
- a kényszerítő eszközök hatékonyságának csökkentése;
- minősített adat vagy egyéb titok jogellenes kezelése;
- a közrend megsértése;
- pénzügyi veszteség okozása;
- a környezet biztonságának veszélyeztetése.

A Kockázat kezelési eljárással és az adatok biztonság osztályozásával kapcsolatos utasításokat minden évben a kapcsolódó szabályozások változása vagy nagyobb informatikai fejlesztések esetén aktualizálni kell és új eljárás keretében az adatokat újra kell osztályozni és a kockázatokat megállapítani. Egyéb esetben az adatok kockázatelemzését a 41/2015. (VII. 15.) BM rendelet szerint kell elvégezni.

Felelősség:

Az osztályozási elvek kialakításának és éves gyakoriságú felülvizsgálatának felelőse a Hivatal Információ biztonsági Felelőse.

4 SZEMÉLYI BIZTONSÁG

4.1 Az alkalmazás előtt

Cél:

Az emberi hibák, lopás, csalárd magatartás vagy a létesítmények és eszközök nem megfelelő használata során fellépő, az előírások szándékos vagy véletlen megsértéséből eredő biztonsági kockázatokat mérsékelni kell, a következők szerint.

Szabályozás:

- A biztonsági követelményeket a munkaerőfelvételnél, a szerződésekben, valamint az egyén foglalkoztatása során egyaránt érvényesíteni kell.
- A munkaerőfelvételi eljárás során minden munkavállalónak, és a rendszerek külső használóinak (a velük kötött szerződés alapján), alá kell írniuk egy titoktartási nyilatkozatot.
- A munkavállalótól csak olyan nyilatkozat vagy olyan adatlap kitöltése kérhető, amely a személyi jogait nem sérti, a munkaviszonyra nézve lényeges tájékoztatást nyújt, és ahhoz az érintett írásban hozzájárult.

Felelősség:

Az új belépő munkatársak és harmadik felek feladatainak és felelősségi köreinek és az informatikai rendszeren a jogosultságainak meghatározásának felelőssége megoszlik az adott Ágazat vezetője és az Informatikai rendszerüzemeltetők és a Jegyző között.

4.1.1 Informatikai biztonság a felvételnél és a munkaköri leírásokban

Cél:

Minden munkaterületre részletes munkaköri leírást kell készíteni.

Szabályozás:

A munkaköri leírásnak tartalmaznia kell az adott munkaterületre vonatkozó, a biztonsággal kapcsolatos követelményeket a felelősség egyértelmű megjelölésével.

A szerepköröket úgy kell meghatározni, hogy azok kölcsönösen egyértelműek legyenek a munkakörökkel: ezáltal a felelősségek is egyértelműen elhatárolhatók.

Az informatikai biztonság szempontjából elengedhetetlen a személyzeti és biztonsági szakterületek

folyamatos együttműködése a be és kiléptetési folyamatokkal kapcsolatban.

A be és kilépéskor a hozzáférési jogosultságokat is meg kell határozni, és azokat a kellő időben érvényesíteni kell.

A Hivatal ennek érdekében sétálópapírt alkalmaz az új belépők munkaköri leírásához és a be és kilépéskori adminisztrációhoz.

4.1.2 A személyzet biztonsági átvilágítása és a személyzeti politika

Cél:

A munkatársakat a felvételi eljárás során a Jegyző utasításainak megfelelően kell megvizsgálni, figyelembe kell venni az összes ide vonatkozó titoktartási, adatvédelmi és alkalmazáson alapuló jogszabályt és törvényt

Szabályozás:

A vizsgálat során az alábbiakat kell ellenőrizni, illetve megerősíteni:

- hivatali és személyi referenciákat;
- a felvételre jelentkező életrajzát teljesség és pontosság szempontjából egyaránt;
- az elvárt legmagasabb iskolai végzettséget és szakképzettséget;
- a hatóság által kibocsátott személyazonosító igazolványt;
- szükség esetén a büntetlen előéletet.

4.1.3 A foglalkoztatás feltételei

Cél:

A foglalkoztatás alapvető biztonsági feltételei az általános és a munkakörre vonatkozó speciális biztonsági előírások megismerése, elfogadása, a titoktartási nyilatkozat aláírása.

Az alkalmazás feltételei tükrözzék a Hivatal biztonsági politikáját, illetve tisztázzák és tartalmazzák a következőket:

Szabályozás:

A szerződéses kötelezettség részeként az alkalmazottak, illetve a szerződő felek egyezzenek meg, és írják alá az alkalmazási szerződésük kikötéseit és feltételeit, amelyek meghatározzák a felelősségüket és a Hivatal felelősségét az informatikai biztonságra vonatkozóan.

- Ahol lehetséges (vezető beosztású vagy más kiemelt munkaköröknél), ezek a felelősségek meghatározott időtartamra terjedjenek ki az alkalmazás megszűnése után is. Ebben fel kell tüntetni a biztonsági követelmények megszegésének jogkövetkezményeit is.
- Az alkalmazás feltételei között szerepeljenek a munkatársak jogai és kötelességei, pl. a szerzői jogokra vagy a személyes adatok védelmére vonatkozóan.
- Az alkalmazási feltételekben szerepeljen a munkatárs adatkezelési és biztonsági osztályba sorolási kötelezettsége, és hogy ezek a felelősségek fennállnak a Hivatal telephelyein kívül is, a munkatárs rendes napi munkaidején túl is, pl. az otthoni munkavégzés alatt is.

- az alkalmazott, illetve a szerződő fél felelősségét a más vállalatoktól vagy külső felektől kapott információ kezeléséért.
- a Hivatal felelősségét a személyes adatok kezeléséért, beleértve a Hivatalnál való alkalmazás során vagy annak következtében keletkezett személyes adatokat.
- Azokat az intézkedéseket, melyeket a Hivatal akkor tesz, ha az alkalmazott vagy a szerződő fél figyelmen kívül hagyja a Hivatal biztonsági követelményeit.

4.2 Az alkalmazás ideje alatt

Cél:

Az alkalmazás ideje alatt folyamatosan gondoskodni kell arról, hogy a felhasználók ismerjék az informatikai biztonsági fenyegetéseket, és motiválva legyenek a Hivatal információvédelmi szabályzatainak és intézkedéseinek betartására. A felhasználókat tájékoztatni kell a biztonsági eljárásokról és az adatfeldolgozó eszközök helyes használatáról a lehetséges biztonsági kockázatok minimalizálása érdekében egy Információbiztonsági kézikönyv segítségével.

Szabályozás:

A vezetőknek biztosítaniuk kell, hogy a munkatársak:

- ismerjék a biztonsági felelősségüket, a biztonsági eljárások alkalmazását és az adatfeldolgozó lehetőségek korrekt használatát, mielőtt az érzékeny információkhoz vagy informatikai rendszerekhez hozzáférnének, hogy ezzel is csökkentsék a lehetséges biztonsági kockázatokat;
- legyenek ösztönözve, hogy a Hivatal biztonsági szabályzatait betartsák;
- alkalmazkodjanak a foglalkoztatás feltételeihez, az ide vonatkozó biztonsági szabályzatokhoz; a biztonságot érintő kérdésekben naprakész jártasságuk legyen.
- Ismerjék az információbiztonsági kézikönyvet.

Felelősség:

A vezetőség felelőssége, hogy megkövetelje az alkalmazottaktól, szerződő felektől és a használó harmadik féltől, hogy biztonsági intézkedéseiket a meghatározott Hivatali szabályzatokkal és eljárásokkal összhangban tegyék meg.

Az új belépő munkatársak és harmadik felek feladatainak és felelősségi köreinek és az informatikai rendszeren a jogosultságainak meghatározásának felelőssége megoszlik az adott Ágazat vezetője és az Informatikai rendszerüzemeltetők között.

4.2.1 Informatikai biztonsági képzés és továbbképzés

Cél:

A Hivatal valamennyi munkatársát – ahol szükséges, a harmadik fél felhasználóit is – megfelelően ki kell képezni a Hivatal biztonsági szabályairól és eljárásairól éves oktatás keretében.

Szabályozás:

Ezeket az ismereteket folyamatos tájékoztatással naprakészen kell tartani. A kézikönyv foglalja magába a biztonsági követelményeket, a jogi felelősséget, az hivatali óvintézkedéseket és az informatikai eszközök helyes használatát, pl. a bejelentkezési eljárást és a munkamenet zárolását..

Az általános biztonságtudatosítási elveket és gyakorlatot a Hivatal teljes személyzetének meg kell ismernie.

4.2.2 Fegyelmi eljárás

Cél:

Azokkal az alkalmazottakkal szemben, akik a Hivatal biztonsági szabályzatait és eljárásait megsértették induljon hivatalos fegyelmi eljárás. Ez visszatarthat olyan munkatársakat, akik egyébként hajlamosak a biztonsági szabályokat megszegni. A biztonsággal összefüggő munkavállalói kötelességszegés gyanúja esetén a vizsgálatot a munkáltató köteles megindítani. A felelősségi, kártérítési eljárást a munka törvénykönyve és – ha van ilyen – a kollektív szerződés szerint kell lebonyolítani.

Szabályozás:

Az eljárás alapja a hatályos büntető és polgári törvénykönyv. Az eljárás keretében, ha súlyos fegyelmi vétség történt, a hozzáférési jogokat azonnal meg kell vonni; ha külső félről van szó az elkövetőt el kell vezetni a helyszínről.

4.3 Az alkalmazás megszűnésekor vagy változásakor

Cél:

A munkaviszony megszűnése, illetve Hivatalon belüli megváltozása nagyjából azonos biztonsági kategória, mivel mindkettő az éppen használt adatfeldolgozó eszközök és jogosultságok leadásával jár.

Szabályozás:

A munkatársak feladatainak elhatárolása alapvető biztonsági követelmény, éppen ezért a felhasználói jogosultságok megvonása az adott Hivatali egységben teljes mértékben indokolt. A Hivatalon belül áthelyezett munkatársat ilyen szempontok alapján gyakorlatilag azonosan kell kezelni a kilépő munkatárssal és így a munakkör átadás-átvételi jegyzőkönyv alkalmazásával kell a munkavállalót vagy külső felet átvezetni az új munkahelyre.

Felelősség:

Az alkalmazás megszűnésekor vagy változáskor a munkatársak feladatainak és felelősségi köreinek és az informatikai rendszeren a jogosultságainak visszavonásának felelőssége megoszlik az adott Ágazat vezetője és az Informatikai rendszerüzemeltetők között.

A Hivatal vezetőségének felelőssége, hogy megkövetelje az alkalmazottaktól, szerződő felektől és a harmadik féltől, hogy biztonsági intézkedéseiket a meghatározott Hivatali szabályzatokkal és eljárásokkal összhangban tegyék meg az alkalmazás megszűnésekor vagy szerepkör változáskor.

4.3.1 A munkaviszony megszüntetésének biztonsági kérdései

Cél:

A munkaviszony megszüntetésekor a Hivatal szempontjából biztonsági alapkövetelmény, hogy az alkalmazottak, a szerződő felek és a használó harmadik fél rendezett módon hagyják el a Hivatalt vagy változtassanak alkalmazást.

Szabályozás:

Gondoskodni kell arról, hogy miután a szerződő felek vagy a használó harmadik fél távozik, az összes berendezést időben küldje vissza, és minden hozzáférési jogosultságot időben visszavonjanak tőle.

Előre közölni kell, és a szerződésbe kell foglalni a munkaviszony megszűnését követő kötelességeket, és ahol szükséges, a titoktartási nyilatkozatban (megállapodásban) szereplő felelősségeket (lásd: 2.1.5.), amelyek még egy megadott ideig a munkaviszony megszűnése után is terhelik a távozó munkatársat.

A munka és szerepkörök változtatását a Hivatalon belül kezeljék úgy, mintha egy korábbi felelősség megszűnne, és egy újabb kezdődne a 4.1. alfejezet szerint.

4.3.2 Eszközök visszavétele

Cél:

Alapvető biztonsági cél, hogy ha egy alkalmazott vagy szerződő fél alkalmazása, szerződése vagy megállapodása lejár, a Hivatal minden vagyontárgyát szolgáltassa vissza, beleértve a szoftvereket, társasági dokumentumokat, informatikai eszközöket, hitelkártyákat, benzin kártyákat, beléptető kártyákat, illetve különféle elektronikus adathordozón tárolt adatokat.

Szabályozás:

Ha az alkalmazott vagy szerződő fél megvette a Hivatal egy adatfeldolgozásra alkalmas eszközét vagy a saját személyi számítógépét használta, a kiléptetési folyamat során az eszközről minden – a Hivatalet érintő – adatot biztonságosan törölni kell.

A kilépést és eszközök odaadásának körülményeit az Munakkör átadás-átvételi jegyzőkönyv lapon és a Munakkör átadás-átvételi jegyzőkönyvon kell dokumentálni.

4.3.3 Hozzáférési jogok visszavonása

Cél:

Távozó munkatársaktól illetve az áthelyezés során a megmaradt jogosultságokat és minden informatikai, logikai és fizikai hozzáférési jogot idejekorán vissza kell vonni. Vissza kell venni az azonosítókat, előfizetéseket, belépőkártyákat, aktív számlákhoz tartozó ismert jelszavakat. A felelős vezetők az érintett alkalmazottakat, harmadik feleket tájékoztassák a személyzeti változásokról.

Szabályozás:

A kilépést és körülményeit a Munakkör átadás-átvételi jegyzőkönyvon kell dokumentálni.

4.3.4 Az átszervezés biztonsági kérdései

Cél:

A Hivatal átszervezése esetén cél a biztonsági kockázatok minimalizálása.

Szabályozás:

Átszervezés előtt az üzletmenetfolytonosság fenntartása érdekében a kockázatokat fel kell mérni.

Ezért a Hivatal vezetőjének az Információbiztonsági vezetőnek az Informatikai üzemeltetési vezetőjének és az érintett ágazatok vezetőinek és a humánpolitikának egyeztetnie kell az átszervezés kérdéseiről.

5 FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG

Cél:

A fizikai és környezeti biztonság megteremtése és fenntartása során a vonatkozó jogszabályoknak, biztonsági és tűzvédelmi szabványoknak, valamint a helyi szabályzatoknak és eljárásrendeknek maradéktalanul meg kell felelni.

Szabályozás:

A Hivatal az alábbi jegyzői utasításokban szabályozza a fizikai és környezeti biztonság területét amelyek:

- a Hivatal Fizikai és Környezeti Biztonsági Utasítása,
- a Közös Elektronikus megfigyelőrendszer jegyzői utasítása,
- Jegyzői utasítás az épület védelem és felügyelet és biztonsági szolgálat működésének szabályairól
- működése jegyzői utasítása,

amelyek leírják a védett hivatali helyiségek felsorolását és a belépés körülményeinek konkrét szabályait.

A Fizikai és Környezeti Biztonsági Szabályzat alapvető szabályozási követelményei:

- A külső falak, az adatfeldolgozó helységek határfalai és a nyílászárók mechanikusan legyenek ellenállók (megfelelő anyagból és technológiával készüljenek).
- Fontos, hogy a felügyelet nélküli helységek bejáratai zárva legyenek.
- A földszinti ablakokat érdemes külső mechanikai védelemmel ellátni.
- A fogadószemélyzettel vagy biztonsági őrrel védett ügyfélteret, recepciót, tárgyalóhelyet a produktív munkaterületektől és az adatfeldolgozó egységektől kellő távolságban kell kialakítani.
- A fizikai biztonság fontos eleme a tűzvédelem: a biztonsági határok, falak, nyílászárók a nemzetközi előírásoknak, szabványoknak megfelelő mértékben legyenek tűzállók. Rendelkezzen a hivatal kiürítési tervvel, tűzrendészeti tervekkel .
- A területileg megosztott, jól particionált biztonsági rendszer támogatja a Hivatalon belüli feladatelhatárolást is.
- A Hivatal által kezelt adatfeldolgozó eszközöket fizikailag el kell választani azoktól, amelyeket harmadik fél kezel.

Felelősség:

A Hivatal Jegyzőjének és a portaszolgálat felelőssége, hogy megkövetelje az alkalmazottaktól, szerződő felektől és a harmadik féltől és ügyfelektől a hivatali helyiségekben történő belépés és viselkedés és biztonsági és tűzvédelmi szabványok betartását.

5.1 Biztonsági szegmensek

Cél:

Az infrastruktúrát és az információt meg kell védeni a jogosulatlan hozzáféréstől, a sérüléstől és az illetéktelen beavatkozástól, ennek érdekében a lehetséges kockázatokat fel kell mérni, majd a kritikus vagy érzékeny hivatali adatokat feldolgozó és tároló eszközöket, létesítményeket szükség szerint alkalmazható fizikaimechanikai, elektronikai és személyi védelemmel kell ellátni , de a biztonsági intézkedések legyenek kockázatarányosak.

Szabályozás:

A belépést feltételekhez kell kötni és dokumentálni kell, a belső mozgásokat pedig a jogi lehetőségek szerint meg kell figyelni. Emellett az „üres asztal – tiszta képernyő" elv követésével csökkenthetjük a papírok, az adathordozók és az adatfeldolgozó eszközök jogosulatlan használatának és rongálásának kockázatát, ezeket az elveket az információbiztonsági kézikönyvekben érvényesíteni kell.

5.1.1 Biztonsági határok

Cél:

A biztonsági területeket informatikai rendszerenként és biztonsági osztályonként egyaránt rögzíteni kell, majd biztonsági zónákra kell osztani.

Szabályozás:

A védelemigényes helyiségekbe vagy egyes biztonsági zónákba a személyek és csoportok belépési jogosultságait az informatikai rendszerben vagy környezetében betöltött szerepük alapján kell meghatározni.

Felelősség:

A biztonsági területeket kijelölése a Biztonsági Szolgálat és a Jegyző közös felelőssége.

5.1.2 Beléptetési intézkedések

Cél:

A biztonsági területekre és az adminisztratív zónákba való belépést, beléptetést ellenőrizni kell. Az állandó belépési jogosultsággal nem rendelkező munkatársak, illetve külső személyek esetén a be és kilépést, valamint a belépő pontos úti célját minden esetben regisztrálni kell.

Szabályozás:

- Külső személyek csak kísérettel tartózkodhatnak a Hivatal objektumain belül.
- Az 1. vagy 2. osztályú biztonsági zónákban az állandó belépési jogosultsággal rendelkező személyek be és kilépését is naplózni kell elektronikus belépőkártya vagy ügyfelek részére adott vonakóddal, valamint a belépést az egyedi azonosító kártyán is ellenőrizni kell.

- A munkatársak minden esetben jelentsék a biztonsági személyzetnek, ha kísérő nélküli látogatóval találkoznak, vagy bárkivel, aki nem visel látható azonosítót.

- A Hivatalnak szolgáltatást adó személyzet hozzáférését korlátozni kell az adatfeldolgozó helységekben. Ha a hozzáférés indokolt és engedélyezett, akkor is kísérjék figyelemmel.
- A biztonsági területekhez való hozzáférési jogokat rendszeresen vizsgálják át, frissítsék, és szükség esetén vonják vissza évente egyszer.

Felelősség:

A biztonsági területeket védelme a Biztonsági Szolgálat és a Jegyző közös felelőssége. A jogosultságok visszavonása az Informatikai üzemeltetés és az Ágazatvezetők felelőssége.

5.1.3 Létesítmények és helyiségek biztonsága

Cél:

Az informatikai rendszerek környezetét legalább a biztonsági osztálynak megfelelő fizikai, mechanikai, elektronikai és személyi védelemmel kell biztosítani (pl. rácsos ablakok, az áttörést megnehezítő üvegezés, acélajtók). Az alkalmazandó védelmi formák körét és kialakításának módját az informatikai biztonságpolitika mentén a biztonsági vezető határozza meg, figyelembe véve a létesítmény sajátosságait.

Szabályozás:

- A kulcsfontosságú eszközöket úgy érdemes elhelyezni, hogy a jogosulatlan hozzáférést elkerüljük.
- Az objektumok ne keltsenek feltűnést, és ne mutassák céljukat: se belülről, se kívülről ne árulkodjanak arról, hogy azokban adatfeldolgozó tevékenység folyik.
- Segédberendezések és eszközök, mint a fénymásolók és szkennerek, biztonsági területeken legyenek elhelyezve.
- Az ajtók és ablakok akkor, amikor nincs a közelben felügyelő személyzet, legyenek lezárva. Az ablakokat – legalább a földszinten – kívülről ráccsal kell védeni.
- A helyiségeket olyan alkalmas behatolásjelző rendszerrel kell védeni, amely az összes külső ajtót és hozzáférhető ablakot (nyílászárót) lefedi és védi.
- A névtárakat és a belső telefonkönyveket, címjegyzékeket, amelyek érzékeny adatfeldolgozó eszközök helyét azonosítják, nem szabad a nyilvánosság számára elérhetővé tenni.
- Veszélyes vagy gyúlékony anyagokat a biztonsági területekről biztos távolságban kell tartani. A tömegesen szállított árut, mint az irodaszereket, felhasználás előtt adminisztratív zónában érdemes tárolni.
- A tartalék berendezést és a tartalékolt adathordozókat a feldolgozás helyétől olyan távolságban kell elhelyezni, hogy a központi telephely katasztrófája esetén ne szenvedjenek kárt.

Felelősség:

A biztonsági területeket védelme a Biztonsági Szolgálat és a Jegyző közös felelőssége. A jogosultságok kezelése és az informatikai feldolgozó eszközöket tároló helyiségek védelme az Informatikai üzemeltetés és az Ágazatvezetők felelőssége.

5.1.4 Védelem a külső és környezeti fenyegetések ellen

Cél:

A Hivatalnak minden esetben fel kell mérnie a közvetlen környezet fenyegetéseit.

Szabályozás:

- Az adatfeldolgozó vagy tároló telephelyek kiválasztásakor figyelembe kell venni a földrajzi elhelyezkedésből és az éghajlatból eredő veszélyeket (pl. árvíz, belvíz, földrengés, hurrikán, erdő vagy bozóttűz). Új telephely létesítésekor az ilyen sajátos fenyegetések feltárását és a kockázatok elemzését szakértőkre el kell végeztetni.
- A Hivatal telephelyének közelében lévő különféle ipari létesítmények (olajfinomítók, erősáramú vezetékek) vagy tevékenységek is komoly veszélyt jelenthetnek. Költözés vagy új telephely választása előtt ilyen irányú kockázatelemzést kell végezni.
- Fontos, hogy a tartalék berendezések és tartalék adathordozók biztonságos távolságban legyenek elhelyezve a produktív területtől (általában a fő telephelytől), hogy elkerüljék a kárt egy olyan biztonsági esemény során, amely a főtelephelyet érinti. Bevált gyakorlat, hogy ha egy Hivatal több telephellyel rendelkezik, akkor tartalék eszközeit vagy biztonsági másolatokat tartalmazó adathordozóit a feldolgozás helyétől eltérő telephelyen tárolja.

Felelősség:

Új hivatali területek épületek kijelölése és beköltözése előtt a Hivatal jegyzője ki kell, hogy kérje az Informatikai biztonsági fórum véleményét (az Információbiztonsági vezető és az informatikai üzemeltetés, az Információbiztonsági felelős) és szükség esetén más szakértők (építészeti hatóság, katasztrófavédelem hatóság) bevonásával együtt.

5.1.5 Munkavégzés a biztonsági szegmensekben

A biztonsági területeken való munkavégzéshez minden, a Hivatalban dolgozó munkavállalónak, külső és harmadik félnek ismernie kell a biztonsági zónákba való a be és kilépés szabályait és a hivatali helyiségekben való tartózkodás, munkavégzés és információfeldolgozás szabályait.

A biztonsági szolgálatot ellátó szerződéses fél és alkalmazottainak a fentieken túl ismerniük kell:

- a Katasztrófahelyreállítási Tervben rájuk tartozó feladatokat.

