8/1/2013

IGAZGATÓI UTASÍTÁS **10/2013.**

---

a CSAPI Információbiztonsági szabályzatának kiadásáról a szabályozás bevezetéséről

A Fővárosi Önkormányzat Csarnok és Piac Igazgatósága „Információbiztonsági Szabályzatát" kiadom. (1. számú melléklet)

A szabályzat előírásai hatályosak 2013. május 01-től. A szabályozás összetettsége azonban indokolttá teszi, hogy a bevezetése többlépcsős folyamat legyen.

A szabályozás bevezetését a jelen utasítás mellékletét képező „CSAPI - ISO 27001 Információbiztonsági Szabályzat (Információbiztonsági Irányítási Rendszer) bevezetési ütemterve" szerint rendelem el. A szabályozáshoz kapcsolódó végrehajtási eljárásrendeket a szabályozás elvei alapján a szerződéses IT Szolgáltató köteles elkészíteni a CSAPI információbiztonsági vezetőjének felügyelete mellett.

A CSAPI információbiztonsági vezetője a gazdasági igazgatóhelyettes, aki szabályozás bevezetését teljes körűen irányítja és ellenőrzi.

A szabályozás bevezetésének végső határideje 2013. július 31. napja.

Jelen utasítás a kiadásának napján lép hatályba, ezzel egyidejűleg a CSAPI korábbi „Informatikai szabályzata" hatályát veszti.

Budapest, 2013.05.02.

FŐVÁROSI ÖNKORMÁNYZAT CSARNOKOK ÉS PIAC IGAZGATÓSÁGA * 1. *

dr. Dénes Ákos
igazgató

Mellékletek:

- „Információbiztonsági szabályzat"
- „CSAPI - ISO 27001 Információbiztonsági Szabályzat (Információbiztonsági Irányítási Rendszer) bevezetési ütemterve"

Információbiztonsági Szabályzat

Előterjesztette:

Kovács János - gazdasági igazgatóhelyettes
információbiztonsági vezető

A szabályzatot jóváhagyom és alkalmazásának bevezetését jelen változat hatálybalépési dátumával elrendelem:

dr. Dénes Ákos
igazgató

Információbiztonsági osztályozás	
Bizalmas	☐
Belső	☒
Nyilvános	☐

Szerzői jogi nyilatkozat

0. TARTALOMJEGYZÉK

0.1 MELLÉKLETEK

Azonosító	Megnevezés	Elérhetőség	Kiadás dátuma
CSAPI_IT_XX_m1	Fogalom meghatározások és rövidítések		
CSAPI_IT_XX_m2	Kapcsolódó belső szabályzó dokumentumok és külső dokumentumok (jogszabályok, szabványok)		
CSAPI_IT_XX_m3	Képzési terv		
CSAPI_IT_XX_m4	Informatikai eszköz használatbavételi nyilatkozat		
CSAPI_IT_XX_m5	Titoktartási nyilatkozat minta		

0.2 MÓDOSÍTÁSOK NYOMONKÖVETÉSE

Verzió szám	A módosítás leírása	Dátum
2.0	Második módosított és újra szerkesztett verzió az ISO 27001 szabvány követelményeit figyelembe véve	2013.05.01.
1.0	Első eredeti verzió	2013.04.22.

1. AZ INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT CÉLJA

Jelen Információbiztonsági Szabályzat (a továbbiakban: IBSZ) célja, hogy a Fővárosi Önkormányzat Csarnok és Piac Igazgatósága (a továbbiakban: CSAPI) üzleti tevékenységéhez kapcsolódóan, szabályozza az üzleti folyamatokhoz tartozó

- információk
- és információkezelő eszközök

bizalmasságát, sértetlenségét és **rendelkezésre állását** biztosító védelmi tevékenységeket.

Az IBSZ szorosan illeszkedik az Információbiztonsági Politikához (a továbbiakban: Politika), követi annak iránymutatásait.

Az információ és az azokat támogató üzleti folyamatok, rendszerek és hálózatok fontos üzleti vagyontárgyak. Az információbiztonság és az Információbiztonság Irányítási Rendszer (a továbbiakban: IBIR) meghatározása, kialakítása, elérése, fenntartása és fejlesztése lényeges annak érdekében, hogy fenntartsuk a készpénzforgalmat, a nyereségességet, a jogi megfelelést és a kereskedelmi arculatot.

Az IBSZ kiadásának további általános céljai

- a CSAPI stratégiája és feladatai megvalósulásának elősegítése;
- a Politika által meghatározott biztonsági tevékenységekre egységes keret-szabályok és értelmezések megadása;
- azon célok és irányelvek rögzítése - átlátható és nyomon követhető formában - melyek segítségével az információbiztonság magasabb fokú kialakításának további teendői, illetve további szabályzatai, leírásai egy komplex, átfogó és széleskörű információbiztonságot eredményeznek.

A célok elérése érdekében a védelemnek működnie kell az egyes rendszer-elemek fennállásának teljes ciklusa alatt – a megtervezéstől az alkalmazáson (üzemeltetésen) keresztül a felszámolásukig, és azt követően az elévülés, illetve a selejtezhetőség időtartama alatt.

Az IBSZ szerkezete követi az ISO 27001:2005 szabvány „A" mellékletének („Szabályozási célok és kontrollok") szerkezetét. Ennek célja, hogy a CSAPI hatékony és a nemzetközi szabványon alapuló IBIR-t alapozzon meg.

2. AZ INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT HATÁLYA

Az IBSZ a CSAPI minden szervezeti egységére általános érvénnyel meghatározza az információbiztonsággal, az információkezelő eszközökkel és azok környezetével kapcsolatos biztonsági szabályokat és intézkedéseket, szervesen illeszkedve a szervezet egyéb működési, ügyrendi és biztonsági előírásaihoz, továbbá meghatározza az eljárások rendjét, a felelősöket, az ellenőrzés rendjét és a szankcionálás módját.

A jelen szabályzatban leírtak végrehajtása a dokumentum hatálya alá tartozó személyekre munka- és/vagy polgári jogi felelősség terhe mellett kötelező.

2.1 Személyi hatály

Az IBSZ személyi hatálya kiterjed a CSAPI által foglalkoztatott munkavállalókra, valamint olyan természetes vagy jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (a továbbiakban együttesen: harmadik személy), amelyek a CSAPI informatikai rendszereivel, üzleti szolgáltatásaival jogviszonyba kerülnek, beleértve a vállalkozási/szolgáltatási/megbízási szerződéssel, vagy egyéb szerződéssel rendelkező szerződő partnereket.

Ezen szerződéseknek kötelezően kell információbiztonsági garanciákat tartalmaznia, amely nem lehet ellentmondásban az IBSZ egyetlen pontjával sem.

A CSAPI informatikai rendszereivel kapcsolatba kerülő személyek kivétel nélkül szerződéses viszonyban állnak a Fővárosi Önkormányzat Csarnok és Piac Igazgatósággal. Ezen szerződéseknek kötelezően kell információbiztonsági pontokat tartalmaznia, amely nem lehet ellentmondásban az IBSZ szabályaival.

2.2 Tárgyi hatály

A Politikában és az IBSZ-ben megfogalmazott irányelveket érvényre kell juttatni a CSAPI tulajdonában lévő vagy az általa üzemeltetett informatikai rendszerek tekintetében azok teljes életciklusa alatt (a fejlesztési igények megfogalmazásától a rendszerből történő kivonásig) továbbá az üzleti folyamatok működtetése során.

Az IBSZ tárgyi hatálya kiterjed a CSAPI valamennyi telephelyén

- a munkavállalók által a feladatok végrehajtása és a folyamatok működtetése során használt, vagy általuk kezelt információkra;
- az egyes munkavállalók által használt, vagy általuk tárolt valamennyi információkezelő eszközre, beleértve azok dokumentációját is;
- a CSAPI által beszerzett és az általa fenntartott (fejlesztett, vásárolt, bérelt vagy nem általa fenntartott kihelyezett tulajdonra) informatikai infrastruktúra elemekre és az azokon kezelt (nyilvántartott, továbbított, tárolt) információkra,
- a CSAPI üzleti folyamatai által kezelt (papír alapú nyomtatott, tárolt, archivált, selejtezett stb.) és szolgáltatott információkra.

Továbbá az IBSZ tárgyi hatálya kiterjed a Fővárosi Önkormányzat Csarnok és Piac Igazgatósága szervezetének érdekkörén belül használt, üzemeltetett és a CSAPI bármilyen üzleti folyamatával, vagy informatikai rendszerével kapcsolatba kerülő eszközre és azokon tárolt adatokra.

Az IBSZ hatályba lépésének időpontjában már üzemeltetett rendszer esetében egyedi eltérés az **Információbiztonsági vezető** jóváhagyásával, meghatározott, átmeneti időszakra megengedhető.

2.3 Területi hatály

A Fővárosi Önkormányzat Csarnok és Piac Igazgatósága felügyelete alá tartozó telephelyek.

2.4 Hatálybalépés

Jelen utasítás kihirdetésének napján lép hatályba. A kihirdetéssel egy időben hatályát veszti (k) a következő szabályzatok / utasítások:

- Informatikai szabályzat

3. FOGALOM MEGHATÁROZÁSOK ÉS RÖVIDÍTÉSEK

A jelen IBSZ alkalmazása szempontjából releváns és használatos fogalmakat és rövidítéseket a „Fogalom meghatározások és rövidítések" című 1. számú melléklet tartalmazza.

4. KAPCSOLÓDÓ BELSŐ ÉS KÜLSŐ DOKUMENTUMOK (JOGSZABÁLYOK, SZABVÁNYOK)

A jelen IBSZ alkalmazása szempontjából releváns és alkalmazandó szabályozó dokumentumokat, jogszabályokat, szabványokat stb., a „Kapcsolódó belső és külső dokumentumok (jogszabályok, szabványok)" című 2. számú melléklet tartalmazza.

5. A VEZETŐSÉG ELKÖTELEZETTSÉGE AZ INFORMÁCIÓBIZTONSÁG IRÁNT

A stratégia elve alapján jelen IBSZ jóváhagyásáért, kiadásáért és az abban foglaltak végrehajtásáért az **igazgató** a felelős.

Az **Információbiztonsági Vezető** (Lásd 7.2 fejezet) az Információbiztonsági Politikával összhangban meghatározza mérhető céljait, melyeket a vezetőségi átvizsgálás során következetesen nyomon követ.

A CSAPI folyamatosan biztosítja alkalmazottai oktatását az IBIR-ben megfogalmazott követelményekről, feladatokról, felelősségekről és jogosultságokról, munkakörökre lebontva. Gondoskodik alkalmazottai tájékoztatásáról a rendszerben történt változásokról, hogy minden alkalmazottja maximálisan meg tudjon felelni a megváltozott követelményeknek.

A vezetés gondoskodik az észlelt, információbiztonsággal kapcsolatos incidensek kezeléséről. Az IBIR-ben megfogalmazottak megsértése esetén, annak súlya és az okozott kár nagyságának megfelelő számonkérésről, illetve felelősségre vonásról.

Az IBIR szabályozásából adódó követelmények betartása és betartatása minden alkalmazott és a Fővárosi Önkormányzat Csarnok és Piac Igazgatósággal jogviszonyban álló külső partner joga és kötelezettsége.

Jelen IBSZ meghatározza a szervezeti egységek közötti feladat-, felelősség- és hatáskör megosztást, definiálja és bemutatja az információbiztonsági rendszereket, ill. azok működését. Felméri a rendszerek működtetéséhez kapcsolódó kockázatokat, és meghatározza azok kezelésének módját, továbbá az üzletmenet folytonosságának biztosítására intézkedési terveket határoz meg.

Jelen IBSZ szabályozó dokumentumként a belső szabályzatokat, törvényeket és kapcsolódó szabványokat veszi alapul, és ezzel összhangban alkalmazza a következő tevékenységeket:

- rögzíti a folyamatokat (Szabályzatokban), (figyelembe véve a szervezet működésének sajátosságait, a hatályos jogszabályokat, a felügyeleti szervek jelzéseit valamint az MSZ ISO/IEC 27001:2006 szabvány követelményeit), amelyekben egyértelmű felelősségeket és hatásköröket határoz meg,
- biztosítja az IBIR működtetéséhez és továbbfejlesztéséhez szükséges erőforrásokat,
- egyértelműen és kellő időben meghatározza és tisztázza az információkezelő rendszer elfogadási követelményeit,
- meghatározza az elvárt információbiztonság eléréséhez szükséges ellenőrzéseket, folyamatokat, szabályzatokat, erőforrásokat és képességeket illetve biztosítja ezeket,
- biztosítja a szolgáltatási folyamat, az ellenőrzési és vizsgálati eljárások és az alkalmazható dokumentáció, valamint a feljegyzések összhangját,
- folyamatosan fejleszti az ellenőrzési, a tesztelési és vizsgálati módszereket a külső és belső elvárásokhoz igazodóan.

5.1 Célok meghatározása és tervezése

Az Információbiztonsági Politikával összhangban az **Információbiztonsági Vezető** határozza az információbiztonságra vonatkozó célokat. A célok elérése érdekében:

- a célokat oly módon rögzíti, hogy azok teljesülése mérhető és ellenőrizhető legyen,
- a célok megvalósításához a vezetőség erőforrásokat, terveket – feladatokkal és felelősséggel -, kapcsolódó feladatokat, felelősöket és határidőket határoz meg,
- a célok elérését a határidők lejártakor az **Információbiztonsági Vezető** értékeli, és amennyiben szükséges a vezetőség további intézkedéseket rendel el.

Terveket kell készíteni abban az esetben is, ha egy jogszabályból, vagy egy szerződéses követelmény teljesítéséből, vagy belső fejlesztésből eredően az IBIR-től eltérő szabályozásokat kell alkalmazni. A tervezés során a szervezet felméri és biztosítja a célok eléréséhez / teljesítéséhez szükséges erőforrásokat.

A tervezéssel kell biztosítani, hogy szervezet fejlesztése, esetleges átalakítása során az IBIR aktuális és hatékony maradjon. A tervek elkészíttetése, a tervezéssel kapcsolatos tevékenységek összehangolása és koordinálása a felső vezetés feladata.

5.2 Kritikus sikertényezők

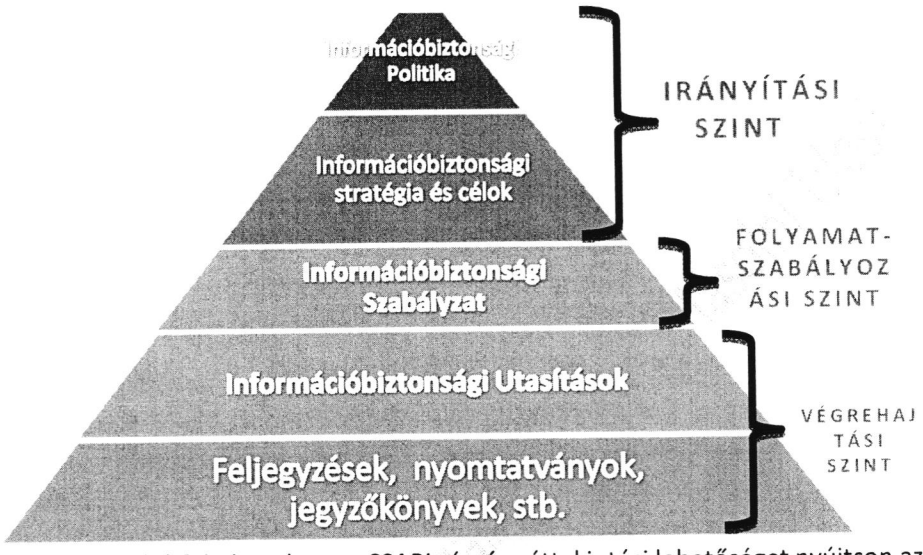
Az IBIR sikeres megvalósítása során nélkülözhetetlen alapfeltételek:

- információbiztonsági politikát, célokat és üzleti célokat tükröző tevékenységek végrehajtása és az azoknak ellentmondó tevékenységek teljes körű megszüntetése;
- látható / kézzelfogható és egyértelmű támogatás és elkötelezettség a **vezetőség minden szintjén**;
- az információbiztonsági követelmények továbbá a kockázatfelmérés és kockázatkezelés jó megértése és elsajátítása mind a **vezetőség** mind pedig az **információ felelősök** által;
- az információbiztonság eredményes (hatékony) kommunikációja a vezetőség, a munkavállalók és a szerződő partnerek között az **Információbiztonsági vezető** által;

- az információbiztonsági politika, továbbá a vonatkozó szabályzatok és a szükséges külső dokumentumok (szabványok, jogszabályok, stb.) elérhetővé tétele a vezetőség, a munkavállalók és a szerződő partnerek számára;
- az IBIR és annak tevékenységeihez szükséges erőforrások biztosítása;
- oktatás;
- eredményes információbiztonsági incidenskezelési folyamat kialakítása;
- olyan mérési rendszer bevezetése, amely segítségével az információbiztonság irányítás kiértékelhető, kontrollálható és a fejlesztési javaslatok visszacsatolhatóak

6. AZ IBIR SZABÁLYOZÁSI STRUKTÚRÁJA

A Fővárosi Önkormányzat Csarnok és Piac Igazgatóságánál a következőkben bemutatott szabályozási struktúra alkalmazandó az IBIR folyamatok irányítása és felügyelete érdekében:



A szabályozási struktúra (térkép) feladata, hogy a CSAPI részére áttekintési lehetőséget nyújtson az IBIR szabályozási szintjeiről, az egyes szabályzatokról és azok rövid tartalmáról.

Az IBIR célja a teljes körű, kockázatarányos védelem deklarálása, és érvényesítése az információbiztonság területén.

A célok (az, amit el szeretnénk érni), a stratégia (az, ahogyan ezeket a célokat elérjük), a politika (azok a szabályok, amelyeket a stratégia megvalósítása során be kell tartanunk), szabályzatok (a politika megvalósítása során alkalmazott módszerek), a vállalati szinttől a szervezet operatív szintjéig hierarchikus rendben épülnek fel, illetve kerültek meghatározásra a CSAPI számára. A szabályozó dokumentumok tükrözik a szervezeti követelményeket, és figyelembe veszik a szervezet esetleges korlátait. A kialakítás és működtetés során kiemelten fontos a vonatkozó dokumentumok, valamint a különböző szervezeti szintek közötti ellentmondásmentes összhang kialakítása és működtetése.

Az IBIR bevezetésének célját 6 fő lépés végrehajtásaként kell elérni a következők szerint:

- Fenyegetések azonosítása és a kockázatok értékelése
- Kockázat menedzsment (felmérés, értékelés, elemzés, kezelés)
- Érintettek bevonása a menedzsmenttől a felhasználókig
- Biztonsági tudatosítás és képzés
- Belső ellenőrzési eljárások kialakítása
- A rendszer folyamatos fejlesztése

Az információbiztonsági politika, célok és stratégia azt fogalmazzák meg, amit IBIR-től a biztonság vonatkozásában elvárunk. Az elvárásokat rendszerint természetes – az átlag felhasználó számára is érthető – nyelven fejezzük ki, azonban szükség lehet arra, hogy mindezeket formálisabb módon, egzaktabb nyelven is megfogalmazzuk.

6.1 Szabályozási struktúra ismertetése

Az előző oldalon bemutatott ábrán láthatóan a struktúra 3 funkcionális szintre, azon belül pedig további alszintekre tagozódik, melyek szerint a következő megkülönböztetést alkalmaztuk:

- Funkcionális szintek:
  - Irányítási:
    - Alszintek
      - Információbiztonsági Politika (IP)
      - Információbiztonsági Stratégia és Célok (ISC)
  - Folyamatszabályozási:
    - Alszintek
      - Információbiztonsági Szabályzat (IBSZ)
  - Végrehajtási:
    - Alszintek
      - Információbiztonsági Utasítások (IU)
      - Információbiztonsághoz kapcsolódó feljegyzések, jegyzőkönyvek, emlékeztetők, nyomtatványok stb.

Az információbiztonsági szabályozások egyes elemei és azok rövid bemutatása a következő:

- **Információbiztonsági Politika (IP)**: Az információbiztonság iránti vezetői elkötelezettséget deklaráló, a CSAPI általános szándékát és irányvonalát tartalmazó dokumentum, melyet a vezetés hagy jóvá. A CSAPI aktuális politikáját az Információbiztonsági Politika című dokumentum tartalmazza.

  A Politikának tartalmaznia kell a felső vezetőség elkötelezettségét és ki kell fejtenie, hogy a CSAPI hogyan közelíti meg az információbiztonság kezelését. A Politikát és az azokból levezetett biztonsági célokat, stratégiát úgy kell megfogalmazni, hogy azok a Fővárosi Önkormányzat Csarnok és Piac Igazgatóságán belül alapját képezzék a hatékony információbiztonságnak, továbbá támogassák a CSAPI üzletmenetét, és együttesen garantálják valamennyi ellenintézkedés ellentmondás mentességét, konzisztenciáját.
- **Információbiztonsági Stratégia és Célok:** Az Információbiztonsági Stratégia az információbiztonság rövid-, közép- és hosszú távú terve, melynek feladata az információ- és üzembiztonság növelése, az időben változó üzleti célok és az azokkal változó informatikai feladatok biztosítása. Célja az információ- és üzembiztonságnak az Információbiztonsági Politikában meghatározott szintre emelése, illetve az időben változó üzleti célokhoz folyamatosan illeszkedő információbiztonsági feladatok biztosítása. Az Információbiztonsági Célok az Információbiztonsági Stratégiából levezetett – általában éves szinten meghatározott – a vezetőség által jóváhagyott információbiztonsággal kapcsolatos célok és az azok alapján készített és elrendelt intézkedési tervek, melyek megfelelően elősegítik az IBIR folyamatos fejlesztését és az üzleti célok teljesülését. A konkrét információbiztonsági célokat általánosan a Vezetőségi átvizsgálások jegyzőkönyvében és a vezetői értekezletek emlékeztetőjében dokumentáljuk.
- **Információbiztonsági Szabályzat (IBSZ):** Az irányítási rendszer alapdokumentuma, összefoglalja az IBIR-t, és tartalmazza a folyamatok, tevékenységek szabályozását, vagy hivatkozik a szabályozásokra. Az Információbiztonsági szabályzatban leírtak betartása kötelező minden érdekelt fél számára, továbbá megállapításokat kell tartalmaznia a következőkre:

- az információbiztonság meghatározása, átfogó céljai, alkalmazási területe, a biztonság fontossága, mint az információ elosztását elősegítő mechanizmus;
- nyilatkozat a vezetőség szándékáról, amely támogatja az információbiztonság céljait és alapelveit a működési stratégiával és a célokkal összhangban;
- a szabályozási célok és intézkedések felállításának kerete, beleértve a kockázatfelmérés és kockázatkezelés felépítését;
- a biztonsági szabályzatok, alapelvek, szabványok és a szervezet számára speciális fontosságú megfelelési követelmények rövid magyarázata, belefoglalva:
  - a megfelelést a jogszabályi, szabályozási és szerződéses követelményeknek;
  - a biztonság képzési, oktatási és tudatossági követelményeit;
  - a működési folytonosság irányítását;
  - az információbiztonsági politika megsértésének következményeit.
- az átfogó és konkrét információbiztonsági irányítási felelősség meghatározása, beleértve az információbiztonsági incidensek jelentését;
- utalások olyan dokumentációra, amely az IK-t alátámaszthatja, pl. részletesebb biztonsági szabályzatok és eljárások egyes információs rendszerekre vagy biztonsági szabályok használókra, amelyeknek meg kell, hogy feleljenek.

- **Információbiztonsági Utasítások** (IU): Egyes részfolyamatok, tevékenységek részletes leírását, a kapcsolódó folyamatokat, feljegyzéseket, felelősöket rögzítő szabályozás.
- **Információbiztonsághoz kapcsolódó feljegyzések, jegyzőkönyvek, emlékeztetők, nyomtatványok** stb.: Az információbiztonsági követelmények teljesítését, teljesülését, megtörténtét igazoló dokumentumok.

A fenti dokumentumok esetén alapvető fontosságú azok ellentmondás mentességének biztosítása. A dokumentumokat a vezetőség hagyja jóvá, teszi közzé és biztosítja annak kommunikálását minden alkalmazottal és az érintett külső felekkel. A dokumentumokat olyan formában kell kommunikálni az egész szervezetben a felhasználók számára, amely az érintettek számára hozzáférhető és érthető.

6.2 Kötelező és rendkívüli felülvizsgálat (revízió) időpontja

A CSAPI információbiztonsági szabályzatai rendszeres felülvizsgálatot és aktualizálást igényelnek, ezért

- bármely, a szabályzatokat érintő új jogszabály, vagy kapcsolódó jogszabály-módosítás hatályba lépését követően,
- továbbá az informatikai architektúra jelentős változása vagy új fenyegetettség (pl. kockázati szint jelentős változása) megjelenése után

haladéktalanul, de legalább évente ellenőrizni kell, tekintettel a legutolsó ellenőrzés óta bekövetkezett változásokra.

