95/2007. (IX. 27.)

A SEMMELWEIS EGYETEM

INFORMATIKAI BIZTONSÁGI POLITIKÁJA ÉS STRATÉGIÁJA

BUDAPEST
2007

Tartalomjegyzék

A Semmelweis Egyetem
S z e n á t u s á n a k

95/2007. (IX. 27.) számú
h a t á r o z a t a :

A Semmelweis Egyetem
Informatikai Biztonsági Politikája és Stratégiája

A Szenátus a Szervezeti és Működési Szabályzat 9. § (12) bekezdése alapján a **Semmelweis Egyetem Informatikai Biztonsági Politikáját és Stratégiáját** az alábbiak szerint alkotta meg:

1. Előszó

Jelen Informatikai Biztonsági Politika és Stratégia az **ISO 1779:2002 szabvány követelményrendszerének** figyelembe vételével készült. Az egyes fejezetekben a minőségbiztosítási rendszer célkitűzéseivel, az erre adandó válaszokat, reakciókat, illetve az annak érdekében megvalósítandó feladatokat, intézkedéseket állítja szembe.

Tekintettel azonban arra, hogy **az informatikai biztonság megteremtése** messze meghaladja és **jóval túlmutat az informatika** és így az informatikai szakemberek **kompetenciáján** – ezért a teljes körű, és érdemi biztonság megteremtése egy hosszabb, akár több éves kitartó munka és folyamat eredménye lehet. Jelen stratégia átolvasása után válik teljesen egyértelművé, hogy mindezen célok megvalósítása nem is lehetséges egy sor műszaki, gazdasági, jogi, humánpolitikai intézkedéssorozat, egy ezt működtető biztonsági szervezet és az egyetemi vezetés elkötelezett és hathatós támogatása nélkül.

Jelen stratégiai célok megvalósítása és **egy átfogó egyetemi biztonsági dokumentum** (szabályzat) készítése is kizárólag a **kapcsolódó területek** (titokvédelem, munkaköri leírások, munka-, fejlesztési, support szerződések, műszaki berendezések, építmények, adatok, információk, rendszerek osztályokba sorolásának megfelelő feltételek biztosítása, stb.) megfelelő **harmonizációjával** valósítható meg.

A fentiek miatt jelen stratégiának **nem** volt és nem is lehetett **célja az informatikai biztonság részletes szabályozása**, hiszen a nem informatikai részek (de még az informatikai jellegű feladatok jó része is) még meglehetősen vázlatosak és kidolgozatlanok. Másfelől meg kell említeni azt a sajátos körülményt is, nevezetesen, hogy ezen a területen ebbe a körbe tartozó tevékenységek eddig jószerivel spontán módon alakultak ki, és korántsem egy teljes rendszer igényével kerültek megfogalmazásra.

Az **informatikai rendszerek** normális és **biztonságos működése** nélkül ma már szinte elképzelhetetlen az üzleti, szakmai, műszaki, vagy pénzügyi-, gazdasági tevékenységek ellátása. Jelen stratégia ennek tudatában és ezen célok érdekében fogalmazta meg azokat az elvárásokat, illetve az ennek érdekében végrehajtandó tevékenységeket és feladatokat, melyek végsősoron az egész Egyetem zavartalan és hatékony működését hivatottak közvetlenül és közvetten is elősegíteni és támogatni.

2. Általános rendelkezések

2.1 Az Informatikai Biztonsági Politika és Stratégia (IBPS) célja

Informatikai Biztonsági Politika és Stratégia (továbbiakban: **SE-IBPS**) célja:

- hogy **általános** informatikai biztonsági **előírásokat és szabályokat** állapítson meg a Semmelweis Egyetem informatikai vagyontárgyainak védelmével kapcsolatosan,
- **megalapozza** a teljes egyetemi, meg nem kerülhető informatikai **biztonsági rendszer kiépítését**, ezen belül is a szabályok, utasítások végrehajtásáért és a végrehajtás ellenőrzéséért felelős **szerepkörök** meghatározását.

2.2 Az Informatikai Biztonsági Politika és Stratégia hatálya

Személyi hatály
Jelen Informatikai Biztonsági Politika és Stratégia (**SE-IBPS**) kiterjed a Semmelweis Egyetem Intézeteiben dolgozó **összes munkatársra**, illetve **közalkalmazottra**, aki bármely informatikai vagyontárggyal bármilyen jellegű kapcsolatba kerül.