5.1.6 Kiszolgáló területek és raktárak biztonsági elkülönítése

Cél:

A kiszolgáló területeket és raktárakat, ahol csak lehetséges, el kell különíteni az adatfeldolgozó eszközöktől. Az ilyen körletek biztonsági követelményeit kockázatelemzés alapján érdemes meghatározni.

Szabályozások:

- A telephelyen kívüli raktárakhoz való hozzáférést az azonosított és felhatalmazott személyzetre kell korlátozni.

- A raktárakat úgy kell tervezni, hogy lerakodásnál a kiszállító személyzetnek ne kelljen belépnie az épület más részeibe.
- A bejövő anyagokat a lehetséges veszélyekre tekintettel kell megvizsgálni (lásd: 5.2.1.), mielőtt azok a raktárból végleges használati helyükre kerülnek.
- A bejövő anyagokat, ha ez megoldható, érdemes már akkor nyilvántartásba venni, amikor a telephelyre érkeznek (lásd: 3.1.).
- A szállításra és tárolásra elkülönített területek külső ajtóit reagáló erővel védjék, amikor a belső ajtókat kinyitják.

5.1.7 A berendezés fizikai védelme

Cél:

Az informatikai berendezéseket, eszközöket fizikailag is védeni kell a fenyegető veszélyektől és a káros környezeti hatásoktól.

Szabályozás:

Az informatikai rendszerek védelmének ki kell terjednie:

- A mechanikai védelemnél, a falazatok, a nyílászárók, a zárak biztonsági kialakításánál a vonatkozó szabványok az irányadók.
- Az objektumok őrzésétvédelmét, nyitását és zárását, a be és kilépést mind munkaidőben, mind azon kívül a hatályban lévő szabályzatok és eljárásrendek szerint kell végezni.
- Az olyan szolgálati helyiségeket, ahol számítástechnikai eszközökkel történik a munkavégzés, a helyiséget távollét esetén zárva kell tartani.
- Biztosítani kell az adathordozók és dokumentációk tűz és vagyonvédett tárolását.
- A tűz elleni védelmet általában a személyi felügyelet és a jelenlévő személyzet biztosítja a helyiségen belül készenlétben tartott – a tűzvédelmi előírásoknak megfelelő – kézi tűzoltókészülékekkel. A készenléti helyeken elsődlegesen gáz halmazállapotú oltóanyaggal feltöltött tűzoltókészülékek legyenek. A készülékek típusát és darabszámát, illetve elhelyezését a helyi tűzvédelmi utasításnak kell tartalmaznia. A készülékeket a szervertermen és a biztonsági szolgálati helyiségen kívül a bejárat mellett, valamint a helyiség erre alkalmas, jól megközelíthető pontjain kell elhelyezni. A helyiségben a vonatkozó szabványok előírásainak megfelelő tűzjelző rendszert kell kiépíteni és üzemeltetni.Az elektromos hálózat feleljen meg az MSZ 1600 sorozatú szabványok előírásainak, az érintésvédelem pedig az MSZ 172 sorozatú szabványok előírásainak.
- A szerverterem elektromos hálózatának a szünetmenetességre, az áthidalási és újratöltési időre vonatkozó követelményeknek megfelelően kell kialakítani, és a betáplálásról külön leágazás megépítésével kell gondoskodni.
- A villámvédelem feleljen meg a kommunális és lakóépületekre vonatkozó előírásoknak.
- A szerverteremben lokális klimatizációról kell gondoskodni.

5.1.8 Műszaki berendezések elhelyezése és védelme

Cél:

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

Szabályozás:

- A műszaki berendezéseket úgy kell elhelyezni, hogy az egyes munkaterületeket illetékteleneknek ne kelljen megközelíteniük (pl. megosztott nyomtató közös helyiségben legyen).
- Az érzékeny adatokat tároló és feldolgozó eszközöket (pl. monitorokat) úgy kell elhelyezni, hogy az ügyfelek előtti használatkor a rálátás kockázatát csökkentsük.
- Az alábbi fenyegetésekre hozott intézkedéseket a Fizikai és Környezeti Biztonsági Utasításban el kell rendelni:
    - lopás,
    - tűz,
    - robbanóanyagok,
    - füst,
    - vízbetörés (vagy a vízellátás meghibásodása),
    - vegyi behatások,
    - áramütés, áramkimaradás,

    .
- Az adatfeldolgozó eszközök közvetlen közelében folytatott étkezést, folyadékfogyasztást és dohányzás nem megengedett,
- A környezeti feltételeket állandóan figyelni kell az olyan helyzetek felismerése érdekében, amelyek az adatfeldolgozó eszközök működését hátráltathatják.
- A Katasztrófaelhárítási és helyreállítási tervekben meg kell becsülni a közelben bekövetkező olyan katasztrófák hatásait, mint a szomszédos épületekben pusztító tűz, a tetőn keresztül vagy a földszint alól betörő víz, vagy valamely utcai robbanás.

5.1.9 Energiaellátás

Cél:

A berendezéseket meg kell védeni a tápáramellátás meghibásodásától és más hasonló villamos rendellenességektől, anomáliáktól. Olyan villamos betáplálást alkalmazzunk, amelyik megfelel a berendezés gyártói specifikációjának.

Szabályozás:

- A szerverteremben szünetmentes tápegységet kell (UPS) alkalmazni;

- Előírás a folyamatos működést és a szabályos kikapcsolási folyamatot szolgáló UPS alkalmazása amelyek az üzlet működésére nézve kritikusak. A Fizikai és Környezeti Biztonsági Utasításban kell rögzíteni minden olyan tevékenységet, amelyet az UPS meghibásodásakor végeznek. Az UPS berendezést évente ellenőrizni kell, hogy elegendőe a kapacitása, és a gyártó ajánlása szerint teszteljék.
- A villámvédelem feleljen meg a kommunális és lakóépületekre vonatkozó előírásoknak.
- Villámvédő szűrőket alkalmazni az épületbe belépő valamennyi külső távközlő vonalra,

Felelősség:

Az szerverterem szünetmentes áramforrásainak felügyelete az Informatikai rendszerüzemeltetők felelőssége.

5.1.10 A berendezés karbantartása

Cél:

A megbízható működés érdekében a berendezések folyamatos használata és rendelkezésre állásának biztosítása érdekében az alábbiakat kell megtenni:

Szabályozások:

- a specifikációban vagy üzemeltetési utasításokban javasolt időközönként el kell végezni a berendezések karbantartását;
- a berendezések kezelését, illetve javítását csak megfelelő szakképzettséggel rendelkező személyek végezhetik;
- az informatikai berendezések külső helyszínen történő javítása, karbantartása esetén gondoskodni kell a berendezésen tárolt adatok végleges (visszaállíthatatlan) törléséről;

5.1.11 A telephelyen kívüli berendezések védelme

Cél:

A tulajdonlástól függetlenül a Hivatal vezetése adjon felhatalmazást minden olyan berendezés használatára, amelyen a Hivatal számára házon kívül végeznek adatfeldolgozást. Az a biztonság, amelyet így látnak el, legyen egyenértékű azzal, amelyet az ugyanazon célra házon belül használt berendezéssel lehet elérni, figyelembe véve azt a kockázatot, amit a Hivatal számára házonkívül végzett munka jelent. Adatfeldolgozó berendezés magában foglalhat bármilyen formában személyi számítógépet, mobiltelefont, papírt vagy bármely olyan eszközt, amelyet az otthoni munkára használnak vagy a szokásos munkahelyről elszállítanak

Szabályozás:

- Az otthoni munkavégzéshez használt laptopok csak MS Office és a Hivatal levelezést érhetik el távolról. Laptopokon BIOS jelszavas védelmet is kell alkalmazni
- A házon kívüli laptop megóvására védő táskát kell használni.
- ASP rendszerek elérésre használt eszközökhoz otthoni hasznáat és irodai használat esetén külön-külön kártyaolvasóval kell rendelkezni.

5.1.12 Berendezési tárgyak biztonságos tárolása és újrafelhasználása

Cél:

A berendezés gondatlan kezelése vagy újrafelhasználása adatvesztéssel járhat Az érzékeny adatot tartalmazó tárolóeszközöket a selejtezési szabályzat alapján kell leselejtezni.

Szabályozás:

A berendezéseknek a tároló közeget tartalmazó valamennyi részegységét, a lemezegységeket ellenőrizni kell olyan szempontból, hogy az érzékeny információt és a vásárolt (licenc szerinti) szoftvereket arról eltávolították és felülírták, mielőtt mások rendelkezésére bocsátották volna.

Az érzékeny információt tartalmazó, de sérült tárolóeszközöket meg kell megsemmisíteni.

5.1.13 Eszközök selejtezése, elvitele

5.1.13.1 Informatikai eszközök selejtezése

Cél:

Biztonsági intézkedésekkel kell megakadályozni, hogy a hibás informatikai eszközök adathordozói

ellenőrizetlenül kerüljenek a Hivatalon kívülre. A selejtezési szabályzatban foglaltak szerint engedélyhez kell kötni, és dokumentálni kell.

Szabályzás:

- A selejtezési jegyzőkönyvben a későbbi félreértések elkerülése végett érdemes feltüntetni a selejtezendő alkatrész gyári számát, típusát, valamint a benne lévő adathordozók törléséről szóló nyilatkozatot, a felelős munkatárs aláírásával.
- A kényes információk kiszivárgásának megelőzése érdekében a selejtezendő adathordozókon a sikeres törlés tényét ellenőrizni kell.

5.1.13.2 Informatikai eszközök kivitele, távoli javítása

Cél:

Biztonsági intézkedésekkel kell megakadályozni, hogy a hibás informatikai eszközök adathordozói ellenőrizetlenül kerüljenek a Hivatalon kívülre. Szintén alapvető követelmény, hogy az elszállítás is vezetői engedélyhez kötött és megfelelően dokumentált legyen.

Szabályozás:

- A jegyzőkönyvben vagy szállítólevélben a későbbi félreértések elkerülése végett, fel kell tüntetni a javítandó alkatrész gyári számát, típusát, valamint a benne lévő adathordozók javításáról vagy elszállításáról szóló nyilatkozatot, a felelős munkatárs aláírásával (az adathordózók újrafelhasználásával, kivitelével kapcsolatos biztonsági intézkedések a 10.7 alfejezetben találhatók).
- A hibás eszköz javítására először ajánlatot kell kérni, amelyben az elvitel és javítás idő fel van tüntetve. Elvitel előtt az adatokat többszörösen felül kell írni. Visszaadásakor ellenőrizni kell a javított eszköz műszak állapotát.

6 HÁLÓZATI ÉS ÜZEMELTETÉSI BIZTONSÁG

Cél:

Az e fejezetben ismertetett intézkedések az adatfeldolgozó eszközök helyes és folyamatos működését szolgálják.

Szabályozás:

Az összes adatfeldolgozó eszköz üzemeltetési eljárásait és az üzemeltetéssel járó felelősségi köröket előre definiálni kell, és rendszeresen felül kell vizsgálni. Az üzemeltetési eljárásokat úgy kell kidolgozni, hogy a feladatok és felelősségek elhatárolhatók legyenek. A jól definiált jogosultságokkal minden munkavállaló csak a munkájához szükséges információhoz kap hozzáférést, így jelentősen csökken a hanyag vagy szándékos visszaélés kockázata.

6.1 Üzemeltetési eljárások és felelősségi körök

6.1.1 Üzemeltetési eljárások dokumentációja

Az üzemeltetési eljárásokat és felelősségi köröket részletesen és szabályszerűen dokumentálni kell. Az üzemeltetési eljárásrendnek a munkafolyamat alábbi szálaihoz részletes utasításokat kell tartalmaznia:

- adatkezelés, (feldolgozás és tárolás);

- tervezett követelmények, más rendszerek bizalmasságának sérülékenysége;
- munkaidőn kívüli tartózkodás a munkahelyen;
- hibaesetekre és rendellenes működésre vonatkozó eljárások;
- hardver és szoftverkarbantartási eljárások;
- munkavégzés közben fellépő rendkívüli események kezelése;
- rendszer újraindítása és visszaállítása.

Az üzemeltetési eljárások dokumentációját az üzemeltetés helyén hozzáférhetővé kell tenni.

Fontos, hogy az üzemeltetési eljárásokat és a dokumentált eljárásokat a rendszer tevékenységeire vonatkozóan hivatalos dokumentumként kezeljék, és a változtatásokat a vezetőség engedélyezze. Az üzemeltetési eljárások tartalmazhatnak kényes adatokat (pl. központi adatbázisok elérési útját, speciális hozzáféréseket, az adatmentés menetét, mentési adathordozók tárolási helyét) – ilyen esetekben a dokumentációt érdemes minősíttetni.

6.1.2 Változáskezelés

Az adatfeldolgozó eszközöket és rendszereket érintő változásokat figyelemmel kell kísérni. Gyakorlati tapasztalat, hogy a sok biztonsági eseményt és rendszerhibát a nem megfelelő változáskövetés okozza.

A berendezés, a szoftverek és az eljárások változásait a formális menedzseri felelősségi körben célszerű ellenőrizni. Az üzemviteli programokat változtatásait részletesen naplózni kell, és a naplókat határozott ideig meg kell őrizni. Az üzemviteli környezet megváltozása hatással lehet az alkalmazásokra is, ezért az üzemviteli és az alkalmazási változásellenőrző eljárásrendet célszerű egy dokumentumba foglalni (lásd:8.5.1.).

Különösen a következő óvintézkedéseket érdemes megfontolni:

- a jelentős változások azonosítását és rögzítését;
- az ilyen változások lehetséges hatásainak felmérését;
- a tervezett változtatások formális jóváhagyási eljárását;
- a változások minden lényeges adatának (részleteinek) a közlését minden arra illetékes személlyel;
- a sikertelen változtatások félbeszakítása és az azokból való visszatérés felelőseit azonosító eljárásokat.

6.1.3 A feladatkörök elhatárolása

A feladatkörök szétválasztása az a módszer, amely minimalizálja a véletlen és a szándékos visszaélésekből eredő kockázatot. Az egyes feladatok vagy felelősségi körök végrehajtását és irányítását szét kell választani annak érdekében, hogy az információ jogosulatlan módosításának és a visszaélésnek csökkenjen az esélye.

A kisebb Hivatalek ezt az ellenőrzési módot nehéznek találhatják, lehetőség szerint mégis érdemes követni. Ha a feladatmegosztás aránytalan nehézséggel jár, egyéb óvintézkedéseket kell megfontolni, mint pl. a tevékenységek megfigyelését (monitorozását), az átvilágítás naplózását vagy a vezetői felügyeletet. A biztonsági átvilágítás auditálása független kell, hogy maradjon.

Fontos, hogy az egyedi felelősségi körben elkövetett csalás letagadhatatlan maradjon. Az események kezdeményezése, beindítása legyen független az arra vonatkozó felhatalmazástól. A következő pontok megfontolandók:

- Az olyan szerepköröket szét kell választani, amelyek összejátszása csalással járhat (pl. megrendelés

kiadását és annak igazolását, hogy az árut átvették).

- Ha összeesküvés fenyeget, akkor el kell érni, hogy két vagy három személy végezze az érintett (egyetlen szerepkörhöz köthető) feladatot.

6.1.4 A fejlesztési és az üzemeltetési feladatok szétválasztása

A fejlesztés, a tesztelés és az üzemeltetés eszközeit szétválasztva könnyebb a szerepkörök elhatárolása is. Szabályzatba kell foglalni, hogy egy szoftvert milyen szempontok alapján lehet a fejlesztés alatt álló szoftverek közül az üzemi szoftverek közé sorolni.

A fejlesztés vagy tesztelés alatt álló szoftverek komoly nehézségeket okozhatnak, pl. hátrányosan módosíthatják az általuk kezelt állományokat vagy a rendszerkörnyezetet, rendszerhibákat idézhetnek elő. Ahol ez mérlegelhető, a fejlesztési és tesztelési, illetve az üzemeltetési környezetet az üzemeltetési nehézségekkel arányos mértékben kell szétválasztani. Hasonlóan érdemes eljárni a fejlesztési és tesztelési funkciók között. Ilyenkor az a cél, hogy fenntartsuk az ismert és stabil környezet, amelyet egy fejlesztési hiba bármikor ismét instabillá tehetne.

Ha a fejlesztő és a tesztelő személyzet hozzáférhet az üzemelő rendszerhez és az üzemi információkhoz, jogosulatlanul beiktathatnak ellenőrizetlen kódrészeket vagy megváltoztathatják az adatbázist. Egyes rendszereken ez csalás bűncselekményét jelenti, és veszélyeztetheti a méltányos hivatali érdeket vagy a minősített adatok biztonságát.

A fejlesztők és tesztelők gondatlanságból is kárt tehetnek a szoftverben vagy az adatokban, illetve megismerhetnek számukra titkos adatokat, ha az érintettek egyetlen számítástechnikai környezeten osztoznak.

A következő óvintézkedéseket kell bevezetni:

- A fejlesztési és az üzemi szoftvert, ahol lehetséges, külön tartományban, számítógépen, processzoron vagy mappában kell futtatni.
- A fejlesztési és tesztelési feladatokat, amennyire lehetséges, szét kell választani.
- Fordítóprogramokat és rendszeradminisztrációs eszközöket nem szabad szükségtelenül elérhetővé tenni az üzemi rendszerből.
- A hibák kockázatának csökkentésére a fejlesztésre és a tesztelésre szolgáló platformon eltérő bejelentkezési eljárást érdemes alkalmazni. A felhasználókat arra kell biztatni, hogy az egyes szerepköreikhez eltérő jelszót használjanak, és felhasználói azonosítójuk utaljon a szerepkörre.
- A fejlesztő személyzetnek csak ott szabad hozzáférést kapnia az üzemi jelszavakhoz, ahol az üzemi rendszer kezelésére való jelszavak kiadásánál óvintézkedések vannak érvényben. Gondoskodni kell arról, hogy az ilyen jelszavakat használat után lecseréljék.

6.1.5 Külső létesítmények üzemeltetése

A Hivatalt adatfeldolgozás biztonsági kockázatot jelenthet, mert egy harmadik fél telephelyén nehezebben garantálható a bizalmasság, a sértetlenség és a rendelkezésre állás. Az ilyen kockázatokat a megállapodás előtt fel kell tárni, és az adatkezelő biztonsági követelményeit az adatfeldolgozó számára szerződéses kötelemként kell rögzíteni (lásd még: 8.2.).

Külső létesítmények üzemeltetése előtt érdemes:

- feltárni azokat az érzékeny vagy kritikus alkalmazásokat, amelyeket helyesebbnek vélünk házon belül tartani;

- jóváhagyást kérni az hivatali alkalmazások tulajdonosaitól;
- a külső létesítmények üzemeltetési szabályait, jellemzőit bevonni az üzletmenetfolytonossági tervbe;
- összeállítani az előírandó biztonsági szabványokat, valamint azt a folyamatot, amellyel a megfelelőséget mérjük;
- kiosztani valamennyi biztonsági tevékenység hatékony megfigyelésének sajátos felelősségeit és eljárásait;
- meghatározni a biztonsági események naplózásának, kezelésének és közlésének eljárásrendjét, illetve az abban betöltendő szerepköröket (lásd: 11.).

6.2 Harmadik fél szolgáltatásának irányítása

Cél:

Az intézkedés célja az informatikai biztonság és szolgáltatás megfelelő szintjének fenntartása, összhangban a harmadik fél szolgáltatási szerződésével. A Hivatal kísérje figyelemmel a szolgáltatási szerződések betartását, és kezelje a változtatásokat.

Szabályozás:

6.2.1 A szolgáltatás színvonala

A szolgáltatás során alapvető biztonsági szempont, hogy a szolgáltatói szerződésekben meghatározott biztonsági intézkedéseket, a szolgáltatás színvonalát a harmadik fél folyamatosan fenntartsa. A megbízónak vésztervvel kell rendelkeznie a szolgáltatás átmenti leállására vagy végleges megszűnésére vonatkozólag. Minden szolgáltatási szerződésben ki kell kötni a vészhelyzet esetén azonnal bevonható helyettesítő szolgáltatókat, a pénzügyi károk enyhítése érdekében.

6.2.2 A szolgáltatás ellenőrzése

A szolgáltatási szerződésekben definiált informatikai biztonsági intézkedések betartása a megbízó számára létkérdés, ezért a szerződésekben meg kell határozni a megbízó Hivatal ellenőrzési jogkörét. A folyamatos, időszakos vagy váratlan informatikai biztonsági ellenőrzés megerősíti a szolgáltató biztonságtudatosságát, elősegíti a biztonságos szolgáltatásnyújtást, valamint a biztonsági események és kockázatok megfelelő kezelését.

A szolgáltatások ellenőrzése során a következő szempontokra érdemes kitérni:

- szolgáltatás színvonalának, valamint szerződési feltételek betartása;
- szolgáltatási jelentések és a gazdasági tervek;
- biztonsági auditdokumentumok, biztonsági események feljegyzései;
- üzemeltetési problémák, meghibásodások, a hibák nyomon követése, problémamegoldó képesség;

A harmadik féllel való kapcsolattartást egy kijelölt személyre vagy szolgáltatáskezelő csoportra érdemes bízni. Ezen kívül a Hivatal érje el, hogy a harmadik fél felelősöket jelöljön ki a szerződésben foglalt követelmények teljesítésére.

6.2.3 Változáskezelés

A változáskezelés szinte minden területen fontos biztonsági intézkedés, amely elősegíti az esetleges üzemeltetési vagy szolgáltatási hibák gyors észlelését.

A változáskezelésbe érdemes bevonni a következőket:

- a Hivatal által végzett változtatások implementációját;
- minden új alkalmazás és a rendszer fejlesztését;
- a Hivatal szabályzatainak és eljárásrendjeinek módosítását vagy frissítését;
- a biztonsági események kezelésére és a biztonság fejlesztésére hozott intézkedéseket;
- új technológiák kezelését és új termékek kibocsátását;
- hálózatok bővítését és átalakítását.

6.3 Informatikai rendszerek tervezése és átvétele

Cél:

Informatikai rendszerek tervezésekor és átvételekor alapvető szempont, hogy a Hivatal minimalizálja a meghibásodások kockázatát.

Szabályozás:

A tervezés kulcseleme a kapacitástervezés, melynek segítségével megbecsülhető, vagy akár kiszámítható a Hivatal informatikai rendszerének hardver és tárigénye.

Célszerű a jövőben várható kapacitáskövetelményt előre feltüntetni, hogy csökkentsük a rendszer túlterhelésének kockázatát. Az új rendszerek üzemeltetési követelményeit átvétel vagy használatba vétel előtt kell megállapítani, dokumentálni és bevizsgálni.

6.3.1 Kapacitástervezés

A rendszerek kapacitásigényét folyamatosan figyelemmel kell kísérni, és meghatározott időnként újra ki kell számítani. A kapacitástervezés célja, hogy az hivatali folyamatokat kiszolgáló feldolgozási teljesítmény és tárhely időben álljon rendelkezésre. A tervek az újabb hivatali és rendszerkövetelményeket, valamint a Hivatal adatfeldolgozásának jelenlegi és várható trendjeit is vegyék figyelembe.

.

Ezen információk birtokában könnyen felismerhetők és elkerülhetők a lehetséges szűk keresztmetszetek, amelyek veszélyt jelenthetnek a rendszerbiztonságra és a felhasználói szolgáltatásokra.

6.3.2 A rendszer átvétele

Az új informatikai rendszerek, korszerűsítések és változatok átvételi követelményeit definiálni kell, és a rendszervizsgálatokat még az átvétel előtt el kell végezni. A vezetők gondoskodjanak arról, hogy az új rendszerek átvételi követelményei egyértelműen legyenek meghatározva, egyeztetve és dokumentálva. Az új rendszer átvétele csak a dokumentált rendszerkövetelmények birtokában történjen meg.