Rendkívüli felülvizsgálatot kell végrehajtani minden olyan esetben, ha

- új munkafolyamatok, szervezeti egységek, szolgáltatások jelennek meg;
- új informatikai technológiák kerülnek bevezetésre, vagy szűnnek meg;
- új, lényeges kockázatok válnak ismertté;
- olyan biztonsági események következnek be, amelyek az információk osztályozása szerint legalább „Bizalmas" minősítéssel rendelkező információkat érintenek.
- a CSAPI igényei, céljai megváltoznak vagy bármilyen más okból az IBSZ nem tölti be szándékolt szerepét.

Az információbiztonsági szabályzatok karbantartásának kezdeményezése és a módosítási javaslatok készítése az **információbiztonsági vezető** feladata. Szükség esetén az összegyűjtött módosítási javaslatokat mérlegelés és a szükséges egyeztetések után lehet hatályba léptetni.

6.3 A szabályozások készítése, jóváhagyása, módosítása és kezelése

A szabályozások készítésével, jóváhagyásával, módosításával és kezelésével kapcsolatos eljárásokra a Fővárosi Önkormányzat Csarnok és Piac Igazgatósága saját szabályozásai az irányadóak a hatályos SZMSZ szerint.

7. AZ INFORMÁCIÓBIZTONSÁG SZERVEZETI STRUKTÚRÁJA, A RÉSZTVEVŐK FELADATAI, JOGAI ÉS HATÁSKÖREI

Az IBIR és a rendszerkörnyezet biztonsága a szervezeti egységek, a biztonság meghatározó területein dolgozó szakemberek, valamint minden munkatárs — az SZMSZ-ekben, illetve a munkaköri leírásokban meghatározott feladat-, jog-, és felelősségi körnek megfelelően — szabályozott tevékenységén keresztül valósul meg.

Az információbiztonságnak a jogszabályokban, a szerződésekben és megállapodásokban, valamint az ügyviteli és a jelen szabályzatban előírt elvárások megvalósításáért az **információbiztonsági vezető** felelős az alábbiak szerint:

- az alárendelt szervezet biztonságáért, ezen belül különösen a szervezeti és személyi feltételek biztosításáért és az ellenőrzés megtételéért,
- a munkaköri feladatok meghatározásakor elkülöníteni egymástól a végrehajtási és ellenőrzési funkciókat. Az információbiztonság szabályozási rendszerének egyik alapvető eszköze a 4 szem elve annak érdekében, hogy megakadályozzuk a felelős tevékenységek és az ellenőrzésükhöz szükséges jogosultságok összeférhetetlen alkalmazását.
- a munkaköri leírások napra készen tartása abból a szempontból, hogy az itt felsorolt feladatok, felelősségek harmonizáljanak a munkaköri leírásban szereplőkkel.

Az IBIR bevezetéséért, működtetéséért és a kapcsolódó szabályozások betartatásáért az CSAPI **információbiztonsági vezetője** a felelős.

Abban az esetben, ha nem valósítható meg az informatikai biztonsággal kapcsolatos tevékenységek előírás szerinti végrehajtása, az információbiztonsági vezető felelőssége az érintett tevékenységek tekintetében a biztonsági naplózás és ellenőrzés végrehajtása, illetve végrehajtatása.

7.1 Információbiztonsági Team

A vezetőség annak érdekében, hogy az információbiztonsággal kapcsolatos összes tevékenységet aktívan támogassa a CSAPI teljes szervezetében, létrehozta az **Információbiztonsági Team**. Az információ biztonsággal kapcsolatos intézkedések hatékony felügyeletéhez és koordinálásához a Team évente megbeszéléseket tart. Sürgős esetben az **információbiztonsági vezető** azonnali megbeszélést hívhat össze. Információbiztonsági incidensek bekövetkezésekor a résztvevők bármelyike kezdeményezheti rendkívüli megbeszélés megtartását is.

A Team résztvevői a következők:

- **igazgató,**
- **információbiztonsági vezető,**
- Egyéb meghívottak lehetnek a témától függően:
  - **Meghívott Információ Felelősök**
  - **Belső Ellenőr**
  - **Meghívott szakértők (szükség esetén külső szakértők is).**

A Team főbb témái:

- a CSAPI információbiztonságára vonatkozó konkrét szerepek, feladatok és hatáskörök,
- a szervezeti egységek információbiztonsági szempontból való gazdasági, technikai, információs és személyi támogatása,

- a konkrét módszerek és folyamatok kialakítása / kialakíttatása, különösen a kockázatelemzés, és információ osztályozás,
- a kockázatok felmérése és a kockázatelemzések aktualizálása,
- az információbiztonsági kockázatok és ezen kockázatok csökkentését célzó intézkedések meghatározása,
- a folyamatokban és az infrastruktúrában történt vagy tervezett változások hatása az IBIRre,
- a stratégiai fejlesztések, beruházások információbiztonsági specifikációinak (beszerzési előterjesztések) elfogadása;
- az alkalmazandó külső szakértők, tanácsadók - információbiztonsági területen - kiválasztási folyamata és annak támogatása, aktuális állapota,
- az incidensek, események vagy lehetséges események, gyengeségek értékelése, elemzése,
- a szükséges intézkedések meghatározása és bevezetése,
- az információbiztonsági célok nyomon követése, értékelése,
- az információbiztonsági tudatosság fenntartásához szükséges intézkedések átvizsgálása,
- az IBSZ és az ehhez kapcsolódó egyéb dokumentációk éves felülvizsgálata, szükség szerint módosítása és elfogadásra előterjesztése

A megbeszélésről, a napirendről és a hozott intézkedésekről az **információbiztonsági vezető** *jegyzőkönyvet* készít, melyet minden résztvevőnek és rajtuk kívül az érintetteknek eljuttat.

7.2 Információbiztonsági vezető

A Fővárosi Önkormányzat Csarnok és Piac Igazgatóságnál a vezetők biztonsággal összefüggő tevékenységét az **Információbiztonsági vezető** támogatja, aki egyben az igazgató közvetlen alárendeltje. Ő felel a szervezetben előforduló minden információbiztonsághoz kapcsolódó kérdésért. Részt vesz a biztonsággal kapcsolatos vezetői döntések előkészítésében, kivizsgálja az informatikai rendkívüli eseményeket, elvégzi a rendszeres biztonsági ellenőrzéseket, és hatáskörében intézkedik, vagy javaslatot tesz a hibák kijavítására. Munkája során szorosan együttműködik a biztonság megvalósításában kulcsszerepet játszó üzleti területekkel, informatikai és egyéb szakemberekkel

Fő feladatai:

- Az információbiztonsági követelmények érvényesítése, az alábbi területeken:
  - Részvétel az információbiztonsági s és ellenőrzési rendszerek kialakításában, igazodva az Fővárosi Önkormányzat Csarnok és Piac Igazgatósága, a jogszabályok és az terület legjobb gyakorlatához.
  - A fejlesztések és beszerzések során a feltárt kockázatoknak megfelelően véleményezés, ellenőrzés és javaslattétel.
  - A kiválasztott védelmi intézkedések véleményezése, ellenőrzése és javaslattétel.
  - Az implementált védelmi intézkedések alkalmazásának ellenőrzése.
- Informatikai biztonsági oktatásokon, képzéseken való részvétel.
- Gondoskodik az ellenőrzés módszereinek és rendszerének kialakításáról és működtetéséről. Jóváhagyásra előkészíti az éves Információbiztonsági belső audit tervet (lásd 18. fejezetet).
- Az üzleti oldal felelőseinek támogatása és szakmai irányítása
  - az információk osztályozásában,
  - az információbiztonsági kockázatértékelés, kockázatelemzés és kockázatkezelés végrehajtásában és értelmezésében az adott szakterületen,

  - az információbiztonság vonatkozásában az üzleti oldal igényeinek megfogalmazásában és specifikálásában.
- A CSAPI informatikai rendszerének olyan mértékű megismerése, hogy annak szereplőit hatékonyan ellenőrizni tudja.
- Összehangolja a biztonságot meghatározó, befolyásoló területek tevékenységét az információbiztonság érdekében.
- Részt vesz az információbiztonság szempontjából fontosnak tartott munkakörök betöltési szabályainak, feltételeinek meghatározásában.
- Elkészíti és karbantartja az IT Katasztrófa Elhárítási Tervet.
- Felméri a szervezet működéséből eredő, az információbiztonsággal összefüggő veszélyforrásokat.
- Információbiztonsági szempontból ellenőrzi az informatikai rendszer szereplőinek tevékenységét.
- Részt vesz a biztonsági követelmények és előírások betartásának ellenőrzésében.
- Rendszeresen, de legalább havonta jelent az igazgatónak és az érintett területek vezetőinek minden információbiztonságot érintő eseményt, hiányosságot.
- Szakmai szempontból közvetlenül irányítja a CSAPI információbiztonsági tevékenységét.
- Szakmai szempontból irányítja az információbiztonságra vonatkozó oktatást.
- Az informatikai rendkívüli eseményeket, az esetleges rossz szándékú hozzáférési kísérletet, illetéktelen adatfelhasználást, visszaélést kivizsgálja. Javaslatot tesz a szervezet vezetőjének a további intézkedésekre, a felelősségre vonásra.
- Ellenőrzi az új információtechnológiai helyiség tervezése és kialakítása során a jelen szabályzatban megfogalmazott, a helyiségek fizikai paramétereire vonatkozó követelmények kielégítését, és a meglevő helyiségek paramétereinek értékét.
- Ellenőrzi az IT helyiségekbe való beléptetési eljárást, az IT helyiségbe belépő személyek körének jogosságát.
  - Ellenőrzi a beléptető rendszer kódjának szükség szerinti cseréjét.
  - Ellenőrzi az IT helyiségekhez tartozó kulcsdoboz használatát.
  - Ellenőrzi a riasztórendszer kódjainak használatát.
- Ellenőrzi / ellenőrizteti a fejlesztő rendszerek elkülönítésének megfelelőségét az éles rendszertől.
- Felügyeli az IT helyiségeket, eszközöket és infrastruktúrát érintő karbantartási terveket.
- Felügyeli a beruházásokat, a fejlesztéseket, és az üzemvitelt Információbiztonsági szempontból, illetve javaslatot tesz rájuk.
- Az új eszközök és szoftverek tesztelésére ajánlásokat fogalmaz meg.
- Összeveti az eszközök törzslapjának tartalmát az eszköz tényleges állapotával.
- Szúrópróba-szerűen ellenőrzi
  - az egyes felhasználói gépek hardverkonfigurációját és a telepített szoftvereket összeveti a felhasználónak engedélyezett szoftverlistával,
  - azt, hogy a rendszerben aktuálisan beállított felhasználói jogosultságok megegyeznek-e a jóváhagyott jogosultságokkal,
  - azt, hogy a javításra kiszállított eszközökön adat ne kerüljön ki,
  - az adathordozók selejtezését.
- Ellenőrzi a kritikus rendszerek eseménynaplóinak működését és információtartalmát.
- Ellenőrzi a víruskereső rendszer naprakész működését, a rendszeres ellenőrzések végrehajtását és a teljes körűséget.
- Ellenőrzi a dokumentációk meglétét és megfelelőségét (teljes körű, aktuális).

- Ellenőrzi, hogy a vonatkozó Információbiztonsági követelményeket a rendszerek fejlesztési és az alkalmazási dokumentációiban is megjelenítik-e.
- Ellátja az információbiztonsággal összefüggő vállalkozók információbiztonsági szempontból való koordinációját (oktatás, rájuk vonatkozó szabályozások átadása / közlése, stb.)

Jogai:

- Amennyiben új fenyegetéseket észlel, vagy hatékonyabb biztonsági intézkedések megtételét tartja szükségesnek, kezdeményezi a védelem erősítését.
- Az adott szakterületek vezetőivel egyeztetve meghatározza az egyes feladatkörökhöz tartozóan az információbiztonsággal kapcsolatosan elsajátítandó ismeretek körét, és ellenőrzi az elsajátítás tényét.
- Javaslatot tesz az információbiztonságot erősítő továbbképzésre.
- Jelen szabályzatot és annak kiegészítéseit évente felülvizsgálja, és
    - a gyakorlati tapasztalatok,
    - az előfordult informatikai rendkívüli események,
    - a jogszabályi környezet változásai,
    - a technikai fejlődés,
    - az alkalmazott új informatikai eszközök,
    - az új, a változó és a megszűnő programrendszerek,
    - a fejlesztési és védelmi eljárások, stb.

  miatt szükségessé váló módosításokra javaslatot tesz.
- a CSAPI teljes területén az információbiztonság vonatkozásában ellenőrzési, véleményezési, javaslattételi, kezdeményezési, betekintési és hozzáférési jog illeti meg.

Az Információbiztonsági vezető jogait és kötelességeit a szabályzat hatálya alá eső területeken gyakorolja.

7.3 Információ-felelős

Az **Információ-felelősnek** a vezetőség által jóváhagyott felelőssége van az információk biztonságáért az általa felügyelt területen. Az információ-felelőst minden esetben a felettes vezetője jelöli ki az adott üzleti folyamatok alapján. Az információ felelősök az egyes szervezeti egységek vezetői.

Konkrét feladatok és felelősségek:

- egyértelműen beazonosítja és nyilvántartja a hozzá tartozó üzleti folyamatok kapcsán kezelendő (kapott, küldött, feldolgozott, továbbított stb.) információkat megjelenési formájuk szerint külön csoportokat azonosítva (az információk lehetnek: elektronikus, kézzel fogható (pl.: papír) és kézzel nem fogható (pl.: szóban elhangzó, szellemi tudás),
- egyértelműen beazonosítja és nyilvántartja az információk előfordulási és tárolási helyeit és azok megőrzési idejét (online és offline),
- meghatározza az információk osztályozását,
- végrehajtja az információk kockázatértékelését
    - kockázatok azonosítása sértetlenség, rendelkezésre állás és bizalmasság szempontjából,
    - a lehetséges üzleti hatások elemzése,
    - jelenlegi kontroll intézkedések azonosítása, hatékonyságának értékelése az Információbiztonsági vezető támogatása mellett,

- a kockázatértékelés igazgatói konszolidációjának támogatása,
- a kockázatértékelés kommunikációja, stb.

- meghatározza, hogy kik férhetnek hozzá az információkhoz és milyen jogosultságokkal. A szervezeti egységek vezetői felelősek a beosztottjaként dolgozó felhasználók számára kért jogosultságok megfelelőségéért, és a megfelelőség hiányából eredő károkért.
- meghatározza a tolerálható szolgáltatás kiesési időtartamokat.

A fenti feladatokat a munkaköri leírásban is rögzíteni szükséges.

7.4 Felhasználók

A felhasználók általános feladata és felelőssége:

- A felhasználó köteles az általa használt informatikai eszköz épségét, annak működőképes állapotát megőrizni. Bármilyen állapot-, vagy működésbeli rendellenességet tapasztal, azt az illetékeseknek jeleznie kell.
- Minden felhasználó, felelős az általa elkövetett szabálytalanságért, valamint a keletkező károkért és hátrányért.
- Az **információbiztonsági vezető** és a **rendszeradminisztrátorok** a saját azonosítójukkal és jelszavukkal jogosultak a felhasználók munkaállomásához hozzáférni a felhasználók távolléte esetén is, ha beállítási, karbantartási, ellenőrzési, szoftvertelepítési műveleteket hajtanak végre. A hozzáféréshez a felhasználók előzetes – akár szóbeli is – hozzájárulása szükséges. Az előbbi hozzájárulás információbiztonsági esemény / incidens esetén nem szükséges!
- Hibajavítás esetén a felhasználó a HelpDesk-en keresztül jelzi a meghibásodást és az üzemeltetés ez alapján kezdi meg a hiba elhárítását.

7.4.1 Kulcs felhasználó

A kulcs felhasználó jogosultságai a feladatkörtől és szakmai területtől függően meghaladják a hagyományos felhasználók jogosultságait:

- A kulcs felhasználó egy adott alkalmazást, vagy szegregált felépítésű program esetén annak egy bizonyos modulját a többi felhasználónál mélyebben ismeri, annyira, hogy újabb igények megjelenésekor párbeszédet tud folytatni az rendszeradminisztrátorral, alkalmazás-gazdával, át tudja venni a fejlesztés eredményét, be tudja azonosítani a hibás működést (meg tudja különböztetni a felhasználói hibát a szoftver hibától), teszteléseket végez és ehhez magasabb szintű jogosultságokat kell biztosítani számára.

7.4.2 Minden felhasználó köteles

- A vonatkozó informatikai-szakmai és a Szabályzatban megfogalmazott szabályokat megismerni és betartani, illetve ezek betartásában az informatikai rendszer használatát irányító személyekkel együttműködni.
- A számára szervezett Információbiztonsági oktatáson részt venni, az ismeretanyag elsajátításáról számot adni.
- A számára rendelkezésre bocsátott számítástechnikai eszközöket megóvni.
- Belépési jelszavát (jelszavait) az előírt időben változtatni.
- Az észlelt rendellenességekről tájékoztatni a közvetlen felettesét és bejelenteni az incidenst a HelpDesk rendszerben.

7.4.3 Minden felhasználónak TILOS

- A mindenkor hatályos, vonatkozó jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (pl. rágalmazó email), tiltott haszonszerzésre irányuló tevékenység (pl. netes szerencsejáték), szerzői jogok megsértése (pl. szoftver vagy egyéb jogvédett szerzői művek [zene, film, stb.] nem jogszerű terjesztése);
- A CSAPI üzleti adatainak harmadik személy számára való továbbítása, kivéve a jogszabályon vagy szerződésen alapuló adatszolgáltatást. A hálózatba kapcsolt rendszereket az üzemeltető(k)nek a mindenkori technikai lehetőségek szerint úgy kell konfigurálni(uk), hogy az ilyen használatot megakadályozzák (pl. levelezőszerver, átjáró);
- Mások vallási, etnikai, politikai, szexuális vagy egyéb hovatartozását sértő, zaklató tevékenység (pl. ilyen jellegű web-lapok böngészése, anyagok közzététele, továbbítása);
- Mások munkájának indokolatlan és túlzott mértékű zavarása vagy akadályozása (pl. kéretlen levelek, hirdetések, lánclevelek);
- Az informatikai hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység (pl. levélbombák, hálózati játékok, kéretlen reklámok);
- Az informatikai hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások – akár tesztelés céljából történő – szisztematikus próbálgatása (pl. TCP port scan);
- A CSAPI erőforrásainak, a hálózaton elérhető adatoknak illetéktelen hozzáférésére, módosítására, megrongálására, megsemmisítésére vagy bármely szándékos károkozásra irányuló tevékenység;
- A CSAPI profiljától, érdekeitől, gazdasági folyamataitól eltérő hírcsoportokba, levelezési listákra, a csoport/lista témájába nem vágó üzenet küldése;
- A munkaállomására telepített aktív vírusvédelem kikapcsolása.
- Belépési jelszavát (jelszavait) másnak átadni (még helyettesítés esetén sem).
- Az informatikai hálózat fizikai megbontása, a számítástechnikai eszközök lecsatlakoztatása, áthelyezése illetve nem CSAPI tulajdonú számítástechnikai eszköz rácsatlakoztatása a hálózatra az informatikai rendszert üzemeltetők tudta és engedélye nélkül.
- Tilos a felhasználó részéről bármilyen illetéktelen beavatkozás, ami a berendezés műszaki állapotában, működésében valamilyen változást okozhat. Ide értendő a számítástechnikai eszközökből összeállított konfigurációk szétszedése, megbontása, átalakítása, vagy bármilyen szoftver telepítése.
- Bármilyen szoftver installálása, Internetről való letöltése, külső adathordozóról merevlemezre való másolása a **rendszeradminisztrátor** engedélye nélkül.
- Modem beszerelése és használata.

7.4.4 Felhasználói felelősségek

A CSAPI tulajdonában lévő informatikai eszközökre vonatkozó szabályok maradéktalan betartásáért a **felhasználók** munkajogi felelősséggel tartoznak.

Felhasználó csak a számára kijelölt, és a munkaköri feladatainak elvégzéséhez biztosított munkaállomásokon dolgozhat. Amennyiben a munkaállomás használatát ideiglenesen átengedi más felhasználó számára, köteles kijelentkezni, az átengedett munkaállomás épségéért mindkét felhasználó felelősséggel tartozik.

Felhasználóknak tilos a meghibásodott gépen tovább dolgozni, a hiba elhárítását önállóan megkísérelni. A munkaállomás meghibásodását a **felhasználó** haladéktalanul jelezni köteles a szervezeti egység vezetőjének és a HelpDesk-nek.

A felhasználónak a számítógépet, a monitort illetve a nyomtatókat a munkavégzés végén a programokból való előírás szerinti kilépési procedúra végrehajtása után áramtalanítania kell. A munkaállomás és monitor kikapcsolásáért a felhasználó, az irodákban elhelyezett hálózati nyomtatókért a szervezeti egység vezető által kijelölt személy a felelős.

7.4.4.1 Felügyelet nélkül hagyott információk és információkezelő eszközök

Az informatikai erőforrások informatikai biztonságát akkor is fenn kell tartani, amikor azok felügyelet nélkül vannak. Ezért a **felhasználóknak** a következő védelmi intézkedéseket kell alkalmazniuk a felügyelet nélkül hagyott munkaállomásokon keresztül történő rosszindulatú belépések, megtévesztést szolgáló tevékenységek, az adat- és konfigurációmódosítás, a hamis e-mailek, a károkozás megelőzése, stb. érdekében:

- a magára hagyott munkaállomást mindig zárolni kell úgy, hogy a zárolás csak az arra jogosult által legyen feloldható;
- jelszóval védett képernyővédőt kell alkalmazni 15 perces inaktív idő eltelte után (kivéve a speciális célszámítógépek esetén, pl.: diszpécser);
- a munkaállomásokon a meghatározott idő után automatikusan aktiválódó képernyővédő beállításáról az **IT szolgáltató** gondoskodik.

Az irodahelyiségekben tárolt informatikai eszközök és papír alapú adathordozók biztonsága érdekében a **felhasználóknak**

- tilos az irodai helyiségben külsős személyt felügyelet nélkül hagyniuk;
- a lehetőségekhez mérten a helyiséget be kell zárniuk, ha a helyiségben más nem tartózkodik;
- a zárt helyiségek kulcsát tilos a zárban hagyni,
- be kell tartaniuk a „Tiszta asztal, tiszta képernyő - politikát".

7.4.4.2 Tiszta asztal, tiszta képernyő - politika

A **munkavállalók** kötelesek környezetükben rendet tartani.

A politika szemléletmódját követve az íróasztalokon csak azok az iratok lehetnek elől munkaidőben, amellyel éppen dolgoznak. Azon iratokat, amelyek aktuálisan a folyamatban lévő munkájukhoz nem szükségesek, rendszerezetten, az azok tárolására kijelölt helyen kell tárolni. Munkaidőn kívül „Bizalmas" vagy „Bizalmas" információk az asztalokon nem lehetnek elől, azokat a munka befejeztével mindig a kijelölt helyre kell elhelyezni.

A **munkavállalók** által használt számítógépek monitorjain csak olyan ikonok / dokumentumok / linkek stb. legyenek elhelyezve (kirakva), melyek munkája elvégzéséhez szükségesek.

8. INFORMÁCIÓS VAGYONLELTÁR ELKÉSZÍTÉSE, OSZTÁLYOZÁS, JELÖLÉS ÉS KOCKÁZAT ÉRTÉKELÉS

A CSAPI célja, hogy egyértelműen beazonosítsa és nyilvántartsa az üzleti folyamatai kapcsán kezelendő (kapott, küldött, feldolgozott, továbbított stb.) információkat és az információkezelő eszközöket.

Jelen szabályozás célja, hogy az információs vagyonleltár alapján végrehajtott kockázatértékelés segítségével **megfelelő** és **arányos biztonsági intézkedéseket** tudjunk **meghatározni**, **bevezetni** és hatékonyan **működtetni** annak érdekében, hogy **védjük** információs **vagyontárgyainkat** és **bizalmat keltsünk** érdekelt feleinkben.

A megfelelő biztonsági intézkedések meghatározásának és ez által a hatékony védelem kialakításának első és legfontosabb lépése, a CSAPI információs vagyontárgyainak számbavétele majd a számbavétel alapján az információs vagyonleltár elkészítése.

Az információs vagyonleltár kapcsolódhat egyéb más nyilvántartásokhoz, amelyekkel számos közös eleme lehet, ugyanakkor az információs vagyonleltárnak nem célja, hogy más számviteli, vagy jogszabály által előírt nyilvántartásokat helyettesítsen.

Az információs vagyon felmérésének első lépéseként, meg kell határoznunk a CSAPI információs vagyontárgyait és azok felelőseit. Az információs vagyonleltárba csak azokat a vagyontárgyakat kell felvenni, amelyek az információbiztonság szempontjából relevánsak. A vagyontárgyak meghatározásának kiindulási pontja minden esetben a CSAPI által azonosított üzleti folyamatok. Ezzel biztosítható, hogy csak és kizárólag olyan releváns és védendő vagyontárgyakat azonosítsunk be, amelyek a CSAPI üzleti folyamatainak **teljesítményét**, **sikerét** és az **érdekelt felek bizalmát befolyásolja**.