Jelen stratégia kiterjed a Semmelweis Egyetem informatikai vagyontárgyaival kapcsolatba kerülő **bármely külső szereplőre** (jogi, illetve jogi személyiséggel nem rendelkező gazdasági társaságra, illetve természetes személyre egyaránt).

Tárgyi hatály
Jelen Informatikai Biztonsági Politika és Stratégia (**SE-IBPS**) tárgyi hatálya kiterjed a Semmelweis Egyetem összes, birtokában és tulajdonában lévő **minden informatikai vagyontárgyra**, így:

- minden szoftverelemre,
- minden hardverelemre (szerverekre, kliens gépekre, nyomtatókra, perifériális eszközökre, stb.),
- informatikai rendszerekhez kapcsolódó infrastrukturális elemekre,
- hálózati eszközökre,
- valamint az informatikai rendszerekbe felvitt, létrehozott, a rendszerek által kezelt, továbbított adatokra a rendszerekhez kapcsolódó papír alapú, , illetve elektronikusan tárolt dokumentumokra.

Informatikai Biztonsági Politika és Stratégia (**SE-IBPS**) hatálya nem terjed ki a következő eszközökre: mérési, adatgyűjtő és laborrendszerekre.

Időbeni hatály
Jelen Informatikai Biztonsági Politika és Stratégia (**SE-IBPS**) a rektor jóváhagyásával és aláírásával lép életbe és visszavonásig érvényben marad.

2.3 Kapcsolódó jogszabályok

Jogszabályok:

- 1959. évi IV. törvény: A Polgári Törvénykönyvről,
- 1969. évi III. törvény A szerzői jogról,
- 6/1988. (II. 12.) MT rendelet: A közületi szervek rendészeti tevékenységéről,
- 1992. évi LXIII. tv. A személyi adatok védelméről és a közérdekű adatok nyilvánosságáról,
- 1992. évi LXVI. Törvény: A polgárok személyi adatainak és lakcímének nyilvántartásáról, a 146/1993. (X. 26.) Kormány rendelettel együtt,
- 1992. évi LXXII. Törvény: A távközlésről
- 43/1994. (III. 29.) Kormány rendelet: A rejtjel tevékenységről
- 1995. évi LXV. Törvény. Az államtitokról és szolgálati titokról a végrehajtására kiadott 79/1995. (VI.30.) Kormány rendelet,

Szabványok:

- *MSZ ISO/IEC 17799:2000* Informatika. Az informatikai biztonság menedzselésének eljárásrendje. Magyar Szabványügyi Testület, 2002. november
- *MSZ ISO7498* szabványsorozat: Információ-feldolgozó rendszerek – Nyílt rendszerek összekapcsolása (Open Systems Interconnection Basic Reference Manual, Part 2: Security Architecture, 1989.)
- *MSZ EN60950*: Adatfeldolgozó berendezések és irodagépek biztonsági előírásai
- *MSZ 172*: Érintésvédelmi szabályzat
- *MSZ 274*: Villámvédelem
- *MSZ 595*: Építmények tűzvédelme
- *MSZ 9785-1*: Tűzjelző berendezés

Ajánlások, irányelvek:

- Számítógépek és adatfeldolgozó rendszerek - Számítóközpont- tervezési és létesítési irányelvek MI-05-12.002
- Számítóközpontok tűzvédelme MI-02-102-79
- Miniszterelnöki Hivatal Informatikai Koordinációs Iroda - Informatikai Tárcaközi Bizottság ajánlásai - Informatikai biztonsági módszertani kézikönyv (8. sz. ajánlás) 1994.
- Common Criteria for Information Teclmology Security Evaluation. Version 1.0. 1996. március.
- Miniszterelnöki Hivatal Informatikai Koordinációs Iroda - Informatikai Tárcaközi Bizottság ajánlásai – Infrastruktúra menedzsment (15. sz. ajánlás) 1998.
- Common Criteria for Information Technology Security Evaluation. Version 2.0. 1998. május.
- Az informatikai biztonság kézikönyve (Szerk.: Muha Lajos, VERLAG DASHÖFER Szakkiadó Kft. & T. Bt., 2004. március)