Ellenőrizni kell a következőket:

- a műszaki és számítási kapacitást;
- a hibajavító és az újraindítási eljárások vészterveit;
- a rutin üzemeltetési eljárások előkészítését és bevizsgálását;
- a megállapodások szerinti biztonsági óvintézkedések megtételét;
- a hatékony kézi (manuális) eljárásokat;
- az üzletmenet folyamatosságának érdekében a 9.1. alfejezet által megkívánt elrendezéseket;

- annak bizonyítékait, hogy az új rendszer üzembe helyezése nem lesz ellenkező, káros hatással a meglévő rendszerekre, különösen nem a feldolgozási csúcsidőkben;
- annak bizonyítékait, hogy igenis figyelmet fordítottak arra a hatásra, amit az új rendszer üzembe helyezése okoz a Hivatal általános biztonságára;
- az új rendszerek üzemeltetésének és használatának a betanítását. Napjaink informatikai rendszereinek sikertényezője a felhasználóbarát program, a könnyű kezelhetőség, ami nagyban hozzájárul a rendszer hatékonyságához, ezért a fejlesztési folyamat minden lépésében konzultálni kell az üzemeltetőkkel és a felhasználókkal.

6.4 Védelem rosszindulatú programok ellen

Cél:

A szoftver és az adatfeldolgozó eszközök sérülékenyek az olyan rosszindulatú szoftverekkel szemben, mint a vírusok, férgek, trójai falovak és logikai bombák. A felhasználóknak tudniuk kell, hogy a jogosulatlan és a rosszindulatú szoftverek milyen veszélyesek. A Hivatalnak minden óvintézkedést meg kell tennie annak érdekében, hogy a rosszindulatú programok bejutását megakadályozzák. Lényeges, hogy a munkaállomásokon és kiszolgálógépeken is tegyünk óvintézkedéseket a számítógépvírusok bejutásának megelőzésére és észlelésére.

Szabályozás:

A felhasználóknak tudniuk kell, hogy rosszindulatú programok a hálózati csatlakozásokon keresztül is bejuthatnak az informatikai rendszerbe. Megfelelő biztosítékok nélkül a rosszindulatú kód rejtett maradhat mindaddig, amíg kárt nem okoz. A kártékony kód hatástalanná teheti a védelmi rendszereket (pl. kitudódnak a jelszavak), tönkreteheti az adatállományokat, lelassíthatja a rendszereket.

A rosszindulatú kódok néhány formáját meg lehet találni és el lehet távolítani speciális keresőprogramokkal. Keresők rendelkezésre állnak tűzfalakhoz, fájl és levelezőszerverekhez, munkaállomásokhoz.

A vírusok, rosszindulatú programok gyors észlelése és eltávolítása érdekében biztosítani kell a keresőszoftver önműködő frissítését.

A felhasználóknak és a rendszergazdáknak tudniuk kell, hogy a keresők nem találnak meg minden rosszindulatú kódot (még az egyetlen fajtához tartozó összes változatot sem), mivel folyamatosan jelennek meg azok új formái. Ezért további biztosítékokra van szükség a keresők által adott biztonság növelésére.

A hálózati csatlakozással rendelkező rendszerek felhasználóinak és rendszergazdáinak azzal is tisztában kell lenniük, hogy a rosszindulatú kódok szempontjából a normálisnál nagyobb kockázattal jár, ha külső kapcsolaton keresztül működnek együtt külső felekkel. A felhasználók és rendszergazdák részére eljárásrendet kell kidolgozni rosszindulatú kód bejutásának meggátlásáról.

A felhasználóknak és rendszergazdáknak különös figyelmet kell fordítaniuk arra, hogy a hálózati kapcsolatban érintett rendszereket és alkalmazásokat úgy állítsák be, hogy minden, az adott körülmények között szükségtelen funkciót letiltsanak. Példa: a PCs alkalmazások esetében a makrók használatát alaphelyzetben ki kell kapcsolni, vagy végrehajtásukat a felhasználó jóváhagyásához kell kötni.

A rosszindulatú kód a bizalmasság elvesztéséhez vezethet, pl. a jelszavak megszerzése és feltárása útján. Ez ellen a biztosítékok az alábbiak:

- Védelem a rosszindulatú kód ellen.

- Események kezelése: bármilyen szokatlan esemény időben történő jelentése korlátozhatja a rosszindulatú kód által okozott kárt. Behatolás elleni védelem alkalmazható a rendszerbe vagy hálózatba történő belépési kísérletek felderítésére.
- Megfelelő titkosítás.
- A rosszindulatú kód a sértetlenség elvesztéséhez vezethet, pl. úgy, hogy egy személy a rosszindulatú kód segítségével megszerzett hozzáférés birtokában adatokat vagy állományokat módosít. Ez ellen a biztosítékok az alábbiak:
- Védelem a rosszindulatú kód ellen.
- Események kezelése: bármilyen szokatlan esemény időben történő jelentése korlátozhatja a rosszindulatú kód által okozott kárt. Behatolás elleni védelem alkalmazható a rendszerbe vagy hálózatba történő belépési kísérletek felderítésére.
- A rosszindulatú kód felhasználható az azonosítási és hitelesítési rendszerek, illetve a kapcsolódó biztonsági tevékenység megtévesztésére, pl. úgy, hogy egy személy a rosszindulatú kód segítségével megszerzett hozzáférés birtokában adatokat vagy állományokat semmisít meg. Ez ellen a biztosítékok az alábbiak:
- Védelem a rosszindulatú kód ellen.
- Események kezelése: bármilyen szokatlan esemény időben történő jelentése korlátozhatja a rosszindulatú kód által okozott kárt. Behatolás elleni védelem alkalmazható a rendszerbe vagy hálózatba történő belépési kísérletek felderítésére.

6.4.1 A rosszindulatú programokat ellenőrző eszközök

A rosszindulatú szoftver elleni védelem érdekében észlelő és megelőző óvintézkedéseket kell hozni, valamint a felhasználók biztonságtudatosságát fenntartó oktatásokat tartani. A rosszindulatú szoftver elleni védelmet a biztonságtudatosságra, a megfelelő hozzáférés és változáskezelési intézkedésekre kell alapozni.

A következő óvintézkedéseket érdemes megfontolni:

- Formális szabályzatot kell kidolgozni, amely megköveteli a megfelelést a szoftverlicenceknek, és megtiltja a jogtalan szoftverhasználatot.
- Formális szabályzatot kell kidolgozni, amely véd az állományok és programok külső hálózatból vagy azokon keresztüli átvételéből, illetve más adathordozó közeggel kapcsolatos kockázatoktól, és megadja, hogy milyen védelmi intézkedéseket kell hozni (lásd még a 8.5. alfejezetet, különösen a 8.5.4. és a 8.5.5. szakaszt).
- Vírusvédelmi szoftvert kell telepíteni, és azt rendszeresen frissíteni: segítségével a számítógépeket és adathordozókat meghatározott időnként, illetve kártevő szoftver jelenlétének gyanúja esetén át kell vizsgálni.
- A kritikus hivatali folyamatokat segítő rendszerek szoftverét és adattartalmát szabályos időközönként felül kell vizsgálni: a mechanizmus állítsa helyre a sérült fájlokat és rendszerleíró kulcsokat.
- Bizonytalan eredetű elektronikus adathordozón kapott, vagy megbízhatatlan hálózatról fogadott állományok fertőzöttségét használat előtt ellenőrizni kell;
- A bejövő elektronikus levelek mellékleteit és a letöltött állományok fertőzöttségét használat előtt ellenőrizni kell. Ez különböző helyeken történhet, pl. az elektronikus levelezőrendszer szerverén, asztali számítógépeken, vagy ott, ahol a Hivatal hoz kapcsolódnak.
- A rendszerek vírusvédelmével, helyes használatának oktatásával, a vírustámadásról szóló jelentés elkészítésével és a helyreállítással kapcsolatos vezetői (menedzseri) eljárásokat és felelősségeket

dokumentálni kell (lásd: 4.3. és 6.1.3.).

- Üzletmenetfolytonossági tervet kell készíteni, amely a vírustámadás utáni helyreállításra vonatkozik, beleértve a szükséges adatmentési, szoftvertartalékolási és visszatérési eljárásokat.
- Ki kell dolgozni a rosszindulatú szoftverek tevékenységének naplózásával és jelentésével kapcsolatos eljárásrendet, illetve figyelmeztető kiadványokkal (bulletinekkel) gondoskodni kell az érintettek pontos tájékoztatásáról. A vezetők a megtévesztés (hoax) és a valódi vírus közötti megkülönböztetésre minősített forrásokból származó anyagokat alkalmazzanak, tekintélyes szaklapokból, megbízható Internet helyszínekről, vagy vírusvédő szoftverek szállítóitól. A személyzetben tudatosítani kell a megtévesztések problémáját, és hogy mit kell tenniük, ha ilyet észlelnek vagy kapnak.
- Ezek különösen fontosak az olyan hálózati fájlszerverek esetében, amelyek sok munkaállomást szolgálnak ki.

6.4.1.1 A vírusvédelmi rendszer kialakítása és működtetése

A rosszindulatú kódok hálózati csatlakozásokon és hordozható lemezeken behozott állományokon és szoftvereken keresztül juthatnak a rendszerbe. Megfelelő biztosítékok nélkül a rosszindulatú kód mindaddig rejtve maradhat, amíg kárt nem okoz. A rosszindulatú kód a biztosítékok működését is lehetetlenné teheti (pl. a jelszavak elfogása és feltörése útján): felfedheti az érzékeny információkat, vagy megváltoztathatja azokat, a rendszer sértetlenségének elvesztéséhez vezethet, de meg is semmisítheti az információkat, vagy illetéktelenül használhatja az erőforrásokat. A rosszindulatú kódok következő fajtáit ismerjük:

- vírusok,
- férgek,
- trójai falovak.

A rosszindulatú kódok hordozói a következők:

- végrehajtható (futtatható) szoftverek;
- adatállományok, melyek végrehajtható makrókat tartalmaznak, pl. szövegszerkesztővel készült dokumentumok vagy táblázatok;
- aktív tartalmat hordozó weboldalak.
- A rosszindulatú kódokat a következő módokon lehet továbbadni:
- leválasztható adathordozók,
- elektronikus levél,
- hálózatok,
- távoli hozzáférés,
- letöltések.

A rosszindulatú kódok megjelenése lehet szándékos tevékenység következménye vagy olyan rendszerszintű kölcsönhatás eredménye, mely akár észre sem vehető a felhasználók számára. A rosszindulatú kódok elleni védelmet a következő biztosítékokkal lehet elérni:

Keresők: A rosszindulatú kódok különböző formáit fel lehet fedni, és el lehet távolítani speciális keresőszoftverekkel és sértetlenségellenőrző eszközökkel. A keresők offline és online módon üzemelhetnek. Az online működés aktív védelmet biztosít, azaz felfedi (és valószínűleg el is távolítja) a rosszindulatú kódot, még mielőtt bármilyen fertőzés történhetne, és károk keletkeznének az informatikai rendszerben. A keresők rendelkezésre állnak különálló számítógépekhez, munkaállomásokhoz, fájl, levelező és proxy

szerverekhez, illetve tűzfalakhoz. Mindazonáltal a felhasználóknak és a rendszergazdáknak tisztában kell lenniük azzal, hogy nem lehet a keresők sem képesek minden rosszindulatú kódot megtalálni (még egy adott fajta összes változatát sem), mivel folyamatosan jelennek meg ezek új formái.

Sértetlenségellenőrző eszközök: Jellemzően egyéb biztosítékok szükségesek a keresők által nyújtott biztonság növeléséhez. Pl. ellenőrző összegeket használnak annak eldöntésére, hogy egy program módosulte. A sértetlenséget ellenőrző szoftverek lényeges részét képezik a rosszindulatú kódok ellen védő technikai biztosítékoknak. Ezt a technikát csak olyan adatállományok és programok esetében lehet használni, amelyek nem tartalmaznak későbbi használatra szánt állapotinformációkat.

Kivehető adattárolók forgalmának ellenőrzése: Az adattárolók (különösen az optikai lemezek és flash memóriák) felügyelet nélküli mozgása jelentősen veszélyezteti a Hivatal informatikai rendszereit. Az adathordozók használatát speciális szoftverekkel vagy eljárási biztosítékokkal (lásd alább) lehet ellenőrizni.

Eljárási biztosítékok: A felhasználók és rendszergazdák számára útmutatót kell készíteni azon eljárások és gyakorlatok bemutatására, melyekkel a rosszindulatú kódok bejutásának lehetőségét minimalizálni lehet. Az útmutatónak ki kell térnie a játékok és egyéb szoftverek betöltésére, a különböző internetes szolgáltatások használatára és különböző adatállományok importjára. A rosszindulatú kódok megelőzését szolgáló szabályzatok és eljárásrendek megszegése esetére biztonságtudatosság növelő képzést kell szervezni, és szankciókat kell bevezetni.

6.4.2 Mobil kód elleni intézkedések

A mobil kód egy szoftver, amely egyik számítógépről egy másikra visz át, ahol önműködően végrehajt egy meghatározott funkciót, minimális felhasználói beavatkozással vagy a nélkül. Egy mobil kód számos szoftverszolgáltatással társulhat. Biztonsági szempontból alapkövetelmény, hogy a mobil kód ne tartalmazzon rosszindulatú kódot, de használatának, működési területének szabályozásával megelőzhető a jogosulatlan rendszerhozzáférés, az alkalmazási rendszerek lefagyása, és az egyéb biztonsági események is.

Ha a rendszerben mobil kód futtatására van lehetőség, akkor a szoftverkonfiguráció biztosítsa, hogy

- az engedélyezett mobil kód a rendszerbiztonsági politika szerint működjön;
- a rendszerben jogosulatlan mobil kódot ne hajthassanak végre.

A jogosulatlan tevékenységet végző mobil kódok elleni intézkedések:

- mobil kód végrehajtása elszigetelt környezetben;
- mobil kód használatának teljes letiltása;
- mobil kód letöltésének megakadályozása;
- mobil kód szabályozását biztosító egyedi rendszer alkalmazása;
- mobil kód rendszerjogosultságainak szabályozása;
- mobil kód egyedi azonosítása kriptográfiai módszerekkel.

6.5 Mentés

A mentések célja az információ és az adatfeldolgozó szoftverek sértetlenségének és rendelkezésre állásának biztosítása.

A folyamatos működés érdekében a Hivatal az Üzemeltetési utasításban írja le a mentés eljárásokat. Mivel az adatmentések lényege a teljes, veszteségmentes visszaállíthatóság, ezért az archívumok visszaállíthatóságát ellenőrizni kell. Minden új backup szoftver vagy hardver vásárlása esetén üzembe

helyezés előtt ki próbálni az adatvisszaállítást egy másik gépen vagy másik tesztkönyvtárban.

6.5.1 Adatmentések

Az üzemi adatok és szoftverek biztonsági rendszeres mentése és ellenőrzése alapvető biztonsági követelmény. A Hivatal az Üzemeltetési utasításban kész biztonsági eljárásokkal rendelkezik arra az esetre is, ha a mentési rendszer hibásodik meg. Az ilyen kockázatok csökkentése érdekében a háttértárakon kívül a Hivatalnak tartalék mentési eszközökről is gondoskodniuk kell.

A következő óvintézkedéseket megfontolandók:

- Az archívumokat és a visszaállítás dokumentált eljárásait a rendeltetési helytől távoli helyen biztonságba kell helyezni – elég távol ahhoz, hogy bármely rongálódástól meg legyenek kímélve, ha a rendeltetési helyen katasztrófa következne be. A lényeges hivatali információk körében a biztonsági mentési állományok legalább három generációját, azaz ciklusát érdemes megőrizni.
- A mentések típusa (pl. teljes vagy differenciált mentés) és gyakorisága álljon arányban a mentett adatok minősítésével, fontosságával.
- A biztonsági mentéseket és az ezeket tároló adathordozókat megfelelő szintű fizikai és környezeti védelemmel kell ellátni, ugyanazon biztonsági előírások szerint, mint amit a feldolgozás helyén alkalmazunk.
- A biztonsági mentések adathordozóit, ahol az megoldható, időről időre meg kell vizsgálni, hogy megtudjuk: használhatóke még. Fontos figyelemmel kísérni a mentési adathordozók garanciájának lejárati idejét, lehetséges tárolási és visszaállíthatósági idejét, és a lejárt eszközöket ki kell vonni a mentési folyamatokból.
- A visszaállítási eljárások hatékonyságát időről időre ellenőrizni kell, hogy megtudjuk: elvégezhetőke annyi idő alatt, amennyit az üzemi eljárások a visszaállításra megszabtak.
- Határozzák meg a lényeges adatok megőrzési időszakát és az állandóan megtartandó, archív példányokra vonatkozó követelményeket.

6.6 Hálózatkezelés

A hálózatkezelés célja a hálózaton áthaladó információ és a támogató infrastruktúra védelme. A hálózatbiztonság kérdése a nyilvános hálózatokon átmenő adatok esetében különösen fontos. Szintén alapvető biztonsági cél, hogy a hálózatokat megfelelően, biztonságosan, dokumentáltan kezeljék és szabályozzák.

A hálózatmenedzsment segítségével kell meghatározni a hálózatok adattartalmának biztonságát és az infrastruktúra védelmét, különös tekintettel a több Hivatalet átfogó hálózatokra.

6.6.1 Hálózatbiztonsági intézkedések

Olyan ellenőrző eszközökről kell gondoskodni, amelyek biztosítják a hálózatokban kezelt és továbbított adatok biztonságát, valamint a kapcsolt szolgáltatásokat megóvják az illetéktelen hozzáférésektől.

- A hálózatok és a számítógépek működtetésének feladatait, felelősségeit szét kell választani.
- A nyilvános hálózatokon keresztül továbbított érzékeny adatok, illetve a kapcsolt rendszerek védelmére pótlólagos ellenőrző eszközökre van szükség.
- Pontosan definiálni kell a hálózat határait. A hálózat biztonságos szegmentálásának kialakításáért az informatikai vezető által kijelölt személy felel.

- Rögzíteni kell a távfelügyeleti eszközök, távoli berendezések irányítási felelősségét és eljárásait.
- Különleges szabályozást kell bevezetni, hogy megvédjék a nyilvános hálózatokon vagy vezeték nélküli hálózatokon átmenő adatok sértetlenségét, bizalmasságát, illetve a hálózati szolgáltatások és az online rendszerek rendelkezésreállását (lásd: 7.4. és 8.3.).
- A hálózati eseményeket megfelelő részletességgel naplózni kell, és lehetővé kell tenni a naplófájlok rendszeres ellenőrzését.

6.6.2 Hálózati szolgáltatások biztonsága

A hálózati szolgáltatások a csatlakozásra és a hálózati forgalom szabályozására, szűrésére terjednek ki, mint pl. tűzfalakra és behatolásészlelő rendszerekre.

Fel kell mérni minden hálózati szolgáltatás biztonsági jellemzőit, irányítási követelményeit, és ezeket rögzíteni kell a szolgáltatási szerződésekben – ki kell kötni a biztonsági intézkedések folyamatos betartását, és azok ellenőrizhetőségét is.

Mivel a különböző hálózatok szolgáltatásainak kínálata rendkívül széles, jelentős részük még számos többletszolgáltatással rendelkezik, ezért fontos, hogy a rendszer telepítése során csak azokat a hálózati szolgáltatásokat illesszük a rendszerbe, melyekre az üzemeltetéshez feltétlenül szükség van. A feleslegesen telepített hálózati szolgáltatások és protokollok jelentősen növelhetik.

A rendszerüzemeltetőnek minden esetben fel kell mérnie, és minden részletre kiterjedően dokumentálnia kell az általa alkalmazott hálózati szolgáltatás egyedülálló, illetve összetett biztonsági jellemzőit. Amennyiben több hálózati szolgáltatás működik a rendszerben, úgy ezek egymásra gyakorolt hatását is elemezni kell biztonsági szempontból. A hálózati szolgáltatások biztonsági beállítása, valamint annak ellenőrzése, karbantartása a hálózatot üzemeltető szerv feladata.

A hálózati szolgáltatások biztonsági jellemzői:

- a hálózati szolgáltatások biztonságára alkalmazott technológia, mint a hitelesítés, rejtjelezés és kapcsolódási intézkedések;
- a hálózati kapcsolatok létrehozásának műszaki paraméterei;
- hálózati hozzáférésvédelmi eljárások.

6.7 Az adathordozók biztonságos kezelése

A védelmi intézkedések célja, hogy az adathordozók fizikai védelmét szabályozzák, megfelelő eljárásokkal védjék a dokumentumokat, a számítógépek adathordozóit (pl. szalagok, lemezek), a bemeneti és kimeneti adatokat, valamint a rendszer dokumentációját a jogosulatlan megszerzésétől, módosítástól, eltávolítástól és rombolástól.

Az adathordozók kezelésének legfontosabb biztonsági követelményei:

- Gondoskodni kell az adathordozók ellenőrzéséről és fizikai védelméről.
- Meg kell előzni a dokumentumok, a számítástechnikai adathordozók (szalagok, lemezek, kazetták), az inputoutput adatok és a rendszerdokumentációk károsodását, eltulajdonítását és engedély nélküli törlését.
- Szabályozni kell az adathordozók beszerzését, tárolását és kezelését.
- Biztosítani kell, hogy az adathordozók kezelése – a vonatkozó iratkezelési szabályok szellemében – az egyenértékű papíralapú dokumentumokkal azonos módon történjék. Az adathordozókról és azok

tartalmáról nyilvántartást kell vezetni.

- A Hivatalnél csak nyilvántartott és egyedi azonosítóval ellátott adathordozót szabad használni.
- A Hivatalen kívüli adatforgalomban használt adathordozók előállítása, kiadása és fogadása az ügyviteli (iratkezelési) szabályzat előírásai szerint a kijelölt helyeken, dokumentált és ellenőrzött módon történhet. Az adathordozókat használatba venni csak az előírt ellenőrző eljárások elvégzése után szabad (pl. vírusellenőrzés).
- Minden adathordozót újraalkalmazás előtt, illetve felszabadítás vagy selejtezés után az adatokat véglegesen megsemmisítő eljárással törölni kell.
- Minősített adatok esetében a minősítés felismerhető jelölését az adathordozón fel kell tüntetni.
- Adathordozótól függetlenül biztosítani kell a tárolt adatok sértetlenségét.

6.7.1 Hordozható adathordozók kezelése

A hordozható adathordozók kezelésének legfontosabb biztonsági követelményei:

- Nem minősített adathordozókat az ügyviteli (iratkezelési) szabályzat előírásai szerint kell kezelni.
- Érzékeny információt tartalmazó adathordozókat az ügyviteli (iratkezelési) szabályzat és a titokvédelmi szabályzat szerint kell tárolni és kezelni.
- Minden adathordozót biztonságos környezetben tároljanak, a gyártó előírásainak megfelelően.

6.7.1.1 Adathordozók tárolása

Az adathordozókat – azokat is, amelyek használaton kívül vannak – biztonságos helyen kell tárolni, vagy amennyiben ezek munkaközi példányok, meg kell semmisíteni. Ezek a következők: kinyomtatott dokumentumok, hang és egyéb adatrögzítés, nyomtatópapír, kimeneti jelentések, egyszer használatos nyomtatószalagok, mágnesszalagok, mobil diszkek és kazetták, optikai tárolóeszközök (összes lehetséges formája, ideértve a telepítőkészleteket gyártó terjesztéséhez alkalmazott adathordozókat), programlisták, tesztadatok, rendszerdokumentáció.

Az érzékeny tételek elhelyezéséről az üzemeltetésért felelős vezetőnek naplót kell vezetnie.

Az adathordozók tárolására vonatkozó fizikai védelem követelményeivel kapcsolatban a rendszerszintű IBSZekben meg kell határozni:

- a tárolók környezetére vonatkozó előírásokat és a paraméterek normál értékeinek biztosítására, ellenőrzésére hozható intézkedéseket;
- az elöregedésből fakadó adatvesztés elleni megelőző intézkedéseket (pl. rendszeres átírás);
- az adathordozók másodpéldányainak biztonságos tárolására vonatkozó előírásokat;
- az adathordozók kölcsönzésével kapcsolatos előírásokat;
- a rendszer és a felhasználói szoftver törzspéldányok biztonságos tárolására, valamint a használati másodpéldányok készítésére vonatkozó előírásokat.