Az információs vagyontárgyak felelőse **felelős** azért, hogy

- a vagyontárgyak meghatározásra kerüljenek,
- a vagyontárgyak csoportosításra kerüljenek,
- a vagyontárgyak attribútumai meghatározásra kerüljenek,
- a vagyontárgyakat osztályozza bizalmasságuk szerint,
- a vagyontárgyak hozzáférését engedélyezze,
- a vagyontárgyakhoz való hozzáférés szabályozását átvizsgálja,
- a vagyontárgyakat rendszeres felülvizsgálja és karbantartsa.

8.1 Információs vagyontárgyak meghatározása és a vagyonleltár elkészítése

A vagyontárgyakat alapvetően két fő csoportba soroltuk annak érdekében, hogy különválasszuk azokat **funkciójuk** és **alkalmazásuk** szerint. Az így alkotott két fő csoport:

- **Információk:** Mindazon információs vagyontárgyak (információk, adatok, adatbázisok stb.), amelyek az egyes üzleti folyamatok során felhasználásra kerülnek, vagy azokkal az egyes munkatársak feladatot hajtanak végre.
- **Információt kezelő eszközök:** Mindazon információfeldolgozással összefüggő vagyontárgyak (alkalmazások, szerverek, számítógépek, védelmi eszközök stb.), amelyek által biztosítható az információk kezelése, feldolgozása és a velük folytatott folyamatok végrehajtása.

Az előzőekben rögzített elvek alapján a folyamat első lépéseként az **igazgató** kijelöli az **információ felelősöket** akik felelősök lesznek a későbbi feladatok végrehajtásáért. Az információ felelősök kijelölését úgy kell végrehajtani, hogy annak során teljes körűen lefedésre kerüljenek a CSAPI által működtetett üzleti folyamatok.

Az információ felelősök részletes feladatait és felelősségeit az adott munkakörhöz tartozó munkaköri leírásban is rögzíteni szükséges.

8.2 Információs vagyontárgyak csoportosítása

Az IBIR hatékony működtetéséhez az információs vagyonleltárnak a következő fő kritériumokat kell teljesítenie:

- az információbiztonság szempontjából teljes körű és releváns legyen,
- hatékonyan elvégezhető legyen a vagyontárgyak osztályba sorolása és a kockázatértékelés,
- a vagyonleltár használata ismert és rendszeresen alkalmazott legyen az **információ felelős** által.

E szempontokat figyelembe véve állítjuk össze a vagyonleltárt. A kockázatelemzés hatékonyan csak abban az esetben végezhető el, ha bizonyos vagyontárgyak vonatkozásában **vagyontárgy-csoportokat képzünk a funkcionálisan és logikusan összekapcsolható vagyontárgyakból**. A teljességet úgy biztosítjuk, hogy egyértelművé tesszük, milyen vagyontárgyak tartoznak egy adott csoportba.

8.2.1 Információk összegyűjtése és csoportosítása

Az információkat az **információ felelős** gyűjti össze a hozzá tartozó üzleti folyamatok alapján. Az információk összegyűjtésével párhuzamosan az információ felelősnek egyben csoportosítania is kell az adott információkat azok megjelenési formája szerint, melyek a következők lehetnek:

- **Elektronikus információk** (pl.: az adott folyamat kapcsán értelmezett pénzügyi, kereskedelmi, műszaki stb. információt tartalmazó adatok és adatbázisok)
- **Kézzel fogható fizikai információk** (az adott folyamat kapcsán értelmezett pénzügyi, kereskedelmi, műszaki stb. nyomtatott jellegű információ pl.: szerződés, számla, eljárásrend, levél, fax, stb.)
- **Kézzel nem megfogható információk** (pl.: az adott üzleti folyamat maga, tudás, üzleti kapcsolat, felhalmozott tapasztalat és általános know-how-k, a vállalati image / brand / kereskedelmi hírnév / ügyfél bizalom, versenyelőny, etika, szóbeli utasítások, stb..

Törekedni kell arra, hogy az információk ne legyenek túl nagyok (általánosítás veszélye), vagy túl kicsik (elaprózás, nehéz nyomon követhetőség).

8.2.2 A vagyontárgyak attribútumai

A vagyontárgyak azonosítását és összegyűjtését követően - a vagyonleltár feltöltésével párhuzamosan - kell azonosítani és rögzíteni az egyes vagyontárgyak attribútumait a következők szerint:

- **Információk esetén**
  - **Információ** [Az adott információ rövid egyértelmű megnevezése.]
  - **Információ leírása** [Az adott információ rövid, tömör de egyértelmű leírása, amely alapján az információ felelős és az adott üzleti folyamatban résztvevő munkatársak értelmezni és beazonosítani tudják azt.]
  - **Információ csoport** [Besorolásait lásd az 8.3.1. fejezet pontban]

- **Utolsó módosítás dátuma** [Azon dátum rögzítése, amikor az információ felelős az utolsó módosítást végrehajtotta az adott információs sor kapcsán]
- **Információ felelős beazonosítása**
- **Kapcsolódó alkalmazás** [Azon alkalmazások felsorolása, melyek az adott információ feldolgozásában / kezelésében részt vesznek]
- **Megőrzési idő (on-line)** [Az adott információ megőrzési ideje]
- **Megőrzési idő (off-line)** [Az adott információ archiválást követő megőrzési ideje]

- **Információt kezelő eszközök esetén**
  - **Egyedi azonosító** [Az adott információt kezelő eszköz egyedi azonosítója, amely alapján a CSAPI-n belül egyértelműen azonosítható]
  - **Szolgáltatás típusa** [Üzleti / belső]
  - **Alkalmazások (szoftverek)**
  - **Információt kezelő eszköz leírás** [Az adott információt kezelő eszköz rövid, tömör de egyértelmű leírása, amely alapján az információ felelős és az adott üzleti folyamatban résztvevő munkatársak értelmezni és beazonosítani tudják azt.]
  - **Operációs rendszer**
  - **Virtuális környezet**
  - **Hardver**
  - **Hardver fizikai helye**
  - **Kapcsolódó informatikai szolgáltatás**
  - **Információt kezelő eszközért felelős**

8.3 Információ osztályozás

Az információs vagyonleltár rendelkezésre állása után az információkat osztályozni kell a megfelelő kezelés és védelem érdekében. Az információ osztályozás célja, hogy

- meghatározza az információ osztályokat bizalmasság és rendelkezésre állás szerint,
- és meghatározza az információk védelmének fő szabályait.

8.3.1 Bizalmasság szerinti osztályozás

Az információk bizalmassága szempontjából a CSAPI a következő négy szintet határozza meg:

Bizalmassági szint	Meghatározás
Nyilvános	A CSAPI által a nyilvánosság számára készült információk illetve azok az információk, amelyek közzététele nincs semmilyen káros hatással a CSAPI-ra.
Belső	Azok a CSAPI által előállított illetve kezelt információk, amelyek belső használatra készültek. Ezen információk illetéktelen kézbe kerülve sérthetik a CSAPInak érdekeit. Az információk külső felek részére történő kiadása csak a közvetlen vezető jóváhagyását követően engedélyezett.
Bizalmas	Azok a CSAPI által előállított illetve kezelt információk, amelyek belső használatra készültek és a CSAPI területéről kikerülve jelentősen vagy súlyosan sérthetik a CSAPI érdekeit. Az információk csak korlátozott, jól meghatározott csoportok illetve egyének számára hozzáférhetőek. A **személyes** információkat (munkaügyi-, orvosi információk, egyéb HR adatok) **bizalmas** osztályba kell sorolni.

8.3.2 Rendelkezésre állás szerinti osztályozás

A rendelkezésre állás az információs vagyontárgy azon tulajdonsága, amely alapján a feljogosított személy a feljogosításban meghatározott kereteken belül az **információhoz hozzáfér**, azon műveleteket képes elvégezni. A rendelkezésre állás 5 különböző szintjét határozzuk meg, melyekben az osztályozást végre kell hajtani:

Osztály	1.szint	2.szint	3.szint	4.szint	5.szint
Maximális megengedett kiesés, eseményenként	5 nap	3 nap	1 nap	8 óra	4 óra
Mely napokon hozzáférhető	hétfő-péntek (5/7)	hétfő-péntek (5/7)	hétfő-péntek (5/7)	Minden nap (7/7)	Minden nap (7/7)
Milyen órákban	7:00-19:00	7:00-19:00	7:00-19:00	24 óra	24 óra
Elvárt rendelkezésre állás	92%	96%	98%	99,4%	99,8%

Az osztályozás során meg kell határozni azt a legkisebb rendelkezésre állási szintet, illetve legnagyobb kiesését, amelyet az egyes információs vagyonelemek hozzáférése, kezelése során **még el lehet fogadni jelentősebb üzleti veszteség nélkül**.

A „Maximális megengedett kiesés" az egy eseményhez tartozó **leghosszabb kiesést** jelenti, amely még jelentős üzleti veszteség nélkül elviselhető. Kényelmetlenség, kisebb mértékű veszteség megengedhető.

Az osztályozás során arra kell törekedni, hogy az információs vagyonelemeket a lehető legalacsonyabb szintre soroljuk, mert a magasabb rendelkezésre állás biztosítása jelentős többlet költséget jelent, ezért csak indokolt esetben alkalmazható.

8.4 Információ jelölés és kezelés

Az alkalmazandó információ védelmi szabályok a következő táblázat szerint leírják a tevékenységeket az információ osztálya szerint annak életciklusa alatt.

A táblázat a minimálisan alkalmazandó szabályokat tartalmazza. Az információjelölési szabályok egyaránt vonatkoznak az információs vagyon fizikai és elektronikus formátumú típusaira is. Az alsóbb osztályokra vonatkozó követelményeket felsőbb szinteken is alkalmazni kell.

A táblázatban a „Nyilvános" osztályozású információk kezelésére vonatkozó előírások nem kerültek rögzítésre, mivel azokkal szemben nincs külön speciális előírás, mivel osztályozásából eredően a nyilvánosság számára készülnek, ebből kifolyólag nem jelent kockázatot azok nyilvános közzététele.

	Belső	Bizalmas
Keletkezés / Megszerzés	„Belső" jelzéssel ellátva	+ Azonosítás és a hozzáférésre jogosultak megjelölése + A felelős megnevezése
Tárolás / Mentés		+ Csak a CSAPI által felügyelt vagy külső szolgáltatás esetén szerződés által kontrollált informatikai rendszeren tárolható + A papír verziók zárt tárolóban (szekrényben, szobában)
Hozzáférés, feldolgozás és frissítés	Titoktartási nyilatkozatot kell aláírattatni, ha külső partner hozzáférhet az információhoz	+ Csak jogosult személyek vagy csoportok férhetnek hozzá
Továbbítás	Figyelmeztető jelzés / felirat elhelyezése / feltüntetése az adott információn	+ Nem továbbítható a felhasználók körén kívül + E-mail törzsében hivatkozás a bizalmasságra
Nyomtatás/ Másolás		+ Nyomtatás helyi nyomtatón vagy közös nyomtatón biztonságos módon (kóddal, vagy kártyával)
Selejtezés	Az elektronikus adatok visszaállíthatatlan törlése. A szervezet hulladékkezelésén keresztül, vagy a nyomatok csíkra vágásával	+ A papíron lévő információk biztonságos gyűjtése zárható tárolóban (pl.: zsák, doboz stb.) majd megsemmisíttetése vagy irodai megsemmisítése keresztvágó papírmegsemmisítővel

8.5 Kockázatértékelés és elemzés

8.5.1 A kockázatértékelés célja

A kockázatértékelés célja, hogy az információbiztonsági kockázatok feltárása, elemzése, kiértékelése, a kockázatértékeléssel kapcsolatban hozott intézkedések és a gyakorlat **elfogadható biztonsági szintet** adjon az **üzleti tevékenységek** és **célok megvalósításához**.

8.5.2 Kockázatértékelés végrehajtása

A kockázatok elemzésére az **FMEA módszertant** alkalmazzuk. A kockázat értékelés kiinduló pontja minden esetben az előzetesen elkészített és rendelkezésre álló vagyonleltár. Az FMEA alapján végzett kockázat értékelést az egyes információs és információt kezelő eszközök vagyonleltárára használatos Excel fájlokban kell rögzítenie az **információ felelősnek**.

Az FMEA során a következőket kell végrehajtani **minden egyes vagyontárgyra vonatkozóan** (egy adott vagyontárgyhoz több fenyegetés / sebezhetőség / intézkedés is tartozhat):

1) A vagyontárggyal kapcsolatosan milyen **fenyegetések** lehetségesek (ismert vagy feltételezett) és ezek milyen forrásból (belső vagy külső, véletlen vagy szándékos stb.) lehetségesek,
2) **Sebezhetőségek** (sebezhető pontok) meghatározása, amelyeket az egyes fenyegetések kihasználhatnak,
3) **Üzletre gyakorolt hatások** azonosítása, melyek kihatással lehetnek a vagyontárgyra, amennyiben sérül a bizalmasság, rendelkezésre állás, sértetlenség
4) A fenyegetésekre vonatkozó **jelenlegi kontrollok** azonosítása,
5) Kockázat **elemzés.**

Az információbiztonsággal kapcsolatos kockázatértékelés koordinálása az **információbiztonsági vezető** feladata és felelőssége.

8.5.2.1 Kockázatok felmérése

A kockázat értékelés során

- fel kell tárni a lehetséges és legjelentősebb **fenyegetéseket** (maximum 10 db-ot), amelyek kárt okozhatnak az információs vagyonban a **rendelkezésre állás**, a **sértetlenség** vagy a **bizalmasság** vonatkozásában,
- a feltárt **fenyegetések alapján értékelni** kell a **jelenlegi intézkedések** hatékonyságát.

A kockázatok kezelését - új kontrollok meghatározása és bevezetése a kockázatok elviselhető mértékűre csökkentése érdekében - ezt követően lehet megkezdeni a kockázat elemzés alapján. A kockázatértékelés eredménye az információs vagyonleltár alapján felmért, elemzett és kiértékelt kockázatok.

8.5.2.1.1 Feltárás

Milyen fenyegetések fordulhatnak elő és ezek milyen forrásból származnak?

Lehetséges fenyegetések feltérképezése minden egyes vagyontárgyhoz kapcsolódóan. Az a feltételezés, hogy a fenyegetés előfordulhat, de nem fordul elő szükségszerűen. A fenyegetés tömör és érthető definiálása fontos, mivel ez a megfelelő irányba tereli az elemzés fókuszát. Egy vagyontárgyhoz meghatározott nagyszámú fenyegetés azt jelezheti, hogy a meghatározott vagyontárgy nem eléggé lényegre törő, túl általános vagy nagyon nagy területet foglal magában (pl.:

vevőkkel kapcsolatos információk; kereskedelemmel összefüggő információk; dokumentumkezelés; stb.).

Sebezhetőségek (sebezhető pontok) meghatározása, amelyeket az egyes fenyegetések kihasználhatnak

Lehetséges sebezhetőségek feltérképezése minden egyes fenyegetéshez kapcsolódóan.

Hatások azonosítása melyek kihatással lehetnek a vagyontárgyra amennyiben sérül a bizalmasság, rendelkezésre állás, sértetlenség

Azon üzleti kár meghatározása, amely abban az esetben valósul meg, ha a fenyegetés bekövetkezik.

8.5.2.1.2 Súlyosság értékelése

A lehetséges hatások jelentőségét az alábbi osztályozás szerint értékeljük.

Súlyosság
Magas
Közepes
Alacsony

8.5.2.1.3 Valószínűség értékelése

Az előfordulás gyakoriságának értékelése. A következő osztályozás alapján meghatározzuk, hogy milyen Valószínűséggel következhetnek be a fenyegetések.

Valószínűség
Magas
Közepes
Alacsony

8.5.2.1.4 Jelenlegi kontrollok (intézkedések)

Jelenleg milyen megelőző / detektáló intézkedések kezelik az eseményeket?

Milyen megelőző / detektáló intézkedések történtek az események bekövetkeztének észlelésére? Milyen intézkedések történtek annak érdekében, hogy a lehetséges következményeket mérsékeljük, illetve ezek bekövetkezését megakadályozzuk.

8.5.2.1.5 A kontrol intézkedések hatékonyságának értékelése

Az adott fenyegetésre vonatkozó jelenlegi kontroll intézkedések hatékonyságának értékelése. A következő osztályozás alapján meghatározzuk, hogy milyen a jelenlegi intézkedések hatékonysága. Amennyiben az adott információ esetén az információ felelős nem tudja egyértelműen meghatározni vagy nem rendelkezik információval a jelenlegi kontrollt illetően akkor ebben az esetben:

1. a jelenlegi kontroll hatékonyságát „közepes"-re kell besorolni,
2. és az információ hiány tényről tájékoztatni kell az információbiztonsági vezetőt.

Hatékonyság
Magas
Közepes
Alacsony

8.5.2.1.6 Kiértékelés és információbiztonsági vezető általi felülvizsgálat

Az egyes **információ felelősök** az elkészített kockázatértékelési tábláikat megküldik az információbiztonsági vezető részére felülvizsgálat céljából. A felülvizsgálat során a következő lépéseket kell végrehajtania az **információbiztonsági vezetőnek**:

- a fenyegetések felülvizsgálata az információbiztonság szempontjából,
- a sebezhetőségek felülvizsgálata az információbiztonság szempontjából,
- az üzletre gyakorolt hatás felülvizsgálata, annak szempontjából, hogy mind a bizalmasság, mind a sértetlenség mind pedig a rendelkezésre állás szempontjából kiértékelésre kerültek az üzleti hatások,
- a rögzített meglévő kontroll intézkedések felülvizsgálata vagy amennyiben ezt az adott felelős nem tudta meghatározni akkor annak rögzítése a kockázatértékelésben,
- a rögzített meglévő kontroll intézkedések hatékonyságának felülvizsgálata az információbiztonság szempontjából vagy amennyiben ezt az adott felelős nem tudta meghatározni akkor annak rögzítése a kockázatértékelésben,
- az RPN értékek felülvizsgálata (kiugró gyanús értékek vizsgálata),
- a módosított kockázatértékelés visszaküldése az adott felelősnek felülvizsgálatra,
- egyeztetések és módosítások iterációjának végrehajtása,
- a kockázatértékelés lezárása amennyiben az adott felelős egyetértett az információbiztonsági vezető által rögzítettekkel.

A kockázat értékelés során meghatározott három jellemző alapján – súlyosság, valószínűség, hatékonyság – kell képezni az RPN – Risk Priority Number - számot.

Az RPN számot a három jellemző szorzata alapján kell meghatározni a következők szerint:

RPN = (Súlyosság * 2) * (Valószínűség * 2) * (Kontroll hatékonyság * 2)

Az RPN értékek meghatározását követően kezdhető meg a kockázatok elemzése és kezelése.

8.5.2.2 Kockázatelemzés

Az **információbiztonsági vezető** a következő feladatokat hajtja végre a kockázat elemzés során:

- az egyes szervezeti egységek által készített és jóváhagyott kockázatelemzések **egységesítése**,
- az egységesítés alapján a **TOP 10** kockázat meghatározása,
- az egységesítés alapján javaslat megfogalmazása az **RPN határértékre** vonatkozóan, melynél a következő főbb szempontokat kell figyelembe venni:
    - az RPN határértéket úgy kell kialakítani, hogy a kockázatértékelés alapján **minimum** az információk / információt kezelő eszközök kockázatainak **30 %-a kezelésre** kerüljön,

- a megállapított **RPN határértékek rögzítése**.

Az így keletkezett RPN határértékek lesznek azon értékek, melyek felett intézkedéseket kell meghatározni és végrehajtani.

8.5.2.3 Kockázatkezelés

8.5.2.3.1 Intézkedések tervezése, felülvizsgálata és jóváhagyása

Az előzőekben meghatározott RPN határértékek felett meg kell határozni azokat a tervezett intézkedéseket, amelyek bevezetésével a kockázatot a kritikus érték alá csökkenthetik.

A tervezett intézkedések meghatározásáért az **információbiztonsági vezető** felelős, szükség szerint bevonva az egyéb **szakterületek felelőseit**. Az egyeztetések és a kompromisszumos intézkedés tervezetek kialakításáért is az **információbiztonsági vezető** felelős. A tervezett intézkedéseket úgy kell kialakítani, hogy az intézkedések hatással legyenek – és ezáltal csökkentsék az adott RPN értéket – az

- adott fenyegetéshez tartozó üzletre gyakorolt hatásra, vagy
- a sebezhetőség bekövetkezésének valószínűségére.

8.5.2.3.2 Tervezett intézkedések bevezetését követő újraértékelés

Az intézkedések bevezetése után a kockázatértékelést és a kockázatelemzést újra el kell végeznie az **információ felelősnek** az **információbiztonsági vezető** támogatása mellett. Ebben az esetben az akció tervben kell rögzíteni a tervezett intézkedések mellett a bevezetett intézkedéseket. Amennyiben a bevezetett intézkedések nem csökkentették megfelelő mértékben a kockázatokat, akkor újabb intézkedések, és azok újra kiértékelése szükséges, mindaddig, amíg elviselhető mértékűre nem csökken a kockázat.

Az aktualizált kockázatértékelési táblák létrejötte után az **információbiztonsági vezetőnek** ismételten el kell végeznie a kockázatelemzést.

8.5.3 Kockázatok nyomon követése és aktualizálása

A vagyonleltár és a kockázatértékelés nyomon követése és aktualizálása különválhat attól függően, hogy milyen változás történt a működési folyamatokban. A kockázatértékelés a következő esetekben válhat el a vagyonleltár aktualizálásától:

- az információ maga és azok attribútumai nem változtak csak újabb fenyegetések, sebezhetőségek jelentek meg,
- újabb intézkedéseket vezettünk be, melyek a fenyegetések üzleti hatását befolyásolják,
- újabb intézkedéseket vezettünk be, melyek a sebezhetőségek valószínűségét befolyásolják,
- új RPN értékek kerültek meghatározásra a menedzsment által,
- stb.

A döntés meghozataláért, hogy a kockázatértékelés aktualizálásával a vagyonleltárt is módosítani szükséges az **információbiztonsági vezető** feladata és felelőssége.

Az alábbi esetekben a kockázatértékelést / kockázatelemzést / kockázatkezelést újra el kell végezni

1) Ha változás történik az üzleti folyamatban:
   a) új szolgáltatást vezetünk be
   b) új rendszert vezetünk be

c) új szolgáltatást veszünk igénybe
d) új belső elvárások jelentkeznek

2) Ha változás van a környezetben
   a) új fenyegetések jelentkeznek
   b) új vevői vagy törvényi követelmények jelentkeznek
3) Egy esetlegesen felmerült problémából vagy incidensből eredően
4) Rendszeresen, évente

9. SZERVEZETI BIZTONSÁG

9.1 Emberi erőforrás (humán) biztonság

A **munkáltatói jogokat gyakorló vezető** köteles gondoskodni arról, hogy valamennyi munkaterületről és valamennyi munkakörről részletes munkaköri leírás készüljön. Minden munkaköri leírásnak tartalmaznia kell az adott területre speciálisan vonatkozó, a biztonsággal kapcsolatos követelményeket is a felelősség egyértelmű megjelölésével.

A felhasználók munkaköri leírásaiban vagy annak mellékleteként titoktartási nyilatkozatot kell a felhasználókkal aláíratni, mely a CSAPI információinak / adatainak bizalmas kezelésére valamint az informatikai rendszerek biztonsági intézkedéseinek betartására, valamint ennek esetleges be nem tartása esetén alkalmazandó szankciókra irányul. Ezen nyilatkozat aláírása nélkül sem állandó, sem alkalmi munkaerő, sem külső személy információkhoz / adatokhoz vagy informatikai eszközökhöz nem férhet hozzá.

A titoktartási nyilatkozatok aláíratása és tárolása a **Munkaügyi osztály** feladata.

9.1.1 Az alkalmazás során követendő előírások

Az alkalmazás során az **információbiztonsági vezető** feladata az információbiztonsággal kapcsolatos előírások teljesítése, és betartatása, illetve ezek megvalósulásának rendszeres ellenőrzése. A biztonsági előírásokat megsértőkkel szemben kisebb súlyú esetben a **közvetlen vezető** jár el, személyes beszélgetés során tisztázva a körülményeket, teendőket. Súlyosabb eset illetve ismétlődés esetén a teendőket és az alkalmazható szankciókat a vonatkozó jogszabályok határozzák meg.

9.1.1.1 Képzés, tudatosság és felkészültség

A munkakörök betöltéséhez szükséges képzettséggel-, a gyakorlati tapasztalattal kapcsolatos követelmények a pozícióra meghatározott munkaköri leírásban kerülnek rögzítésre.

A folyamatos információbiztonság fejlesztése érdekében az **információbiztonsági vezető** éves *Képzési tervet* állít össze. A *Képzési tervet* az **Információbiztonsági Team** hagyja jóvá. A képzési tervben szereplő képzések nyomon követése az **információbiztonsági vezető** feladata.

Az oktatások megszervezéséről és lebonyolításáról – az **információbiztonsági vezető** közreműködésével – a **Munkaügyi osztály** kell gondoskodnia.