3. Informatikai Biztonsági Politika és Stratégia

Célkitűzés: Egyetem vezetése legyen elkötelezett az informatikai biztonság irányítására, támogatására, tűzze ki biztonságpolitikájának irányvonalát, mutassa ki, hogy támogatja az informatikai biztonságot és elkötelezett az informatikai biztonság mellett. Ennek érdekében az Egyetem teljes szervezetrendszerére vonatkozóan elkészít és karbantart egy Informatikai Biztonsági Politikát és Stratégiát.
MSZ ISO/IEC 17799:2002

Jelen Informatikai Biztonsági Politikát és Stratégiát az **Informatikai Biztonságért Felelős Felsővezetőnek** (továbbiakban: **IBFF**) is jóvá kell hagynia.

Jelen **Informatikai Biztonsági Politikát és Stratégiát** (továbbiakban: **SE-IBPS**) Semmelweis Egyetemen belül megfelelő körben közzé kell tenni.

Jelen Informatikai Biztonsági Politika és Stratégia (**SE-IBPS**) **alapját képezi** az informatikai vagyontárgyakhoz kapcsolódó rendszerszintű informatikai biztonsági szabályzatoknak, ugyanakkor **nem rendelkezik** az egyes informatikai rendszerekre vonatkozó **speciális, egyedi szabályokról,** ezekkel a konkrét kérdésekkel ugyanis a rendszerszintű informatikai biztonsági szabályzatoknak kell foglalkozniuk, ezen **alapvető szabályoktól eltérni** csak a Semmelweis Egyetem **Informatikai Biztonsági Vezető** (továbbiakban: **IBV**) **engedélyével** lehetséges. Eltérést a rendszerbiztonsági felelősnek megfelelően indokolnia és dokumentálnia kell.

A rendszerszintű informatikai biztonsági szabályzatoknak **összhangban kell állniuk** az Egyetem és szervezeti egységek egyéb szabályzataival.

3.1 Felülvizsgálat és értékelés

Az Egyetem informatikai biztonsági helyzetét célszerű lenne egy külső informatikai biztonságtechnikai tanácsadó cég segítségével - **egy átfogó biztonságtechnikai audit** - keretében átvilágítani. Semmelweis Egyetem elkötelezett a **minőségbiztosítási rendszer** bevezetésében és az ezzel kapcsolatos előkészítő munkák már részben el is kezdődtek, az ezzel kapcsolatos munkálatokat jelentősen megkönnyíti az a körülmény, hogy a jelen stratégia is a **minőségbiztosítási követelményrendszerek figyelembe vételével** került kidolgozásra.

Informatikai Biztonsági Politika és Stratégia (SE-IBPS**) gazdája** az Informatikai Biztonságért Felelős Felsővezető (**IBFF**).

Informatikai Biztonsági Politika és Stratégia (SE-IBPS) alapján **elkészített rendszerszintű informatikai biztonsági szabályzatok** gazdái a rendszerbiztonsági felelősök.

Informatikai Biztonsági Politika és Stratégiát (SE-IBPS) és a rendszerszintű informatikai biztonsági szabályzatokat **rendszeresen felülvizsgálni**, és igény szerint aktualizálni kell.

A **Biztonsági szakértői tanácsadó testület** végzi a felülvizsgálatot és értékelést a saját feladatköre szerint.

3.2 Informatikai kockázatok kezelése

A Semmelweis Egyetemen belül folyamatosan **ki kell alakítani** és **bevezetni** az informatikai **kockázatkezelési rendszert**. Az egyetemi működés **egészét átfogó kockázatkezelési dokumentum elkészítésére** – tekintettel arra, hogy az Egyetem ilyen szakemberekkel nem rendelkezik - célszerűen **külső szakértők bevonásával** kerülhet sor.

Ezt megelőzően - a kockázatkezelési rendszer kidolgozása előtt - **az egyetemi informatikai biztonság teljes auditját is el kell végezni**, annak érdekében, hogy a jelenlegi helyzet objektív állapota, vagyis az „induló helyzet" rögzítésre kerüljön.

A rendszer kialakításáért, bevezetéséért és a folyamatos működtetéséért az Informatikai Biztonságért Felelős Felsővezető (**IBFF**) felel. Feladata a rendszer részletes működési tervének, illetve a kapcsolódó részletes felelősségi rendszernek a kidolgoztatása. Az informatikai kockázatkezelési rendszer működésének elindításáért is az IBFF felel.