A fokozott biztonsági osztályba sorolt minősítésű adathordozók tárolása csak megbízhatóan zárt helyiségben, minimum 30 percig tűzálló szekrényben történhet.

6.7.1.2 Adathordozók kivitele

Számítástechnikai eszközöket, adathordozókat, programokat kizárólag a Hivatali egységek vezetőinek engedélyével szabad kivinni a munkahelyről. A Hivatal területéről kivitt eszközöket a leltárfelelősöknek nyilván kell tartaniuk.

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

Meghibásodott eszköz cseréje esetén – még garanciális esetben is – adathordozó csak úgy vihető ki, ha arról minden adatot visszaállíthatatlanul töröltek. A szállítás során be kell tartani a biztonsági eljárásokat.

6.7.2 Adathordozók újrahasznosítása, selejtezése

Alapvető biztonsági cél, hogy az adathordozókat visszaállíthatatlanul, dokumentáltan selejtezzék. A különféle szabványokban definiált adattörlési és megsemmisítési eljárások a lehető legkisebbre csökkentik az információ kiszivárgásának kockázatát. Az érzékeny információt tartalmazó adathordozó selejtezési eljárásai arányosak legyenek az információ érzékenységével, értékével.

- Az érzékeny információt tartalmazó adathordozót biztosan visszaállíthatatlan módon selejtezzék, pl. égetéssel, aprítással, az adatok törlésével, vagy különféle biztonsági felülírási eljárások használatával.
- Egyszerűbb a selejtezés, ha minden adathordozót a legerősebb biztonsági eljárással selejteznek – így nem kell az érzékeny tételek kiválogatásával foglakozni.
- Adathordozók selejtezésével foglalkozó cégekkel csak úgy szabad megállapodni, ha előzőleg felmérték a biztonsági szintjét, és számára a biztonsági követelményeket szerződésben kikötötték.
- Az érzékeny tételek eltávolítását naplózzák, és ha lehet, az informatikai biztonsági vizsgálatok kísérő dokumentumaként kezeljék.
- Amikor az adathordozókat selejtezésre összegyűjtik, fontolják meg a halmozódási hatást, amely szerint az egy helyen központosuló nagy mennyiségű nem érzékeny adat érzékenynek tekintendő.
- Az érzékeny információ kiszivároghat az adathordozók gondatlan selejtezése által is, pl. számítógépek selejtezésénél, ha nem megfelelően törlik le vagy semmisítik meg az adathordozókat (lásd: 7.2.6.).
- Azokat az adathordozókat, amelyeket nem lehet engedélyezett módon törölni (pl. működésképtelennek látszik) újrafelhasználni tilos, nem kerülhet ki a védelmi intézkedések hatóköréből, meg kell semmisíteni.
- Az adathordozó védelme csak az adatok törlését és az adathordozó felülírását követően oldható fel. A felülírás tényét, módszerét, végrehajtóját, annak időpontját dokumentálni kell. Az adathordozó védelmére vonatkozó intézkedéseket továbbá csak akkor szabad visszavonni, ha az újraírható adathordozóról a bizalmas adattartalomra utaló valamennyi jelzést és utalást eltávolították. Ha ez nem lehetséges, a védelem nem szüntethető meg.
- Amennyiben az adathordozó olyan mértékben sérült vagy elhasználódott, hogy a további használata lehetetlen vagy ésszerűtlen, azt az ügyviteli szabályok szerint jegyzőkönyvben kell selejtezni. Ebben az esetben – ha lehetséges – a tartalmát törölni kell, és magát az adathordozót „SELEJT" felirattal az ügyviteli szervnek kell átadni, ahol gondoskodni kell a szabályszerű megsemmisítésről.
- Az érzékeny információ kiszivároghat az informatikai eszközökben található adathordozók gondatlan selejtezése által is (lásd még a 7.2.6. szakaszt az informatikai eszközök eltávolításával kapcsolatban).

6.7.2.1 Adathordozók újrahasznosítása

Védett informatikai rendszerben használt adathordozót olyan módszerrel kell törölni, hogy az adatok a későbbiekben ne legyenek helyreállíthatók. Ilyen például az adathordozó többszöri felülírása.

Az adathordozó felülírására engedélyezett módszer a következő. Miután az adathordozó

működőképességéről meggyőződtek, valamennyi tároló területet kilencszer kell felülírni:

1. először az „1" bináris számjeggyel;
2. másodszor a „0" bináris számjeggyel;
3. majd egy tetszőleges bitmintával (pl. „0011 0101");
4. végül a fenti lépéseket még kétszer meg kell ismételni.

A tárhelyek tartalmát mindig ellenőrizni kell, hogy a felülírás sikeres volte.

6.7.2.2 Adathordozók megsemmisítése

Mágneses adathordozók megsemmisítésére, különféle speciális demagnetizáló berendezések vannak forgalomban. Ezek az eszközök garantáltan törlik a mágneses adattárolók tartalmát. A berendezés kiválasztásánál a demagnetizáló eszköz hitelesítését ellenőrizni kell.

Amennyiben ilyen eszközökkel az adott Hivatal nem rendelkezik, úgy számára marad a selejtes adathordozók egyéb úton történő megsemmisítése.

Az adathordozók megsemmisítése a következő módszerekkel engedélyezett:

- mágnesszalagok: el kell távolítani a tokból, majd mechanikusan be kell zúzni, kémiai úton megsemmisíteni vagy elégetni. (Az utóbbi esetben a szalagokat be kell tenni az égetőbe rövid darabokban vagy lazán betöltve jól összekeverve sokkal nagyobb mennyiségű papírhulladékkal együttesen. Nem szabad azokat az égetőbe feltekercselve vagy összepréselt blokkokban betenni, mert nem semmisülnek meg teljes mértékben.)
- floppy vagy más (pl. CD) lemezek: a floppy lemezeket el kell távolítani a házukból, a lemezt szabálytalan alakú darabokra kell vágni (legalább 8 darabra), a darabokat deformálni kell vagy elégetni;
- merevlemezek: fel kell nyitni, és el kell égetni; vagy a mágneses felületet el kell távolítani dörzspapírral vagy más durva módszerrel, vagy szét kell szedni és az adathordozót apró darabokra vágni, pl. lemezvágó ollóval;
- más szilárd anyagú tárolók: össze kell törni, vagy el kell égetni.

6.7.3 Adatkezelési eljárások

Az adatok illetéktelen közzétételének és felhasználásának megelőzéséhez adatkezelést (tárolást, feldolgozást) szabályozó eljárásokra van szükség. Ezeknek az eljárásoknak – az adatok minősítésének megfelelően – igazodniuk kell az előírásokhoz, szabályzatokhoz, számítástechnikai rendszerekhez, hálózatokhoz, a használt számítástechnikai eszközökhöz, távközlési, hangátviteli és multimédiás, levelező stb. rendszerekhez. Az adatkezelési eljárások kidolgozásakor a következőket kell figyelembe venni:

- Az összes adathordozó kezelése és címkézése
- Az illetéktelen személyek kiszűrése, hozzáférésük megtagadása
- A bemenő adatok teljességének, az adatfeldolgozás teljességének és a kimenő adatok hitelességének ellenőrzése
- A be és kimenő adatok védelme: a védettség mértéke legyen arányban az adatok érzékenységével.
- Az adatok elosztásának szabályozása, ellenőrzése és korlátozása
- Az adatok minősítését, kezelési utasítását kötelezően alkalmazni kell, és a címkézés változásait

automatikusan naplózni kell.

- Rendszeresen ellenőrizni kell az adatminősítés gyakorlatát.
- A biztonsági naplófájlokat csak az arra feljogosított személy, és csak a rendszer minősítésének megfelelően kezelheti és értékelheti.
- Az észlelt rendellenességeket (hibás kezelés, jogosulatlan hozzáférés kísérlete) haladéktalanul ki kell vizsgálni, és az eredményt jegyzőkönyvben kell rögzíteni – ezért az adott Hivatali egység vezetője a felelős.

6.7.4 A rendszerdokumentáció biztonsága

Az informatikai rendszerek dokumentációja érzékeny adatokat is tartalmazhat – ilyen lehet a felhasználás folyamatainak leírása, az eljárás, az adatszerkezetek, vagy az engedélyezési folyamatok ismertetése.

Az illetéktelen hozzáférés megelőzése érdekében

- gondoskodni kell a rendszerdokumentációk biztonságos tárolásáról;
- minimálisra kell csökkenteni azok számát, akik hozzáférhetnek a rendszerdokumentációkhoz;
- gondoskodni kell a nyilvános hálózaton keresztül elérhető, vagy azon keresztül továbbított dokumentáció védelméről;
- az informatikai rendszer biztonságával kapcsolatos dokumentációt a rendszer biztonsági osztályának megfelelő módon kell kezelni;
- az informatikai rendszer (vagy annak bármely elemének) dokumentációját változáskövető mechanizmussal kell naprakészen tartani;
- gondoskodni kell a változások kezeléséről és a biztonságot érintő változások, változtatások naplózásáról;
- a rendszerben feldolgozandó, legalább 3. biztonsági osztályba sorolt adatok és a hozzájuk kapcsolódó jogosultságok nyilvántartását elkülönítve kell kezelni;
- az informatikai rendszer beszerzéséhez, fejlesztéséhez és rendeltetésszerű üzemeltetéséhez a következő dokumentációk szükségesek: Késztermék Fejlesztett termék Szállítási dokumentáció, minőségi bizonyítvány Architektúra és konfigurációszintű dokumentáció
- Rendszerelemek, egységek dokumentációi Modulszintű dokumentáció Teljes rendszerdokumentáció Teljes rendszerdokumentáció Rendszertesztdokumentáció Tesztkövetelmények és eljárások dokumentációja modulszinten Üzemeltetési dokumentáció (normál üzemeltetés, hibaelhárítás, újraindítás) Tesztkövetelmények és eljárások dokumentációja rendszerszinten Felhasználói dokumentáció Felhasználói dokumentáció Átadásátvételi dokumentáció Biztonsági rendszer dokumentációja Biztonsági rendszer dokumentációja Üzemeltetési dokumentáció (normál üzemeltetés, hibaelhárítás, újraindítás)
- a biztonsági rendszerek, alrendszerek dokumentációjának tartalmaznia kell a biztonsági funkciók leírását, azok telepítését, aktiválását, leállítását és használatát a fejlesztés, valamint az üzemeltetés során. A biztonsági rendszer vagy alrendszer dokumentációját csak az informatikai biztonsági Hivatali egység munkatársai, illetve a biztonsági vezető által felhatalmazott személyek kezelhetik.

6.8 Adatok és programok cseréje

A Hivatalek között cserélt adatok és programok elvesztésének, módosításának vagy illetéktelen felhasználásának lehetőségét is meg kell akadályozni. Az adatok és a programok Hivatalek közötti átadását, cseréjét ellenőrizni kell. A cserének meg kell felelnie a hatályos törvényeknek és egyéb szabályozóknak.

6.8.1 Adatcserére vonatkozó szabályzatok és eljárások

Mérlegelni kell az elektronikus adatcsere, az elektronikus kereskedelem és az email hivatali és biztonsági kockázatát, annak következményeit, és az ellenőrző eszközök alkalmazására vonatkozó követelményeket.

Bizalmas adatok esetében meg kell fontolni a hálózati adatforgalom titkosítását. A titkosítási eszközök használatával kapcsolatban a következőket kell figyelembe venni:

- az alkalmazandó jogszabályokat és más szabályozásokat;
- a kulcskezelés követelményeit és a legyőzendő nehézségeket, hogy miközben növeljük a biztonságot, jelentős új sérülékenységeket ne okozzunk;
- a titkosító mechanizmus alkalmasságát, tekintettel az adott hálózati kapcsolatra és a kívánt védelemi szintre.

A hálózati forgalomban meg kell fontolni az elektronikus aláírás vagy az üzenet sértetlenségét garantáló mechanizmusok használatát, ha érzékeny adatokat továbbítunk. Az üzenethitelesítő kódok védenek a véletlen vagy szándékos megváltoztatás, hozzáadás vagy törlésellen. Az elektronikus aláírást védő mechanizmusok ezen kívül a letagadhatatlanságot is biztosítják.

Az elektronikus aláírás és az üzenethitelesítő biztosítékok alkalmazása közötti döntéskor figyelembe kell venni a következőket:

- az alkalmazandó jogszabályokat és más szabályozásokat;
- az alkalmazható nyilvános kulcsú infrastruktúrákat;
- a kulcskezelés követelményeit és a legyőzendő nehézségeket, hogy miközben növeljük a biztonságot, jelentős új sérülékenységeket ne okozzunk;
- a védelmi mechanizmus alkalmasságát, tekintettel az adott hálózati kapcsolat sajátosságaira és a kívánt védelemi szintre;
- a felhasználóknak és szerepköröknek a kulcsokkal kapcsolatos megbízható (ahol megoldható: hiteles) regisztrációját az elektronikus aláírási rendszerekben.

6.8.1.1 Az adatcsere egyéb formái

Megfelelő eljárásokkal és ellenőrző eszközökkel gondoskodni kell a távközlési és adatátviteli eszközökön közölt információk védelméről. Az információ nem biztonságos felhasználásának lehetséges okai: a szükséges ismeretek hiánya, az ilyen eszközök használatára vonatkozó irányelvek és eljárások elégtelen ismerete.

A távközlési eszközökben bekövetkező üzemzavar, az eszközök túlterheltsége vagy a kapcsolat kimaradása esetén a folyamatos üzletmenet megszakadhat, valamint illetéktelen személyek is hozzáférhetnek a különböző hivatali információkhoz.

A munkavállalók a távközlési és adatátviteli eszközök használata során kötelesek a következő irányelveket és eljárási szabályokat betartani:

- Tekintettel arra, hogy nem hozhatnak nyilvánosságra minősített adatokat, a telefonbeszélgetések során ügyelniük kell
- a közvetlen környezetükben tartózkodó emberekre, különösen mobiltelefon használata során;
- a telefonbeszélgetések – illetve a készülékek – lehallgatására és letapogató eszközök, vevőkészülékek alkalmazására;
- a hívott félnél tartózkodó személyekre;

- arra, hogy ne folytassanak bizalmas telefonbeszélgetéseket nyilvános helyeken vagy nyitott irodákban;
- arra, hogy ne tároljanak feleslegesen üzenetet az üzenetrögzítő készülékeken, illetve nyilvános rendszereken, mert ezeket illetéktelen személyek visszajátszhatják, elolvashatják. Az üzeneteket megismerés után le kell törölni, vagy biztonságos helyen kell tovább tárolni.
- A faxgépek használata során a következő fenyegetésekkel találkozhatunk:
- A dokumentumok és üzenetek címzése hibás lehet.
- A faxgépeket szándékosan vagy gondatlanul úgy programozhatják, hogy az egy meghatározott címre üzeneteket továbbít.
- Illetéktelenek hozzáférhetnek a beépített üzenettárolókhoz, az üzeneteket visszakereshetik és lehallgathatják.
- A személyzetet emlékeztetni kell, hogy korszerű faxgépekben és fénymásoló gépekben belső oldalgyorsító memóriatárak, esetlegesen merevlemezek és laptárolók vannak, a papír vagy a továbbítás hibája esetére. Ez fenyegetést jelenthet, ha a bizalmas anyagok nyomtatása folytatódik, miután a hibát kiküszöbölték. Minősített esetben az ilyen veszélyforrások kiküszöböléséig a felhasználó ne hagyja el a helyszínt, és a problémát mihamarabb jelentse az illetékes munkatársnak.

6.8.2 Megállapodások az adatok és programok cseréjéről

A Hivatal más Hivataltel adat és programcserét kizárólag írásbeli szerződés alapján bonyolíthat, melyben utalni kell az érzékeny információk kezelésére is.

A csere biztonsági feltételeire vonatkozó megállapodásokban meg kell határozni

- az adatátvitel, feladás és átvétel ellenőrzésének és bejelentésének eljárási szabályait;
- a biztonságos adatátvitel előkészítésének és megvalósításának műszaki szabványait;
- az adatvesztéssel kapcsolatos kötelezettséget és felelősséget;
- az adatátvitel során a biztonságos (szükség esetén rejtjelezett) környezet előírásait minden érintett félnél;
- az érzékeny adatok védelméhez használatos speciális eszközöket (pl. kriptográfiai kulcsokat).

6.8.3 Adathordozók szállítása

A számítástechnikai adathordozók biztonságos szállítása érdekében az alábbi elveket érdemes követni.

- Szállítást – telephelyen kívülre – csak a Hivatali egység vezetője rendelhet el.
- Szállítás során átadásátvételi bizonylat szükséges.
- A szállítást – lehetőség szerint – több embernek kell végeznie.
- A szállítást végző embereket mindig azonosítani kell.
- Minősített esetben érdemes lehet a szállítmány több részre bontani, és különböző útvonalakon szállítani.
- Telephelyen kívüli szállításhoz a legrövidebb és leggyorsabb útvonalat kell kiválasztani.
- Tömegközlekedési eszközön – lehetőség szerint – ne szállítsanak adathordozót.
- Telephelyen kívüli szállításhoz – pl. a MABISZ ajánlását figyelembe vevő – megfelelő zárható tárolóeszköz szükséges.
- Elektronikusan rögzített adatokat tartalmazó mágneses adathordozó szállításakor kerülendő a nyilvánvalóan erős mágneses tér (pl. nagyfeszültségű távvezetékek).

- Szállítás során a vagyonbiztonságra fokozottan ügyelni kell.
- Az adathordozókat tilos őrizetlenül hagyni.
- Az adathordozókat óvni kell a fizikai sérülésektől.
- Speciális csomagolással és zárcímkékkel letagadhatatlanná tehetjük a felbontást vagy az arra tett kísérleteket.
- Az adathordozókon a minősítést megváltoztathatatlanul kell feltüntetni.
- Rendkívüli esemény esetén a Hivatali egység (a szállítást elrendelő) vezetőjét – szükség esetén a rendőrséget is – értesíteni kell. A vezetőnek haladéktalanul meg kell tennie a további károk elkerülése érdekében szükséges lépéseket, valamint ezzel egy időben tájékoztatnia kell a biztonsági vezetőt az eseményről és a megtett intézkedésekről.
- Érzékeny információkat tartalmazó adathordozót posta vagy futárszolgálat útján ne szállítsunk.

6.8.4 Az elektronikus levelezés biztonsága

Az elektronikus levelezés az hivatali hírközlésben csaknem egészen kiváltotta a hagyományos postai levelet és telexet: felülmúlja azokat sebességben és közvetlenségben, azonban sérülékenyebb a rosszhiszemű kezeléssel szemben. Mivel az email, az azonnali üzenetküldés és az online konferenciák egyre fontosabb szerepet játszanak az hivatali célú egyeztetésben, ezek kockázatait a papíralapú üzenetváltással arányos szintűre kell csökkenteni.

Az elektronikus levelezés területén az alábbi sérülékenységek és fenyegetések merülnek fel:

- megbízhatatlan szolgáltatás használata;
- a hírközlő közeg kapacitásának változása, a címzési házirend módosítása (formális levelet küldhetnek jogi vagy természetes személy nevében, illetve számára is);
- a küldemény származásának, a feladásának, a kézbesítésének, átvételének letagadhatósága (elektronikus aláírás hiányában);
- távoli felhasználók bejelentkezése a levelezőszerverre;
- adatszolgáltatás vagy azonnali üzenetküldés nyilvános hálózaton;
- nyilvános hálózatokról kezdeményezett hozzáférések.
- jogosulatlan hozzáférés vagy módosítás, a kézbesítő szolgáltatás kiesése;
- téves címzés vagy irányítás;
- bizalmas adatok továbbítása, és annak következményei;
- visszaélés a nyilvános címjegyzékekkel;
- Az alábbi biztonsági intézkedéseket kell megfontolni:
- A levelezőrendszer vírusvédelmét folyamatosan frissíteni kell, valamint követni kell az új mailvírusok megjelenését.
- Az elektronikus levelező eszközök, elsősorban a szerverek fizikai és logikai védelméről folyamatosan gondoskodni kell (pl. nyomon kell követni új komponensek, szervizcsomagok és biztonsági frissítések megjelenését).
- Az elektronikus levelező rendszeren keresztül történő támadások esetén – amennyiben a rendszer védelme átmenetileg nem biztosított (pl. olyan vírus fenyegetettség esetében, amikor a vírusvédelmi rendszerek még nem nyújtanak kellő védelmet) – az intranetet meghaladó elektronikus levélforgalmat ideiglenesen le kell állítani. Ezt az informatikai vezető és az informatikai biztonsági vezető rendelheti el.
- Rögzíteni kell a felhasználók felelősségét.

- Az elektronikus üzenetek bizalmasságát és hitelességét rejtjelező eszközökkel (PKI, kulcsok hosszát, tárolásuk módját) kell védeni.
- Kilépéskor archiválni kell és a kilépés napjától számított 1 évig meg kell őrizni minden olyan felhasználó elektronikus levezését, akiknek munkaviszonya, illetve a jogosultság alapját képező megbízása, szerződése megszűnt. Megőrizendők továbbá azok az elektronikus levelek, amelyek peres eljárások alapját képezhetik.
- A nem hitelesíthető, kétes forrásból származó üzeneteket eredetét és célját fel kell kutatni.
- Az elektronikus levelezés forgalmát tartalmilag szűrni kell, a bizalmas adatok kiszivárgásának elkerülése érdekében.
- Minden felhasználót fel kell világosítani arról, hogy a Hivatal levelezőrendszerén tárolt és továbbított levelek a Hivatal tulajdonát képezik, ezért a szabályzatokban és utasításokban feljogosított ellenőrző szerveinek ezekbe indokolt esetben betekinthetnek.
- A Hivatal levelezőrendszere a egyéb üzletmenetétől idegen reklám, valamint egyéb hivatali célokra nem használható.
- A Hivatal elektronikus levelezési címjegyzéke semmilyen célból nem szolgáltatható ki harmadik félnek.

6.9 Az elektronikus kereskedelem biztonsága

6.10 A biztonsági megfigyelő rendszer használata

Az illetéktelen hozzáférések, a tiltott tevékenységek kiszűrése érdekében

- figyelemmel kell kísérni a hozzáférési irányelvektől való eltéréseket, és rögzíteni kell a megfigyelhető eseményeket, hogy adott esetben bizonyítékul szolgáljanak a biztonsági események kivizsgálásához, és segítséget nyújtsanak a szabályzat aktualizálásához;
- a rendszer nyomon követése tegye lehetővé az ellenőrző eszközök hatékonyságának ellenőrzését és egy, a hozzáférési irányelveknek való megfelelés hitelesítését;
- a biztonsági monitorrendszert csak az arra feljogosítottak használhatják, és tevékenységüket naplózni kell.

6.10.1 Biztonsági események naplózása

A rendkívüli és a biztonságot fenyegető eseményeket eseménynaplóba kell bejegyezni és azt a letagadhatatlanság érdekében meg kell őrizni.

- Az elszámoltathatóság és felülvizsgálhatóság érdekében a naplózási rendszert (biztonsági naplót) úgy kell kialakítani, hogy abból utólag megállapíthatók legyenek az informatikai rendszerben bekövetkezett fontosabb események, különös tekintettel azokra, amelyek a rendszer biztonságát érintik. Ezáltal ellenőrizni lehet a hozzáférések jogosultságát, meg lehet állapítani a felelősséget, valamint az illetéktelen hozzáférést vagy az arra tett kísérletet.
- A naplózási rendszernek alkalmasnak kell lennie mindegyik felhasználó vagy felhasználói csoport által végzett művelet szelektív regisztrálására. A következő eseményeket sikerességét és sikertelenségét feltétlenül naplózni kell:
  - rendszerindítások, leállítások;
  - rendszeróraállítások;
  - be és kijelentkezések;

- programleállások;
- az azonosítási és a hitelesítési mechanizmus használata;
- hozzáférési jog érvényesítése azonosítóval ellátott erőforráshoz;
- azonosítóval ellátott erőforrás létrehozása vagy törlése;
- felhatalmazott személy műveletei, amelyek a rendszer biztonságát érintik.