Az információbiztonság irányítási rendszerben bekövetkezett változások esetén a változást érintő területeken dolgozó munkavállalóknak a változás bekövetkeztekor oktatást kell tartani a korábban leírtaknak megfelelően.

Az oktatásokra vonatkozó további feladatok kapcsán a CSAPI szabályozások az irányadók.

9.1.1.1.1 Új belépők képzése

Az új belépők oktatásáról az alábbi felelősök gondoskodnak:

- általános információbiztonsági képzéséről valamint a kiterjesztett információbiztonsági képzéséről az **információbiztonsági vezető**.

Az oktatásnak új belépő esetén a tényleges önálló munka-végzést megelőzően, a későbbiekben évente legalább egyszer meg kell történnie.

A képzésnek ki kell terjednie

- biztonsági követelményekre,
  - általános informatikai biztonsági oktatás;
  - vírusvédelemmel és a vírusvédelmi rendszerekkel kapcsolatos oktatás;
  - a biztonsági események jelentésével, kezelésével kapcsolatos oktatás;
  - új, bevezetésre kerülő rendszerekkel kapcsolatos biztonsági oktatás minden, a rendszer bevezetésében érintett felhasználó körében;
  - egyéni, a felhasználó beosztásának, munkakörének megfelelő további informatikai biztonsági oktatás;
- a jogi felelősségre,
- az üzleti óvintézkedésekre,
- valamint az informatikai eszközök helyes használatára (pl. a bejelentkezési eljárásokra, a szoftverek használatára stb.).

A képzést az előtt kell lefolytatni, mielőtt a felhasználók megkapnák a hozzáférési jogot az informatikai rendszerekhez, vagy az információkhoz / adatokhoz.

9.2 Alkalmazás megszűnése, megváltozása

Az alkalmazás megszűnése, megváltozása esetére vonatkozó előírásokat a 12. Hozzáférés-szabályozás című fejezet szabályozza.

9.3 Szerződő partnerekkel szemben támasztott biztonsági követelmények

A CSAPI igénybe vesz szerződő partnereket.

A biztonsági kockázatokat és az ellenőrzés, valamint a felügyelet követelményeit fel kell mérni. A felmérésért a szerződést – üzleti oldalról – **előkészítő személy** - az **információbiztonsági vezető** bevonása mellett - a felelős. A külső személlyel megkötött szerződésben egyértelműen meg kell határozni az előzőekhez kapcsolódó elvárásokat. Szerződő partnerek hozzáférésénél további résztvevők (pl.: alvállalkozók) közreműködésére is szükség lehet. A hozzáféréséről rendelkező szerződésekben rendelkezni kell arról, hogy más, arra jogosult közreműködők is hozzáférhetnek a különböző eszközökhöz, és rögzíteni kell a hozzáférés feltételeit. Jelen szabályzat betartása az ilyen szerződések létrejöttének, valamint az adatfeldolgozás vállalkozásba adásának elengedhetetlen feltétele.

Egy szerződő partner hozzáférésének engedélyezésénél a következő szempontokat kell megvizsgálni:

- A szerződő partner megbízhatóságát / hitelességét szakmai (referenciák), stratégiai és biztonsági szempontból.
- A szerződő partner által elvégzendő munka részfeladatait, a szolgáltatási szintek meghatározását és a rögzített szolgáltatási szintek minőségének mérésére vonatkozó módszereket.
- A szolgáltatás során a megismerhető adatok körét, az elvégzett munka informatikai hátterét.
- Azon kockázatokat melyekkel az információbiztonság szempontjából számolni lehet.
- Az érintett rendszereket, logikai és fizikai hozzáférés szempontjából.
- Az információk / adatok nyilvánosságra kerülését megelőzendő egy esetlegesen szükséges beavatkozás során alkalmazandó közvetlen irányítás és menedzselés lehetőségeit, eljárásait.

- A biztonsági események, szabálysértések jelentésére, azok kezelésére és eszkalációjára vonatkozó eljárásokat.
- Az elvégzett munka CSAPI oldali HR vagy informatikai igényét.
- A munka mennyiben befolyásolja a napi üzleti / támogató tevékenységek menetét.
- A CSAPI auditálási jogát a szolgáltatási szerződésben foglaltak ellenőrzésére vonatkozóan.

A CSAPI informatikai eszközeit csak a szervezet feladatából eredő indokolt esetben és ellenőrizhető módon teszi hozzáférhetővé szerződő partnerek számára. A szerződő partnerek hozzáféréseit minden esetben rendszeresen ellenőrizni kell. Az ellenőrzésért a CSAPI részéről felelősként, kapcsolattartóként meghatározott **vezetője**, illetve az **általa kijelölt személy**. Az ellenőrzés végrehajtásának ellenőrzéséért az **Információbiztonsági vezető** felelős.

A hozzáférést a szerződő partnerek számára megtagadja a CSAPI, amennyiben azt nem a szerződésben meghatározott, és kifejezetten megjelölt személyek végzik. A megállapodások megkötése során a **szerződést előkészítő** és az **információbiztonsági vezető** feladata és a **szerződést aláíró** felelőssége, hogy a szerződésbe belekerüljenek a jelen szabályzatban rögzített alapelvek és követelmények.

Szerződő partner számára hozzáférési lehetőséget kérni kizárólag a HelpDesk-en keresztül lehetséges, dokumentált formában.

9.3.1 Szerződések tartalmi követelményei

Külső felekkel, minden esetben írásos szerződést kell kötni. Az együttműködés jellege és a kockázati kitettség alapján az alább felsorolt szempontokat részben vagy teljes körűen tartalmaznia kell a szerződésnek:

- titoktartási megállapodás
- teljes körű felelősség a szerződés keretében foglalkoztatott munkatársakért
- egyértelmű és előírt változáskezelési folyamat
- folyamatos jelentéstételi kötelezettség a tevékenységről (pl. munkanapló)
- rendelkezések az informatikai biztonsági incidensek és biztonsági sértések jelentésére és az incidensek kezelésére
- a szolgáltatások előirányzott szintjei és a szolgáltatás el nem fogadható szintjei
- fizikai és logikai hozzáférések meghatározása, ezen belül
    - nyilvántartás a feljogosított személyekről
    - nyilatkozat: minden olyan hozzáférés, amely nem engedélyezett: TILOS
- jog, hogy a szerződésben meghatározott követelmények teljesülését ellenőrizni (auditálni) lehessen, akár harmadik fél által is.

9.3.2 Folyamatos tevékenységet ellátó szerződő partner fizikai hozzáférésének szabályozása

Az előzőekben leírtak betartásán felül a szerződés aláírását követően, a szolgáltatás folyamatos végrehajtása során a következő szerződő partner esetében lehetséges a fizikai hozzáférés a CSAPI felügyelete alá tartozó, nem a vásárló közönségnek fenntartott területek esetében:

- takarítást végző,
- biztonsági szolgálat munkavállalói,
- karbantartó,
- egyéb, folyamatos szerződéses jogviszonyban álló harmadik személy.

A takarítást végzőket a telephelyeken az információvédelem szempontjából jelentős értékeket tartalmazó helységekben kamerás biztonsági rendszerrel tartjuk ellenőrzés alatt.

A szerverszoba takarítása két módon történhet:

- a takarító személyzet nem léphet be a szerverszobába és azt **az alvállalkozó informatikus** takarítja;
- vagy a takarító személyzet csak és kizárólag **az alvállalkozó informatikus munkatárs folyamatos** felügyelete mellett végezheti munkáját.

A takarító személyzet az íróasztalokat nem takarítja, azokon nem rakhat rendet. Az asztalokon nem hagyható olyan információ, amelynek elől maradása üzleti vagy egyéb személyes adatvédelmi kockázatot jelent.

Az alvállalkozók felügyelete minden esetben a **szerződés melléklete szerinti kapcsolatot tartó személyek** feladata.

10. FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG

Az információkezelő eszközöket lehetőség szerint a telephelyeken belül kell elhelyezni. Nem végezhető olyan tevékenység, amely az információkezelő eszközök vagy adathordozók épségét, működését károsan befolyásolná vagy akadályozná.

A CSAPI fizikailag több elkülönült, felügyelete alá tartozó kereskedelmi egységnél végzi tevékenységét, melyek a jogszabályi előírásoknak megfelelő tárgyi, technikai és elektronikai védelemmel vannak ellátva.

A védelmet úgy alakítottuk ki, hogy az arányban álljon a megállapított kockázatokkal. Az illetéktelen hozzáférés megakadályozása, a dokumentumok, az adathordozók védelme és az adatfeldolgozó létesítmények kockázatának mérséklése érdekében beléptetési és megfigyelési szabályokat vezetünk be.

Az alkalmazott védelmi formák körét, azok kialakítását az **információbiztonsági vezető** határozza meg jelen IBSZ elveinek megtartása mellett, az adott létesítmény védelmi igényének és speciális feltételeinek figyelembe vételével.

A helyiségek kockázatarányos fizikai védelmének biztosítása érdekében a következő biztonsági zónák kerültek meghatározásra:

- Géptermi zóna;
- Irodai zóna;
- Infrastruktúra zóna;
- Vendég zóna;
- Nyilvános hozzáférés, szállítási és rakodási területek.

Az információkezelő eszközöket (informatikai berendezéseket, eszközöket; irattároló szekrényeket; stb.), fizikai valójukban is védeni kell a biztonságot fenyegető veszélyektől és a káros környezeti hatásoktól. Az információkezelő eszközök fizikai védelmére azért van szükség, hogy ily módon is mérsékeljük az információkhoz való illetéktelen hozzáférés kockázatát, valamint gondoskodjunk az információk és eszközök megfelelő védelméről. Erre már a berendezések elhelyezése során is tekintettel kell lenni.

Az információkezelő eszközök védelmét a következő területekre kell kiterjeszteni:

- az extrém hőmérsékletek és a meg nem engedett mértékű levegő nedvességtartalom elleni védelemre (klimatizálás),
- a fémes adatvezetékek elektromágneses impulzusok elleni védelmére (elektromágneses besugárzás elleni védelem),
- külső tényezők (tűz, víz, vihar, stb.) elleni védelemre, így különösen a tűzjelző berendezések meglétére és működőképességére, illetve a vízelvezetésre,
- épületek belső szerkezeti felépítésére (villamos hálózat terhelése, falba épített víz, gázcsőhálózat pl.: csőtörés veszélye)
- áramellátó-rendszerek kiesésének következményeinek elhárítására (akkumulátoros és generátoros szükség áramellátással), az áramellátás területén a villámcsapások elsődleges és másodlagos hatásai, illetve egyéb túlfeszültségek elleni védelemre,
- elektrosztatikus kisülések hatásainak elhárítására (a helyiségek és munkahelyek megfelelő kialakításával, amelyekbe az információkezelő eszközöket telepítették).

A védelemnek

- az információk feldolgozását, tárolását, a hálózat működését biztosító berendezéseken túl ki kell térnie a tárolt szoftverek, adatok és dokumentációk védelmére is,
- arányban kell lennie
  - az alkalmazások rendelkezésre állásának szükséges mértékével,
  - a hardver és a szoftver beszerzési értékével,
  - és az adatok pótlásának költségével,
- teljes körűnek és mindenre kiterjedőnek kell lennie. A teljes körűségről már a helyiségek kialakítása során gondoskodni kell.

Az egyes zónák őrzés-védelmét, nyitását és zárását, a be- és kilépést mind munkaidőben, mind azon kívül a hatályban lévő szabályzatok és az érvényes előírások alapján biztosítani és érvényesíteni kell. Az őr- és a biztonsági személyzet létszámát úgy kell megállapítani és őket olyan eszközökkel kell ellátni, hogy esemény esetén az érintett személy figyelmeztetni, riasztani tudjon. A munkavégzés helyére belépni szándékozókat azonosítani kell, és a belépőkről nyilvántartást kell vezetnie az **őrzés-védelemmel megbízott személyeknek**.

Az információkezelő eszközöket úgy kell elhelyezni, hogy lehetőleg megakadályozzuk az illetéktelen hozzáférést, és a helyiségek észrevétlen megközelítését. A környezeti hatások és a lehetséges veszélyforrások folyamatos vizsgálatával és elemzésével kell törekedni a szükséges működési feltételek biztosítására.

Amennyiben lehetséges az épületek ne legyenek hivalkodók és a legkevesebb jelét adják céljuknak, ne legyenek szembetűnő jelek az épület külső vagy belső oldalán, amely azonosítaná az információ feldolgozó tevékenység jelenlétét.

10.1 Információkezelő eszközök védelme

Szerződő partner feladata a gépterem vonatkozásában az elektromos áramfelvételi igény, a kapacitás összhangjának biztosítása, figyelemmel kísérése. További feladata figyelni és felügyelni a gépterem környezeti paramétereit: hőmérséklet, páratartalom, energiaellátás. Az ezeket kiszolgáló berendezések (klíma, szünetmentes tápegység) üzemképességét is biztosítja.

Meghibásodásuk esetén kezdeményezik javításukat, és szükség esetén leállítják az informatikai berendezéseket. Ezen szabályok betartásának ellenőrzése az **információbiztonsági vezető** feladata.

A megbízható működés érdekében az eszközök folyamatos használata és rendelkezésre állásának biztosítása érdekében a specifikációban javasolt időközönként el kell végezni a berendezések karbantartását. A karbantartások megszervezése, az erre szerződött partnerekkel való kapcsolattartás az **IT Üzemeltetési szerződött partner** feladata. A karbantartás az üzemeltetési dokumentációkban és karbantartási szerződésekben foglaltak szerint történik. A szerződések megkötése az **információbiztonsági vezető** felelőssége. A berendezések kezelését, illetve javítását csak megfelelő szakképzettséggel rendelkező személyek végezhetik.

Az **IT Üzemeltetési szerződött fél munkavállalói** figyelik a berendezések megfelelőségét és üzemképességét, meghibásodás esetén kezdeményezik javíttatásukat.

Az informatikai vagyontárgyak illetéktelen eltávolításának, telepítésének kísérletét jelenteni kell az **információbiztonsági vezetőnek**.

Az információkezelő eszközök külső helyszínen történő javítása, karbantartása esetén gondoskodni kell a berendezésen tárolt „Bizalmas" információk törléséről.

10.1.1 Mobil eszközök használata és védelme

A notebook-ok használatával kapcsolatban a következő biztonsági paraméterek betartása kötelező:

- A munkavállalók az állandó használatra kapott mobil eszközöket külön engedély nélkül is kivihetik a CSAPI területéről.
- Valamennyi a CSAPI tulajdonát képező hordozható személyi számítógépet rendszeres szoftver-, adat- és biztonsági ellenőrzéseknek kell alávetni.

Nem a CSAPI tulajdonában lévő, illetve szerződő partner munkavégzéséhez nem szükséges mobil eszköz csatlakoztatása a belső hálózathoz, szigorúan tilos.

A mobil eszköz használatát az **információbiztonsági vezető** jogosult engedélyezni a HelpDeskre beérkező igény alapján. A használati engedély egyben tartalmazza az eszközök szervezeten kívülre történő elvitelére való feljogosítást is. Azon felhasználók számára, akik munkájukhoz hosszabb ideig, vagy folyamatosan hordozható személyi számítógépeket vesznek igénybe az engedélyt az esetleges időbeni korlátozások megjelölésével, ennek megfelelően kell kiállítani. Az **információbiztonsági vezető** felelőssége továbbá, hogy a felhasználók megfelelő oktatásban részesüljenek ezen eszközök helyes és információbiztonsági szempontból megfelelő használatáról. A szabályokat a felhasználókkal el kell fogadtatni, és tudatosítani kell bennük a biztonsági kockázatokat.

A személyi számítógépeket és az ahhoz kapcsolódó számítástechnikai berendezéseket **szállító személyeknek** a következő előírásokat kell betartani azok használata során:

- Kötelesek a számítógépet a szállítás idejére nem szem előtt lévő módon elhelyezni.
- Tilos a számítógépet a gépjárműben hagyni.
- Repülés, vagy vonatút alatt a személyi számítógépet kézipoggyászként kell szállítani.
- Tilos az eszköz engedély nélküli átruházása vagy adatainak közlése.
- Tilos a számítógépet bármilyen indokolatlan veszélynek kitenni vagy nem rendeltetésszerűen használni.

10.1.2 Teendők számítógép eltulajdonítása esetén

Az **eszköz használójának**:

- Telefonon azonnal, majd írásban jelenteni kell a számítógép eltulajdonításának tényét a HelpDesknek és az **információbiztonsági vezetőnek**.
- Értesíteni kell a rendőrséget, és a rendőrségi jegyzőkönyv másolatát el kell juttatni az **információbiztonsági vezetőnek**.
- Értesíteni kell a szálloda vezetését, ha a számítógépet a szállodai szobából, vagy a szálloda ingatlanján álló kocsiból lopták el.
- Valamennyi rendőrségi és biztosítói jegyzőkönyvet, jelentést meg kell őrizni, és másolatát az **információbiztonsági vezetőnek** át kell adni.

10.1.3 Rendszeres karbantartás

Az **IT üzemeltetés szerződött partnerének** felelőssége, hogy tervezetten és rendszeresen történjen meg az informatikai eszközök karbantartása.

A karbantartások végrehajtásához kapcsolódó leállások lehetséges időpontjai miatt egyeztetnie kell az információbiztonsági vezetővel.

Az **IT üzemeltetés szerződött partnerének** 5 nappal a karbantartás előtt kell jeleznie az **információbiztonsági vezető** részére a leállás időpontját és annak hosszát. Az **információbiztonsági vezető** a leállás előtt 3 nappal kell jelezni, ha nem megfelelő az időpont számukra és javasolniuk kell egy másik időpontot.

A végrehajtandó karbantartásokról előzetesen tervet kell készíteni, amelyben dokumentálni kell pontosan a feladatot és a kapcsolódó felelős, végrehajtó szerepköröket is. A tervet jóvá kell hagynia az **információbiztonsági vezetőnek**. A végrehajtott karbantartások tekintetében az érintett **rendszeradminisztrátoroknak** karbantartási naplót kell vezetni.

10.1.4 Az eszközök újbóli használata, illetve tárolása használaton kívül

Az eszközök használaton kívül helyezése előtt gondoskodni kell az összes érzékeny, illetve minősített adat, szolgálati szoftver visszaállíthatatlan eltávolításáról vagy felülírásáról. A használaton kívül helyezett eszköz és a CSAPI összes hálózata közötti összeköttetést meg kell szüntetni. A használaton kívüli informatikai berendezés újbóli rendszerbeállításakor úgy kell eljárni, mint egy új eszköz üzembeállítása során.

10.1.5 Információkezelő eszközök szervezeten kívülre történő elvitele

Információkezelő eszközöket, adathordozókat, programokat kizárólag az információbiztonsági vezető engedélyével szabad kivinni a munkahelyről. Felhatalmazás nélkül nem lehet informatikai eszközt, információt vagy szoftvert szervezeten kívülre elvinni.

Az eszközök elvitele esetén minden esetben egy időkorlátot kell meghatározni. Visszaadáskor a **visszavételért felelős munkatársnak** ellenőriznie kell azt megfelelőség szempontjából.

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 az érzékeny információk törlésre kerültek.

10.1.6 A CSAPI és a felügyelete alá tartozó kereskedelmi egységeken kívüli információkezelő eszközök biztonsága

A CSAPI és a felügyelete alá tartozó kereskedelmi egységeken kívüli adatfeldolgozás csak az előző fejezetekben szabályozott módon megengedett. Az alkalmazandó biztonsági előírásoknak meg kell egyezniük a CSAPI és a felügyelete alá tartozó kereskedelmi egységeken hasonló feladatokhoz használt eszközökre vonatkozó előírásokkal. Az egyes külső helyszínek között jelentős különbségek lehetnek a biztonsági kockázatok (károkozás, lopás, lehallgatás, stb. veszélye) mértéke között. Ezt figyelembe kell venni a szükséges biztonsági eszközök és eljárások kiválasztásánál.

10.1.7 Információkezelő eszközök (beleértve az adathordozókat) biztonságos selejtezése, újrafelhasználása

Az **információbiztonsági vezető** feladata gondoskodni a biztonságos selejtezésre adásért azon információkezelő eszközök esetén, melyek információtároló egységet tartalmaznak. Kizárólag a biztonsági törlésen megfelelően átesett eszközök adhatók tovább selejtezés, illetve újrahasznosítás céljából.

11. BIZTONSÁGI MENTÉSEK

11.1 Biztonsági mentés célja

Az adatok biztonsági mentése a következő folyamatokat támogatja:

- Incidens vagy katasztrófa utáni helyreállítási folyamatok
- Törvényi kötelezettségek teljesítése (meghatározott adatok, állapotok hosszú távú megőrzése)
- Felhasználói igények kiszolgálása (egy dokumentum korábbi változatának helyreállítási igénye)

11.2 Tervezési szempontok

Az adatmentéseket úgy kell megtervezni, illetve felülvizsgálni, hogy annak eredménye megfeleljen a CSAPI kockázatértékelésében meghatározott kritériumoknak. A kritériumokat az adott adatcsoport **Információ Felelősének** kell definiálni a következők szerint:

- Az adat mentések gyakorisága (az elfogadható adatvesztési időtartam)
- Előző állapotok visszaállítási igénye
- Mentett adatok megőrzési ideje
- Archiválási igény

11.2.1 A mentések kialakítása

Minden új rendszer bevezetésénél, illetve működő mentés felülvizsgálata során a következő feladatokat kell elvégezni.

- Ellenőrizni kell a kapacitáskorlátokat
- Meg kell határozni a mentést végző rendszert / módszertant
- El kell készíteni a mentést végző alkalmazások programozását
- Meg kell határozni a szükséges ellenőrzési folyamatokat, és meg kell határozni az ebben résztvevő személyeket, valamint azok feladatait

A mentések technikai részleteit *Mentési Utasításban* kell rögzíteni, amelyet naprakészen kell tartani.

11.2.2 Követelmények a mentésekkel szemben

A mentési adathordozókat védett helyen kell tárolni. A mentési adathordozókat a forrás adatokat tároló szerverektől / eszközöktől elkülönítve kell tárolni.

A mentési adathordozók kezelésére felelőst kell kinevezni, amely felelősség vonatkozik mind a mentési eljárásra, mind a szállításra és tárolásra.

A mentések sikerességét rendszeresen ellenőrizni kell és időszakosan visszaállítási tesztet kell végezni.

11.2.3 Munkaállomásokon tárolt adatok mentése

A **munkavállalók** felelőssége, hogy a munkaállomásaikon tárolt, a CSAPI üzletvitelével kapcsolatos érzékeny információikat a kijelölt központi tárterületen helyezzék el. A **munkavállalók** feladata, hogy a rendelkezésükre bocsátott területtel ésszerűen gazdálkodjanak.

11.3 Személyi felelősségek

Információbiztonsági vezető

- Az adatmentési koncepció elfogadása
- Az új rendszerek mentési követelményének meghatározása

- Az adatmentési utasítások jóváhagyása
- Adatmentési folyamatok időszakos, periodikus ellenőrzése
- Jelentések értékelése
- Időszakos ellenőrzések az adatbiztonság szempontjai szerint
- Incidensek kivizsgálása

Adatmentésért felelős informatikus

- Adatmentési koncepció alapján az adatmentési eljárások kidolgozása, rögzítése a *Mentési Utasításban*
- Az adatmentések beállítása, ütemezése, végrehajtása
- Adatmentések eredményének napi kontrollja, adatmentések és adatvisszatöltések végrehajtása
- Mentési médiák kezelése
- Incidensek jelentése a Help Desk rendszeren keresztül

11.4 A mentési utasítás

Az adatmentések technikai részletei a *Mentési Utasítás* alapján történik. Az utasítás legalább a következőket tartalmazza:

- Adatmentésért felelős személy neve és elérhetősége
- A mentett adatállományok
    - Adatbázisok
    - Fájl rendszerek
    - Image-ek
- A mentés eszközei
    - Mentési hardver elemek – az adatmentést megvalósító IT infrastruktúra eszközök összessége (szerverek, mentési médiák, a médiákat használó eszközök, stb.)
    - Mentési szoftver elemek – az adatmentést megvalósító, az adatmentési koncepciót leképező alap- és alkalmazás szoftver modulok
- Az adatmentés beállítása
    - Időzítések
    - Parancsfájlok
    - Segédprogramok
- Médiakezelés, a mentett állományok tárolási helyei, példányszáma
- Ellenőrzések
- Kontrollok, jelentések,
- A visszaállítás folyamata

11.5 A mentési adathordozók kezelése

11.5.1 Ellenőrzés

Minden mentés eredményességét ellenőrizni kell (ezt általában a mentőrendszer elvégzi). Amennyiben a mentés nem sikerült, riasztást kell generálni (incidens!) és a mentést megismételni.

A mentési állományokat visszaállítási tesztekkel is ellenőrizni kell, minden mentés típusra vonatkozóan, évente legalább egy alkalommal.

11.5.2 Nyilvántartás

Valamennyi használatban levő mentési adatokat tartalmazó médiáról nyilvántartást kell vezetni.