Informatikai Biztonsági Vezető (IBV) elkészíti az éves informatikai **kockázatkezelési tervet**, koordinálja és felügyeli a rendszer működését, képviseli az informatikai területet a szervezeti szintű kockázatkezelés kérdéseinél, évente beszámol a rendszer működéséről az IBFF-nek, valamint előterjeszti a kockázatkezelési rendszerre vonatkozó fejlesztési javaslatait.

3.2.1 Az informatikai kockázatkezelési rendszer

Informatikai kockázatkezelési stratégia meghatározása
A Semmelweis Egyetem informatikai kockázatkezelési stratégiájában hosszú távra kerülnek meghatározásra a főbb célkitűzések és a követendő kockázatkezelési alapelvek.

Informatikai kockázatkezelés kereteinek kijelölése:
- a **stratégia** részletes **lebontása**, amely megadja a kockázatkezelés szervezeti és működési kereteit, illetve
- az aktuális időszakra vonatkozó éves informatikai **kockázatkezelési terv** kidolgozása: az elvégzendő feladatok, felelősök, erőforráskeretek meghatározásával, módszertanok rendelkezésre bocsátása a kockázatkezelés elvégzése érdekében.

3.2.2 Az informatikai kockázatkezelés folyamata

A fentiekben meghatározott keretrendszerben történik a kockázatkezelési mechanizmusok folyamatos működtetése, vagyis a következő feladatok végrehajtása:
- **Kockázatok azonosítása**: teljes körű kockázatfelmérés és aktualizálás rendszeres időközönként. Az azonosított kockázatokról dokumentációt kell készíteni, megjelölve az egyes kockázatok „gazdáit" is, akik az adott kockázat kezeléséért felelnek.

- **Kockázatok elemzése**: egyrészt évente az egész Egyetemre teljes körűen, másrészt az új induló projektekre vonatkozóan kell elvégezni. Ennek keretében történik a feltárt kockázati tényezők kvalitatív értékelése, a kritikus tényezők kiválasztása, majd szükség esetén a kritikus tényezők mélyebb, kvantitatív elemzése.

- **Kockázatok „kezelése**", az eredmények értékelése: az értékelés alapvetően a kockázatok bekövetkezési valószínűsége és hatásuk nagysága, súlyossága alapján történik. Ez alapján meghatározható a kockázatok prioritása, kezelési kategóriákba sorolása. A kockázatok bekövetkezési valószínűsége és a hatás nagysága alapján kell meghatározni azokat a teendőket, amelyek a kockázatok kezelését, bekövetkezés megakadályozását szolgálják.

- **Kockázatok monitorozása,** megfigyelése: a kockázatok értékelése alapján meghatározható, hogy a kockázatokra, kockázati kategóriákra vonatkozóan, az egyes kockázatokat, és a hatásuk csökkentése érdekében végrehajtott feladatokat milyen gyakorisággal kell felülvizsgálni. A kockázatok a kategóriától, az adott kockázattól függően évente, havonta, vagy folyamatos megfigyelésekor tapasztalt eredményekről a kockázatgazdák kötelesek írásban jelentést készíteni. Ezeket az IBF által meghatározottak szerinti a kockázatkezelési felettesüknek kell átadni.

- **Értékelése**: évente végre kell hajtani az informatikai kockázatkezelési rendszer **értékelését** és a továbbfejlesztési lehetőségek feltárását a rendszer működésében közreműködők bevonásával.

- Az összegyűjtött, összegzett és jóváhagyott **fejlesztési javaslatokat** az IBV terjeszti elő jóváhagyásra az IBFF-nek.

- Informatikai kockázatkezelési rendszerben **közreműködők képzése**:
  Ez egyrészt az informatikai kockázatkezelési rendszer működésében, irányításában közreműködők továbbképzését jelenti, másrészt a szervezetek mindazon munkatársainak tájékoztatását és oktatását, akik valamilyen módon kapcsolatba kerülnek a kockázatkezeléssel. A képzések terve az **éves informatikai kockázatkezelési terv** része kell, hogy legyen.