A biztonsági naplóban az egyes eseményekhez kapcsolódóan a következő adatokat is rögzíteni kell:

- a felhasználó azonosítása és hitelesítése esetén:
  - dátum,
  - időpont,
  - a felhasználó azonosítója,
  - az eszköz (pl. terminál) azonosítója, amelyről az azonosítási és hitelesítési művelet kezdeményezése történt,
  - a hozzáférési művelet eredményessége vagy sikertelensége.
- az olyan erőforráson kezdeményezett hozzáférési művelet esetén, amelynél a hozzáférési jogok ellenőrzése kötelező:
  - dátum,
  - időpont,
  - a felhasználó azonosítója,
  - az erőforrás azonosítója,
  - a hozzáférési kezdeményezés típusa,
  - a hozzáférés eredményessége vagy sikertelensége.
- az olyan erőforrás létrehozása vagy törlése esetén, amelynél az ehhez fűződő jogok ellenőrzése kötelező:
  - dátum,
  - időpont,
  - a felhasználó azonosítója,
  - az erőforrás azonosítója,
  - a kezdeményezés típusa,
  - a művelet eredményessége vagy sikertelensége.
- a felhatalmazott felhasználók (pl. rendszeradminisztrátorok) olyan műveletei esetén, amelyek a rendszer biztonságát érintik:
  - dátum,
  - időpont,
  - a műveletet végző azonosítója,
  - az erőforrás azonosítója, amelyre a művelet vonatkozik,
  - a művelet eredményessége vagy sikertelensége.

Alapvető naplózási követelmények:

- Kerüljön naplózásra a biztonságot érintő összes tevékenység.
- A naplófájlok tartalmát megadott időosztással képernyőn és nyomtatón is meg lehessen jeleníteni.
- A naplóállományokat tilos megsemmisíteni, felülírni, módosítani: azokat archiválni kell.
- A naplóállományok kódoltak, ellenőrző összeggel ellátottak legyenek.
- A fokozott és kiemelt biztonsági osztályba sorolt rendszerek biztonsági naplóit egy másik számítógépen is tárolni kell (annak érdekében, hogy védve legyenek a törlés és illetéktelen

hozzáférés ellen). Ezért az elektronikus információs rendszer biztonságáért felelő személy felel.

- Rögzíteni kell a hibás bejelentkezési kísérletek számát.
- Szükség van egy olyan nyilvántartásra, melyből lekérdezhető, hogy adott képernyőhöz melyik felhasználói csoport és milyen joggal férhet hozzá; illetve egy olyan nyilvántartásra, melyből az kérdezhető le, hogy egy adott felhasználói csoport mely képernyőkhöz és milyen joggal férhet hozzá.
- Rögzíteni kell a jelszócserék dátumát.
- A biztonsági napló adatait rendszeresen, de legalább havonta egy alkalommal ellenőrizni és archiválni kell.
- A biztonsági napló értékelése során meg kell határozni, hogy mely eseményeket kell jegyzőkönyvezni, melyek azok az események, amelyek szankciókat vonnak maguk után, és mik ezek a szankciók.
- A biztonsági naplók alapján felvett jegyzőkönyveket archiválni kell, és ennek során a megőrzési határidőket meg kell határozni.
- A biztonsági eseménynapló (naplófájl) és a jegyzőkönyvek adatait védeni kell az illetéktelen hozzáféréstől.
- A biztonsági eseménynaplófájlok vizsgálatához és karbantartásához a rendszernek megfelelő eszközökkel és ezek dokumentációjával kell rendelkeznie. Ezen eszközök állapotának regisztrálhatónak és dokumentálhatónak kell lennie.
- A rendszerben a biztonsági eseménynaplófájlok auditálásához szükséges eszközöknek lehetővé kell tenniük egy vagy több felhasználó tevékenységének szelektív vizsgálatát.
- Ki kell alakítani a biztonság belső ellenőrzésének rendszerét, amely során meg kell határozni a felügyeleti és megelőzési tevékenységek eljárásrendjét.
- A biztonsági eseményeket meg kell nevezni a biztonsági szabályzatban, és meg kell határozni a biztonsági naplóbejegyzések élettartamát is.
- Az eseményrekord (bejegyzés) a következő mezőket kell, hogy tartalmazza:
- felhasználónevet,
- dátumot,
- időpontot,
- az esemény típusát,
- az esemény sikerességét (sikeres, sikertelen).
- A biztonsági naplóban a következő eseményeket kell rögzíteni:
- rendszerindítást;
- felhasználók be és kijelentkezését;
- jogosultságok megváltozását felhasználóra és felhasználói csoportra vonatkozólag;
- biztonsági menedzsment rendszerre vonatkozó változásokat, beleértve a naplózási funkciókat is;
- naplózási szolgáltatás elindítását és leállítását.
- A biztonsági naplót a létrához zásától kezdve folyamatosan karban kell tartani, valamint védeni kell az illetéktelen módosítástól és törléstől, ezért ember számára olvasható formában is kell tárolni.

6.10.2 A rendszerhasználat megfigyelése

A felhasználók által elvégzett tevékenységeket – az ellenőrizhetőség érdekében – rögzíteni, naplózni kell.

- Az informatikai rendszer üzemeltetéséről (a biztonsági napló mellett) üzemeltetési naplót kell vezetni, amelyet az informatikai Hivatali egység felelős vezetőjének és az Informatikai biztonsági

vezetőnek rendszeresen ellenőriznie kell.

- Az informatikai rendszer üzemeltetéséről (adatkérések, adatszolgáltatások, adatfeldolgozások, stb.) nyilvántartást kell vezetni, amelyet az arra illetékes személynek rendszeresen ellenőriznie kell.
- Az eseménynaplózási adatokat folyamatosan kell archiválni és karbantartani.
- A rendszereseményeket automatikusan kell archiválni, a naplóbejegyzéseket (eseményrekordokat) folyamatosan felül kell vizsgálni, a rendszernek alkalmasnak kell lennie a biztonsági események automatikus detektálására.

6.10.2.1 Kockázati tényezők

A naplózás és ellenőrzés eredményeit rendszeresen felül kell vizsgálni. A felülvizsgálat gyakorisága az adott kockázattól függjön. Az alábbi szempontokat kell figyelembe venni:

- az alkalmazások és szolgáltatások kritikusságát;
- az érintett információ értékét, érzékenységét és kritikusságát;
- a rendszerbe való beszivárgásról és a rendszerrel való visszaélésről szóló korábbi tapasztalatokat;
- a rendszerkapcsolatok kiterjedtségét (különös tekintettel a nyilvános hálózatokra).

6.10.2.2 Az eseménynaplózás és értékelése

A naplóellenőrzés során felismerhetők azok az informatikai rendszereket érintő fenyegetések és sérülékenységek, illetve a támadó módszerei. A 7.7.1. szakasz olyan véletlennek tűnő biztonsági eseményekre hoz példát, amelyek további vizsgálatot igényelnek.

A rendszernaplók gyakran nagy mennyiségű információt tartalmaznak, aminek nagy része a biztonsági megfigyelés szempontjából érdektelen. Az arra alkalmas üzenetfajtákat érdemes automatikusan átmásolni egy második naplóba, de rendszersegédprogramokkal vagy átvilágítási eszközökkel is vizsgálhatjuk a naplófájlok sértetlenségét.

A naplóvizsgálat területén érdemes a megfigyelés és kiértékelés szerepét érdemes különkülön személyre bízni.

6.10.3 Naplózási információk védelme

Különös figyelmet kell fordítani a naplózó eszközök biztonságára, mert ha jogtalanul módosítják, akkor hamis biztonságérzetet kelthetnek. Óvintézkedéseket kell hozni, hogy az alábbi helyzeteket elkerüljük:

- a naplózási rendszer kiesése;
- az üzenetfajták felsorolásának jogtalan bővítése;
- naplóbejegyzések törlése vagy átszerkesztése;
- betelt naplózási tár, aminek következtében az újabb eseményeket nem lehet feljegyezni, vagy azok a régebbieket írják felül.

Hivatali szinten előírható, hogy a biztonsági naplókat archiválják, mint a rendszerhasználat bizonyítékait, így ezek az információk későbbi vizsgálatokhoz is felhasználhatók. (lásd: 11.2.3.).

6.10.4 Adminisztrátori és operátori tevékenységek naplózása

Az elszámoltathatóság és felülvizsgálhatóság érdekében olyan naplózási rendszert kell kialakítani, hogy utólag megállapíthatók legyenek az informatikai rendszerben bekövetkezett fontosabb események, különös tekintettel azokra, amelyek a rendszer biztonságát érintik. Egyúttal lehessen ellenőrizni a hozzáférések

jogosultságát, meg lehessen állapítani a felelősséget, valamint az illetéktelen hozzáférést vagy az arra tett kísérletet.

A rendszernek képesnek kell lennie minden egyes felhasználó vagy felhasználói csoport által végzett művelet szelektív regisztrálására. A minimálisan regisztrálandó események a következők:

- rendszerindítások, leállások, leállítások;
- rendszerhibák és korrekciós intézkedések;
- programindítások és leállások, leállítások;
- azonosítási és hitelesítési mechanizmus használata;
- hozzáférési jog érvényesítése azonosítóval ellátott erőforráshoz;
- adatállományok és kimeneti adatok kezelésének visszaigazolása;
- azonosítóval ellátott erőforrás létrehozása vagy törlése;
- felhatalmazott személy műveletei, amelyek a rendszer biztonságát érintik.

Az informatikai rendszer üzemeltetése során operátori naplót kell vezetni, amelyet az informatikai Hivatali egység felelős vezetőjének és az elektronikus információs rendszer biztonságáért felelős személynek rendszeresen ellenőriznie kell.

Ki kell alakítani a biztonság belső ellenőrzésének rendszerét, amely során meg kell határozni a felügyeleti és megelőzési tevékenységek eljárásrendjét.

Az informatikai rendszer konfigurációs változásairól nyilvántartást kell vezetni, amelyet az informatikai vezető által kijelölt személynek rendszeresen ellenőriznie kell.

6.10.5 Rendszerhibák naplózása

Az üzemzavarok bejelentését követően gondoskodni kell a helyreállításról. A felhasználók által jelentett, az adatfeldolgozás vagy átviteli rendszerek működésében észlelt hibákat naplózni kell.

Az üzemzavarok kezelésének szabályai:

- a hibanapló kiértékelése és a reagálás ellenőrzött módon történjen;
- a helyreállítás, az erre vonatkozó tervezés és jóváhagyás ellenőrzött módon történjen.

6.10.6 Rendszerórák szinkronizálása

Az operációs rendszer és az alkalmazások dokumentációjával összhangban különös figyelmet kell fordítani a rendszerdátum és rendszeridő beállítására, mert minden tevékenység visszakereshetőségének alapja a hiteles, pontos dátum és idő. A rendszerdátum és a rendszeridő beállítására kizárólag az informatikai vezető által kijelölt munkatársak jogosultak. Az időpont beállítását jegyzőkönyvezni kell.

Ahol számítógépi vagy távközlési eszköz képes valós időben órajelet szolgáltatni, ott azt egyezményes időhöz érdemes igazítani, pl. az Egyetemes Koordinált Időhöz (UTC), vagy valamely helyi szabványos időzítéshez. Természetesen helyi jellegzetességeket (pl. nyári időszámítás) is figyelembe kell venni. Mivel az egyes órák járása egymással nem teljesen azonos, egy Hivatali szinten definiált eljárással rendszeresen szinkronizálni kell őket a Hivatalszintű időhöz.

A dátum és időformátum megbízhatósága az alkalmazásokban és az adatbáziskezelő rendszerekben használatos időbélyegző pontosságát is befolyásolja. Az ilyen hibák – főleg nagy adatbázisokban – nehezen korrigálhatók.

A számítógépek óráinak helyes beállítása az auditnaplók pontossága érdekében is fontos. Ezt megkívánhatják különféle informatikai biztonsági események kivizsgálásánál, vagy bizonyítékként, jogi vagy fegyelmi esetekben. A pontatlan auditnaplók akadályozhatják a fenti nyomozati cselekményeket és árthatnak az ilyen bizonyítékok hitelességének.

Ahol rendelkezésre áll egy nemzeti atomóra alapján, rádión közvetített időhöz kapcsolt mesteróra, akkor ez az eszköz a naplózási rendszerek vezérlőórájaként is használható. Hálózati időprotokoll használatával pedig az összes szerver szinkronba hozható a vezérlőórával.

7 HOZZÁFÉRÉSELLENŐRZÉS

7.1 A hozzáférésellenőrzéshez fűződő működési követelmény

7.1.1 Hozzáférésellenőrzési szabályozás

Cél:

A dokumentumokhoz, információkhoz, adatokhoz történő hozzáférés ellenőrzése.

Szabályok:

Az információhozzáférés szabályozása

Jogosultság és hozzáférés kezelési szabályzat kialakítása, bevezetése, betartatása; a szabályzat periodikus felülvizsgálata és módosítása elengedhetetlen.

Dokumentált hozzáférésellenőrzési szabályzatot kell kialakítani és azt a hozzáférésre vonatkozó, működési és biztonsági követelmények alapján időszakosan felül kell vizsgálni. A szabályozás révén csökkenhet az információk kiszivárgásának és az illetéktelen hozzáférések kockázata.

Alapelv, hogy minden felhasználó csak azokhoz az erőforrásokhoz/információkhoz férhessen hozzá, amelyek a munkájához mindenképp szükségesek.

További szabályozás

Az információhozzáférés szabályozása a Hivatal Üzemeltetési Utasításban található.

Felelősség

A szabályzat elkészítése és időszakos felülvizsgálata az Informatikai biztonsági felelős hatáskörébe tartozik.

7.1.2 Felhasználói hozzáférés irányítása

Cél: Az erőforrásokhoz és információkhoz való hozzáférési jogok megadásának és megvonásának szabályozása.

Szabályok

A hozzáférési jogok kezelésének eljárásrendje

Valamennyi információs rendszerhez és szolgáltatáshoz való hozzáférés megadására és visszavonására hivatalos felhasználó regisztrálási és regisztráció megszüntetési eljárást kell alkalmazni. A felhasználók hozzáférési jogait rendszeresen át kell tekinteni, hogy minden felhasználó csakis azokhoz az információkhoz

férhessen hozzá, amelyek munkájához aktuálisan szükségesek.

További szabályozás

A hozzáférési jogok kezelésének eljárásrendje a Hivatal Üzemeltetési Utasításban található.

Felelősség

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Információbiztonsági felelős és az Informatikai rendszerüzemeltetők feladata.

7.1.3 Speciális jogosultságok kezelése

Cél:

A speciális jogosultságok megszerzésének és alkalmazásának korlátozása.

Szabályok:

A speciális jogosultságok kezelésének eljárásrendje

Az általános összeférhetetlenségi szabályoktól való speciális eltérés kockázati tényező, ezért az ilyen jogosultságok kiadását mindenképp kerülni kell. Amennyiben valamilyen elkerülhetetlen ok miatt mégis létre kell hozni ilyent, akkor azt csak dokumentáltan, s csak a feltétlenül szükséges időtartamra szabad adni.

Az eljárásrend alkalmazásának hatására csökken annak a kockázata, hogy a speciális jogosultságok nem megfelelő menedzselése miatt a rendszer működésében hibák keletkeznek; vagy illetéktelen helyre kerülnek védendő adatok.

További szabályozás

A speciális jogosultságok kezelésének eljárásrendje a Hivatal Üzemeltetési Utasítástalálható.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Információbiztonsági felelős feladata.

7.1.4 Felhasználói jelszavak kezelése, gondozása

Cél:

A jelszavak kezelésének biztonságos megvalósítása.

Szabályok:

A felhasználói jelszókezelés szabályozása

A jelszavak felhasználói kezelését szabályozni kell, figyelve arra, hogy a felhasználók titokban tartsák, és megfelelő időközönként változtassák jelszavaikat. Emellett biztosítani kell, hogy a jelszavak kiosztásakor, illetve használatakor csakis a tulajdonos szerezzen tudomást a jelszóról.

További szabályozás:

A felhasználói jelszókezelés szabályozása a Hivatal hatályos Üzemeltetési Utasításés a Felhasználói szabályzatában található.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Információbiztonsági felelős feladata.

7.2 Felhasználói felelősségek

7.2.1 Jelszóhasználat

Cél:

Megfelelő erősségű jelszavak használata.

Szabályok:

A jelszóhasználat szabályozása

A felhasználók számára olyan használati rendet kell kialakítani, amely biztosítja megfelelő erősségű jelszavak használatát és ezen jelszavak megfelelő gyakoriságú cseréjét.

További szabályozás:

A felhasználói jelszókezelés szabályozása a Hivatal Üzemeltetési Utasítások a Felhasználói szabályzatában található.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Információbiztonsági felelős feladata.

7.3 Őrizetlenül hagyott felhasználói berendezések kezelése

Cél:

Az őrizetlenül hagyott berendezéseken való jogosulatlan hozzáférések megelőzése.

Szabályok:

Felhasználói informatikai biztonsági követelmények

A külső felhasználókat a kapcsolati alrendszerek megfelelő kialakításával, a belső felhasználókat (alkalmazottakat) szabályzatokkal kell kötelezni arra, ha őrizetlenül hagyják a berendezéseiket, akkor (akár logikailag, akár fizikailag) zárják le azokat.

A belső felhasználókat (alkalmazottakat) kötelezni kell arra, hogy csak az aktuális munkához szükséges dokumentumokat tartsák az asztalon/képernyőn, és ne hagyják ezeket a dokumentumokat, adatokat felügyelet nélküli hozzáférhető helyen.

További szabályozás

A felhasználói viselkedés szabályozása a Hivatal Felhasználói szabályzatában található.

Felelősség

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Információbiztonsági felelős feladata.

7.4 Hálózati szintű hozzáférésellenőrzés

7.4.1 Hálózati szolgáltatások használatára vonatkozó szabályzat

Cél:

A hálózatra telepített szolgáltatások védelme.

Szabályok:

A hálózati szolgáltatások használatára vonatkozó szabályozás

A hálózati szolgáltatások használatát szabályzatban kell rögzíteni, és azt be kell tartatni. A szabályzatnak tartalmazni kell, hogy milyen felhasználói kör milyen hálózati területhez férhet hozzá.

További szabályozás:

A hálózati szolgáltatások használatára vonatkozó szabályozás a Hivatal Üzemeltetési Utasításta lálható.

Felelősség:

A szabályzat elkészítése és időszakos felülvizsgálata az Információbiztonsági felelős hatáskörébe tartozik.

7.4.2 Felhasználó hitelesítése külső hozzáférés esetén

Cél:

A távoli felhasználók megbízható hitelesítése.

Szabályok:

Külső hozzáférés kezelése:

A külső összeköttetéseket csak a feltétlenül elérni szükséges rendszerekhez szabad engedélyezni, és kriptográfiai védelmi módszereket kell alkalmazni.

További szabályozás:

A távoli felhasználókra vonatkozó szabályozás a Hivatal hatályos Üzemeltetési Utasításta lálható.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Információbiztonsági felelős feladata.

7.4.3 Távdiagnosztikai és konfigurációs portok védelme

Cél:

A távdiagnosztikai és a konfigurációs portok védelmének biztosítása.

Szabályok:

A távdiagnosztikai és a konfigurációs portok védelme

A távdiagnosztikai és a konfigurációs portokhoz való fizikai és logikai hozzáférést ellenőrizni, szabályozni kell. A hozzáféréshez a rendszerben alkalmazott legszigorúbb azonosítási eljárásokat és naplózási rendet kell használni.

További szabályozás:

A távdiagnosztikai és a konfigurációs portok védelmére vonatkozó szabályozás a Hivatal Üzemeltetési Utasításátalálható.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Információbiztonsági felelős feladata.

7.5 Operációs rendszer szintű hozzáférésellenőrzés

7.5.1 Biztonságos bejelentkezési eljárások

Cél:

Szabályzat az operációs rendszerek hozzáférési eljárásainak beállítására és használatára.

Szabályok:

Hozzáférés az operációs rendszer funkciókhoz

Az operációs rendszerekbe való bejelentkezési eljárásokat – a jogosulatlan hozzáférés, a szándékos károkozás elkerülése érdekében – szabályozni kell. Fontos a különböző szerepköröknek megfelelő hozzáférési jogosultság meghatározása és az ehhez tartozó jogok beállításának szabályozása (igénylés, engedélyezés, beállítás, visszavonás).

További szabályozás:

Az operációs rendszer funkciókhoz való hozzáférés szabályozása a Hivatal Üzemeltetési Utasításátalálható.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Információbiztonsági felelős feladata.

7.5.2 Felhasználó azonosítása és hitelesítése

Cél:

Az operációs rendszer szintű felhasználók azonosítása és hitelesítése.

Szabályok:

A felhasználók azonosításának és hitelesítésének szabályozása

A felhasználók egyedi azonosítására, hitelesítésére megbízható módszert kell választani, annak használatát szabályzatban kell rögzíteni, használatát szigorúan meg kell követelni. A szabályzatnak ki kell terjednie az azonosítás és hitelesítés teljes életciklusára (igénylés, engedélyezés, beállítás, visszavonás).

Meg kell határozni a biztonságos jelszóra vonatkozó követelményeket, szabályozni kell a jelszavak létrehozására, módosítására, tárolására, használatára, visszavonására vonatkozó eljárásokat. A felhasználók a jelszóhasználattal kapcsolatos feladatait és kötelezettségeit szintén szabályzatba kell foglalni, és rendszeresen ellenőrizni kell annak betartását.

További szabályozás:

A felhasználók azonosításának és hitelesítésének szabályozása a Hivatal Üzemeltetési Utasításталálható.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Információbiztonsági felelős feladata.

7.5.3 Rendszersegédprogramok használata

Cél:

Átlátható, ellenőrzött, dokumentált, a biztonságot nem veszélyeztető rendszersegédprogram használat megvalósítása.

Szabályok:

A rendszersegédprogramok ellenőrzött, biztonságos használata

A rendszersegédprogramok használata lehetőségeket teremt nehezen ellenőrizhető manipulációkra, ezért ezek használatát különös figyelemmel kell szabályozni és a szabályzatban foglaltakat ellenőrizni. A fejlesztő eszközökhöz, az adatbázis közvetlen hozzáféréseket lehetővé tevő segédprogramokhoz való hozzáférés csak indokolt esetben engedélyezhető és a tevékenység végén az engedélyt vissza kell vonni, és lehetőleg ki kell zárni az ellenőrizhetetlen származású programok használatát.

További szabályozás:

A rendszersegédprogramok használatának szabályozása a Hivatal Üzemeltetési Utasításталálható.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Információbiztonsági felelős feladata.

7.6 Alkalmazás és adatszintű hozzáférésellenőrzés

7.6.1 Adathozzáférés korlátozása

Cél:

A konkrét alkalmazás egyes funkciói elérésének, használatának korlátozása.

Szabályok:

Alkalmazás szintű adathozzáférés korlátozása

Alkalmazás funkciónként, illetve egyes adatkörökre (adatminősítés, biztonsági szint, stb. szerint) vonatkozóan szükséges a hozzáférés szabályozása, a jogosulatlanok kizárása. Fontos az egyes manipulációk, jogosulatlan kísérletek naplózása, a naplóállomány rendszeres értékelése (ld. **Hiba! A hivatkozási forrás nem található.**. sz. fejezet). A funkció, illetve adatkörre vonatkozó korlátozások lehetőségét az alkalmazás fejlesztésének időszakában kell megtervezni és az alkalmazást ennek megfelelően implementálni, mivel ez utólag már nehezen megvalósítható.