A nyilvántartásnak minimálisan az alábbi jellemzőket kell tartalmaznia **mentések** esetén:

- A média egyedi azonosítója (vonalkód, címke, stb.)
- Mentett adat neve
- Mentett adat eredeti helye
- Adatmentés dátuma
- Adatmentést végző személy neve
- Adatmentő szoftver neve, verziószáma

A nyilvántartásnak minimálisan az alábbi jellemzőket kell tartalmaznia **archiválás** esetén:

- Adatarchiválást igénylő személy adatai
- Adatarchiválást végző személy adatai
- Archívum keletkezésének időpontja
- Archívum példányszáma
- Archívum azonosítója
- Archívum létrehozásához használt szoftver neve, verziószáma
- Archívum megőrzésének dátuma
- Archívum utolsó olvashatósági ellenőrzésének eredménye
- Archívumhoz hozzáféréssel rendelkező személyek adatai

A nyilvántartásban minden változást új bejegyzésként (új sor) kell felvezetni, minden egyes sornál a tevékenységet végző nevének és a bejegyzés dátumának is szerepelnie kell.

A nyilvántartást Excel táblában kell vezetni, a táblázatot olyan helyen kell elhelyezni, ami napi mentésre kerül. A nyilvántartás vezetését a **mentésért felelős informatikus** végzi.

11.5.3 Tárolás

A mentési adathordozókat a mentett rendszerektől távol – lehetőleg külön épületben – kell tárolni. A mentési adathordozók tároló helyéneknek fizikailag védettnek kell lennie (pl. páncélszekrény).

11.5.4 Szállítás

Amennyiben a mentési médiát nyilvános területen keresztül mozgatjuk, biztosítani kell, hogy a média szállítása közben ne legyen olyan pont, amikor a felelős személy nem azonosítható egyértelműen. A szállításról a *Mentési Utasításban* kell rendelkezni.

11.5.5 Karbantartás

A mentési eszközök időszakos karbantartásáról gondoskodni kell. Évente egyszer akkor is felül kell vizsgáltatni a rendszert, ha az adott időszakban nem volt meghibásodás. A felülvizsgálat és a mentési eszközök karbantartási feladatait a gyártó és a CSAPI vonatkozó utasításai alapján végezni.

11.5.6 Selejtezés

A médiák selejtezését a média fizika megsemmisítésével kell elvégezni. A selejtezésről minden esetben jegyzőkönyvnek kell készülni.

11.5.7 Naplózás

A mentési folyamatot naplózni kell. A napló fájlok tartalmazzák a mentés tárgyát, sikeres/sikertelen voltát, a mentés időpontját. A mentési napló fájlokat naponta menteni kell.

11.6 Események kezelése

A következők biztonsági eseményként kezelendők:

- A mentőrendszer nem képes mentést végrehajtani
- Egy vagy több média elveszett, nem fellelhető
- A mentési média meghibásodott, a visszaállított információ sérült
- A mentési médián található információ illetéktelen birtokába jutott
- A visszaállítási teszt sikertelen
- A mentett információ nem elérhető (megsemmisült, véletlenül törölték)
- A mentés ütemezése sérült, a beállított ütemezés nem megfelelő, vagy a mentés leállt.

A fenti eseményeket a Help Desk rendszeren keresztül jelenteni kell.

12. INFORMÁCIÓS RENDSZEREK FEJLESZTÉSE

12.1 Bevezetés

A fejlesztési tevékenységet úgy kell megtervezni, hogy a biztonság az információs rendszer szerves része legyen.

Az információs rendszer fejlesztése magába foglalja a következő tevékenységeket:

- kereskedelmi termékek beszerzése,
- egyedi fejlesztések.

12.2 Kereskedelmi termékek beszerzése

Az információs rendszerek fejlesztése kapcsán a kereskedelmi termék alatt következőket értjük:

- hardver eszközök
- szoftver eszközök
- kiegészítő, támogató eszközök (klímaberendezés, lemezszekrény stb.)

A kereskedelmi termékek beszerzése a *Beszerzési Szabályzatban* meghatározottak alapján történik, a következő kiegészítésekkel:

- a beszerzéseket során az biztonsági szempontok érvényesítése az **információbiztonsági vezető** feladata
- biztonsági szempontból szabályozni szükséges a felhasználók által letöltött (ingyenes vagy éppen fizetős) szoftverek használatát is, ebben az esetben egy egyszerűsített jóváhagyási eljárást kell érvényesíteni.

12.2.1 Biztonsági szempontok érvényesítése

Az informatikai szervezett által beszerzett kereskedelmi termékek beszerzésénél alkalmazott biztonsági szempontok:

- Az **információbiztonsági vezető** előzetes jóváhagyása szükséges a beszerzések indításához.
- A termékeket a CSAPI biztonságosnak tekinti abban az esetben, ha a termék **megbízható gyártótól** származik.
- Az **információbiztonsági vezető** a beszerzendő termék felhasználása kapcsán **kockázatelemzést** végez és ennek alapján javaslatot tesz a beszerzési követelmények változtatására (ha szükséges).

Az egyes termékek bevezetését követően a biztonság fenntartását az üzemeltetési eljárások, a műszaki sebezhetőségek kezelése és a rendszeres átvizsgálások (auditok) biztosítják.

12.2.1.1 Megbízható gyártók

Megbízható gyártónak tekinthetőek azok a gyártók, akik az adott szakterület legjobbjaihoz tartoznak a világpiacon.

Azon gyártók esetében, akik kevésbé ismertek, további vizsgálódások szükségesek: pl. referenciák, független szervezetek véleménye, tesztelések.

A kereskedelmi termékek vonatkozásában a CSAPI számára elfogadható szállítókat és termékcsoportokat az **információbiztonsági vezető** hagyja jóvá. A jóváhagyásról feljegyzést kell készíteni és azt az informatika dokumentumai között meg kell őrizni.

12.2.1.2 Információbiztonsági kockázatelemzés

Az **információbiztonsági vezető** – szükség esetén belső vagy külső szakértő(k) bevonásával – megállapítja, hogy a beszerzendő eszköz milyen információbiztonsági kockázatot jelent a CSAPI számára. Az azonosított kockázatok alapján szükséges lehet:

- a beszerzési követelményeket módosítani és/vagy
- további biztonsági intézkedéseket (kontrollokat) megtervezni és bevezetni

12.2.2 Egyszerűsített jóváhagyási eljárás

A beszerzési eljárás keretében beszerzett és az informatika által támogatott rendszereken túlmenően a felhasználóknak szükségük lehet szoftver termékek közvetlen, a felhasználó által végzett beszerzésére (letöltésére).

Ebben az esetben a biztonsági szempontok érvényesítése úgy valósul meg, hogy a felhasználók csak a *„Tűrt szoftverek"* listáján szereplő szoftvereket tölthetik le.

Amennyiben az igényelt szoftver nem szerepel ezen a listán, annak felvételét kell kérni a Help Desk *Változás kezelési eljárása* keretében.

A **felhasználó** a saját számítógépén nem tud telepíteni szoftvereket, csak és kizárólag a rendszergazdai joggal nem rendelkező programok esetén képes ezt megtenni.

A felhasználó által letöltött és telepített szoftverek esetében a **felhasználó** kötelessége:

- a szoftver licensz feltételeit betartani
- a szoftver frissítéséről gondoskodni.

12.3 Egyedi fejlesztések

Egyedi fejlesztés alatt értjük a CSAPI kezdeményezése alapján végzett szoftver (alkalmazás) fejlesztéseket, amelyek a CSAPI folyamatok speciális igényeit elégítik ki. Ebbe a körbe tartoznak azok a szoftver-fejlesztések is, amelyek kereskedelmi szoftver keretrendszerek testre szabását jelentik. (Kereskedelmi szoftverek konfigurálása nem tartozik ebbe a körbe.)

12.3.1 Beszerzési, szerződéskötési folyamat

Külső felek által végzett szoftver fejlesztések minden esetben szerződés alapján történnek. Belső fejlesztés esetén írásbeli megbízás szükséges.

A fejlesztési igények, elvárások kezdeményezése a **területi vezetők** hatásköre. Az igények rögzítése a Help Desk rendszerben történik, ahol a *Változás kezelési* folyamat mentén valósul meg a fejlesztés.

A fejlesztési megvalósításáról született döntést követően a megkötésre kerülő fejlesztési szerződésekben érvényesíteni kell az információbiztonsági szempontokat a következőben leírtak szerint.

12.3.2 Fejlesztési szerződések tartalmi követelményei

A szoftver-fejlesztési szerződéseknek tartalmaznia kell a következőket:

- A külső felekre vonatkozó szerződési feltételek
- A fejlesztés elvárt eredményeinek funkcionális és technikai specifikációja
- Információbiztonsági követelmények
- Részletes átvételi eljárás

A specifikáció és az átvételi eljárás részeként ki kell alakítani a tesztelési szabályokat a következők szerint:

- Részletes tesztelési tervet kell készíteni, és a tesztet annak megfelelően kell elvégezni.
- A teszt eredményeket részletesen dokumentálni kell, és a dokumentumokat meg kell őrizni.
- A teszt környezetnek el kell különülnie az üzemelési (éles) rendszerektől, ugyanakkor a lehető legnagyobb mértékben hasonlítania kell az alkalmazott éles rendszerhez.
- A tesztelést a fejlesztőktől független szakembereknek kell végezniük a CSAPI **információbiztonsági vezetőjének** felügyelete alatt.
- A tesztek elvégzésébe kulcsfelhasználókat is be kell vonni.

12.3.3 Az információbiztonsági szempontok érvényesítése a fejlesztési folyamatban

A fejlesztések teljes életciklusa során a biztonsági szempontokat érvényesíteni kell a következők szerint:

- Kezdeményezési fázis
  - az Üzleti specifikációban az igénylőnek meg kell határoznia a specifikált termékhez/szolgáltatáshoz kapcsolódó fontosabb üzleti kockázatokat, biztonsági elvárásokat
- Tervezési fázis
  - a rendszertervben meg kell határozni a biztonsági követelményeket a megfogalmazott üzleti kockázatok és a legjobb gyakorlatok figyelembevételével
- Végrehajtási fázis

- a fejlesztés során érvényesíteni és rendszeresen ellenőrizni kell a biztonsági követelmények megvalósulását a tesztelési terveknek megfelelően
- Lezárási, átadási fázis
  - az átadás átvétel során el kell végezni a biztonsági követelmények ellenőrzését
  - a lezárt fejlesztés eredményeképpen átadott végtermék dokumentációjában meg kell határozni az üzemeltetésre vonatkozó alapvető biztonsági követelményeket

A fejlesztési folyamat során meg kell vizsgálni a következőkben felsorolt biztonsági intézkedések (kontrollok) szükségességét és **döntést kell hozni** rájuk vonatkozó konkrét követelményekről:

12.3.3.1 Rendelkezésre állási elvárások teljesítése

- A megrendelő által megfogalmazott üzletmenet folytonossági (BCP) elvárások teljesítése az IT szolgáltatásfolytonossági (ITCP) követelmények meghatározásával és megvalósításával.
- Az IT alkalmazások/rendszerek rendelkezésre állásnak kiesésének kockázatát megelőző intézkedésekkel szükséges csökkenteni.
- Katasztrófa helyzetek esetén a visszaállítási feladatok (DRP) követelményeinek meghatározása, a végrehajtás megtervezése és a szükséges erőforrások biztosítása.

12.3.3.2 Bizalmassági és sértetlenségi elvárások teljesítése

- Titkosítás használata
  - jelszavak titkos tárolása
  - rendszeradminisztrátori hozzáférések tikosítása
  - szigorúan bizalmas adatok tárolása (ha szükséges)
- Forráskód tulajdonlásának igénye
  - történjen intézkedés arról a helyzetről, amikor a beszállító nem képes többé a fejlesztési és hibajavítási tevékenységét ellátni
- Szigorú fejlesztési verziókövetés
  - szerepalapú hozzáférést kell megvalósítani, amely lehetővé teszi a hozzáférések korlátozását a feladatvégzéshez szükséges minimumra
- Felhasználói hozzáférés szabályozás
- Naplózás
  - A fejlesztendő alkalmazás rendelkezzen logolási képességgel, aminek segítségével a használat során bekövetkező minden lényeges művelet felhasználóhoz és időponthoz köthető.
- A legveszélyesebb kódolási hibák elkerülése
  - A szerződő vállalkozásnak (a fejlesztőnek) a kódolási hibák ellenőrzésére megfelelő eljárásokkal kell rendelkeznie.

12.3.4 Leszállítandó dokumentumok jegyzéke

Meg kell határozni a fejlesztés során elkészítendő dokumentumokat.

A fejlesztési feladat terjedelmétől függően az alábbi dokumentumok vagy témakörök elkészítéséről illetve módosításáról kell döntést hozni:

- Üzemeltetési kézikönyv

- Felhasználói kézikönyv
- Migrációs terv
    - Visszaállási terv
- Oktatási terv és oktatási anyagok
- Mentési utasítás
- Visszaállítási utasítás (üzemzavart/katasztrófát követően)

13. RENDSZERÜZEMELTETÉS ÉS AZ ELEKTRONIKUS KOMMUNIKÁCIÓ BIZTONSÁGA

13.1 Rendszer-üzemeltetés és dokumentálás

A CSAPI rendszereinek üzemeltetését és adminisztrálását dokumentált eljárások alapján kell végezni. Ezen dokumentumokat elektronikus formában minden érintett számára elérhető helyen, rendszerezve, informatikai erőforráson kell elhelyezni.

Az alkalmazás üzemeltetőjének feladata az adott rendszerhez tartozó dokumentációk naprakészen tartása és hozzáférésének biztosítása.

Az üzemeltetési szabályzatokban a következő tevékenységeket kell szabályozni:

- az üzemeltetéshez kapcsolódó szerepkörök felelősségei;
- a rendszerek üzemeltetési feladatainak leírása;
- a hibáknak és olyan, más kivételes helyzeteknek a kezelése, amelyek a munkafeladat végrehajtása során léphetnek fel, beleértve a rendszer segédprogramok használatára vonatkozó korlátozásokat is;
- a biztonsági frissítések tesztelési és telepítési eljárásrendje;
- a váratlan üzemeltetési és műszaki nehézségek eseteire vonatkozó támogatási szerződések és kapcsolattartók;
- a rendszerek újraindításának és visszaállításának eljárásai, melyeket hibák fellépése esetén alkalmaznak.

Az **információbiztonsági vezető** feladata a dokumentációk meglétének ellenőrzése és hatályosságának felülvizsgálata a jelen szabályzatban rögzített biztonsági követelmények figyelembevételével.

Az alkalmazások üzemeltetőinek dokumentált és naprakész hardver- és szoftverleltárt kell vezetniük minden hozzájuk rendelt eszközről, berendezésről és szoftverről. A dokumentumnak tartalmaznia kell az eszközök fellelhetőségének helyét, a kapcsolódó felelősségeket, valamint a használatra vonatkozó adatokat.

13.2 Rendszerüzemeltetés

Az **IT üzemeltetés** a munkavállalók részére munkakörük ellátásához szükséges általános irodai szoftverekkel ellátott munkaállomást (asztali számítógépet), az informatikai hálózathoz való csatlakozási lehetőséget, Internet használatot, valamint az elektronikus levelező rendszerben postafiókot biztosít. A rendeltetésszerű használatot az **adott munkavállaló felettes szervezeti vezetője** ellenőrzi.

13.2.1 Az informatikai rendszer felépítése és működése

A CSAPI informatikai rendszerének elemeit (számítógépes erőforrások és az üzemeltetési mód szempontjából) részletesen a Hálózati rajz tartalmazza.

13.2.2 Hardver / szoftver – kezelés, leltár és nyomon követés

13.2.2.1 Szoftver

Az új szoftvereket vagy a régiek módosításait minden esetben tesztelni kell az éles bevezetés előtt.

A számítógépekre a szoftvereket a **rendszeradminisztrátor** vagy a **szoftvert szállító cég munkatársa** telepíti. Meglévő programokat módosítani, lecserélni, vagy kitörölni csak az **IT üzemeltetés** jogosult.

Az információbiztonság teljes körű megvalósításához szorosan hozzájárul a jogtiszta szoftverek használata, ebből kifolyólag a CSAPI-nál csak jogtiszta szoftverek üzemelhetnek. Ennek ellenőrzése érdekében az **információbiztonsági vezető** rendszeres szoftver-auditokat végeztet.

A rendszeres szoftver-vizsgálat során ellenőrizni kell:

- A használatban lévő szoftverek rendelkeznek-e licence-el,
- A megvásárolt licencek számának a használt szoftverek mennyiségével arányban kell lenniük,
- A használt szoftverek verziószámát,
- A ténylegesen használt szoftverek megegyeznek-e a szoftverleltárban foglaltakkal.

A CSAPI eszközein kizárólag olyan alkalmazói és/vagy rendszer szoftver használható, amelyet a CSAPI vásárolt, fejlesztett vagy fejlesztetett, illetve az **információbiztonsági vezető** annak a használatát engedélyezte.

A CSAPI szoftvereinek nyilvántartása érdekében az **IT üzemeltetés** a szoftverekről nyilvántartást vezet, mely az alábbi adatokat tartalmazza:

- a szoftver azonosítója,
- a szoftver neve,
- a szoftver verzió száma,
- a szoftver készítőjének (egyedi fejlesztés esetén) neve,
- a szoftver telepítési (licence kulcs) azonosítója.

13.2.2.2 Hardver

A számítástechnikai hardver eszközök beszerzésénél a 12. fejezetben meghatározott szempontokat kell figyelembe venni.

A számítógépek telepítését, üzembe helyezését csak az **IT üzemeltetés rendszergazdái** végezhetik.

Amennyiben egy informatikailag támogatott üzleti folyamat kritikussága megköveteli azt, hogy helyileg elérhető tartalék eszközök álljanak rendelkezésre, az adott informatikai hátteret redundánsan kell megvalósítani, biztosítva azt, hogy egy-egy, a rendszeren belül üzemeltetett eszköz meghibásodása, kiesése ne fenyegesse az adott munkafolyamat működtetését.

A tartalékeszközök rendelkezésre álló mennyiségének el kell érnie a minimális működéséhez szükséges mennyiséget. A tartalék eszközöket mindig megfelelő műszaki állapotban kell tartania a **rendszeradminisztrátornak**.

13.2.3 Védekezés vírusok, rosszindulatú és mobil kódok ellen

A védekezés célja a CSAPI informatikai rendszerének rosszindulatú/kártékony programok elleni védelmének biztosítása.

A védelmi rendszer minimális elemei:

- kizárólag jogtiszta szoftverek használata, ellenőrizhető forrásból
- tűzfalas védekezés (internet kijáratokon kívül a notebook-okon kötelezőként beállítandó),
- internetre és levelezésre kiterjedő tartalomszűrés,
- kéretlen levél (spam) elleni védelem,
- és vírusvédelmi rendszer.

A CSAPI informatikai rendszereinek biztonságos üzemeltetéséhez az **IT üzemeltetés** feladata gondoskodni a vírusvédelmi rendszer kialakításáról és működtetéséről, illetve annak szabályozásáról. Ezen tevékenységekre központi rendszert kell működtetni, automatikus frissítésekkel.

13.2.3.1 Aktív védelem

Valamennyi számítógépre telepíteni kell az **információbiztonsági vezető** által jóváhagyott vírusvédelmi rendszert és annak állandóan működnie kell, továbbá rendszeres verziófrissítést kell végrehajtani a legutolsó verzió használatának céljából. Az aktív védelem kikapcsolása tilos!

Az a **felhasználó**, aki az adatait és adathordozóit a vírus ellenőrzés vagy vírusvédelmi intézkedés (vírusirtás) alól bármilyen indokkal kivonja, az abból eredő károkért teljes felelősséggel tartozik.

13.2.3.2 Elektronikus levelezés vírusvédelme

Az elektronikus levelezés a vírusok továbbításának leggyorsabb és leggyakoribb módja, ezért erre külön figyelmet kell fordítani.

Ha a levél vagy a csatolt állomány fertőzött, arról a víruskereső szoftver értesíti a felhasználót és a rendszeradminisztrátort. Ha az aktív védelem nem képes a fertőzés eltávolítására, akkor a víruskereső rendszer a fertőzött állományt karanténba helyezi.

Az e-mailben ok nélkül, váratlanul vagy a levél szövegében nem indokoltan érkezett állomány esetében a melléklet tartalmának személyes (pl. telefonos) vagy e-mailben történő ellenőrzése szükséges.

Az elektronikus levelező rendszeren keresztül történő támadások esetén, amennyiben a rendszer védelme átmenetileg nem biztosított, az intraneten kívül eső elektronikus levélforgalmat ideiglenesen le kell állítani. Ennek elrendelésére az **információbiztonsági vezető** jogosult.

13.2.3.3 Passzív védelem (offline ellenőrzés)

A passzív védelem feladata a teljes állományrendszer átvizsgálása, tekintet nélkül az állományok használatba vételére.

A munkaállomásokon a víruskereső programokat úgy kell beállítani, hogy havonta egyszer megtörténjen az automatikus és kikényszerített vírusteszt futtatása. A tesztek eredményét automatikusan ellenőrizhető logfile(ok)ba kell rögzíteni. A rendszerbe kívülről bekerülő adatokat (akár pendrive-on beérkező, akár az Internetről letöltött adatról van szó) felhasználás előtt vírusellenőrzésnek kell alávetni.

Felhasználói tulajdonú adathordozók használata esetén az adott eszköz használata következtében okozott károkért a CSAPI rendszereiben **felhasználóként belépett személy** a felelős (pl. vírusos USB kulcs), amennyiben az adott felhasználó felelőssége egyértelműen megállapítható.

13.2.3.4 Telepítés

A víruskereső rendszerek telepítése az IT üzemeltetés feladata, ennek eredményeképpen minden külső adat fogadására alkalmas munkaállomáson rendszeresen frissített vírus-figyelő és törlő programnak kell működnie.

Az újonnan rendszerbe állított, illetve újratelepített számítógépeken gondoskodni kell a víruskereső rendszer azonnali telepítéséről. Vírusvédelemi rendszer nélkül sem hálózati, sem önálló számítógép nem üzemeltethető.

A központi gépeken és a tűzfalon a vírusvédelem programjait úgy kell installálni, hogy minden file-megnyitás, futtatható file indítása, és file írási műveletet automatikusan ellenőrizzenek. Az ellenőrzés felfüggesztése tilos!

13.2.3.5 Frissítések

A víruskereső programok frissítését, valamint a kliens eszközökre történő replikációt úgy kell beállítani, hogy az automatikusan, naponta legalább egyszer megtörténjen.

A víruskereső rendszert fejlesztő cégektől érkező figyelmeztetésekre reagálva indokolt esetben azonnali kiegészítő vírusadatbázis-frissítés szükséges.

A vírusvédelemmel kapcsolatos valamennyi frissítést (vírus adatbázis, biztonsági frissítések, keresőmotor, stb.) az **IT üzemeltetés** végzi.

13.2.4 Hálózatmenedzsment és védelem

A CSAPI számítógépes hálózatának, a CSAPI birtokában lévő információk jogosulatlan hozzáféréstől, támadástól való védelmének, a vírus- és spam-védelemnek, a portok védelmének, a hálózati és kommunikációs struktúra, elkülönítések, valamint a jogosultsági rendszerek kialakításának technikai megvalósítása, kivitelezése, az üzemeltetési rend kialakítása, figyelemmel kísérése az **IT üzemeltetés** feladata.

13.2.5 Tűzfal és hálózati rendszerkörnyezet

Az **IT üzemeltetés** feladata a tűzfal- és hálózati eszközök üzemeltetése. A CSAPI belső hálózatához csatlakoztatott személyi számítógépeket tilos egyidejűleg külső hálózathoz is csatlakoztatni.

A tűzfalak biztonsági beállításainak meg kell felelniük az alábbi elvárásoknak és a feladatok elvégzését biztosítani kell:

- A tűzfalszabályokat illetve azok változtatását az **információbiztonsági vezető**nek engedélyezni kell
- A tűzfalak beállításainak és naplóállományainak mentése (naponta)
- A tűzfalak szabályainak felülvizsgálata (évente legalább egy alkalommal)
- A tűzfal rendszer és a hálózati szegmentáció kialakításának felülvizsgálata (évente legalább egy alkalommal)
- A hibák kezelésének felelőse a kijelölt rendszergazda.
- A normál működéstől eltérő eseményekről tájékoztatni kell az információbiztonsági vezetőt
- A tűzfal rendszerrel kapcsolatosan dokumentálni kell az alábbiakat:

- A tűzfalon felismerhető biztonsági incidenseket, azok megszüntetésére tett intézkedéseket,
- Működési incidenseket, azok megszüntetésére tett intézkedéseket,
- A tűzfalak frissítéseinek (biztonsági frissítések, verziófrissítések) végrehajtását.