3.2.3 Informatikai kockázatkezelési módszerek (minta)

Kockázatkezelési módszerek

Informatikai kockázatkezelési folyamatok keretében történik a kockázatok azonosítása, elemzése, értékelése, azok „kezelése", valamint a monitorozásuk. Kockázatok azonosítását, elemzését és értékelését támogató alapvető módszerek alkalmazása révén az Egyetem képes csökkenteni, semlegesíteni a különböző típusú kockázatok egy részét, másrészt a fennmaradó kockázatok ismerete lehetővé teszi a vezetésnek ezek tudatos kezelését.

Módszerek a kockázatok azonosítására

Informatikai kockázatok azonosítása közös **ötletgyűjtés** (brain storming) formájában történik. Javasolt, hogy évente egyszer kerüljön sor ilyen értekezlet lebonyolítására. Töre-

kedni kell arra, hogy minden mérvadó terület képviselője legyen ott a brain stormingon, mivel így biztosítható az eredmények valószerűsége és megbízhatósága.

- Az **azonosított kockázatok szűrése**, megvitatása keretében valamennyi résztvevő elmondhatja véleményét az összegyűjtött kockázatokról. A cél, hogy konszenzus alakuljon ki közöttük arra vonatkozóan, hogy melyek a ténylegesen **figyelembe veendő kockázati tényezők**.
- Végül a szűrt kockázati lista elemeit **csoportosítani** kell. Ennek célja egy átfedésmentes, **logikus osztályozás** pl. a következő szempontok mentén:
  - külső / belső kockázatok, illetőleg
  - működési / technikai stb. kockázatok.

Az így összegyűjtött, rendszerezett, dokumentált kockázatok kerülhetnek további elemzésre. A **kockázatok elemzése** dönti el, hogy melyek azok az azonosított **kockázati tényezők**, melyekhez nevesített **felelősök, illetve intézkedési tervek** tartoznak majd.

Módszerek a kockázatok elemzésére és értékelésére
Az összegyűjtött, és közösen meghatározóként elfogadott kockázatok elemzésének célja a **kockázatok minősítése**, mely minősítés **meghatározza a szükséges intézkedéseket**. A kockázatelemzés feladatai az azonosításhoz hasonló **csoportos megbeszélés** keretében végezhetők el.

A kockázatelemzési feladatok végrehajtásánál - különösen a kezdeti szakaszban a szükséges gyakorlati ismeretek elsajátítása érdekében - **tapasztalt külső szakértők bevonása** moderálási, véleményezési, illetve elemzési céllal szükséges lehet.

A kockázatelemzés menete:
- A kockázatok csoportjain végighaladva egyenként **értékelni** kell **a kockázatokat** a bekövetkezés **valószínűsége és a hatás súlyossága alapján**.
- A bekövetkezés valószínűségének, illetve a **hatás súlyosságának értékelésére** 3, illetve 5 fokozatú skála alkalmazása ajánlott. A két skála által „kifeszített" táblázatban elhelyezhetőek és ezáltal minősíthetőek a kockázatok.

Példa: Egy adott csoporthoz tartozó kockázatok elhelyezkedése a táblázatban. (A kockázatok azonosítása sorszámokkal történik, melyek alapján a kockázati listában egyértelműen beazonosíthatóak.)

Bekövetkezés valószínűsége	**A hatás súlyossága** csekély	kritikus	katasztrofális
Valószínű	A	B	C
Biztos	B	C	D

A kategóriák döntő mértékben meghatározzák, hogy miként kell kezelni az adott kategóriához tartozó kockázatokat.

"A" kategória – Ezek a kockázatok nagyon **kis eséllyel** következnek be, és / vagy jellemzően **kis hatással** járnak, ezért **nem igényelnek jelentős kockázatkezelési lépéseket,** fontos számon tartani ezeket is, de nem szükséges nevesített felelőst kijelölni felügyeletükre.

"B" kategória – Ezek a kockázatok vagy **nagyobb valószínűséggel** bekövetkeznek, **de csekély hatással** járnak, vagy **kisebb a bekövetkezés** valószínűsége, de **jelentősebb károkat okozhatnak.** A vezetés felelősöket jelöl ki ezen kockázatok figyelemmel kísérésére. Különösen a vélhetően nagy károkat okozó kockázati események megelőzése és a károk mérséklése lényeges, ezért ebben az esetben a monitoringra, illetve az értékelések évenkénti felülvizsgálatára kell hangsúlyt fektetni.