További szabályozás:

Alkalmazás szintű adathozzáférés korlátozásával kapcsolatban további szabályozás található a Hivatal

Üzemeltetési szabályzatában.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Információbiztonsági felelős feladata.

7.7 Mobil számítógép használata és távmunka

7.7.1 Mobil számítógép használata és a vele történő kommunikáció

Cél:

Mobil számítógép kátyaolvasók biztonságos használatának szabályozása.

Szabályok:

Távoli és helyi mobil számítógép kártyaolvasók használat szabályai

A mobil számítógépek (notebook, okostelefon, tablet, stb.) biztonságos használatának érdekében szabályozni kell ezen eszközök esetében a hozzáférést, a logikai és fizikai biztonságot, az adatmentések megvalósítását, illetve a biztonságos környezeten kívüli munkavégzés szabályrendszerét.

További szabályozás:

A biztonságos távoli és helyi mobil számítógép használat szabályozása a Hivatal Felhasználói szabályzatában találhatók.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Információbiztonsági felelős feladata.

7.7.2 Távoli elérés

Cél:

A biztonságos távoli elérés megvalósítása.

Szabályok:

Távoli elérés szabályai:

Szabályozni kell, hogy a biztonságos távoli hozzáférés, érdekében milyen tevékenységek és technikai feltételek szükségesek. Távoli hozzáférés csak indokolt esetben engedélyezhető, és a hozzáférés, adatcsere biztonsága érdekében külön eljárásokat kell meghatározni és megvalósítani.

További szabályozás:

A távoli elérés szabályozása a Hivatal Felhasználói Informatikai Biztonsági Szabályzatában található.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Információbiztonsági felelős feladata.

8 FEJLESZTÉS ÉS KARBANTARTÁS

8.1 Információs rendszerek biztonsági követelményei

8.1.1 Biztonsági követelmények elemzése és meghatározása

Cél:

Annak biztosítása, hogy a biztonság az informatikai rendszerek szerves részét képezze.

Szabályok:

Biztonsági követelmények meghatározása

A fejlesztés vagy beszerzés kezdete előtt, az információs rendszerekre vonatkozó biztonsági kockázatokat elemezni kell, ez alapján meg kell határozni a vonatkozó biztonsági intézkedéseket. A biztonsági elvárásokat rögzíteni kell az ajánlatkérési dokumentációban, teljesítésük módját, megfelelőségét pedig értékelési szempontként kell meghatározni.

Felelősség:

A biztonsági követelmények elemzése és meghatározása a fejlesztés vagy beszerzés előtt az Informatikai biztonsági vezető felelőssége.

8.2 Helyes adatfeldolgozás az alkalmazásokban

8.2.1 Bemenő adatok érvényesítése

Cél:

Az informatikai rendszerek helyes működéséhez szükséges bemenő adatok megfelelőségének biztosítása.

Szabályok:

Adatbeviteli ellenőrzési eljárások

Az alkalmazások jogosultsági rendszerét úgy kell beállítani, hogy az adatfelviteli képernyőkhöz csak az illetékes, megfelelő szakértelemmel bíró és a felhasználói oktatásban részesült munkatársak férhessenek hozzá.

Az alkalmazások tervezése során annak belső logikáját úgy kell kialakítani, hogy az képes legyen a különböző összefüggések vizsgálatára, tartalmi, és formai ellenőrzésére (pl. ellenőrző számok, adatok határértékei, kötelező adatok), a bemenő adatok érvényesítésére. A konkrét pénzmozgással járó banki terminál használatakor az utalások két személy engedélyével történhetnek (aláíró jelszó).

Felelősség:

Az adatbeviteli ellenőrzési eljárások kialakításáért az egyes rendszerfejlesztések során az Informatikai rendszerüzemeltetők ,és az Információbiztonsági vezető és az érintett szervezeti egység vezetője felelősek.

8.2.2 Belső feldolgozás ellenőrzése

Cél:

A belső feldolgozás során mind a szándékos, mind a véletlen károkozás kockázatának minimálisra csökkentése.

Szabályok:

Érvényességi ellenőrzések

Az alkalmazásokba érvényességi ellenőrzéseket kell beépíteni, hogy észlelni lehessen az információk feldolgozási hibákból vagy akár a szándékos cselekedetekből adódó bármilyen sérülést.

Amennyiben ez nem lehetséges, úgy a fokozott és kiemelt biztonsági osztályba sorolt informatikai célrendszerek esetében időszakosan (pl. év végén), vagy bizonyos munkafázisok végrehajtását követően (pl. rendszerek közötti adatátadások alkalmával) egyezető listákat kell készíteni, melyek alapján a rendszeren belül az adatok konzisztenciája leellenőrizhető.

Felelősség:

Az alkalmazás szintű érvényességi ellenőrzések megkövetelése a fejlesztés során az Informatikai rendszerüzemeltetők és az Információbiztonsági vezető és az érintett szervezeti egység vezetője, míg a manuális ellenőrzés végrehajtása az érintett irodák feladata.

8.2.3 Üzenetek hitelessége és sértetlensége

Cél:

Az alkalmazások közötti kommunikáció során a hitelesség és a sértetlenség biztosítása.

Szabályok_

Érvényességi ellenőrzések:

Még az egyes alkalmazások beszerzését megelőzően a Hivatalnak meg kell határoznia, hogy az alkalmazások közötti kommunikáció során milyen eszközökkel (például aszimmetrikus kulcsú digitális aláírás, szimmetrikus vagy aszimmetrikus titkosítás, időbélyegek alkalmazásával) lehet biztosítani a sértetlenséget és a hitelességet; illetve hogy ezen óvintézkedés mely üzenettípusok esetén szükséges.

Ezen biztonsági elvárásokat rögzíteni kell az ajánlatkérési dokumentációban, teljesítésük módját, megfelelőségét pedig értékelési szempontként kell meghatározni.

Felelősség:

A biztonsági követelmények elemzése és meghatározása a fejlesztés vagy beszerzés előtt az Informatikai rendszerüzemeltetők és az Információbiztonsági vezető feladata.

8.2.4 Kimenő adatok ellenőrzése

Cél:

A kimenő adatok érvényessége, a tárolt információk későbbi feldolgozása helyes és a körülményeknek megfelelő legyen.

Szabályok:

Kimenő adatokat érvényesítése

Biztosítani kell, hogy mind az automatikus, mind a manuális illesztő felületeken (interfészeken) a megfelelő időben, a megfelelő (szabályozott) struktúrában és adattartalommal jelenjen meg a kimenő információ. Ezt a követelményt a rendszerek megtervezésekor (követelményspecifikáció) figyelembe kell venni, illetve a felhasználói teszteléskor le kell ellenőrizni.

Ezt követően az üzemi alkalmazásból kimenő adatok (pl. határozat, banki adatok) helyességéért az ügyintéző, illetve az irodavezető felel; ezek ellenőrzése az adatok átadásakor kell, hogy megtörténjen.

Utólagos rendszeres és eseti ellenőrzéseket belső (Belső ellenőr, intézményi ellenőr) és külső (Közigazgatási Hivatal, NAV, Állami Számvevőszék, stb.) szervezetek is végeznek, melyek a KET megfelelőségen túlmenően az adatok ellenőrzésére is kiterjednek.

Felelősség:

A kimenő adatokra vonatkozó ellenőrzési eljárások kialakításáért az egyes rendszerfejlesztések során az Informatikai rendszerüzemeltetők és az Információbiztonsági vezető valamint az érintett szervezeti egység vezetője felelősek.

8.3 Rendszerfájlok biztonsága

8.3.1 Üzemelő szoftverek ellenőrzése

Cél:

Megbízható szoftverek használata.

Szabályok:

Megbízható szoftverek használata

A Hivatal számítógépein, valamint alkalmazások futtatására alkalmas egyéb eszközein (pl. okostelefon, tablet) kizárólag az Informatikai rendszerüzemeltetők alkalmazások használhatók. Emellett a megbízható szoftverek használata, az információ kiszivárgási veszélyének csökkentése érdekében:

- szabályozni kell a szoftverek telepítésének és üzemeltetésének elvárt folyamatát,
- létre kell hozni a központi, illetve intézményi szoftverkatalógust, és csak az abban szereplő (előzetesen bevizsgált) szoftvereket szabad a számítógépekre telepíteni
- biztosítani kell, hogy a fejlesztők és karbantartók csak azokhoz a rendszerekhez férjenek hozzá, amelyekre munkájukhoz feltétlenül szükségük van.

További szabályozás:

Megbízható szoftverek használatával kapcsolatban további szabályozás található a Hivatal Üzemeltetési Utasításában és Felhasználói szabályzatában.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikai rendszerüzemeltetők és az Információbiztonsági felelős feladata.

8.3.2 Programok forráskódjához való hozzáférés ellenőrzése

Cél:

A programok forráskódjához való hozzáférés szabályozása.

Szabályok:

A programok forráskódjához való hozzáférés korlátozása

A programok forráskódjához való hozzáférést korlátozni kell.

A belső fejlesztések esetében a forráskód a fejlesztés ideje alatt a Fejlesztő gépén található, majd annak lezárulta után a szerveren egy külön könyvtárban, annak dokumentációjával együtt archiválásra kerül. A könyvtárhoz olvasási/írási joggal a rendszer fejlesztője, valamint az Informatikai rendszerüzemeltetők és az Információbiztonsági vezető férhet hozzá. A forráskódhoz való hozzáférést naplózni szükséges.

Külső fejlesztések esetében a forráskód a fejlesztő cég tulajdona marad, így azt az Hivatal nem kapja meg, ahhoz hozzáférése nincs. Ettől eltérő esetben a forráskóddal kapcsolatos eljárás megegyezik a belső fejlesztéseknél rögzített eljárással, azzal, hogy olvasási joggal csak az Informatikai rendszerüzemeltetők és az Információbiztonsági vezető rendelkezhet.

További szabályozás:

A forráskóddal kapcsolatban további szabályozás található a Hivatal hatályos Üzemeltetési utasításásban.

Felelősség:

A forráskódok elhelyezésének felelőse az Informatikai rendszerüzemeltetők és az Információbiztonsági vezető.

8.4 Biztonság a fejlesztési és támogató folyamatokban

8.4.1 Változáskezelés szabályozási eljárásai

Cél:

A változtatások megvalósításának ellenőrzés alatt tartása.

Szabályok:

A változáskezelés szabályozása

A változtatások végrehajtására változáskezelési eljárásokat kell bevezetni, kidolgozni és betartatni. Biztosítani kell, hogy a fejlesztők és karbantartók csak azokhoz a rendszerekhez férjenek hozzá, amelyekre munkájukhoz feltétlenül szükségük van.

Az új rendszerek bevezetését projektszerű keretek között kell lebonyolítani, ahol a bevezetéssel kapcsolatos feladatok (specifikálás, dokumentálás, tesztelés, stb.) a projekt indításakor rögzítésre kerülnek.

A meglévő rendszerek változáskezelésével kapcsolatban a karbantartási szerződésekben kell rögzíteni a vonatkozó előírásokat.

További szabályozás:

A változáskezelés szabályozása a Hivatal hatályos Üzemeltetési Utasításban található.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikai rendszerüzemeltetők és az Információbiztonsági felelős feladata.

8.4.2 Alkalmazások műszaki átvizsgálása az üzemelő rendszerek megváltoztatását követően

Cél:

A változtatás ne okozzon működési zavart a szervezetben és biztonságában.

Szabályok:

Eljárás használatban lévő rendszerek változásakor

A használatban levő rendszerek megváltozásakor meg kell vizsgálni, hogy (főleg a működés szempontjából kritikus) alkalmazások működésére az adott változtatás nincse káros hatással. Ennek érdekében meg kell követelni a sikeres vállalkozói tesztelés igazolását, illetve – lehetőség szerint – a Hivatalnak is el kell végeznie a felhasználói tesztelést.

További szabályozás:

A rendszerek változáskezelésének szabályozása, beleértve a rendszerek tesztelését is, a Hivatal hatályos Üzemeltetési Utasításában található.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikai rendszerüzemeltetők és az Információbiztonsági vezető, illetve az érintett rendszert használó szervezeti egységek hatáskörébe tartozik.

8.4.3 Szoftvercsomagok változásának korlátozása

Cél:

A szoftvercsomagok módosításának visszaszorítása a feltétlen szükséges esetekre.

Szabályok:

Szoftvercsomagok változáskezelése

A szoftvercsomagok (ideértve pl. az operációs rendszereket, adatbázis kezelőket, irodai szoftvereket, hivatali, hivatali alkalmazásokat) módosítását vissza kell szorítani, valamennyi változtatás szükségességét, indokoltságát ellenőrizni kell. A szoftvercsomagok esetén csak a szükséges változásokat (pl. hibajavítás, jogszabályi előírások) kell telepíteni, és azok hatását legalább a kritikus rendszerek esetében ellenőrizni kell.

Változtatás esetén az eredeti verziót meg kell őrizni, s a fejlesztést, változtatást egy másolaton kell végezni. Az új verziót alapos tesztelésnek kell alávetni, éles bevezetése csak ez után lehetséges.

További szabályozás:

A rendszerek változáskezelésének szabályozása a Hivatal hatályos Üzemeltetési Utasításban található.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikai rendszerüzemeltetők és az Információbiztonsági felelős feladata.

8.4.4 Veszélyes (forrás)kódok kiszűrése

Cél:

Meg kell előzni az információk kiszivárgását.

Szabályok:

Veszélyes (forrás)kódok kiszűrése

A Hivatal számítógépein, valamint alkalmazások futtatására alkalmas egyéb eszközein (pl. okostelefon, tablet) kizárólag az Információbiztonsági felelős által telepített alkalmazások, forráskódok használhatók.

Az információk kiszivárgásának elkerülése érdekében az Informatikus/IBFnek minden rendelkezésre álló forráskódot le kell vizsgálni/vizsgáltatni használat előtt. Csak tiszta forrásból szabad programokat beszerezni. Csak ezen vizsgálatok után lehet bármely programot a végleges rendszerbe engedni.

További szabályozás:

Veszélyes (forrás)kódok kiszűrésével kapcsolatban további szabályozás található a Hivatal Üzemeltetési Utasítások Felhasználói szabályzatában.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikai rendszerüzemeltetők és az Információbiztonsági felelős feladata.

8.5 Műszaki sebezhetőség kezelése

8.5.1 A műszaki sebezhetőségek ellenőrzése

Cél:

A műszaki sebezhetőség minimális szinten tartása.

Szabályok:

Külső szoftverfejlesztés ellenőrzése:

Fel kell mérni az informatikai célrendszerek sebezhető pontjait, és az ezekből fakadó kockázatot meg kell szüntetni (illetve minimalizálni a kockázattal arányosan) megfelelő védelmi intézkedések meghozásával.

További szabályozás:

- A Hivatal informatikai célrendszereinek kockázatfelmérésének, biztonsági osztályba sorolásának módszertana, illetve egyes informatikai célrendszerek besorolása, a védelmi intézkedése meghatározása a mindenkori Kockázatkezelési és Elemzési eljárás és mellékleteiben található.

Felelősség:

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikai rendszerüzemeltetők és az Információbiztonsági felelős feladata.

9 INFORMATIKAI BIZTONSÁGI ESEMÉNYEK KEZELÉSE

9.1 Informatikai biztonsági események és sérülékenységek jelentése

Cél:

A biztonsági sérülékenységek és események ismertek legyenek, azokra megfelelő választ adjon a Hivatal .

Szabályok:

Biztonsági események osztályozása

Biztonsági eseménynek minősül az informatikai rendszer védelmi állapotában beállt illetéktelen változás, melynek hatására az informatikai rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.

Biztonsági események például a vírus, hacker, spamtámadás, betörés, lopás, áramszünet, vagy a hozzáférés megsértése.

Biztonsági események osztályozása

Az informatikai erőforrások rendelkezésre állásának megszakadása alapján a biztonsági események a következő kategóriákba sorolhatók:

I. **Kategória:** az informatikai erőforrások az érintett központban nem állnak rendelkezésre, az ottani informatikai rendszer működése megszakad.

Ezt okozhatják például a tűz és a víz okozta katasztrófák. Jellegüknél fogva ezek nagy pusztításokat jelentenek a számítástechnikai eszközökben és/vagy a kiszolgáló infrastruktúrában. A helyreállítás időigényes és költséges.

II. **Kategória:** az érintett központban egyes erőforrások nem állnak rendelkezésre, és az ottani informatikai rendszer működése megszakad.

Ide tartozik pl. az energiaellátás kiesése. Jellegénél fogva a sérülés lokalizált, a helyreállítás kevésbé költséges és időigényes, mint az I. Kategóriába sorolt biztonsági események esetében.

A II. Kategóriát az igényeknek és a helyi adottságoknak megfelelően két alkategóriára bontjuk:

II/a **Kategória:** emberi vagy eszköz erőforrások megsemmisülése, illetve ezek olyan, hosszabb idejű üzem, munkaképtelensége (kiesése), amely jelentős problémát okoz az informatikai rendszer működésében azáltal, hogy küldetéskritikus vagy lényeges rendszert érint.

II/b **Kategória:** emberi vagy eszköz erőforrások nem semmisülnek meg és hosszabbrövidebb idejű üzem, munkaképtelensége (kiesése) nem okoz jelentős problémát az informatikai rendszer működésében azáltal, hogy nem küldetéskritikus vagy lényeges rendszert érint.

III. **Kategória:** az érintett központban csak erőforráselem(ek) sérül(nek) meg, de az informatikai rendszer működése folyamatos.

A III. Kategória veszélyforrásai az Informatikai Üzemeltetési Utasítás tárgykörébe esnek. A veszélyforrások képezte fenyegetés bekövetkezése az Informatikai Üzemeltetési Utasításban és mellékletében tárgyalt védelmi intézkedések alkalmazásával előzhetők meg, illetve bekövetkezés esetén

ugyancsak ezen védelmi intézkedések alkalmasak a károk mértékének csökkentésére.

Informatikai katasztrófának minősülnek az I. és II/a Kategóriába sorolható események.

Informatikai veszélyhelyzetnek minősülnek a II/b Kategóriába sorolható események.

Nem minősülnek katasztrófának a III. Kategóriába sorolt események.

Biztonsági események jelentése

A biztonsági eseményeket az észlelő (pl. felhasználó, rendszerüzemeltető) köteles bejelenteni az Informatikai rendszerüzemeltetőknek.

Az Informatikai rendszerüzemeltetők haladéktalanul elvégzi a biztonsági esemény kategorizálását, majd I. vagy IIes kategóriájú esetben intézkedéseket foganatosít a Katasztrófaelhárítási tervben meghatározottak szerint.

Felelősség

A vonatkozó szabályozás elkészítése, felülvizsgálata, használatának ellenőrzése az Informatikai rendszerüzemeltetők feladata.

9.2 Informatikai biztonsági események kezelése

Cél:

Az informatikai biztonsági események gyors, hatékony kezelése.

Szabályok:

Biztonsági események kezelése

A bejelentett biztonsági eseményekkel kapcsolatban az Informatikai rendszerüzemeltetők a szükséges lépéseket gyorsan és hatékonyan köteles megtenni.

Az I. és II/a. kategóriába sorolt biztonsági események esetén a Katasztrófaelhárítási tervben található releváns akcióterv szerint kell eljárni.

A II/b. és a III. kategóriába sorolt biztonsági események esetén azok kezelésére az Informatikai Üzemeltetési Utasítás ban leírtak az irányadók.

Biztonsági események nyilvántartása és értékelése

A feltárt és dokumentált eseményeket gyűjteni és rendszeresen értékelni kell. Ennek során az események okozta hibákat analizálva meg kell határozni a hibák okát, az események kezeléséhez bizonyítékokat kell gyűjteni, valamint a megtett intézkedéseket is dokumentálni kell annak érdekében, hogy később előforduló hasonló eseményeket már a kialakított módon lehessen kezelni vagy megelőzni.

További szabályozás

A biztonsági események kezelésével kapcsolatos eljárásrendet a Működés folytonosság és Katasztrófaelhárítási terv, valamint az Informatikai Üzemeltetési Utasításnak kell tartalmaznia.

Felelősség

A biztonsági események nyilvántartása, az elhárításban való részvétel, az események értékelése és javaslatok kidolgozása az Informatikai rendszerüzemeltetők feladata.

9.3 Informatikai biztonsági problémakezelési eljárás kialakítása

Cél:

Az informatikai biztonsági problémák megelőzése, illetve hatékony védekezés kialakítása.

Szabályok:

Problémakezelési eljárás kialakítása

Az informatikai biztonsági problémák megállapítására és kezelésére vonatkozó eljárást, valamint a biztonsági eseményekkel kapcsolatban nyilvántartást az előző alfejezetek tartalmazzák.

A biztonsági események értékelését és a problémák megelőzését, detektálását, javítását szolgáló javaslatok megtételét az Informatikai rendszerüzemeltetők köteles megtenni.

A működésfolytonossági akciótervet érintő biztonsági esemény esetén az értékelést a Üzletmenetfolytonossági és Katasztrófaelhárítási terv alapján kell végrehajtani.

Ezen túlmenően az értékelés során Informatikai rendszerüzemeltetőknek el kell végeznie az érintett szabályzatok (pl. Üzletmenetfolytonossági és Katasztrófaelhárítási terv, Informatikai Üzemeltetési Utasítás) felülvizsgálatát és szükség szerinti aktualizálását.

A problémák ellen védelmi intézkedéseket kell hozni, az általuk képviselt kockázatok arányában; ezt az alapelvet a problémák megelőzését, detektálását, javítását szolgáló javaslatok megtételekor szem előtt kell tartani.

További szabályozás

A biztonsági események kezelésével kapcsolatos eljárásrendet a Üzletmenetfolytonossági és Katasztrófaelhárítási terv, valamint az Informatikai Üzemeltetési Utasítás tartalmazzák.

Felelősség

A biztonsági események nyilvántartása, az elhárításban való részvétel, az események értékelése és javaslatok kidolgozása az Informatikai rendszerüzemeltetők feladata.

10 ÜZLETMENETFOLYTONOSSÁG

10.1 Az üzletmenetfolytonosság informatikai biztonsági szempontjai

Alapvető biztonsági cél, hogy a Hivatal tartsa fenn üzletmenetét, védje a kritikus tevékenységeit az informatikai rendszerek hibáinak hatásától, és biztosítsa a gyors újraindítás lehetőségét.

Működésfolytonossági irányítást kell bevezetni, hogy csökkenjen a kiesések káros hatása, és a Hivatal túlélje az információs vagyontárgyak elvesztését, történjen az természeti katasztrófa, baleset, berendezések hibái vagy rosszindulatú beavatkozás miatt.

Azonosítani kell a kritikus működési folyamatokat, és a működésfolytonosságot be kell építeni az informatikai biztonságirányítási követelményekbe, figyelembe véve a személyzettel, nyersanyaggal, munkaeszközökkel és szolgáltatással való folyamatos ellátás igényét. Az üzemzavarokat, eszközhibákat, szolgáltatáskieséseket hatáselemzésnek kell alávetni.

Az informatikai biztonság szerves része legyen az átfogó működésfolytonossági folyamatnak és más irányítási folyamatoknak a Hivatalen belül. A működésfolytonosság irányítása tárja fel és mérsékelje a sajátos kockázatokat, kiegészítve az átfogó kockázatkezelést; korlátozza a biztonsági események káros hatását, és biztosítsa, hogy a működésfolytonossághoz megkívánt információ könnyen rendelkezésre álljon.