13.2.5.1 Hálózati rendszer üzemeltetése

Az informatikai hálózat üzemeltetése során a **rendszergazdának**

- minden esetben meg kell változtatnia az alapértelmezett (gyári) beállításokat a rendszerben található hálózati elemeken;
- gondoskodnia kell a hálózati architektúrában található aktív hálózati elemek rendszerbe történő beállításáról és a folyamatos szoftver-frissítésekről
- dokumentálniuk kell a CSAPI Internet hozzáférésének beállításait, logikai és fizikai struktúráját (Hálózati rajz). A dokumentáción keresztül az információbiztonsági vezetőnek meg kell bizonyosodnia arról, hogy a hozzáférési jogosultságok szabályait teljes körűen alkalmazták-e.

Harmadik felek csatlakozása CSAPI hálózatához:

- Kizárólag az **információbiztonsági vezető** adhat engedélyt egy harmadik fél számára, hogy a CSAPI hálózatára csatlakozzon.
- Harmadik fél kizárólag fix hálózati (IP) címeket használhat azokon a gépeken, amelyekkel a CSAPI hálózatára kapcsolódnak.
- Az **IT üzemeltetésnek** meg kell határoznia azon számítógépek és erőforrások címeit a CSAPI hálózatában, amelyekhez elérési lehetőséget biztosít a harmadik fél felé.
- A CSAPI és a harmadik fél IP címeit egymáshoz kell rendelni az engedélyeknek megfelelően, ezzel biztosítva, hogy az egyes emberek csak a meghatározott szerverekhez, szolgáltatásokhoz férhessenek hozzá.
- A tűzfal beállításain csak az **információbiztonsági vezető** engedélyével lehet változtatni.

13.2.5.2 Vezeték nélküli hálózatok (Wi-Fi)

A CSAPI által használt vezeték nélküli hálózatot tűzfallal kell elválasztani a hálózat többi részétől. A tűzfal beállítására és ellenőrzésére a „Tűzfal és hálózati rendszerkörnyezet" pontban leírtakat kell érvényesíteni.

A vezeték nélküli hálózatra csatlakoztatott eszközök közvetlenül nem érhetik el a CSAPI belső hálózatát, csak az internetre kapcsolódhatnak. Az interneten keresztüli csatlakoztatás a belső hálózathoz a távoli munkavégzés szabályai szerint kell, hogy történjen.

13.3 Csoportmunka (osztott) könyvtárak és fájlszerverek

Az **IT üzemeltetés** feladata elegendő központi tárterület biztosítása, ahol a felhasználók a csoportmunka könyvtárakba elhelyezhetik az általuk munkaállomásaikon kezelt, üzleti szempontból érzékeny adatokat, információkat.

Ezeken a tárterületeken kialakított adatstruktúrák és adatkönyvtárak szerkezetét, felépítését az **IT üzemeltetés** az **egyes szervezeti egységek vezetőivel** együttműködve határozza meg. A könyvtárak megnevezéseit lehetőség szerint, úgy kell megadni, hogy azok a bennük lévő állományok milyenségére, a kapcsolódó munkafeladatra, projektre, vagy az állományok felhasználójára útmutatást adjanak. Az állománynevek pedig a bennük tárolt adatok tartalmára utaljanak.

A **felhasználók** kötelesek ügyelni arra, hogy a csoportmunka könyvtárakban csak a valóban fontos, üzleti szempontból érzékeny adatokat tárolják. A **felhasználók** feladata, hogy a rendelkezésre álló területtel ésszerűen gazdálkodjanak. Egy könyvtárban lehetőleg csak összetartozó információk legyenek. Más felhasználó adatait egy adott - pl. azonos szervezeti egységben dolgozó - felhasználónak módosítani, kitörölni csak az adatok tulajdonosának tudtával és egyetértésével lehet.

A központi tárterületeken tárolt információk rendelkezésre-állásért és azok biztonsági mentéséért az **IT üzemeltetés** a felelős.

13.4 Adathordozók biztonságos kezelése

Biztonsági események (elvesztés, eltulajdonítás, illetéktelen hozzáférés, engedély nélküli kivitel) elkerülése érdekében szabályozzuk és felügyeljük az eltávolítható adathordozók kezelését.

A papíralapú dokumentumok és iratok kezelését, selejtezését az Iratkezelési Szabályzat rögzíti.

13.4.1 Külső tároló eszközök

Szigorúan tilos saját, felhasználói tulajdonban lévő külső tároló eszközöket a személyi számítógépekre kötni. Külső tárolónak a következő eszközök tekintendők:

- USB pendrive-ok,
- memória kártyák,
- merevlemez-meghajtók,
- okos telefonok, PDA-k, tabletek, stb.

Amennyiben az adott munkakörhöz szükséges, a felhasználónak kell igényelni eszközt a HelpDesk rendszeren keresztül. Használati engedélyt az **információbiztonsági vezető** adhat. Jelen tiltás a beépített CD/DVD írókra nem vonatkozik.

A munkavégzés céljából az egyes munkavállalók számára biztosított vállalati tulajdonú külső eszközökért, és az azon tárolt adatokért az **adott felhasználó** kiemelt felelősséggel tartozik.

„Bizalmas" információkat tartalmazó adatokat, fájlokat csak megfelelő titkosítással ellátott adathordozón tárolhatóak, mozgathatóak.

13.5 Elektronikus kommunikáció

13.5.1 Az Internet biztonságos használatának szabályozása

Az Internetet a **felhasználók** a munkaköri leírásukban meghatározott feladataik elvégzéséhez, mint szolgáltatást használhatják, betartva az ide vonatkozó szabályokat, utasításokat. Ezen szolgáltatás minden magán és egyéb célú használata során esetlegesen bekövetkezett károkért a **felhasználó** teljes felelősséggel tartozik.

Az internet szolgáltatás minőségének szinten tartása és a CSAPI érdekeinek biztosítása céljából, a **rendszeradminisztrátor** az **információbiztonsági vezető** engedélyével bizonyos korlátozásokkal élhet. A korlátozások a következőkre térhetnek ki:

- Bizonyos file típusok letöltésének korlátozása,
- Alapvető etikai normákat sértő oldalak látogatásának tiltása,
- Illetve a látogatható web oldalak körének behatárolása és a maximális file letöltési méret korlátozása.

A CSAPI munkavállalói csak az **IT üzemeltetés szerződött partnere** által engedélyezett internet kijáratokon keresztül csatlakozhatnak az Internethez. Bármely egyéb módon történő internet elérés létesítése az azt kialakító munkavállaló felelősségre vonását eredményezi. Tilos továbbá a felhasználóknak a Web-böngészők biztonsági beállításait megváltoztatni. Hálózati munkaállomások az Internethez kizárólag a CSAPI hivatalos Internet kijáratán (központi tűzfalán) keresztül csatlakozhatnak.

Az informatikai rendszer biztonsága érdekében az internet felhasználók által meglátogatott oldalak az **IT üzemeltetés szerződött partnere** által folyamatosan naplózásra kerülnek. A naplók szigorúan titkosak, azokat az adatvédelmi előírásoknak megfelelően kell kezelni. Tilos tudatosan kihasználni az esetlegesen előforduló szoftver hibákat, védelmi hiányosságokat. Tilos a felhasználóknak jogosulatlan, a CSAPI érdekeivel ellentétes cselekményt végrehajtaniuk az Internet használata közben. Tilos a felhasználóknak az Internet használata során törvény- vagy jogellenes tevékenységet megvalósítaniuk.

Az Internet eléréssel kapcsolatos teljes forgalmat tartalmi (böngészés) és mennyiségi szempontból rendszeresen (de legalább negyedévente) ellenőrizni kell, mely a **rendszeradminisztrátor** feladata. Ezekről az ellenőrzésekről, illetve annak eredményéről a **rendszeradminisztrátor** köteles írásban tájékoztatni az **információbiztonsági vezetőt**. Ezt akkor is meg kell tennie, ha mindent rendben talált.

13.5.2 Az elektronikus levelezés biztonságos használatának szabályozása

Felhasználóknak az elektronikus levelezéshez, mint szolgáltatás hozzáféréséhez az **információbiztonsági vezető** engedélye szükséges. Az elektronikus levelezést a felhasználók munkaköri leírásaikban meghatározott feladataik elvégzéséhez használhatják. Ezen szolgáltatás minden magán és egyéb célú használata során esetlegesen bekövetkezett károkért a **felhasználó** teljes felelősséggel tartozik.

A CSAPI levelező rendszerén tárolt és továbbított levelek, a CSAPI tulajdonát képezik, ezért az IBSZ-ben és az egyéb CSAPI szabályzatokban feljogosított ellenőrző munkavállalóknak ezekhez az állományokhoz, a vizsgálathoz szükséges mértékig betekintési joga van. Ha az e-mail címben a felhasználó (munkavállaló) neve, illetve a név töredéke fel van tüntetve, akkor azt adatvédelmi szempontból úgy kell kezelni, mint a hagyományos személyes levelezést, így a munkáltató az érintett hozzájárulása nélkül annak tartalmát nem ismerheti meg, az érkező küldeményeket (elektronikus levelek, üzenetek) nem tarthatja vissza, és nem semmisítheti meg.

Az informatikai rendszer működőképességét veszélyeztető fenyegetés (vírus-fertőzés, levélbombák, egyéb külső támadás stb.) esetén a **rendszeradminisztrátor** illetve az **információbiztonsági vezető** a postafiók használatát felfüggesztheti, az érintett felhasználó hozzájárulásával és jelenlétében a veszély megszüntetése érdekében azt átvizsgálhatja és szükség esetén újra konfigurálhatja. A postafiók átvizsgálása során esetlegesen megismert személyes adatok vonatkozásában az **átvizsgálást végző informatikai munkatársat** titoktartási kötelezettség terheli. Az átvizsgálási-intézkedési kérelem elutasítása esetén a postafiók megszüntetésre kerül. Az intézkedésekről az **információbiztonsági vezető** tájékoztatja az érintett felhasználót és a munkáltatói jogokat gyakorló vezetőjét.

Az elektronikus levelezés során a következő szabályok betartását kell megkövetelni:

- A felhasználóknak tilos a CSAPI nevében olyan e-mailt küldeni, csatolt fájlt megjelentetni elektronikus hirdetőtáblákon vagy egyéb fórumokon, melyek:

- a CSAPI hírnevét, vagy az ügyfelekkel való kapcsolatát ronthatják, illetve a CSAPI ügyfeleinek érdekét sérthetik,
- törvényt illetve a CSAPI belső szabályait sértik
- a CSAPI bizonyos területekre vonatkozó álláspontját képviselik, fejezik ki,
- szerzői jogokat sérthetnek,
- vírusokkal fertőzhetnek meg bármely hálózatot,

- A levelet csak akkor szabad megnyitni, ha a levél megbízható feladótól származik. Nem szabad megnyitni például az angol nyelven írt, nyereményekre és ismeretlen, megrendelt küldeményekre utaló leveleket, ezeket haladéktalanul törölni kell. Ha a felhasználó bizonytalan a levéllel kapcsolatos teendőt illetően, segítséget a HelpDesk-től kérhet.
- A felhasználóknak tilos láncleveleket készíteni és továbbítani. Tilos továbbá más felhasználóktól, illetve külső hálózatról kapott támadó, vagy „szemét" („junk") jellegű, a hálózat túlterhelését célzó e-mailek továbbítása.
- Az elektronikus levelek olvasás nélkül történő automatikus továbbítása csak a szervezeten belül engedélyezett.
- Az **információbiztonsági vezető** meghatározni azoknak az információknak a körét, amelyek elektronikus levelezés útján történő forgalmazása korlátozható.
- Tilos tudatosan kihasználni az esetlegesen előforduló szoftver hibákat, védelmi hiányosságokat.
- A CSAPI-t elhagyó elektronikus levél tartalmát automatikusan ki kell egészíteni az adatvédelmi záradékkal.
- 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. Ezen levelek meghatározásáért az **információbiztonsági vezető** a felelős.
- A nem azonosítható, kétes forrásból származó üzeneteket, lehetőség szerint nem szabad megnyitni és ki kell vizsgáltatni az érintett informatikus munkatárssal.
- A CSAPI levelező rendszere az üzletmenettől idegen reklám, valamint egyéb üzleti célokra nem használható.
- A CSAPI elektronikus levelezési címjegyzéke nem szolgáltatható ki harmadik félnek, semmilyen célból.
- A tárterületek védelmének érdekében a CSAPI informatikai rendszerén belül minimalizálni kell a fájlok küldését. A fájl hozzáférhető módon történő elhelyezése után, lehetőség szerint a fájlra mutató linket kell elküldeni elektronikus levélben. Általános szabály, hogy törekedni kell arra, hogy egy fájl, csak egy példányban legyen tárolva a rendszerben. A csatolmányok maximális mérete bejövő és kimenő leveleknél 10 MB lehet,
- „Bizalmas" információk esetén a küldött csatolt és/vagy tömörített állományok jelszavazása kötelező, mely a **feladó** felelőssége,
- Az egyes felhasználói postafiókok mérete nem haladhatja meg az 500MB-ot.

13.5.3 Távközlési eszközök (telefon, fax stb.) biztonságos használata

Minden munkavállaló a távközlési és adatátviteli eszközök használata során köteles a következő szabályokat betartani:

- Az információk nyilvánosságra kerülésének elkerülése érdekében a telefonbeszélgetések során ügyelniük kell:
  - a közvetlen környezetükben tartózkodó emberekre, különösen mobiltelefon használata során,
  - a hívott félnél tartózkodó személyekre.
- Ne folytassanak bizalmas telefonbeszélgetéseket nyilvános helyeken vagy nyitott irodákban.
- Ne tároljanak feleslegesen üzenetet az üzenetrögzítő készülékeken, illetve nyilvános rendszereken, mert ezeket illetéktelen személyek visszajátszhatják, elolvashatják. Megismerés után le kell törölni, vagy biztonságos helyen kell tovább tárolni.
- A faxgépek használata során a következő eshetőségeket kell figyelembe venni:
  - a dokumentumok és üzenetek téves számra való elküldése,
  - a gépek szándékos vagy véletlen programozása egy meghatározott címre szánt üzenetek továbbítására,
  - illetéktelen hozzáférés a beépített üzenettárolókhoz, az üzenetek visszakeresése és lehallgatása.

A CSAPI munkavállalóin kívüli további személyek (vendégek, külsős partnerek, szolgáltatók stb.) a CSAPI tulajdonú telefonokat kizárólag vészhívásokra használhatják.

13.6 Elektronikus kereskedelem

A Társaság elektronikus kereskedelmi szolgáltatásokat nem nyújt partnereinek, ilyen követelmény vele szemben nem merülhet fel.

A CSAPI internetes honlapjaival kapcsolatos tevékenységek és kommunikáció összehangolásáért az **információbiztonsági vezető** a felelős.

13.7 Forráskód-könyvtárak védelme

Az **információbiztonsági vezető** felelőssége, hogy a fejlesztés és/vagy tesztelés alatt álló rendszerek tekintetében a következő védelmi intézkedések érvényesítésre kerüljenek:

- megfelelően szét kell választani az üzemeltetési környezetet a teszt, illetve a fejlesztési környezettől;
- a **rendszeradminisztrátoroknak** a forráskódot tartalmazó könyvtárakhoz való hozzáférési jogosultságait korlátozni kell, csak az arra **felhatalmazott fejlesztők** végezhetnek ott műveleteket;
- fejlesztés, vagy karbantartás alatt álló rendszereket nem szabad forráskódokat tartalmazó könyvtárakban tárolni, kezelni;
- a forrásprogramok korábbi verzióit archiválni kell, pontosan megjelölve azok keletkezésének dátumát, illetve éles üzemben történt alkalmazásuknak időpontját;

13.8 Műszaki sebezhetőség kezelése

Az üzemelő információs rendszerek műszaki sebezhetőségeiről aktuális információkat kell beszerezni, azokat elemezni kell és intézkedéseket kell hozni a kapcsolódó kockázatok kezelésére.

Műszaki sebezhetőségi vizsgálatot kell végezni **kétévente egyszer** az összes szerverre és a hálózati aktív eszközökre, valamint a munkavállalói gépek meghatározott mintacsoportjára.

A műszaki sebezhetőségek feltárását a tématerületre szakosodott szakértők segítségével, professzionális sérülékenység vizsgálati eszközök felhasználásával kell végrehajtani. Bizonyos területek részletesebb vizsgálatára, adott esetben betörés tesztet (etikus hackelés) kell végezni.

A kritikus és súlyos sérülékenységek javítását 3 hónapon belül el kell végezni.

A sérülékenységek kezelése három módon történik:

- javító biztonsági patch-ek telepítése
- a hibás konfiguráció kijavítása
- valamilyen átmenti megoldás (work-around)

A műszaki sebezhetőségek feltárása és azok megfelelő kezelése az **információbiztonsági vezető** feladata illetve felelőssége.

13.8.1 Patch menedzsment

A patch-ek letöltése kizárólag megbízható forrásból hajtható végre, egyéb oldalakról patch-eket letölteni tilos. A lehetséges további sebezhetőségek elkerülése érdekében a letöltött patch-eket hitelesíteni kell, továbbá minden esetben vírus ellenőrzés alá kell vetni. Ezen feladatok végrehajtásáig a patch nem installálható. Amennyiben lehetséges az adott patch-eket az éles rendszerhez hasonló teszt környezetben futassuk ezzel kikerülve az előre nem látható hibákat.

14. HOZZÁFÉRÉS-SZABÁLYOZÁS

A CSAPI információs vagyonához való jogosulatlan hozzáférések és a véletlen módosítások megakadályozása érdekében a CSAPI minden informatikai berendezését, alkalmazási rendszerét, szolgáltatását, szerveren tárolt információját megfelelő hozzáférési szabályok védik. A védelem a felhasználók azonosításával és hitelesítésével – felhasználói név és jelszó megadásával – valósul meg.

A hozzáférések munkakörhöz, ellátandó feladathoz kapcsolódnak, és munkakör változásakor változnak.

Az üzemelő rendszerhez külső munkatárs csak indokoltan, átmenetileg, ellenőrzötten és tevékenységét dokumentáltan kaphat hozzáférési jogosultságot.

14.1 Általános hozzáférési szabályok

A hozzáférési jogosultságok körét úgy kell kialakítani, hogy:

- a meghatározott jogosultsági körök alkalmazásával minimalizálható legyen a rosszindulatú vagy egyéb jogosulatlan hozzáférés,
- kizárólag a munkavégzés végrehajtásához szükséges jogosultsági körök legyenek meghatározva
- az egyes területek kapcsán meghatározott jogosultsági körök összhangban legyenek az információk osztályozásával,
- legkisebb szükséges jogosultság beállításának elve: A felhasználók részére a CSAPI informatikai eszközeihez minden esetben azt a lehető legkisebb hozzáférést biztosító jogosultsági struktúrát kell kialakítani, amely a részére meghatározott tevékenységek elvégzéséhez minimálisan szükséges.
- Felhasználók nem rendelkezhetnek a rendszergazdai jogosultsággal.
- A CSAPI informatikai rendszereiben bármilyen típusú rendszergazdai jogosultságot csak az kaphat, aki informatikai rendszeradminisztrációs tevékenységet végez. Ebben az esetben is alkalmazni kell a legkisebb szükséges jogosultság beállításának elvét. Rendszeradminisztrátori jogosultság kizárólag az **információbiztonsági vezető** jóváhagyását követően lehetséges, tevékenységének teljes körű naplózása mellett.
- összhangban legyen a feladat és felelősségi körök szétválasztásával;
- legyen lehetőség a jogosultságok számonkérésére, ellenőrzésére, visszavonására.

Az **információbiztonsági vezető** felelőssége meghatározni és dokumentált formában rögzíteni:

- azon eljárásokat, amelyek alkalmazásával a felhasználó az informatikai erőforrásokhoz hozzáférési jogosultságot igényelhet;
- azon eljárásokat, amelyeket végre kell hajtani a felhasználók áthelyezése, távozása esetén;
- azon eljárásokat, amelyeket végre kell hajtani a hozzáférési jogosultságok naprakészen tartása érdekében.

Az **információbiztonsági vezető** félévente gondoskodik annak ellenőrzéséről, hogy az alkalmazott és a rendszerben beállított hozzáférési jogosultságok összhangban vannak-e a munkaköri feladatok ellátásához szükséges jogosultságokkal. Az **információbiztonsági vezető** feladata annak ellenőrzése, hogy a rögzített jogosultságigénylési eljárások megfelelően kerülnek-e alkalmazásra.

14.2 Hozzáférési jogosultságok kezelése (kiadása, visszavonása, felfüggesztése, nyilvántartása)

A felhasználók azonosítása alatt az informatikai rendszerhez hozzáférő felhasználók személyazonosságának (identitásának) a rendszerben történő egyedi, egyértelmű és hiteles megjelenítését értjük.

A jogosultságok kiosztásakor az információbiztonsági vezető szükség esetén (például a munkakörre jellemző tipikus jogoktól történő eltérés esetén) egyedileg is dönthet a jogosultsági szintről.

A felhasználó azonosítónak meg kell felelni az egyediség kritériumának: különböző felhasználók számára egyazon azonosító nem adható ki, azonban egyazon fizikai személynek több azonosítója is lehet az adott hozzáféréstől függően.

Kivételt képez a csoportos e-mailek használata, melyekhez az **információbiztonsági vezető** felhatalmazásában megnevezett felhasználók férhetnek hozzá.

A felhasználói azonosítók képzésére és új felhasználók rendszerbe történő felvitelére kizárólagosan a **rendszeradminisztrátor** jogosult. A hozzáférési jogosultságok kezelése, a jogosultság igénylés folyamata a HelpDesk rendszeren keresztül történik.

14.3 Felhasználói szintű hozzáférés

Felhasználói státuszra a felhasználó a munkaviszonyának kezdetétől a munkavégzés alóli felmentésének időpontjáig jogosult.

A felhasználók kiindulásként hozzáférést kapnak az alap hálózati szolgáltatásokhoz. A munkakörhöz kapcsolódó alkalmazásokhoz szükséges további hozzáférési jogosultságot az adott munkakörbe helyezéskor kapják meg.

A felhasználók számára személyenként külön felhasználó azonosítókat (user ID) kell alkalmazni azért, hogy a felhasználói tevékenységek ellenőrizhetők legyenek. A hozzáférési igényt az **információbiztonsági vezető** bírálja el. Jóváhagyás esetén a felhasználó azonosítót az **rendszeradminisztrátor** hozza létre, és regisztrálja az új felhasználót a következőkben bemutatott metodika szerint.

A belsős munkavállalók felhasználói név konvenciója a következő:A felhasználó nevéből képzett azonosítót kell alkalmazni, a következő szabály szerint:

Munkaviszonnyal rendelkezők esetén: Ékkezetlenített Vezetéknév + "." + Ékkezetlenített Keresztnév. Példa:

- Minta Árpád a következők szerint alakul: minta.arpad@csapi.hu
- Amennyiben két vagy több azonos nevű Minta Árpád dolgozik a CSAPI-nál akkor növekvő sorszámmal a következők szerint: minta.arpad1@csapi.hu; minta.arpad2@csapi.hu; stb.

Ezzel a szabállyal biztosítható, hogy nem fordulhat elő azonos név, ezért nem szükséges definiálni további egyezősség kezelést.

A jelszavak tárolása védett módon kell, hogy történjen, mely az Információbiztonsági vezető számára sem nyilvános. Amennyiben a felhasználó elfelejti jelszavát, abban az esetben csak a **felhasználó** által jóváhagyott felülírására van lehetőség.

Minden rendszerhozzáférés esetén a felhasználó kezdeti jelszót kap, melyet köteles az első bejelentkezés alkalmával megváltoztatni a jelszópolitikának megfelelően.

Az engedélyezett és a jelenleg beállított felhasználói jogosultságok rendszeresen (félévente) történő ellenőrzése, felülvizsgálata az **információbiztonsági vezető** feladata és felelőssége.

Minden jogosultsággal kapcsolatos igény, változás, beállítás dokumentálásra kell, hogy kerüljön.

A képzésre, tesztelésre használt felhasználói azonosítókat el kell különíteni az üzleti folyamatok felhasználói azonosítóitól, és tilos, hogy oktatások során bármilyen hozzáférést adjanak az éles üzleti rendszerekhez.

14.3.1 Külsősök, illetve ideiglenes hozzáférési jogosultságok

Meghatározott időre szóló hozzáférési jogosultságok esetén (pl.: külső alkalmazásfejlesztők, szerződés keretében szakértői tevékenységet folytató személyek stb.) az informatikai rendszerekhez ideiglenes hozzáférési jogosultságot kell igényelni, mely határozott időtartamú, de legfeljebb fél évig érvényes.

Szerződő partner esetében mindig meg kell határozni a jogosultság élettartamát.