"C" kategória – Ezek a kockázatok (szinte) biztosan, **jelentős kárértékkel** vagy pedig **mérsékeltebb valószínűséggel**, de **katasztrofális hatásokat** maguk után vonva következnek be. Olyan kockázatkezelési intézkedéseket kell megfogalmazni és végrehajtani, amelyek következtében a vezetés által kitűzött, elfogadható szintre sikerül mérsékelni a kockázatot.

A kockázatok felelősei:
- **a kockázat elkerülésével** (pl. saját előállítási tevékenység a beszerzés okozta kockázat semlegesítésére),
- a kockázat **csökkentésével** (pl. tartalékkeretek fenntartása kockázati események bekövetkezésére),
- a kockázat **áthárításával** (pl. megfelelő kivitelezői szerződés, biztosítás kötése),
- a kockázat **megosztásával** (pl. tartós, felelős együttműködésen alapuló szállítói kapcsolat kialakítása)

komoly kockázatkezelési eredményeket érhetnek el.

"D" kategória – Ezek a kockázatok valójában már nem is kockázatok, hanem lényegében létrejött, vagy **biztosan megtörténő, jelentős súlyú problémák**, **„katasztrófák".** Ebben a kategóriában már nem is a megelőzésen van a hangsúly, hanem a károk kezelésén, a normál működés lehetőség szerinti fenntartásán, vagy annak minél előbbi helyreállításán. A felelősök speciális feladata olyan ún. **„katasztrófa-elhárítási tervek"** kidolgozása és megvalósítása, amelyek átfogó megoldást jelentenek a kérdésre.

Kritikusnak minősített kockázatok esetén a kockázati dokumentációban rögzíteni kell:
- az azonosított **kockázat megnevezését** és **azonosító kódját**,
- a kockázat részletes ismertetését (a valószínűséget, a hatást és az ezek alapján adódó kategóriát is,
- a **kockázat felelősét** – gazdáját (összhangban az IT biztonság egyéb feladataival),
- a kockázat kezelése érdekében megfogalmazott **intézkedési tervet**, meghatározott feladatokkal, határidőkkel és erőforrás-keretekkel. Ennek kidolgozása a kockázat gazdá-

jának felelőssége. Kidolgozása történhet egyénileg, külső szakértő bevonásával, vagy csoportmunkában, esetleg más kockázatokkal együtt kezelve is. A kockázatkezelési felettes jóvá kell, hogy hagyja a tervet.

- **a kockázat előzményeit, történetét** visszamenőleg a korábbi évekre is: tartalmazza a monitoring során tapasztaltakat, a megtett lépéseket, a bekövetkezett kockázati esemény kezelésének menetét, illetve azok eredményeit stb.

Informatikai kockázati dokumentáció része egy általános, **Semmelweis Egyetem szintű összefoglaló** is. Az informatikai kockázatok azonosítása, elemzése és értékelése kapcsán összeálló informatikai kockázati dokumentáció Semmelweis Egyetem szintű elkészítéséért, tartalmának összehangolásáért, illetve aktualizálásáért az IBF a felelős.

Külön kiemelendő az **informatikai projektek** kockázatainak kezelése. A projektek esetében a kockázatok befolyásolhatják a határidőket, a terjedelmet / a minőséget, valamint a költségeket.

Módszerek a kockázatok monitorozására

Informatikai kockázatok monitorozásakor **alapszabály**, hogy minden, az Informatikai Biztonsági Politika és Stratégia (SE-IBPS) hatálya alá tartozó **minden személy köteles a tapasztalt kockázatok, vagy az azokból adódó problémák jelzésére** – a biztonsági eseményeknél leírtak szerint.

Emellett az informatikai kockázatok értékelése alapján a konkrét azonosított kockázatra vonatkozóan elő kell írni a kockázatgazdák számára az **elvárt kockázatkövetést**. Irányelvként megfogalmazható, hogy valamennyi kockázatgazda felelős azért, hogy folyamatosan nyomon kövesse és értékelje a hozzá tartozó kockázatok állapotát, szükség esetén lépéseket kezdeményezzen azok kezelésére.

Általánosan előírható az, hogy:

- a ”B” kategóriába tartozó kockázatokról félévente,
- a **”C” kategóriába** tartozó kockázatokról negyedévente,
- a ”D” kategóriába tartozó kockázatokról pedig havonta

kell **státuszjelentést** készíteni a felelősöknek, és benyújtani ezeket az IBV által kijelölt kockázatkezelési felettesüknek.