10.1.1 Az informatikai biztonsági szempontok érvényesítése az üzletmenetfolytonosság irányításában

A kritikus hivatali és informatikai folyamatok védelmében

- az üzletmenetfolytonosság fenntartását, a megelőzést és helyreállítást szolgáló eljárások (üzletmenetfolytonossági terv, katasztrófaelhárítási terv) együttes alkalmazásával mérsékelni kell a különböző rendellenességek és a biztonsági rendszer meghibásodása által okozott fennakadásokat (ezek lehetnek természeti katasztrófák, balesetek, berendezésekben keletkezett hibák, vagy szándékos cselekmények következményei);
- elemezni kell a meghibásodások, fennakadások és üzemzavarok következményeit;
- az üzletmenetfolytonosság irányításának keretében rögzíteni kell a kockázatkezelés eszközeit, csökkenteni kell a biztonsági események hatásait, és időben újra kell indítani a kritikus folyamatokat;
- meg kell becsülni a Hivatalet érintő kockázatok valószínűségét és időbeli hatását, illetve rangsorolni kell az általa okozott kár mértéke szerint (lásd: 10.1.2.);
- át kell tekinteni a kritikus működési folyamatok által érintett minden vagyontárgyat (lásd: 3.1.1.);
- meg kell becsülni, hogy a biztonsági események milyen kieséseket okozhatnak (fontos, hogy olyan megoldásokat találjanak, amelyek kisebb hatású biztonsági eseményeket éppúgy kezelnek, mint a súlyos, a Hivatalet alapjaiban megrengető eseményeket), és ki kell tűzni az adatfeldolgozó eszközök működési céljait;
- érdemes a kritikus adatvagyonra és eszközökre biztosítást kötni;
- kiegészítő, megelőző és mérséklő intézkedéseket kell bevezetni;
- elegendő pénzügyi, Hivatali, műszaki és környezeti forrást kell biztosítani arra a meghatározott informatikai biztonsági követelmények teljesítésére;
- a személyzet, az adatfeldolgozó eszközök és egyéb vagyontárgyak védelméről egyaránt gondoskodni kell;
- ki kell dolgozni az informatikai biztonsági követelményeket érintő működésfolytonossági tervet, összhangban az egyeztetett működésfolytonossági stratégiával (lásd: 10.1.3.);
- a terveket és folyamatokat rendszeresen felül kell vizsgálni, és szükség esetén frissíteni kell (lásd: 10.1.5.);
- a működésfolytonosság irányítását be kell építeni a Hivatal folyamataiba és felépítésébe. Ennek felelősségét a Hivatal valamely vezető beosztottjára bízni (lásd: 2.1.1.).

10.1.2 Az üzletmenetfolytonossági hatásvizsgálatok és a kockázatok elemzése

A megfelelő üzletmenetfolytonosság az informatikai rendszer folyamatos üzemszerű működésének az a szintje, amely mellett a kiesés kockázata a Hivatal számára még elviselhető. A tűréshatárt az üzletmenet – támogatás szempontjából – kritikus rendszereinek egy meghatározott (maximált) kiesési ideje határozza meg.

Az üzletmenetfolytonosságot a szükséges megelőző, illetve helyreállító intézkedésekkel kell fenntartani, amelyhez előre el kell készíteni az üzletmenetfolytonossági és a katasztrófaelhárítási tervet.

Az üzletmenetfolytonossági terv részletesen meghatározza a kívánt üzletmenetfolytonosság fenntartásához szükséges feltételeket, Hivatali és szervezési lépéseket, valamint szabályozza a megvalósítás módját.

Az üzletmenet informatikai biztonsági szempontjai azon eseményeken alapulhatnak, amelyek a Hivatal működési folyamatainak megszakadását okozhatják, mint pl. a berendezés meghibásodása, emberi hibák, lopás, tűz, természeti katasztrófák és terrorcselekmények. A kockázatelemzés során meg kell határozni az ilyen megszakadások valószínűségét, időbeli hatását, a kár mértékét és a helyreállítás időtartamát.

A működésfolytonosság kockázatát a működési források és folyamatok tulajdonosainak bevonásával mérjék fel. Ez a felmérés terjedjen ki az összes működési folyamatra, és ne korlátozódjon az adatfeldolgozó eszközökre, de tartalmazza az informatikai biztonságra jellemző eredményeket. Fontos, hogy a különböző kockázati szempontokat összekapcsolják, hogy a Hivatal működésfolytonossági követelményeiről teljes képet kapjanak.

A felmérés azonosítsa, számszerűsítse, és rangsorolja a kockázatokat a Hivatalre vonatkozó kritériumok és célok szerint, beleértve a kritikus erőforrásokat, a megszakadás hatásait, a megengedhető kiesési időket és a helyreállítási prioritásokat.

A kockázatelemzés eredményétől függően fejlesszenek ki egy működésfolytonossági stratégiát, hogy meghatározzák a működésfolytonossághoz való átfogó közelítést. Ha ez rendelkezésre áll, a vezetőség hagyja jóvá, és készítsen egy tervet, amelyet megvalósítja ezt a stratégiát.

10.1.3 Az üzletmenetfolytonossági terv kidolgozása

Az üzletmenetfolytonossági terv tartalmazza, hogy a támogató folyamatok és eszközök (pl. informatikai rendszerek) sérülése vagy kiesése esetén hogyan lehet a Hivatal működését fenntartani.

Az üzletmenetfolytonossági terv célja, hogy a Hivatalfolyamatait támogató informatikai erőforrások üzemidőben a lehető legjobb időkihasználással és a legszélesebb funkcionalitással álljanak rendelkezésre.

Az üzletmenetfolytonossági tervnek részletesen me g kell határoznia a kívánt üzletmenetfolytonosság fenntartásához szükséges megelőző, helyettesítő és visszaállító intézkedések megvalósításához szükséges feltételeket, a Hivatali és szervezési lépéseket, valamint a megvalósítás módját.

A tervezés egyik lényeges eleme a kiesési kockázatok elemzése, amelynek során mérlegelni kell az okozható kár nagyságát, illetve az üzemzavarok és vészhelyzetek várható gyakoriságát.

A tervnek le kell fednie a lehetséges szituációk minél szélesebb körét:

- különböző hosszúságú kieséseket;
- különböző eszközök és létesítmények elvesztését;
- a helyszínekhez való fizikai hozzáférés teljes elvesztését;
- a rendeltetésszerű működéshez való visszatérés igényét.

A helyreállítási terv tartalmazza, hogy miként kell visszaállítani a váratlan eseménnyel érintett informatikai rendszereket. A helyreállítási terv tartalmazzák:

- a katasztrófát jelentő körülményeket;
- a helyreállítási tervek alkalmazásának felelősségét;
- a különböző visszaállítási tevékenységekért való felelősségeket;
- a helyreállítási tevékenységek leírását.

Az üzletmenetfolytonosság terv fő részei:

- Helyzetfelmérés és értékelés
  - projektelőkészítő megbeszélés (feladat, behatárolás, humán és eszközerőforrás, illetve az adminisztrációs feltételek tisztázása, projektterv megbeszélése, felhasználandó dokumentumok előzetes meghatározása);
  - részletes projektterv elkészítése;
  - projektindító megbeszélés (célok, feladatok, várható eredmények prezentációja; pontos feladatmeghatározás; projektHivatal összetétele; felhasználandó dokumentumok listája; projekt megkezdése);
  - előzetes helyzetfelmérő interjúterv elkészítése és véglegesítése (területek, személyek);
  - az interjúk megszervezése (személyek és időpontok egyeztetése), tematikák elkészítése;
  - interjúk elkészítése és feldolgozása dokumentumokban (kritikus hivatali folyamatok és az ezeket támogató alkalmazások; a kiesések következményei, kockázatai és rangsorolása az eredményes működés szempontjából, a rendelkezésre állás követelményei, potenciális üzemzavari és katasztrófaesemények palettája, tartalékolási és visszaállítási stratégiák és módszerek).

- Megelőzési terv és intézkedések
  - Tartalmazza mindazon szabályzatokat, dokumentumokat és intézkedéseket, amelyek az informatikai rendszer folytonos üzemének fenyegetéseit kezelik. Megelőzés nélkül elkerülhetetlenek a nagyobb üzemzavarok vagy katasztrófaesemények, és nem biztosított a nagyszámú, de kisebb üzemeltetési és felhasználási problémák miatt sérülő alkalmazások rendelkezésre állása.
  - A megelőzési terv a következőkre terjed ki:
    - az informatikai rendszer megbízható üzemeltetésére és az ahhoz kapcsolódó feladatokra;
    - az informatikai rendszer kritikus elemeinek üzemi és vésztartalék megoldásaira, valamint az ezek üzemkészségét biztosító intézkedésekre;
    - az informatikai rendszer üzemét biztosító környezeti rendszerek karbantartására, illetve az ezekkel kapcsolatos biztonsági intézkedésekre;
    - az üzemeltetési dokumentumok rendszerezett és biztonságos tárolására;
    - az adathordozók rendszerezett és biztonságos tárolására;
    - az üzemeltető, a karbantartó és a kárelhárító személyzet rendelkezésre állását és bevethetőségét biztosító intézkedésekre;
    - a külső szervizre, a tartalékképzési megoldásokra vonatkozó, és a biztosítási szerződésekkel kapcsolatos intézkedésekre;
    - mentési tervre, amely meghatározza a mentési rendszer generációit és hierarchiáját;
    - az üzemelő rendszer konfigurációjában és az üzemelő szoftverben megvalósítandó változások szabályozott kivitelezésére, valamint a szoftverfejlesztések elkülönített kivitelezésére és a fejlesztett szoftverek rendszerbe illesztésére vonatkozó legfontosabb intézkedésekre;
    - vírusvédelmi és víruskezelési intézkedésekre, figyelembe véve a Hivatalnél hatályos vírusvédelmi szabályzatot;
    - megelőzésre, amelyben fontos szerepet játszik az alkalmazói rendszerek használatára történő rendszeres oktatás, valamint az informatikai biztonság olyan szintű oktatása, amely kiterjed a kezelt adatok bizalmasságát, sértetlenségét és rendelkezésre állását

célzó szabályokra, illetve a szükséges védelmi intézkedésekre;

- tesztelési és tréningtervre, amely meghatározza a tesztelés formáit. Két formája javasolt: audit jellegű teszt, amelyet egy előre elkészített ellenőrzési lista alapján független belső vagy külső auditorok végeznek, illetve valós üzemzavari vagy katasztrófaesemények szimulációja.

- Visszaállítási terv
  - A visszaállítási terv alapvető célja az, hogy üzemzavar vagy katasztrófaesemény után mihamarabb észleljék az eseményt, mozgósítsák a szükséges emberi és eszközerőforrások, és Hivatalten állítsák vissza az üzemszerű állapotot.
  - A visszaállítási terv a következőket tartalmazza:
    - a visszaállítási terv célját és használatát;
    - az üzemzavarok és katasztrófaesemények megnevezését;
    - az események bekövetkezésének várható idejét és kezelési módját;
    - az eseménykezelő csoport összetételét, feladatait és hatáskörét;
    - részletes iránymutatást a következő lépésekre: azonnali reagálás (riadóterv), futtatókörnyezet helyreállítása, funkcionális helyreállítás, üzemeltetési szintű helyreállítás, áttelepülés (katasztrófa esetén), normalizálás az áttelepülés után.

Az intézkedések kiterjednek a központi erőforrásokra, azok fizikai és személyi környezetére, a végponti munkaállomásokra és az azokhoz kapcsolt kártyaolvasókra és a kommunikációs rendszer területeire.

Véglegesíteni kell az előzetes intézkedési tervet, amely tartalmazza mindazon feltételeket teljesítő lépéseket, melyek nélkül az üzletmenetfolytonossági terv alkalmatlan, illetve a következő projektfázisban elvégzendő tesztelést és tréninget nem szabad megkezdeni.

- Oktatás, tréning és tesztelés

Az oktatás célja az üzletmenetfolytonosság jelentőségének tudatosítása, az üzletmenetfolytonosság tervezési alapismereteinek átadása, a megelőzési és visszaállítási terv megismerése és elsajátítása.

A teszt és tréning akkor kezdhető meg, ha az üzletmenetfolytonossági terv készítési fázisa végén elfogadott intézkedési terv olyan szinten megvalósult, hogy az üzletmenetfolytonossági terv tesztje és tréningje meghatározott üzemzavarra vagy katasztrófaeseményre alkalmazható.

Az üzletmenetfolytonossági tervet szimulált eseményekkel, azokat a terv szerint elhárítva kell tesztelni: ennek során az eseménykezelő csoport, az üzemeltető személyzet és a felhasználók a valós körülményeknek megfelelően gyakorolják a visszaállítási terv végrehajtását.

10.1.4 Az üzletmenetfolytonossági tervek vizsgálata, karbantartása és újraértékelése

10.1.4.1 A tervek tesztelése

Az üzletmenetfolytonossági tervben teszteléssel felfedezhetjük az elavult hivatkozásokat, a hiányosan dokumentált személyzeti vagy berendezésbeli változásokat, és más figyelmetlenségeket. Ezt a vizsgálatot rendszeresen el kell végezni, hogy a terv naprakész és hatékony maradjon. Ilyenkor a helyreállításban részt vevő új munkatársak is jobban megismerhetik, tudatosíthatják a tervet.

Az üzletmenetfolytonossági terv tesztelését úgy kell ütemezni, hogy a módszertant is megadják. A terv

sajátos összetevőit gyakrabban érdemes vizsgálni, mint a formakövető részeket. Módszertanok egész választéka áll rendelkezésünkre, hogy meggyőződjünk terveink működőképességéről:

1. különböző forgatókönyvek kerekasztalos vizsgálata, ahol példaként hozott biztonsági eseményekre válaszul megvitatjuk az üzletmenet helyreállítási lépéseit;

2. szimulációk, melyekkel felkészítjük a személyzetet, hogyan viselkedjenek váratlan események bekövetkezése után, kríziskezelő szerepben;

3. műszaki helyreállítási vizsgálat, amely szavatolja, hogy az informatikai rendszerek hatékonyan visszaállíthatók;

4. a helyreállítás vizsgálata alternatív helyszínen, amikor a visszaállítást az hivatali folyamatokkal párhuzamosan, a főhelyszíntől távol végzik;

5. annak vizsgálata, hogy a harmadik fél által szállított termékek és szolgáltatások megfelelneke a szerződéses kötelmeknek;

6. teljes beszámoltatás arról, hogy a Hivatal, a személyzet, a berendezés, az eszközök és a szolgáltatások képeseke megbirkózni az üzemkiesésekkel.

Ezeket a módszereket bármely Hivatal követheti, figyelembe véve az adott helyreállítási terv sajátosságait.

A tervet legjobban egy szimulált eseménnyel és annak e terv szerinti visszaállításával lehet tesztelni. Elvárható, hogy ezzel a módszerrel az eseménykezelő Hivatal, az üzemeltető személyzet és a felhasználók a valós körülményeknek megfelelően legalább évente egyszer gyakorolják a visszaállítási terv végrehajtását.

A teszt értékelése során az üzletmenetfolytonossági tervet szükség szerint módosítani vagy frissíteni kell, és be kell illeszteni a szabályozási környezetbe.

10.1.4.2 A tervek karbantartása és újraértékelése

Az üzletmenetfolytonossági tervet rendszeresen felül kell vizsgálni, és aktualizálni kell, hogy hatékonysága megmaradjon (lásd még: 10.1.5.1.). A Hivatal változáskezelő programjában szerepelnie kell üzletmenetfolytonossággal foglalkozó eljárásrendnek.

Az üzletmenetfolytonossági terv felülvizsgálatában ki kell jelölni a felelősségi köröket, és az üzletmenetben bekövetkezett, de még nem dokumentált változásokat a tervben rögzíteni kell.

Ha egy körülmény vagy biztonsági esemény alapján a tervet felül kell vizsgálni, mérlegelni kell új eszközök beszerzését, az üzemeltetői rendszer modernizálását, és hogy az alábbi területeken hogyan változik a kockázat:

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

11 SZABÁLYOZÁSI KÖRNYEZET

11.1 Beilleszkedés a hatályos szabályozási környezetbe

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

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 Hivatalszintű érvényesüléséhez le kell fektetni a Hivatali informatikára vonatkozó biztonsági kritériumokat – azok személyi és tárgyi feltételeivel együtt –, valamint a szabályozás hazai gyakorlatát a nemzetközi szabványokhoz kell igazítani.

A Hivatal szabályzóit a hatályos jogszabályok, szabványok és ajánlások figyelembevételével kell elkészíteni (lásd: 8.1.1.). Kétség esetén konkrét követelményekről ki kell kérni a Hivatal informatikai biztonsági vezetőjének véleményét.

11.1.1 Vonatkozó hatályos jogszabályok, szabványok és ajánlások

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

Jogszabályok:

Az informatikai biztonsággal kiemelten foglalkozó jogszabályok:

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 301/2013. (VII. 29.) kormányrendelet a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról
- 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 vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről
- 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
- 151
- 208/2011. (X. 19.) kormányrendelet a minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól
- 180/2004. (V. 26.) kormányrendelet az elektronikus hírközlési feladatokat ellátó Hivatalek és a titkos

információgyűjtésre, illetve titkos adatszerzésre felhatalmazott Hivatalek együttműködésének rendjéről

- 303/2013. (VII. 31.) kormányrendelet az egyes nemzetbiztonsági ellenőrzés alá eső jogviszonyokról és a nemzetbiztonsági ellenőrzéssel összefüggő lényeges adatokról, valamint a lényeges adatok bejelentésének 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
- 85/2012. (IV. 21.) Korm. rendelet az elektronikus közigazgatási ügyintézésről és a kapcsolódó szolgáltatásokról
- 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
- 83/2012. (IV. 21.) kormányrendelet a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról
- 78/2010. (III. 25.) kormányrendelet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól
- 335/2005. (XII. 29.) kormányrendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről
- 13/2005. (X. 27.) IHM rendelet a papíralapú dokumentumokról elektronikus úton történő másolat készítésének szabályairól
- 45/2005. (III. 11.) Kormányrendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat és hatásköréről, valamint eljárásának részletes szabályairól
- 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
- 152
- 9/2005. (VII. 21.) IHM rendelet az elektronikus aláírási termékek tanúsítását végző Hivatalekről, illetve a kijelölésükre vonatkozó szabályokról
- 4/2006. (IV. 19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról
- 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 133351:2004 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 200001:2005 Information technology – Service management – Part 1: Specification
- ISO/IEC 200002:2005 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 133351:2004 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 133352:1997 Information technology – Guidelines for the management of IT Security – Part 2: Managing and planning IT Security
- ISO/IEC TR 133353:1998 Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security
- ISO/IEC TR 133354:2000 Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards
- ISO/IEC TR 133355:2001 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) – CM(2002)49 /AC/35D/2000 Directive on Personnel Security, AC/35D/2001 Directive on Physical Security, AC/35D/2002 Directive on Security of Information, AC/35D/2003 Directive on Industrial Security, AC/35D/2004 Primary Directive on INFOSEC, AC/35D/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 ,

11.1.2 A szellemi tulajdonjog védelme

Eljárásrendbe kell foglalni a Hivataltől idegen szellemi tulajdonban álló termékek jogszerű használatának ellenőrzési módját, különös tekintettel a szerzői és tervezői jogokra, valamint a védjegyekre.

A jogszabályi, szabályozói vagy szerződéses követelmények korlátozhatják a Hivatal tulajdonát képező dokumentumok másolását olyan anyagokra, amit maga a Hivatal állított elő, illetve olyanokat, amelyekre jogot szerzett (licencet vett), vagy a fejlesztő maga adta át a Hivatalnak.

A saját tulajdonú szoftvertermékeket többnyire olyan licencszerződések hatálya alatt szállítja az alvállalkozó, amely meghatározott gépre korlátozza e termékek használatát, és azok másolását is csak a tartalék másolat készítésére korlátozza.

A következő óvintézkedések megfontolandók:

- Olyan szabályzatot kell kiadni, amely meghatározza, hogy mi számít a szoftverek jogszerű használatának.
- Érdemes olyan ipari szabványokat kiadni, melyek a szoftverbeszerzést szabályozzák.

- A személyzetben tudatosítani kell a szerzői jogot, a beszerzési szabályokat, és szabályszegés esetére a fegyelmi eljárás lehetőségét.
- A szoftverekre is kiterjedő vagyonleltárt kell vezetni.
- A licencek, mesterlemezek, kézikönyvek stb. tulajdonlásáról szóló okmányokat és bizonyítékokat biztonságosan meg kell őrizni.
- Biztosítani kell, hogy egy szoftvert a licencben megengedettnél több felhasználó ne vehessen igénybe.
- Kizárólag jogtiszta szoftvereket szabad telepíteni.
- Szabályzatba kell foglalni a licenceknek megfelelő állapot fenntartásának módját.
- Szabályzatba kell foglalni a szoftverhasználat átruházásának követelményeit.
- A személyzet által használt szoftverek átvilágításához automatizált mechanizmusokat, segédeszközöket kell használni.
- A nyilvános hálózatokról szerzett szoftverek és adatok felhasználási feltételeit be kell tartatni.

11.1.3 A Hivatal adatainak biztonsága

A Hivatal fontos dokumentumait védeni kell a lopással, sérüléssel és hamisítással szemben. Egyes dokumentumokat jogszabály alapján vagy hivatali érdekből kiemelt biztonságban kell őrizni. Ezek közé tartoznak azok az iratok, amelyek a Hivatal jogszerű működését bizonyítják a felügyeleti szervek számára, a hatékony és nyereséges működést pedig a tulajdonosok és partnerek számára. Az egyes adatokat jogszabály szerinti időtartamig kell megőrizni.

A dokumentumokat fajtánként kell osztályozni: pl. számlák, adatbázisok, tranzakciók naplói, az átvilágítás feljegyzései, üzemeltetési eljárások dokumentumai – ezek mindegyikéhez rögzíteni kell a kötelező megőrzés időtartamát és az adathordozók fajtáját: pl. papír, mikrofilm, mágneses vagy optikai adathordozó. A rejtjelezett archívumokhoz és az elektronikus aláírásokhoz használatos bármely kriptográfiai kulcsot (lásd: 10.3.) csak kellően biztonságos helyen szabad tartani, és az arra felhatalmazott személyeknek – amikor szükségük van rá – hozzáférhetővé kell tenni.

Fel kell készülni az adathordozók amortizációjára. A tárolást és a kezelést a gyártó ajánlásainak betartásával kell megoldani. A tárolás során a fizikai környezetre (hőmérséklet, páratartalom stb.) kiemelt figyelmet kell fordítani.

Amennyiben elektronikus adathordozót választunk, akkor a megőrzési időszakban gondoskodni kell arról, hogy az adathordozóknak állaga fennmaradjon, és az adatok az eredeti rögzítési formátum szerint olvashatók maradjanak akkor is, amikor a technológiai változások miatt az adathordozó ipari támogatása megszűnik. Az adattároló rendszereket úgy kell megválasztani, hogy a kezelt adatokat a hatóságok számára jogilag is elfogadható módon lehessen visszakeresni, pl. bármely információt elfogadható időn belül és formátumban lehessen megjeleníteni.

A tároló és kezelőrendszernek garantálnia kell, hogy az adatok a kötelező megőrzési időtartamon belül egyértelműen azonosíthatók maradnak. A tároló és kezelőrendszer tegye lehetővé, hogy az adatokat ezen időszak lejártával, ha a Hivatal számára már nem szükségesek, biztonságosan megsemmisíthessék.

Az adatok megőrzéséről, tárolásáról, kezeléséről és a velük való rendelkezésről útmutató kézikönyvet (használati utasítást) kell kiadni.

Megőrzési ütemtervet kell készíteni, amelyben azonosítunk minden adatfajtát, és azt az időtartamot, amelyben azokat meg kell őrizni.

11.1.4 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. Az Infotv. alapján adatvédelmi felelőst kell kijelölni, aki erre vonatkozó útmutatást ad a vezetőknek, felhasználóknak és szolgáltatóknak egyéni felelősségükről, valamint azokról a különleges eljárásokról, amelyeket követniük kell.

11.1.5 A védelmi eszközökkel elkövethető visszaélések megelőzése

A Hivatal adatfeldolgozó eszközeit hivatali célra hozták létre, melyeket a vezetőségnek elérhetővé kell tennie az illetékes személyzet számára. Ezen eszközök bármilyen, az hivatali céloknak ellentmondó vagy felhatalmazás nélküli használatát rendellenesnek kell tekinteni. Ha megfigyeléssel vagy más módon észleljük, hogy ilyen tevékenység előfordult, akkor erre fel kell hívni a vonatkozó fegyelmi eljárásért felelős vezető figyelmét.