Szerződő partner hozzáférési jogosultságinak kezelési eljárásai:

- csak érvényes és hatályos szerződés alapján férhet szerződő Partner a CSAPI hálózatához,
- a szerződés részeként titoktartási nyilatkozatban kell kötelezettséget vállalnia a szerződő Partnernek,
- minden szerződő partnernek kell a CSAPI-n belüli kapcsolattartót kijelölni,
- a CSAPI és a szerződő Partner közötti kommunikáció, annak közegétől függetlenül, csak a belső kapcsolattartón keresztül engedélyezett,
- a **belső kapcsolattartónak** a szerződő Partner részére szükséges hozzáférési jogosultságokat kell igényelnie,
- az **információbiztonsági vezetőnek** felülvizsgálati joga van az igénylés tekintetében,
- a szerződő partnernek kiadandó jogosultságot csak meghatározott időintervallumra lehet engedélyezni, beállítani,
- a belső kapcsolattartó felelőssége biztonságosan eljuttatni a szerződő Partnernek a hozzáférési jelszavát (a jelszóra vonatkozó szabályozás megegyezik a munkavállalókra vonatkozó szabályozással),
- a szerződő Partner felhasználói név konvenciója (VPN esetében): vezetéknév.keresztnév,
- a szerződő Partner felhasználói név konvenciója (domain esetében): vezetéknév_keresztnév,
- a szerződő Partner felhasználói név konvenciója az érintett alkalmazások esetében eltérő,
- a szerződő Partnernek kötelessége azonnal jelezni a belső kapcsolattartónak, ha munkavállalói változásai érintik a kiadott hozzáférési jogosultságokat.

Az **rendszeradminisztrátorok** feladata, hogy az ideiglenes jogosultságok beállítása során rögzített lejárattal állítsák be az engedélyezett jogosultságokat, ahol ez műszakilag támogatott. A rögzített lejárat maximális ideje 6 hónap lehet.

14.4 Felhasználó-hitelesítés

14.4.1 Felhasználói jelszavak kezelése

A felhasználóknak gondoskodniuk kell az általuk használt jelszó bizalmasságának megőrzéséről. A felhasználók azonnal kötelesek jelenteni a HelpDesk részére, ha jelszavuk kompromittálódott, és haladéktalanul intézkedniük kell felhasználói fiókjuk letiltásáról vagy jelszavuk megváltoztatásáról.

A **felhasználók** felelőssége, hogy

- a jelszóválasztás során a rendszerben előírt minőségű jelszavakat válasszanak;
- a választott személyes jelszavaikat titokban tartsák;
- a választott jelszavakat lehetőség szerint nem szabad feljegyezni papírra, vagy más, illetéktelenek számára hozzáférhető helyre, tárgyra,
- a jelszó és a felhasználói azonosító soha ne kerüljön postai küldeménybe vagy elektronikus levelezésbe.

A jelszóválasztással kapcsolatosan a **rendszeradminisztrátoroknak**, illetőleg a jelszót kezelő **alkalmazások tervezőinek**, **fejlesztőinek** a feladata, hogy számítógépes eljárások alkalmazásával (pl.: jelszógondozó rendszer alkalmazása, domain policy) a felhasználókat az IBSZ előírásainak megfelelő jelszóválasztásra kényszerítsék.

Bejelentkező névhez tartozó jelszót csak a kijelölt **rendszeradminisztrátorok** állíthatnak be, illetve közölhetnek (külön csatornákon) abban az esetben, ha

- Új felhasználó felvétele, vagy egyéb ok (pl. elfelejtés) miatt a felhasználó előtt még ismeretlen új belépési jelszót definiált.
- Ebben az esetben a következő szabályok érvényesek:
  - Elfelejtés esetén a felhasználó a **rendszeradminisztrátortól** igényelhet új jelszót. A felhasználó azonosítása a **rendszeradminisztrátor** feladata.

A felhasználói jelszavak minőségével kapcsolatos követelmények a CSAPI előírásaival összhangban:

- a felhasználóknak meg kell változtatniuk ideiglenes jelszavaikat az első bejelentkezéskor;
- a jelszó megváltoztatásakor a felhasználónak meg kell adni a régi jelszót, mielőtt létrehozhatná az újat;
- a jelszónak tartalmaznia kell a következő karakterek közül háromfélét (lehetőség szerint szűrő segítségével kell biztosítani a jelszavak megadása során):
  - angol ABC kisbetűi (a..z),
  - angol ABC nagybetűi (A..Z)
  - tízes számrendszer számai (0..9),
  - speciális karakterek (pld.: !%$_),
- A jelszóban kerülni kell:
  - az ékezetes betűk használatát, valamint a „0", „z" és az „`", „y" billentyűzetenkénti felcserélődése miatt adódó bizonytalanságot.
  - jelszóként a jelszó tulajdonosával kapcsolatba hozható vagy ismert szót, kifejezést választani.
- A jelszó nem lehet azonos a felhasználói azonosítóval.
- a jelszóknak minimum 8 alfanumerikus karakterből kell állniuk (nem lehetnek köznevek, szótári szavak vagy kifejezések);

- a rendszeradminisztrátori jelszavak minimális hossza 12 karakter.
- az új jelszónak különböznie kell a régitől, úgy, hogy a felhasználó ne egy kiszámítható mintát kövessen, pl. apple1a, apple2b, apple3c;
- a jelszókat titokban kell tartani, azaz nem szabad megosztani, számítógépes rendszereken tárolni, vagy programokba kódolni;
- a jelszókat legalább 6 havonta változtatni kell;
- jelszócserénél a korábban használt 4 db jelszó már nem adatható meg, tehát minden jelszócserénél új jelszót kell kialakítani,
- Tilos az informatikai rendszerben ismert parancsot vagy alkalmazás nevet jelszóként használni.

A jelszavak kezelésével kapcsolatos általános szabályok

- A jelszavakat email-en elküldeni nem szabad, kizárólag abban az esetben, ha egyéb más alternatív csatornák használatára nincs lehetőség.
- A jelszavakat a számítógépes rendszerben nyílt formában tárolni tilos, gondoskodni kell megfelelő titkosítási védelemről
- Belépéskor a beírt jelszó ne legyen olvasható a képernyőn,
- Egy jelszó minimum 1 napig érvényes (1 napon belül nem lehet kétszer megváltoztatni).
- Mind a sikeres, mind a sikertelen belépési és kilépési kísérleteket naplózni kell.
- Ha egy felhasználói azonosító 60 napig inaktív, akkor azt a szervezeti egység vezetőjének tájékoztatása mellett a rendszert üzemeltető rendszergazdának fel kell függeszteni.

Csakis azok az informatikai és távközlési eszközök, amelyről kimutatható, hogy nem rendelkeznek a fenti valamelyik kritérium megvalósítását lehetővé tévő funkcionalitással mentesülhetnek a jelszavakra vonatkozó biztonsági követelmények alól. A mentesülés engedélyét az **információbiztonsági vezető** kell kiadnia.

14.4.2 Bejelentkezés

A **rendszeradminisztrátorok** feladata a felhasználói munkaállomások tekintetében a megfelelő paraméterek beállítása úgy, hogy a bejelentkezési folyamat során:

- A rendszer használhatóságának határain belül minimalizálni kell az olyan üzenetek megjelenítését a bejelentkezés folyamata alatt, amely segíthetné a jogosulatlan hozzáférési kísérleteket.
  - a rendszer vagy az alkalmazás ne jelezze ki a felhasználó nem publikus azonosítóját, amíg a bejelentkezési folyamat sikeresen be nem fejeződött,
  - ne jelezze ki a legutoljára belépett felhasználó nevét, azonosítóját,
  - nem szabad olyan hibaüzenetet szolgáltatnia, amely a jogosulatlan felhasználót bármilyen információ gyűjtésében segíthetné (felhasználói név, IP cím stb.),
  - bármilyen hiba is okozta a hibahelyzetet, a rendszernek nem szabad jeleznie, hogy a megadott bejelentkezési adatok mely része helyes vagy hibás,
- A bejelentkezést csak akkor lehet érvényesíteni, ha a bejelentkezéshez szükséges összes adat sikeresen átesett a hitelesítési procedúrán. Ha hibafeltétel jelentkezik, a rendszernek a használhatóság határain belül csak minimális jelzést szabad adnia, hogy az adatoknak melyik része helyes vagy helytelen.
- Ahol technikailag kivitelezhető, korlátozni kell a sikertelen bejelentkezési kísérletek számát.

14.4.3 Sikertelen bejelentkezés

Az **információbiztonsági vezető** felelős annak ellenőriztetéséért, hogy ahol **technikailag kivitelezhető**, az adott rendszerbe történő sikertelen bejelentkezési eljárások során alkalmazásra kerüljenek a következők:

- ideiglenesen fel kell függeszteni a felhasználói hozzáférési jogosultságokat a 3. próbálkozást követően;
- rögzíteni kell a sikertelen kísérletet;
- korlátozni kell a bejelentkezésre rendelkezésre álló maximális időt, és ha a folyamat túllépi a megengedett határt a rendszer automatikusan léptesse ki a felhasználót,
- a zárolt fiók feloldása vagy a **rendszeradminisztrátor** által oldható fel vagy automatikusan kerüljön feloldásra a zárolási idő (pl.: 15 perc) letelte után.

14.5 Alkalmazás és információ szintű hozzáférés

Az adatbázisok védelmét az alkalmazásokra kialakított jogosultsági rendszer biztosítja. Az adatbázisok sajátos védelmi technikáit a felhasználókkal nem szabad megismertetni.

Az információkhoz és alkalmazási rendszer funkcióihoz való felhasználói hozzáférés szabályainak megalkotása, a hozzáférés szükséges minimális szinten tartása az alkalmazás fejlesztési folyamata során az **információbiztonsági vezető** feladata. A **fejlesztő** felelőssége minden rendszerhez elkészíteni – a vezető jóváhagyja – a felhasználók és a rendszer által nyújtott szolgáltatások felhasználói mátrixát. Az alkalmazások ellenőrzéséhez való hozzáférés biztosítása a **rendszeradminisztrátor** feladata.

14.6 Változáskezelés

A rendszerekben bekövetkező illetve azokat érintő változtatásokat dokumentált formában kell végrehajtani. A változások engedélyezését, majd végrehajtását csak az arra feljogosított személyek végezhetik el.

Az engedélyezett változtatásokat tesztelni, a tesztelés eredményeit dokumentálni kell, és ki kell dolgozni a változtatás végrehajtásának tervét, illetve a sikertelen változtatás esetén a visszaállítási eljárásokat.

A módosítások végrehajtását követően az adott rendszerdokumentációt a végrehajtott változás szerint aktualizálni szükséges az adott **rendszerért felelős munkatársnak**.

A szükséges hardver és rendszer-szintű szoftverváltoztatások bevezetéséről az **Információbiztonsági vezető** dönt. A szoftver, hardver változások nyilvántartásáról, leltározásáról, a változáskezelésről az **IT üzemeltetés** gondoskodik.

A változáskezelés folyamata részleteiben az IT Szolgáltatásmenedzsment (Help Desk) projekt során kerül kidolgozásra.

14.7 Rendszer-hozzáférések ellenőrzése, monitorozása

A felhasználók tevékenységéről, a rendszerek működéséről, a mentésekről, a gépteremben történt eseményekről naplóállományok készülnek és kerülnek megőrzésre oly módon, hogy utólag megállapíthatóak legyenek az informatikai rendszerben bekövetkezett fontosabb események, különös tekintettel azokra, melyek a rendszer biztonságát érintik.

A naplózás legfőbb célja az elszámoltathatóság és auditálhatóság biztosítása.

Az információbiztonsági szempontból naplózandó adatok körét az **információbiztonsági vezető** határozza meg. Minimális követelményként az alábbi események naplózása szükséges:

- sikeres és sikertelen bejelentkezések és kijelentkezések;
- a biztonsággal kapcsolatos paraméterek, beállítások változtatása, különös tekintettel a felhasználói profilokra és engedélyekre, biztonsági politikákra.

A CSAPI szerverein az **IT üzemeltetésnek** biztosítania kell a naplózást és a naplóállományok megőrzését.

Naplóbejegyzés készül az alábbi eszközök vonatkozásában:

- szerverek
- tűzfalak
- alkalmazások

A naplóbejegyzések terjedjenek ki a következőkre:

- rendszerindítások, leállások
- rendszeróra-állítások
- be-kijelentkezések
- programleállások és indítások
- rendszeradminisztrátorok műveletei

A naplózással szemben támasztott követelmények:

- a naplóállományokat a forrásgéptől elkülönítve kell gyűjteni egy erre célra kialakított logszerver segítségével
- a naplóállományok mentéséről gondoskodni kell

A napló állományok utólagos módosításának lehetőségét minimalizálni kell, ezért az éles rendszerek adminisztrátorai nem adminisztrálhatják a logszervert, erre a feladatra másik személyt kell megbízni. A naplózandó eszközök órajeleit szinkronizálni kell.

15.MEGBÍZHATÓ MŰKÖDÉS BIZTOSÍTÁSA

15.1 Rendelkezésre-állási követelmények

Az **információbiztonsági vezető** felelőssége, hogy az **IT üzemeltetéssel** történő egyeztetés alapján meghatározza az egyes informatikai szolgáltatások rendelkezésre állási követelményeit az információ-osztályozás (lásd 8.3 pont) alapján.

Az egyes IT szolgáltatásokat megvalósító rendszerek úgy kell megtervezni és üzemeltetni, hogy megfeleljenek a meghatározott rendelkezésre állási követelményeknek.

15.2 IT szolgáltatásfolytonosság irányítása

Az IT szolgáltatásfolytonossági követelmények azonosítása, felmérése az információs vagyon kockázatelemzése keretében történik. A kockázatelemzés során meghatározott **kritikus üzleti folyamatok** támogatására IT Szolgáltatásfolytonossági Tervet kell készítenie az **IT üzemeltetésnek** az **Információbiztonsági vezető** szakmai irányítása mellett.

A terv két fő területe:

- Megelőző Intézkedések
- IT Katasztrófa Elhárítási Terv

15.2.1 Megelőző intézkedések

A megelőző intézkedések a szolgáltatásfolytonossági tervezés része, azokat az intézkedések jelenti, amelyek a folyamatos működés megszakadásának valószínűségét csökkentik.

A megelőző intézkedések kidolgozásakor a következőket kell elsősorban figyelembe venni:

- Technikai meghibásodások elleni védelem
  - Redundáns rendszerek használata
  - Szerverek környezeti védelme (szerverszoba)
  - Eszközök életciklusának menedzselése
- Szünetmentes tápellátás biztosítása
  - UPS rendszerek használata
  - Diesel generátorok alkalmazása

15.2.2 IT Katasztrófa Elhárítási Terv kialakítása és karbantartása

Bármilyen gondosan is tervezzük a megelőző intézkedéseket, bekövetkezhetnek olyan események, amelyek az IT szolgáltatás megszakadásához vezetnek. Ebben az esetben az incidenskezelési eljárás (16. fejezet) szerint kell eljárni. Amennyiben az incidenskezelési eljárás súlyos üzemzavart azonosít, abban az esetben az IT Katasztrófa Elhárítási terv szerint kell eljárni.

Az IT Katasztrófa Elhárítási Tervnek a következőket kell tartalmaznia:

- A katasztrófa elhárítási terv érvényességének behatárolása.
- A katasztrófa elhárítási tervhez kapcsolódó felelősségek és hatáskörök behatárolása.
- A katasztrófa elhárításában résztvevő személyek feladatai jogai és kötelességei.
- A katasztrófa elhárítás közben történő jelentési kötelezettségek.
- A katasztrófahelyzet kezelésének menete.
- A katasztrófa utáni helyreállítási intézkedések.

16. INFORMÁCIÓBIZTONSÁGI INCIDENSEK KEZELÉSE

Jelen fejezet szabályozza az információbiztonságot érintő események kezelésének hatékony, szervezett és dokumentált folyamatát, valamint az incidenskezelő folyamatok szerinti működés feltételeit, valamint az ezt támogató Help Desk rendszer ide vonatkozó funkcióit.

16.1 A Help Desk szerepe

A Help Desk-nek meghatározó szerepe van az incidensek kezelésében. Minden információbiztonsági incidenst a lehető legrövidebb időn belül jelenteni kell a Help Desk felé, ahol a bejelentés rögzítésre kerül.

A bejelentés forrásai a következők lehetnek:

- felhasználók
- IT üzemeltetés
- automata (IT management rendszerek riasztásai)

A Help Desk beviteli felületei:

- Web interfész
- E-mail
- telefon (csak a felhasználók számára és csak incidensek esetén)

Kategorizálás 1.szint, a bejelentéseket az alább megadott két kategória körébe kell sorolnia a bejelentést fogadó **incidens menedzsernek:**

- Incidens
- Változáskérés (ide tartozik a fejlesztési igény is)

A változáskérések rögzítésre kerülnek, azok további kezelését a *Változáskezelési Utasítás* tartalmazza.

Az incidensek kezelését a jelen incidenskezelési leírás tartalmazza.

16.2 Az információbiztonsági incidens kezelés célja és kategóriái

Az információbiztonsági incidens kezelés elsődleges célja zavar esetén a normál szolgáltatási feltételek visszaállítása, amilyen gyorsan az lehetséges, minimalizálva az üzleti tevékenységre gyakorolt káros hatását, így biztosítva a szolgáltatás minőségének lehetséges legjobb színvonalát.

Az információbiztonsági incidensek természetük szerint két fő kategóriába sorolhatók:

- Biztonsági incidens – az adatok bizalmasságát, sértetlenségét veszélyeztető esemény
- Rendelkezésre állási incidens – az informatikai rendszerek hibás működése vagy működésképtelensége, amely a felhasználó számára nem teszi lehetővé az adotok illetve a szolgáltatások elérését

16.3 Biztonsági incidens

Biztonsági incidensről akkor beszélünk, amikor bizalmas adatok illetéktelen tudomására jutnak, vagy ennek a gyanúja felmerül, illetve amikor a Vállalat adatainak megszerzésére vagy az informatikai rendszer megkárosítására irányuló cselekményt észlelünk.

- A naplózási/nyilvántartási kötelezettségek.
- A katasztrófa szintek meghatározása.
- A megelőzés szabályainak és alapelveinek meghatározása.
- A felkészülés szabályainak és alapelveinek meghatározása.
- A jelzési és riasztási rendszer kialakítása.
- A katasztrófahelyzet esetén végrehajtandó tevékenységek.
- A pótlólagos helyiségek kiválasztása és kijelölése.
- A katasztrófahelyzetből és a katasztrófa elhárítási folyamatból levont tapasztalatok kezelése.
- A katasztrófahelyzet kezelési tervben foglaltak tesztelési és felülvizsgálati gyakorisága.

Az **IT üzemeltetés** és az **információbiztonsági vezető** feladata gondoskodni, hogy az elkészült IT Katasztrófa Elhárítási Terv

- oktatásra és szétosztásra kerüljön a megfelelő körben,
- tesztelése megtörténjen,
- folyamatos felülvizsgálata és karbantartása rendszeres időközönként megtörténjen.

Az **információbiztonsági vezető** feladata gondoskodni az IT Katasztrófa Elhárítási Terv és másolati példányainak két, egymástól független telephelyen történő elhelyezéséről.

Biztonsági incidens lehet például:

- Informatikai eszközök elvesztése
- Fizikai vagy logikai hozzáférések megsértése
- Biztonsági szabályzatok, utasítások megszegése
- Egyéb „gyanús" esemény (hacker vagy vírustámadás, phising)

Az azonnali intézkedések megtétele az **incidens menedzser** felelőssége és feladata.

Az azonnali intézkedések részeként az **incidens menedzser** értesíti az **információbiztonsági vezetőt.**

A további intézkedések megtétele, az incidens kivizsgálása az **információbiztonsági vezető** feladata.

Az esemény súlyossága indokolhatja külső szervezetek, hatóságok bevonását a vizsgálatba. Külső felek bevonása csak az **vezérigazgató** engedélyével történhet.

16.4 Rendelkezésre állási incidens

A rendelkezésre állási incidens súlyossága alapján megkülönböztetünk:

- meghibásodást,
- üzemzavart és
- súlyos üzemzavart.

Az azonnali intézkedések végrehajtása az **incidens menedzser** felelőssége és feladata.

További intézkedések is az **incidens menedzser** feladatába tartoznak, de az incidens súlyossága alapján az irányítási felelősséget adott esetben át kell adnia az **információbiztonsági vezetőnek.**

16.4.1 Meghibásodás

Meghibásodásnak tekintünk minden olyan felhasználói számítógépet érintő hibát vagy egy-egy szerver rövid idejű leállását, amely nem zavarja számottevően a normális munkavégzést és a napi üzemeltetési feladatok sorában gyorsan kijavítható.

A meghibásodások elhárítása az **incidens menedzser** feladata.

A meghibásodásról az elhárítás közben kiderülhet, hogy komolyabb problémáról van szó, azaz a meghibásodások nagyobb számú felhasználót érintenek, több szerver hibásodott meg, illetve nyilvánvalóvá válik, hogy a normál működési állapot nem állítható vissza a Help Desk üzemeltetési eljárásában meghatározott időtartamon belül. Ebben az esetben az **incidens menedzser** üzemzavarnak minősíti az eseményt.

16.4.2 Üzemzavar

Üzemzavarnak nevezzük azokat a meghibásodásokat, amelyek nagyobb számú felhasználót érintenek, pl.: több szerver meghibásodik vagy nem elérhető. Üzemzavar esetén az **incidens menedzser** értesíti az **információbiztonsági vezetőt,** aki az incidens elhárítási tevékenységet közvetlenül irányítja, és szükség esetén dönt további erőforrások bevonásáról.

Üzemzavar esetén az **információbiztonsági vezető** döntése alapján a **kulcsfelhasználók** is bevonásra kerülnek a hibaelhárítási, kárenyhítési folyamatokba.

16.4.3 Súlyos üzemzavar

Súlyos üzemzavarnak nevezzük azokat az üzemzavarokat, eseményeket, amelyek következményei jelentős anyagai és/vagy erkölcsi kárt okozhatnak a CSAPI-nak.

Ezekben az esetekben az **információbiztonsági vezető** értesíti a **vezérigazgatót** illetve a **területi vezetőket** és a továbbiakban a **vezérigazgató** irányításával történik a súlyos üzemzavar elhárítása.

A súlyos üzemzavarok kezelését a CSAPI IT Katasztrófa Elhárítási Terve alapján kell elvégezni.

16.5 Az incidens kezelés fő lépései

16.5.1 Azonnali intézkedések

Azonnali intézkedések alatt értjük azokat az eljárásokat és tevékenységeket, amelyeket az üzemzavar bekövetkeztének pillanatától kell végezni, annak érdekében, hogy a CSAPI hatékonyan és érdemben tudjon reagálni az eseményekre. Ezek a következők:

- azonnali kárelhárítás,
- tevékenységek, szolgáltatások leállítása,
- bizonyítékok gyűjtése és megvédése,
- eszkaláció.

Az azonnali intézkedések megtételéért **az incidens menedzser** a felelős.

16.5.1.1 Azonnali kárelhárítás

Magába foglal minden olyan tevékenységet, ami az incidens továbbterjedését, súlyosabbá válását megakadályozhatja. Például: tűzoltás, emberek kimenekítése, vízbefolyás megszüntetése, illetéktelenek eltávolítása stb.

16.5.1.2 Tevékenységek, szolgáltatások leállítása

Szükség esetén ki kell kapcsolni az áramszolgáltatást, a gázellátást (robbanásveszély), számítógépeket, vagy informatikai szolgáltatásokat kell lekapcsolni (pl. veszélyes vírustámadás, vagy behatolás)

16.5.1.3 Bizonyítékok gyűjtése és megvédése

Az incidenseket okozhatja szándékos cselekmény (bűntény), ezért a bizonyítékok megvédésére és összegyűjtésére tekintettel kell lenni.

16.5.1.4 Eszkaláció

Az incidens felmérése során, vagy későbbiekben a visszaállítási tevékenység alatt kiderülhet, hogy a probléma súlyosabb, mint az első értékelés alapján megállapított szint.

Amennyiben az incidens menedzser úgy ítéli meg, hogy saját hatáskörben nem képes az elvárt idő alatt elvégezni a meghibásodás kijavítását:

- értesíti az **információbiztonsági vezetőt** – 2. szint: Üzemzavar

Amennyiben az **információbiztonsági vezető** úgy ítéli meg, hogy az üzemzavar jelentős anyagai és/vagy erkölcsi kárt okozhat a CSAPI-nak:

- értesíti a vezérigazgatót – 3. szint: Súlyos üzemzavar

16.5.2 Kommunikáció

Informatikai üzemzavar esetén az eseménnyel kapcsolatos belső kommunikációra csak az **incidens menedzser** és az **információbiztonsági vezető** jogosult.

Tilos külső felekkel (pl. media, ügyfelek) – kivéve az érintett támogató szervezetek, személyeket – az incidenssel kapcsolatos bármilyen információt közölni. Külső felekkel való kommunikációra csak az a **vezérigazgató** jogosult.

Az üzemzavar elhárítást végző informatikusnak tájékoztatnia kell a **HelpDesk**-et, az elhárítás várható időtartamáról, illetve minden, a felhasználót érintő új eseményről.

16.5.3 Működés visszaállítási terv

Működés visszaállítási terveket kell készíteni a CSAPI kritikus rendszereire, annak érdekében, hogy komolyabb meghibásodások esetén a visszaállításhoz szükséges tudás és erőforrás rendelkezésre álljon.