A használat monitorozása akkor jogszerű, ha a munkatársakat a megfigyelésről előre tájékoztatjuk. Mielőtt megfigyelési eljárást indítanánk, érdemes jogtanácsos véleményét kikérni.

Az információs rendszer vagy adat megsértése bűncselekmény, ezért lényeges, hogy minden felhasználó legyen tudatában a saját engedélye szerinti jogosultságának, az engedélyezett hozzáférési körének. Ezt azzal lehet elérni, hogy a felhasználók írott formában kapják meg a felhatalmazásukat, amelynek egy példányát a felhasználóval alá kell íratni, és biztonságosan meg kell őrizni. A Hivatal munkatársait éppúgy, mint a harmadik félhez tartozó felhasználókat, tájékoztatni kell arról, hogy semmilyen más hozzáférés nincs megengedve, csak az, amelyre felhatalmazást kaptak.

A bejelentkezési felületen érdemes mindig feltüntetni, hogy a rendszer, amelybe a felhasználó belépni készül, magántulajdonú, és abba a jogosulatlan belépés tilos. Ezt célszerű a fel

használóval nyugtáztatni, és elvárni tőle, hogy a képernyőn megjelenített üzenetre kellő módon válaszoljon ahhoz, hogy a bejelentkezési folyamatot folytathassa.

11.1.6 A kriptográfiai eszközök kezelésének szabályozása

Egyes országok egyezményeket kötöttek, jogszabályokat alkottak, és más eszközöket is bevetettek annak érdekében, hogy a kriptográfiai mechanizmusokhoz való hozzáférést és azok használatát ellenőrzésük alatt tarthassák. Az ilyen óvintézkedés magában foglalhat

- kriptográfiai funkciókat végrehajtani képes hardver vagy szoftver importját és exportját;
- a kriptográfiai funkciót végrehajtó kiegészítéseket támogató hardver vagy szoftver importját és exportját;
- az országok kötelező vagy önkéntes hozzáférési módjait a tartalom bizalmasságát szavatoló hardverrel vagy szoftverrel titkosított információhoz.

Érdemes jogi tanácsot kérni, mielőtt rejtjelezett információt vagy kriptográfiai eszközöket más országba továbbítunk. Minősített adatok esetében a rejtjelezést csak Mavtv. és végrehajtási rendeletei szerint szabad végezni.

11.2 Az informatikai biztonsági szabályzatnak, szabványoknak és műszaki követelményeknek való megfelelés

Gondoskodni kell arról, hogy a rendszerek megfeleljenek a Hivatal biztonságpolitikájának, szabályzatainak és a szabványoknak. Az informatikai rendszerek biztonságát időről időre felül kell vizsgálni.

Ezeket a felülvizsgálatokat a vonatkozó biztonsági szabályzatoknak megfelelően kell végezni; hasonlóképpen auditálni kell a műszaki és informatikai rendszereket a biztonságos megvalósítás és üzemeltetés szabványai szerint.

11.2.1 Az informatikai biztonsági előírásoknak való megfelelés

A szakmai vezetők felelősséggel tartoznak a hatáskörükbe tartozó biztonsági eljárások helyes végrehajtásáért. Időről időre az üzletmenet minden területét felül kell felülvizsgálni, hogy megfelelneke a biztonsági szabályzatoknak és szabványoknak. 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.

Az informatikai rendszerek tulajdonosaitól (lásd: 3.1.) elvárható, hogy tűrjék és segítsék rendszereik átvilágítását. A rendszerhasználat üzemviteli megfigyelését a 7.7. alfejezet tárgyalja.

Az audit az alkalmazott biztosítékok felülvizsgálatát és elemzését jelenti: azt mutatja ki, hogy az informatikai rendszerek és szolgáltatások megfelelneke az informatikai biztonságpolitikában és az informatikai biztonsági szabályzatban lefektetett követelményeknek. A biztonsági megfelelőséget a következő esetekben kell ellenőrizni:

- új informatikai rendszerek vagy szolgáltatások bevezetésekor,
- meglévő informatikai rendszerek vagy szolgáltatások esetében adott időszakonként (pl. évente),
- ha változás történt a rendszerszintű informatikai biztonságpolitikában (annak érdekében, hogy lássuk: milyen változtatások szükségesek a kívánt biztonsági szint fenntartásához).

Biztonsági auditot külső vagy belső személyzet, valamint a NEIH egyaránt végezhet, elsősorban a rendszerszintű informatikai biztonságpolitikára épülő ellenőrzőlisták segítségével.

Az informatikai rendszert védő biztosítékokat a következő módon lehet ellenőrizni:

- rendszeres vizsgálatokkal és tesztekkel;
- a működési teljesítmény mérésével, valós biztonsági események bekövetkezésekor;
- szúrópróba jellegű vizsgálatokkal, ha egyes meghatározott érzékenységű vagy profilú területeken a biztonsági szintek és célok összhangját kívánjuk felmérni.

Az események teljes történetének követését segíti, ha az audit során átvizsgáljuk a biztonsági naplókat és az automatizált naplózásra alkalmas szoftvereket.

A biztonsági auditot az elfogadott biztosítékok listáira kell építeni, melyeket a legutóbbi kockázatelemzés eredményei, a rendszerszintű informatikai biztonságpolitika és az informatikai vezetés által előírt biztonsági eljárások határoznak meg. Azt kell megállapítani, hogy a biztosítékokat megvalósítottáke egyáltalán, jól

tettéke, jól használjáke, és ahol lehetséges volt, teszteltéke.

A biztonsági megfelelőséget ellenőrző személynek végig kell járnia az épületet egy normál munkanapon, és meg kell figyelnie a biztonsági eszközök használatának módját. Természetesen a szóbeli beszámolók is fontosak, de ezek valóságtartalmát külön ellenőrizni kell.

Nagy segítséget adhat egy átfogó ellenőrző lista és az, hogy a jelentéseket egységes formátumban készítik el. Az ellenőrző listáknak tartalmazniuk kell általános azonosítási információkat, pl. konfigurációs részleteket, környezeti beállításokat, felelősségi köröket, politika jellegű dokumentumok felsorolását.

A fizikai biztonság vizsgálatakor olyan szempontokat kell figyelembe venni, mint a szabadtéri épületeket, csatornanyíláson keresztüli megközelíthetőséget, falazatot, zárakat, tűzvédelmet, riasztórendszert, folyadékérzékelést és a tartalék energiaellátás kiépítettségét.

Fokozottan figyelni kell továbbá

- olyan területekre, ahol a fizikai behatolásnak vagy az eszközök kijátszása valószínű (pl. a kódzárral vagy kártyával nyitható ajtók kiékelésével);
- hibás vagy hibásan felszerelt eszközökre, hiányos vagy rossz elosztásra, esetleg nem megfelelő típusú érzékelőkre. Vane elegendő füst ill. hőérzékelő egy adott területen, és a megfelelő magasságban vannake? Vane megfelelő reagáló erő? Megfelelően vannake bekötve a riasztók egy ellenőrző pontra? Vane bármilyen új veszélyforrás, mint pl. valaki egy alkalmatlan helyiséget kezd használni gyúlékony anyagok tárolására? Létezike megfelelő védelem az áramingadozás vagy kimaradás ellen? A megfelelő kábeltípusokat használjáke, és azok nincseneke kitéve mechanikai sérülés veszélyének?

A sérülékenységek feltárásához az alábbi kérdések további segítséget nyújthatnak:

- Munkavállalók biztonsági ellenőrzése: figyeljük meg a felvételi folyamatot. Valósake a referenciák? Az esetleges hiátusok hátterét ellenőriztéke? A humán erőforrás területe
- jól tájékozotte a biztonsági szempontokkal kapcsolatban? Megbízhatónak tekinthetőe a kulcspozícióba kijelölt személy?
- Adminisztratív biztonság: valójában hogyan kezelik a dokumentumokat? A használatban levő dokumentációk naprakészeke? A kockázatelemzés, a státuszellenőrzés és az események jelentése kapcsán rendeltetésszerűen használjáke azokat? Az üzletmenetfolytonossági terv pontosan fedie az egész üzletmenetet, és naprakésze?
- Hardver és szoftverbiztonság: vane kellő tartalék? Mennyire megbízható a felhasználói azonosítás és hitelesítés rendje? Vane olyan minősített eszköz, mely megfelel a megállapított követelményeknek?
- Kommunikációbiztonság: vane kellő tartalék? Ha van betárcsázási lehetőség, a szükséges berendezéseket használjáke, és jól teszike ezt? Ha titkosítás vagy üzenethitelesítés is szükséges, milyen hatékony a kulcskezelési rendszer és a kapcsolódó művelet?

Összefoglalva: a biztonsági megfelelőség ellenőrzése nem kis feladat, sikeres végrehajtása nagy gyakorlatot és tudást igényel. Az audit a belső ellenőrzéstől független tevékenység.

11.2.2 A műszaki követelményeknek való megfelelés

Időről időre ellenőrizni kell, hogy az informatikai rendszerek megfelelneke a biztonsági szabványoknak. A műszaki audit során vizsgálni kell az üzemeltetési rendszert, hogy ezzel lehessen szavatolni a hardveres és szoftveres óvintézkedések helyességét, pontosságát. Ez a fajta megfelelőségellenőrzés műszaki szakértői

elemzést igényel, amit egy gyakorlott rendszermérnökkel érdemes végrehajtatni – akár személyesen, akár olyan automatizált szoftvercsomaggal készített műszaki jelentést továbbításával, amelyet a műszaki szakértő később kiértékelhet.

Az audit egyebek közt az alkalmazásmélység (elterjedtség, behatolási mélység, penetráció) vizsgálatát is tartalmazza, amelyet erre a célra külön szerződtetett független szakértők hajtanak végre. Ez hasznos lehet a rendszer sérülékenységeinek felderítésében és annak ellenőrzésében, hogy mennyire hatékonyak az óvintézkedések e sérülékenységeket kihasználó jogtalan hozzáférésekkel szemben. Az alkalmazásmélységet kiemelt körültekintéssel kell vizsgálni, mert a vizsgálat könnyen veszélyeztetheti a rendszer biztonságát, és egyéb sérülékenységeket illetéktelenek tudomására hozhat.

Bármely műszaki megfelelőségellenőrzés elvégezhető, amennyiben csak az illetékes, erre felhatalmazott személyek végezik vagy felügyelik azt.

11.2.3 Az informatikai rendszerek biztonsági ellenőrzésének szempontjai

Maximalizálni kell az auditálás hatékonyságát, és minimalizálni kell az általa okozható zavarokat az informatikai rendszerekben. Intézkedéseket kell hozni az üzemelő rendszer védelmére, és hogy megóvjuk az auditeszközök sértetlenségét, és megelőzzük az azokkal való visszaélést.

Az ellenőrzés egy folyamatos tevékenység, amely azt vizsgálja, hogy a rendszer és felhasználói, valamint a környezet fenntartjae az informatikai biztonsági tervben (illetve szabályzatban) meghatározott biztonsági szintet. Napokra lebontott ellenőrzési tervet kell készíteni kiegészítő iránymutatásokkal és eljárásokkal, a folyamatos biztonságos működés támogatására. A felhasználóknak, az üzemeltető személyzetnek és a biztonsági tervezőknek rendszeresen konzultálniuk kell annak érdekében, hogy az összes biztonsági célkitűzést megvalósítsák, és az informatikai biztonsági terv naprakész maradjon.

Az informatikai biztonsági ellenőrzés rendszerességét azért kell fenntartani, hogy időben felismerhessük és rangsorolhassuk az új kockázatokat. Ilyenkor többek között össze kell írni az eszközöket, értéküket, sérülékenységeiket, biztosítékaikat, valamint az eszközöket érintő fenyegetéseket. Az új kockázatok a technológiában, a Hivatal céljaiban, az informatikai rendszerben működő alkalmazásokban, az informatikai rendszerben feldogozott adatokban és magukban az informatikai eszközökben bekövetkezett változásokból erednek.

A biztosítékok teljesítményét és hatékonyságát is rendszeresen ellenőrizni kell: lehetséges, hogy ezt a megváltozott eszközök, fenyegetések és sérülékenységek befolyásolják. Ha új informatikai rendszereket vezetnek be, vagy megváltoztatják a meglevőket, akkor igény keletkezik, hogy a hasonló változások ne befolyásolják a meglévő biztosítékokat, és az új rendszereknek megfelelő biztosítékok álljanak rendelkezésre.

Ha rendellenességet találunk, akkor azt ki kell vizsgálni, és a megállapításokat jelenteni kell a felső vezetésnek a biztosítékok lehetséges felülvizsgálatához, vagy indokolt esetben a rendszerszintű biztonságpolitika felülvizsgálatához és a kockázatfelmérési tevékenységhez.

A biztonsági politikával való összhang érdekében megfelelő erőforrásokat kell elkülöníteni az alábbiak naponkénti ellenőrzésére:

- meglévő biztonsági mechanizmusok,
- új rendszerek vagy szolgáltatások bevezetése,
- tervezett változtatások a meglévő rendszerekben vagy szolgáltatásokban.

Sok biztonsági eszköz készít napló formájú kimenetet az eseményekről. Ezeket a naplókat statisztikai módszerekkel kell feldolgozni a trendváltozások és az ismétlődő események korai érzékelése érdekében. Ki kell jelölni, hogy ki a felelős a naplók elemzéséért.

Elosztott rendszerekben a naplók csak egy adott környezet eseményeiről adnak számot. Egy összetett esemény valós megértéséhez egyetlen eseményrekorddá kell egyesíteni a különböző naplók bejegyzéseit – ebben segítenek a kapcsolathordozó adatok. Ezután ezt az eseményrekordot kell elemezni.

A naponkénti ellenőrzéshez dokumentálni kell a műveleti eljárásokat: ez ahhoz szükséges, hogy hosszú távon minden rendszer és szolgáltatás biztonsági szintjét fenntarthassuk.

A biztonsági konfiguráció frissítésének lépéseit is dokumentálni kell: fel kell tüntetni a változtatott biztonsági paramétereket, és frissíteni kell minden biztonságszervezési információt. Ezt a dokumentumot jóvá kell hagyni a konfigurációkezelés során. A rendszeres karbantartás folyamán ügyelni kell arra, hogy a biztonság ne sérüljön.

A biztosítékok ellenőrzési folyamatát írásba kell foglalni. Rögzíteni kell a biztonsági naplók vizsgálatának gyakoriságát és annak megközelítését. Ki kell térni a statisztikai eszközök és módszerek használatára. Útmutatást kell adni arról, hogy különböző működési körülmények között milyen vizsgálati küszöbértékeket alkalmazunk.

11.2.4 . Rendszerauditálási óvintézkedések

Az üzemelő rendszer auditálását gondosan meg kell tervezni, és annak feltételeit egyeztetni kell az érintettekkel, hogy ezzel minimalizálni lehessen az üzemkiesés kockázatát. Az alábbi szempontokat érdemes figyelembe venni:

- Az auditálás követelményeit egyeztetni kell az illetékes vezetőséggel.
- Az ellenőrzés tárgyát egyeztetni kell és jóvá kell hagyatni a vezetőséggel.
- A szoftverek és az adatok ellenőrzése a „csak olvasás" jellegű hozzáférésre legyen korlátozva.
- Az olvasástól eltérő kívüli hozzáférést csak akkor szabad engedélyezni, ha az a rendszerfájlok elkülönített másolatát érinti – ilyen esetben az auditálás befejeztével ezeket az állományokat meg kell semmisíteni.
- Az ellenőrzéseket végző informatikai eszközöket pontosan azonosítani kell, és rendelkezésre kell bocsátani.
- A különleges vagy kiegészítő feldolgozás követelményeit azonosítani és egyeztetni kell.
- Hivatkozási napló készítéséhez minden egyes hozzáférést monitorozni és naplózni kell.
- Az auditra vonatkozó minden eljárást, követelményt és felelősséget írásba kell foglalni.

11.2.5 Rendszerauditálási eszközök védelme

Az audithoz használatos programokat és adatállományokat védeni kell az illetéktelen hozzáféréstől, hogy kizárjuk a lehetséges visszaéléseket. Ezeket az eszközöket el kell különíteni az üzemeltetési és a fejlesztési eszközöktől, és nem szabad azokat az üzemi archívumokkal együtt vagy a felhasználói körzetekben tárolni, hacsak nincsenek ellátva alkalmas szintű kiegészítő védelemmel.

Ha az auditot harmadik fél végzi, könnyen visszaélhetnek az auditálási eszközökkel, és jogosulatlanul betekinthetnek az hivatali titkokba. A 4.2.1. és a 7.1.2. szakasz segít ennek elkerülésében.

Adat

Az adat az információ megjelenési formája, azaz tények, elképzelések nem értelmezett, de értelmezhető közlési formája.

Adatbiztonság:

Az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési, szabályozási intézkedések és eljárások együttes rendszere.

Adathordozó:

Adathordozónak tekinthetők a következő eszközök: floppy, CD/DVD, egyéb hordozható háttértároló, pl. memóriakártya, USB drive, mobiltelefon.

Adatkezelő:

Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely a személyes adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.

Adatkezelés:

Az alkalmazott eljárástól függetlenül a személyes adatokon végzett bármely művelet vagy a műveletek összessége, így például gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. Adatkezelésnek számít a fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése is.

Adattovábbítás:

Ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik.

Adattörlés:

Az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.

Adatzárolás:

Az adatok továbbításának, megismerésének, nyilvánosságra hozatalának, átalakításának, megváltoztatásának, megsemmisítésének, törlésének, összekapcsolásának vagy összehangolásának és felhasználásának véglegesen vagy meghatározott időre történő lehetetlenné tétele.

Adatmegsemmisítés:

Az adatok vagy az azokat tartalmazó adathordozó teljes fizikai megsemmisítése.

Adatfeldolgozás:

Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

Adatfeldolgozó:

Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely az adatkezelő megbízásából – beleértve a jogszabály rendelkezése alapján történő megbízást is – személyes adatok feldolgozását végzi.

Adatállomány:

Az egy nyilvántartó rendszerben kezelt adatok összessége.

Harmadik személy:

Olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, amely, vagy aki nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval.

Bizalmasság:

Az adat azon tulajdonsága, amely arra vonatkozik, hogy csak és kizárólag az arra jogosultak számára ismerhető meg, válik kezelhetővé.

Hitelesség:

A hitelesség az entitás egy olyan biztonsági tulajdonsága, amely egy vagy több hozzá kapcsolódó tulajdonságot más entitás számára bizonyíthatóvá tesz.

Információ védelem:

Az informatikai rendszerben tárolt adatok hitelességének, bizalmasságának és sértetlenségének védelme.

Informatikai biztonság:

Az informatikai biztonság a védelmi rendszer olyan, a szervezet számára kielégítő mértékű állapota, amely az informatikai rendszerben kezelt adatok, illetve a rendszerelemek bizalmassága, hitelessége, sértetlensége, funkcionalitása és rendelkezésre állása szempontjából zárt, teljes körű, egyenszilárd, folytonos és kockázatokkal arányos.

Kockázattal arányos védelem:

Kockázatokkal arányos védelemről akkor beszélünk, ha kellően nagy időintervallumban a védelem költségei arányban állnak a potenciális kárértékkel.

Közérdekű adat:

Közérdekű adat az állami, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, valamint a tevékenységére vonatkozó, a személyes adat fogalma alá nem eső adat.

Közérdekből nyilvános adat:

Közérdekből nyilvános adat minden olyan természetes személy, jogi személy vagy jogi személyiséggel nem rendelkező szervezet kezelésében lévő vagy rá vonatkozó, a közérdekű adat fogalma alá nem tartozó adat, amelynek nyilvánosságra hozatalát vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

Magántitok:

Magántitok: a joggyakorlat a magán titok körébe tartozónak tekint minden olyan tényt vagy körülményt, amelynek titokként való megőrzéséhez az érintettnek méltányolandó érdeke fűződik.

Megbízható működés:

Az informatikai rendszernek – beleértve a tárolt adatokat is – rendelkezésre állása és funkcionalitásának védelme.

Rendelkezésre állás:

Az informatikai rendszerelem és adattartalmának azon tulajdonsága, amely arra vonatkozik, hogy az informatikai rendszerelem a szükséges időben és időintervallumban használható. A rendelkezésre állást százalékos értékben szokás megadni, két érték meghatározása a jellemző:

- éves szinten meg kell határozni százalékban, milyen mértékű a rendelkezésre állás
- meg kell határozni a maximális hosszát az egy alkalommal történő leállásnak óraszámban (downtime)

Teljes körű védelem:

Teljes körű a védelem, ha az informatikai rendszer összes elemére kiterjed.

Zárt védelem:

Zárt a védelem, ha az összes releváns fenyegetést figyelembe veszi.

Kockázat:

Veszélyforrások által okozható károk bekövetkezésének lehetősége, amely az MgSzH -nál veszteséget vagy szolgáltatási, működési zavarokat okozhat.

Mailware:

Az angol malware kifejezés az angol malicious software ami szó szerint azt jelenti rosszindulatú szoftver(magyarul is nevezik kártevő szoftvenek, kártékony szoftver, káros szoftver, összevonásából kialakított mozaikszó. Mint ilyen, a rosszindulatú számítógépes programok összefoglaló neve. Ide tartoznak a vírusok, férgek, kémszoftver, zsarolószoftver, agresszív reklámszoftver, a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök (rootkit). A számítógépes kártevő programok mennyisége folyamatosan növekszik, és időről időre új típusok terjednek el. Az ellenük való védekezés a köznyelvben víruskereső programnak nevezett szoftverekkel történik.

Ransomware:

A ransomware (zsarolószoftver) olyan kártékony szoftver, azaz számítógépes program, amely valamilyen fenyegetéssel próbál pénzt kicsikarni a felhasználóból. Ez rendszerint azt jelenti, hogy használhatatlanná teszi a számítógépet vagy elérhetetlenné a rajta lévő adatokat, és csak pénzért vásárolható meg az a kód, aminek a hatására visszaállítja az eredeti állapotot.

Nyilvánosságra hozatal:

Ha az adatot bárki számára hozzáférhetővé teszik.

Sértetlenség:

Az adat azon tulajdonsága, hogy az adat bizonyítottan, vagy bizonyíthatóan csak az eredeti, vagy jogszerűen módosított tartalommal bír, az adat fizikailag és logikailag teljes. A bizonyíthatóság garantálása az adatot

tároló és kezelő rendszer feladata.

Személyes adat:

Bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt - közvetlenül vagy közvetve - név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.

Személyesadat-nyilvántartó rendszer (nyilvántartó rendszer):

Személyes adatok bármely strukturált, funkcionálisan vagy földrajzilag centralizált, decentralizált vagy szétszórt állománya, amely meghatározott ismérvek alapján hozzáférhető.

Tiltakozás:

Az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri;

Ügyviteli leírás:

Azon hivatali, ügyviteli terület leírása, amelynek részleges vagy teljes támogatására az adott informatikai rendszer készült.

Üzleti Titok:

Üzleti titoknak minősül - a Ptk. 81.§ (2) bek. szerint - a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ, megoldás vagy adat, amelynek nyilvánosságra hozatala, illetéktelenek által történő megszerzése vagy felhasználása a jogosult jogszerű pénzügyi, gazdasági vagy piaci érdekeit sértené vagy veszélyeztetné, és amelynek titokban tartása érdekében a jogosult a szükséges intézkedéseket megtette. (A Ptk. ezen meghatározását átveszi a Btk. 300. §-a is.)

Személyes adat:

Személyes adat az Avtv. 2. §-a szerint bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt - közvetlenül vagy közvetve - név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.

RFID hacking:

Bankkártyák és pay pass, és e-személyigazolványok illetéktelen leolvasása.