16.5.4 Alternatív működési eljárás

Súlyosabb, várhatóan hosszabb ideig tartó szolgáltatás kiesés esetén az informatikának meg kell vizsgálnia, hogy a normál működés visszaállításáig valamilyen helyettesítő (alternatív) szolgáltatást nyújtható-e a felhasználóknak. Az alternatív működés általában alacsonyabb szolgáltatási szintet jelent, mint a normál működés, de lehetővé teszi a CSAPI kritikus üzleti folyamatainak bizonyos szintű működtetését. Kisebb szolgáltatás kiesések esetében is érdemes helyettesítő folyamatot alkalmazni, ha az viszonylag egyszerű, kézenfekvő. Meg kell fontolni, hogy az alternatív működés költsége arányba áll-e az általa biztosított előnnyel.

16.5.5 Tartalék erőforrások biztosítása

A működés visszaállítási tevékenységhez szükséges olyan tartalék erőforrásokat (eszközöket) meghatározni és rendelkezésen tartanai, amelyek képesek pótolni az incidensek következtében megsérült vagy nem elérhető erőforrásokat.

16.5.6 Az incidens lezárása

Az incidens lezárási szakaszában elvégzendő feladatok:

- a kulcsfelhasználó értesítése és visszaigazolás kérése az adott rendszer / szolgáltatás működőképességéről
- adminisztratív lezárás a Help Desk rendszerben

16.6 Az incidenskezelés dokumentálása és elemzése

Az incidenseket a Help Desk rendszerben dokumentálni szükséges. A dokumentálása két részből áll:

- Feljegyzések az incidensről, amely az incidens kezelés során meghozott döntéseket és a történéseket tartalmazza.
- Az incidens elemzése

16.6.1 Az incidens elemzése

Az incidensek elemzésének célja a tanulságok levonása. Ez a tevékenység legalább a következőket tartalmazza:

- az incidens bekövetkezésének körülményeit,
- az incidens közvetlen és közvetett kiváltó okait
- a lehetséges intézkedéseket, amelyek csökkenthetik az incidens ismételt bekövetkezésének valószínűségét.
- elemzést az incidens során tett intézkedések hatékonyságáról,
- szükség esetén javaslatokat az incidens kezelési folyamat javítására
- további feladatok meghatározása

Az elemzés mélysége legyen arányban az esemény súlyosságával.

Az incidensek elemzésé az **információbiztonsági vezető**nek kell jóváhagynia.

17.KISZERVEZÉS (OUTSOURCING)

A kiszervezett tevékenységek üzletmenet folytonosságának tekintetében az **információbiztonsági vezető** feladata gondoskodni arról, hogy a szerződésekben az informatikai biztonság szempontjai érvényesüljenek.

A kiszervezés feltételeinek és körülményeinek meghatározását ún. Szolgáltatási Szint Megállapodás – SLA (Service Level Agreement) dokumentumban kell meghatározni. Ezen belül rögzíteni kell az információbiztonságra vonatkozó elvárásokat is, amelyek alapján az **Információbiztonsági Teamnak** kell mérlegelnie a kiszervezendő tevékenység szerződésének információbiztonsági követelményeit. Ennek megfelelően a dokumentumnak tartalmaznia kell:

- a harmadik fél hitelességét a szakmai, stratégiai és biztonsági szempontból;
- a szolgáltatás minőségét a CSAPI üzleti elvárásainak szempontjából;
- a szolgáltatás megbízhatóságát;
- a titoktartásra vonatkozó követelményeket;
- a szolgáltatás során a megismerhető adatok körét;
- a biztonságos, akkreditált eszközök használatának kötelezettségét;
- a felek felelősségvállalását;
- a szolgáltatás nem megfelelő minőségéből eredő üzleti kockázatokat;
- az adatok nyilvánosságra kerülését megelőzendő esetlegesen egy szükséges beavatkozás során alkalmazandó közvetlen irányítás és menedzselés lehetőségeit, módszereit;
- az adatkezelési és védelmi módszereket;
- az előre nem látott események tekintetében az alkalmazandó katasztrófa-elhárítási terveket.

18.AZ INFORMÁCIÓBIZTONSÁG FÜGGETLEN VIZSGÁLATA (IBIR-AUDITOK)

Az IBIR hatékony működésének elősegítése érdekében a rendszer részterületeit, elemeit és működését éves terv alapján legalább egyszer ellenőrizni, illetve felülvizsgálni szükséges. A CSAPI IBIR-ét teljes körűen felül kell vizsgálni annak érdekében, hogy a hatékonyság igazolást nyerjen.

18.1 A belső audit tervezése

Az IBIR hatékony működésének elősegítése érdekében a rendszer részterületeit, elemeit és működését éves terv alapján legalább egyszer ellenőrizni, illetve felülvizsgálni szükséges. Az auditok sorrendjét, időbeli ütemezését, a vizsgálandó területeket és / vagy folyamatokat, valamint a vizsgálatot végző személyeket a *Belső audittervben* kell összefoglalni. A belső auditterv elkészítése az **információbiztonsági vezető** feladata.

Auditot csak a társaság azon tagjai végezhetnek, akik:

- ismerik a jelen fejezetben meghatározott, belső auditokra vonatkozó követelményeit, az alkalmazandó mellékleteket és azok használatát,
- az audit elvégzésében járatosak,
- függetlenek az auditált területen végzett munkáért közvetlenül felelős személyektől.

Az **információbiztonsági vezető** - az **igazgató** engedélyével - megfelelően képzett külső auditorokat is bevonhat a belső audit végrehajtásába. Ilyen esetben elfogadható a külső auditorok által alkalmazott módszertan és bizonylatolási forma, de a feltárt nem megfelelőségeket minden esetben írásban kell kérni.

Az éves *Belső auditterv* jóváhagyása az **igazgató** feladata.

Az **információbiztonsági vezető** közreműködésével a jóváhagyott *Belső audittervet* a társaság hálózatán az érintett munkavállalóknak elérhetővé teszi.

Abban az esetben, ha valamely területen belül az auditkritériumok működtetése során ismétlődő nem megfelelőség merül fel, az **igazgató** - az **információbiztonsági vezető** javaslatára is - az audittervtől függetlenül rendkívüli belső auditot kezdeményezhet. A mérlegelés alapja a probléma súlyossága, amelynek megítélése az **igazgató** feladata és felelőssége. A rendkívüli belső auditot a *Belső audittervben* kell feljegyezni. A sorszámát 1-től kezdődően "/R" jelzéssel kell megadni és időpont egyeztetést követően kell indítani.

18.2 Felkészülés a belső auditra

Az auditorok az audit megkezdése előtt a felülvizsgálandó területekre vonatkozóan összeállítják a *Belső audit kérdés listát*, melyen meghatározzák az audit kérdéseit.

A Belső audit kérdés lista és ezzel a felülvizsgálat tervezett módszerének és irányának jóváhagyása az **információbiztonsági vezető** feladata.

18.3 A belső audit lefolytatása és követő intézkedései

Az audittervben meghatározott és az **érintett szervezettel** egyeztetett időpontban az ellenőrzési listán rögzített módon a **megbízott auditor** lefolytatja az auditot.

Az **érintett szervezet vezetője** felelős az audit végrehajtásának elősegítéséért, hatékony támogatásáért.

A felülvizsgálatok során a tárolt adatok esetében biztosítani kell a felülírás elkerülését.

A **megbízott auditor** a vizsgálatról audit jelentést készít, ahol rögzítésre kerülnek azon eltérések, amelyek az *Audit kérdéslistán* vannak feltüntetve

Az **auditorok** ezután áttekintik az *audit jelentést* az **auditált terület vezetőjével**, és szükség szerint együttesen meghatározzák és rögzítik:

- a javító intézkedéseket,
- a végrehajtás határidejét,
- a végrehajtásért felelős személy (ek) et,
- a fejlesztési javaslatokat, amennyiben van,
- az auditált szakterület vezetőjének véleményét az audittal kapcsolatosan, amennyiben erre igény tart.

Ha az audit során az auditorok olyan nem megfelelőséget tapasztalnak, melyet az audit által érintett szervezeti egység vezetője saját hatáskörben nem tud megoldani, akkor a *Nem megfelelőségi jelentést* és az *auditjelentéssel* együtt továbbítják az **információbiztonsági vezető** részére.

A helyesbítő intézkedést és a végrehajtásért felelős kijelölését a *Nem megfelelőségi jelentés* 6. sz. rovatában az **információbiztonsági vezető** határozza meg.

A kijelölt felelős a *Nem megfelelőségi jelentés* átvételét a 7. pontban aláírásával igazolja.

A helyesbítő tevékenység végrehajtásának ellenőrzés eredményét a 8. pontban a **megbízott auditor** dokumentálja.

Az elrendelt intézkedések határidőre történő hatékony végrehajtásáért és azok eredményeinek dokumentálásáért a feladat elvégzésével megbízott személyek a felelősek.

Egy audit csak az összes *Nem megfelelőségi jelentés* eredményes helyesbítő és / vagy megelőző tevékenységgel történő lezárását követően nyilvánítható befejezettnek. Az auditok előrehaladását az **információbiztonsági vezető** köteles a *belső audittervben* vezetni. A belső auditok tapasztalatai a vezetőségi átvizsgálás bemenő adatai.

A belső audit feljegyzéseit 3 évig az **információbiztonsági vezető** köteles megőrizni.

19. VEZETŐSÉGI ÁTVIZSGÁLÁS

Az IBIR kiértékelésére minimum évente egy alkalommal a belső auditokat követően kerül sor. A vezetőségi átvizsgálás az **Információbiztonsági Team** egy kijelölt megbeszélése kapcsán kerül megtartásra.

A vezetőségi átvizsgálásban az **Információbiztonsági Team** résztvevőin kívül a következők vehetnek részt az **információbiztonsági vezető** általi meghívás alapján

- **információ felelősök,**
- **belső auditor.**

Az átvizsgálás az alábbi területekre terjed ki:

- kockázatértékelések eredménye, elfogadási szintek értékelése, akció tervek összefoglalása,
- az IBIR auditjának – belső és harmadik fél általi – eredményeinek kiértékelésére,
- az érdekelt felek visszajelzésére,
- a megelőző és helyesbítő tevékenységek tapasztalatainak kiértékelésére,
- az IBIR teljesítésének és hatásosságának fejlesztésére felhasznált eljárásokra, technikákra, termékekre,
- azokra a gyenge pontokra és fenyegetésekre, amelyeket a szervezet nem kezelt megfelelően a korábbi kockázat értékeléskor,
- hatékonysági mérések eredményeire – pl. incidensek, IT auditok -,
- a korábbi vezetőségi áttekintésen hozott intézkedések kiértékelésére,
- változtatásokra, amelynek hatása lehet az IBIR-re,
- a titoktartási nyilatkozat felülvizsgálatára,
- illetve a rendszer fejlesztésére vonatkozó javaslatokra.

Az átvizsgálásról az **információbiztonsági vezető** az **igazgató** támogatásával *Jegyzőkönyvet* készít, amelynek tartalmaznia kell a bemenő adatokra vonatkozó döntéseket, döntési javaslatokat és beavatkozásokat a következőkkel kapcsolatban:

- IBIR hatásosságának fejlesztése,
- Kockázatértékelés – információ leltár – frissítése, RPN értékek felülvizsgálata és jóváhagyása,
- Az információbiztonságot befolyásoló eljárások és intézkedések szükség szerinti módosítása, hogy összhangban legyenek azokkal a belső, vagy külső eseményekkel, amelyek hatással lehetnek az IBIR-re – működési-, biztonsági- követelmények, folyamatok, jogi szabályozás, szerződéses követelmények, kockázati és/ vagy kockázat elfogadási szintek.
- Erőforrás szükséglet,
- Intézkedés hatékonysága mérésének fejlesztése.

Az egyes jegyzőkönyveket azok dátuma és megnevezése azonosítja.

20. AZ IBIR FEJLESZTÉSE

20.1 Folyamatos fejlesztés

A CSAPI az IBIR folyamatos fejlesztése érdekében az alábbi tevékenységeket végzi, és azok eredményeit használja fel:

- Kockázatértékelés és elemzés eredményeit,
- A kockázatértékelés eredményei alapján készített akciótervek,
- Információbiztonsági incidensek kiértékelésének eredményei,
- Belső- és harmadik fél általi auditok és eredményeit,
- Helyesbítő- és / vagy a megelőző tevékenységet és eredményeit,
- Vezetőségi átvizsgálás és megállapításait,
- Célok meghatározása és azok felülvizsgálata a vezetőségi áttekintés során.

Tevékenységeink során és az IBIR-ben előforduló nem-megfelelőségek újbóli előfordulásának, vagy lehetséges előfordulásának megakadályozásáért a kockázati szintek csökkentése érdekében helyesbítő és megelőző tevékenységeket kell végezni. A helyesbítő, vagy megelőző intézkedések összhangban vannak a felmerült problémák súlyával és lehetséges következményeivel.

20.2 Helyesbítő tevékenység

Azon problémák, melyekre helyesbítő tevékenységek indíthatók, a következő folyamatok során merülhetnek fel:

- szoftverfejlesztési problémák, illetve szoftver hibák, hardver hibák,
- folyamatok működése során jelentkező problémák, melyek az információ biztonsággal kapcsolatosak,
- bevont szerződő partnerekkel kapcsolatos problémák, információ sérülés esetében,
- ügyfelekkel, partnerekkel való kommunikációs problémák (nem szakmai jellegű),
- információbiztonsággal kapcsolatos incidensek kivizsgálása.

A problémák feltárása történhet:

- belső és harmadik fél általi auditon,
- érdekelt fél jelzése alapján
- bármely munkatárs napi munkavégzése kapcsán.

Minden munkatárs feladata, hogy ha olyan problémát észlel, melynek megoldásával a szolgáltatást, vagy az IBIR működését javíthatja, illetve ha ilyen ötlet fogalmazódik meg, akkor azt írásban jelezze az **információbiztonsági vezető** felé.

Az **információbiztonsági vezető** feladata, hogy a jelzéseket fogadja és eldöntse, szükség van-e további felelős munkavállalók bevonására. A helyesbítő tevékenység indításáról annak megfelelő előkészítését követően dönt is.

A helyesbítő, vagy megelőző tevékenység egyes lépéseit az adott témában érintett felelős személyesen végezheti, vagy a *Jegyzőkönyvben / Nem megfelelőségi jelentésen* azok végzésével más munkavállalókat bízhat meg.

A helyesbítő tevékenységek végrehajtásának lépései a következők:

- A nem-megfelelőséget, problémát az **érintett felelős** azonosítja, feladatban rögzíti.

- Az **érintett felelős** kivizsgálja a probléma okát, és rögzíti a felvett *Jegyzőkönyvben / Nem megfelelőségi lapon*.
- Meghatározza a helyesbítő tevékenységet, a kapcsolódó feladatokat, felelősségeket, határidőket
- A meghatározott intézkedések végrehajtását követően a **kijelölt személy** ellenőrzi a tevékenység hatékonyságát. Belső auditon feltárt probléma esetén a hatékonyság ellenőrzése a **belső auditor**, egyéb esetekben a **döntést hozó felelős vezető**, vagy az **általa megbízott személy** feladata.
- A helyesbítő tevékenység lezárása az előző bekezdésben rögzítésre került **felelősök** feladata, amennyiben a probléma hatékonyan megoldódott. Ellenkező esetben új helyesbítő tevékenységet kell indítani.

20.3 Megelőző tevékenység

Megelőző tevékenységet általában az alábbi esetekben folytatható:

- információ biztonsággal kapcsolatos kockázatelemzés alapján,
- különösen a jelentősen megváltozott kockázatokra,
- lényegesen új folyamatokra való felkészülés esetén,
- lényegesen új szolgáltatásra való felkészülés esetén,
- lényegesen új információkezelő rendszer bevezetésére való felkészülés esetén,
- helyesbítő tevékenységhez kapcsolódóan a probléma általánosításából származó nem-megfelelőség okának megszüntetésére,
- javítás céljából.

Megelőző tevékenységet **bármely munkatárs** kezdeményezhet.

A megelőző tevékenységeket a helyesbítő tevékenységhez hasonlóan *Jegyzőkönyvben / Nem megfelelőségi lapon* kell rögzíteni. A megelőző tevékenység lépései megegyeznek a helyesbítő tevékenységnél leírtakkal:

- A kockázatos lépés, tevékenység azonosítása
- A lehetséges probléma okainak feltárása
- Intézkedés megbízhatóbb, biztonságosabb módszerek kialakítására
- Intézkedések végrehajtását követően a kockázat mértéke csökkenésének értékelése

A megelőző tevékenységek fontossági sorrendjét a kockázatfelmérés eredményei alapján az **Információbiztonsági vezető** határozza meg.

21. MEGELŐZŐ TEVÉKENYSÉGEK

Lehetséges problémák	Probléma oka	Megelőző intézkedés

22.FELJEGYZÉSEK KEZELÉSE

Feljegyzés neve	Megőrzéséért felelős	Megőrzés helye	Megőrzési idő		Megjegyzés
			Online	Offline	
<név> és/vagy <fájl név>	< a felelős munkaköre, pozíciója >	<ahol megtalálható>	<mennyi ideig tároljuk>	<mennyi ideig tároljuk>	<egyéb információ>

CSAPI - ISO 27001 Információbiztonsági Szabályzat (Információbiztonsági Irányítási Rendszer) bevezetési terve

Fázis	Feladat(ok) leírása	Prioritás	Jelenlegi státusz	Végrehajtó személyek	Határidő
Általános feladatok					
Szabályozások jóváhagyása és bevezetése					
	Formai követelmények ellenőrzése és a nemmegfelelősségek tisztázása	Magas	Folyamatban	Kovács János	2013.04.25
	Vélemények egyeztetése és átvezetése a dokumentumokon	Magas	Nem indult el	Kovács János	2013.04.29
	Dokumentumok utolsó átvizsgálása, rendezése és felterjesztése jóváhagyásra	Magas	Nem indult el	Kovács János	2013.05.01
Régi szabályozások megszüntetése					
	Informatikai szabályzat	Magas	Nem indult el	Kovács János	2013.05.01
Feladatok, felelősségi körök hozzárendelése személyekhez					
	Információbiztonsági Team kijelölése	Magas	Nem indult el	Kovács János	2013.05.10
	Információ-felelősök meghatározása és kijelölése	Magas	Nem indult el	Kovács János	2013.05.10
Kommunikáció, oktatás					
	Vezetők tájékoztatása	Közepes	Nem indult el	Kovács János	2013.05.10
	Informatikusok oktatása	Magas	Nem indult el	Kovács János	2013.05.10
	Felhasználók oktatása	Közepes	Nem indult el	IT szolgáltató	2013.05.10
Vagyonleltár					
	Információs vagyonleltár elkészítése	Magas	Nem indult el	Információ felelősök	2013.05.15
	Információs vagyonleltár elemeihez felelős rendelése	Magas	Nem indult el	Kovács János	2013.05.10
	Információs vagyonleltár elemeinek osztályozása	Magas	Nem indult el	Információ felelősök	2013.05.15
Kockázat-értékelés, -elemzés, -kezelés					
	Fenyegetések azonosítása és a kockázatok értékelése	Magas	Nem indult el	Információ felelősök	2013.05.31
	Kockázat menedzsment (felmérés, értékelés, elemzés, kezelés)	Magas	Nem indult el	Információ felelősök	2013.05.31
A nem IBIR szabályzatokkal kapcsolatos további feladatok (pl.: aktualizálás)					
	Munkaköri leírásokba az információbiztonsággal kapcslatos feldatok és felelősségi körök rögzítése	Alacsony	Nem indult el	Kovács János	2013.05.31
	Szerződések átvizsgálása a információbiztonsági kockázatok szempontjából	Alacsony	Nem indult el	Kovács János	2013.05.31
	Beszerzési szabályzat aktualizálása	Alacsony	Nem indult el	Kovács János	2013.05.31
	Üzletmenet folytonossági terv (BCP) (üzleti terület) elkészítése	Alacsony	Nem indult el	Kovács János	2013.05.31
	Fizikai biztonsági utasítás (belépési rend, őrzés-védelem stb.)	Alacsony	Nem indult el	Kovács János	2013.05.31
	Iratkezelési szabályzat	Alacsony	Nem indult el	Kovács János	2013.05.31
	Selejtezési szabályzat (informatikai biztonsági szempontok figyelembe vétele)	Alacsony	Nem indult el	Kovács János	2013.05.31
Információbiztonsági szabályzat alapján részletezett feladatok					
Információbiztonsági Politika					
	IT stratégia módosítása az új politika és az IBIR szerint (amennyiben szükséges)	Alacsony	Nem indult el	Kovács János	2013.06.30
	Információbiztonsági Célok kialakítása és jóváhagyása	Alacsony	Nem indult el	Kovács János	2013.06.30
Információbiztonsági Kézikönyv					
Mellékletekkel kapcsolatosan					
	2. számú melléklet - Kapcsolódó belső szabályzó dokumentumok és külső dokumentumok (jogszabályok, szabványok) összegűjtése	Alacsony	Nem indult el	Kovács János	2013.06.30

CSAPI - ISO 27001 Információbiztonsági Szabályzat (Információbiztonsági Irányítási Rendszer) bevezetési terve					
Fázis	**Feladat(ok) leírása**	**Prioritás**	**Jelenlegi státusz**	**Végrehajtó személyek**	**Határidő**
	3. számú melléklet - Képzési terv kialakítása	Alacsony	Nem indult el	Kovács János	2013.06.30
	4. számú melléklet - Informatikai eszköz használatba vételi nyilatkozat	Közepes	Nem indult el	Kovács János	2013.05.31
	5. számú melléklet - Titoktartási nyilatkozat minta bevezetése a napi ügymenetbe	Közepes	Nem indult el	Kovács János	2013.05.31
Új utasítás(ok) kialakítása / elkészítése / aktualizálása / átalakítása / megszüntetése stb.					
	IT rendszerek üzemeltetési szabályzata	Magas	Folyamatban	IT szolgáltató	2013.05.31
	IT eszközök karbantartási utasítása	Magas	Nem indult el	IT szolgáltató	2013.05.31
	Mentési utasítás aktualizálása	Magas	Folyamatban	IT szolgáltató	2013.05.31
	Help Desk változáskezelési eljárás kialakítása	Magas	Nem indult el	Kovács János / IT szolgáltató	2013.05.31
	Help Desk incidenskezelési eljárás kialakítása	Magas	Nem indult el	Kovács János / IT szolgáltató	2013.05.31
	IT szolgáltatásfolytonossági terv (ITCP) kialakítása	Magas	Nem indult el	Kovács János / IT szolgáltató	2013.06.30
	IT katasztrófa elhárítási terv (DRP) kialakítása	Magas	Nem indult el	Kovács János / IT szolgáltató	2013.06.30
Egyéb feladatok					
	Nyilvántartás kialakítása és aktualizálása a mentési adathordozókról	Alacsony	Folyamatban	IT szolgáltató	2013.05.31
	Tűrt szoftverek listájának kialakítása	Közepes	Nem indult el	IT szolgáltató	2013.05.31
	Hozzáférési jogosultságok szabályainak beállítása az egyes rendszerekben és azok végrehajtásának és betartásának ellenőrzése	Magas	Folyamatban	Kovács János / IT szolgáltató	2013.05.31
	Jelszó policy beállítása az egyes rendszerekben és azok végrehajtásának és betartásának ellenőrzése	Magas	Folyamatban	Kovács János / IT szolgáltató	2013.05.31
	Hálózati rajz	Alacsony	Elvégezve	IT szolgáltató	2013.05.01
	Hardver / szoftver leltár (nyilvántartás és folyamatos aktualizálás)	Közepes	Folyamatban	IT szolgáltató	2013.05.31
	Tűzfal szabályok dokumentálása	Közepes	Nem indult el	IT szolgáltató	2013.05.31
	Fejlesztési folyamat átalakítása az IBSZ előírásainak megfelelően	Magas	Nem indult el	Kovács János / IT szolgáltató	2013.05.31
	Help Desk kialakítása	Magas	Nem indult el	Kovács János / IT szolgáltató	2013.05.31
	Szolgáltatás Szint megállapodás -SLA (Service Level Agreement)	Közepes	Nem indult el	Kovács János / IT szolgáltató	2013.06.30
Folyamatos fejlesztés					
	Végrehajtandó feladatok (vírusírtás, hozzáférések, tűzfal, file server, frissítések, parch man., fejlesztés, rendszerüzemeltetés, Wi-Fi, VPN, stb.) folyamatos ellenőrzése az IBSZ előírásait figyelembe véve	Magas	Folyamatban	Kovács János	Folyamatos
	Auditterv készítése és a belső IBIR auditok végrehajtása integrálva az ISO 9001-el	Közepes	Nem indult el	Kovács János	2013.06.30
	Problémák elemzése	Közepes	Nem indult el	Kovács János	2013.07.31
	Helyesbítő és megelőző tevékenységek	Közepes	Nem indult el	Kovács János	2013.07.31

CSAPI - ISO 27001 Információbiztonsági Szabályzat (Információbiztonsági Irányítási Rendszer) bevezetési terve					
Fázis	**Feladat(ok) leírása**	**Prioritás**	**Jelenlegi státusz**	**Végrehajtó személyek**	**Határidő**
	Vezetőségi átvizsgálás végrehajtása integrálva az ISO 9001-el	Alacsony	Nem indult el	Kovács János	2013.08.31