Ugyancsak szükséges sort keríteni az **előző év kockázatkezelési tevékenységek értékelésére**. Ennek keretében **valamennyi kockázatfelelős** köteles beszámolni kockázatkezelési felettesének a hozzá tartozó kockázatok elmúlt éves történetéről.

4. Szervezet biztonsága

4.1 Informatikai biztonság elemei

Célkitűzés: Az informatikai biztonságot menedzselni kell a szervezeten belül.

Menedzselési rendszert kell létrehozni, hogy a szervezeten belül kezdeményezzék és ellenőrizzék az informatikai biztonság megvalósítását.

A vezetőség irányítása alatt vezetői „**menedzselési fórumot"** kell létrehozni, amelyek **jóváhagyják** az informatikai biztonsági szabályzatot, **kiosztják** a biztonsági szerepeket és **összehangolják** a biztonság megvalósítását a szervezeten belül.

Biztonsági szakértői tanácsadó testületre van szükség. Szerződést kell kötni külső biztonsági szakértőkkel, akik a várható változások trendjét, irányát követik, a szabványokat és az értékelési módszereket figyelemmel kísérik, valamint a biztonsági események kezelésére alkalmas külső kapcsolatrendszert biztosítanak. Az informatikai **biztonság sokoldalú megközelítését** kell előnyben részesíteni, beleértve a felhasználók, az adminisztrátorok, az alkalmazástervezők, a menedzserek, az auditorok, és a biztonsági munkatársak együttműködését, valamint a szakmai gyakorlatot olyan területen, mint a biztosítás és a kockázatkezelés.
MSZ ISO/IEC 17799:2002

4.1.1 Vezetői fórum

Informatikai biztonság egyetemleges felelősség, amelyet a Semmelweis Egyetem vezetői, illetve a munkatársai egyaránt viselnek.

Az informatikai **biztonság menedzselése** a következő szervezeti keretek között történik:

Vezetői fórum

Informatikai Biztonsági Felelős Felsővezető (**IBFF**)	- SMFI főigazgató
Informatikai Biztonsági Vezető (**IBV**)	- Informatikai Igazgatóság igazgató
Informatikai Biztonsági Felügyelő (**IBF**)	- IT biztonsági szakértő, vagy cég.
Biztonsági szakértői tanácsadó testületet	- Külső szakértők

Informatikai vezetők – rendszerbiztonsági felelősök

Egyetemi szint:

Informatikai Igazgatóság - vezető
Központi informatikai rendszer 1.
Rendszerbiztonsági felelős - RBF1

Központi informatikai rendszer 2.
Rendszerbiztonsági felelős - RBF2
.

Egyetemi szintű informatikai rendszerek

Informatikai szervezet 1. - vezető
Egyetemi informatikai rendszer 1.
Rendszerbiztonsági felelős - RBF1
.

Egyetemi informatikai rendszer 2.
Rendszerbiztonsági felelős - RBF2
.

Informatikai szervezet 2. - vezető
Egyetemi informatikai rendszer 1.
Rendszerbiztonsági felelős - RBF1
.

Egyetemi informatikai rendszer 2.
Rendszerbiztonsági felelős - RBF2
.

Kari szint:

Kari Informatikai Vezető 1.
Kari informatikai rendszer 1.
Rendszerbiztonsági felelős - RBF1
.

Kari informatikai rendszer 2.
Rendszerbiztonsági felelős - RBF2
.

Kari Informatikai Vezető 2.

Kari informatikai rendszer 1.
Rendszerbiztonsági felelős - RBF1
.

Kari informatikai rendszer 2.
Rendszerbiztonsági felelős - RBF2
.

Intézeti szervezeti szint:

Intézeti informatikai rendszer 1.
Rendszerbiztonsági felelős - RBF1
.

Intézeti informatikai rendszer 2.
Rendszerbiztonsági felelős - RBF2
.

A helyi informatikai felelősök: akik a területükön az IT biztonsági kérdésekért is felelnek.

4.1.2 Biztonság menedzselése - szerepkörök

Semmelweis Egyetemen belül – méreténél fogva – szükség van a különböző szervezeti egységek informatikai biztonsági tevékenységeinek összehangolására, koordinálására.

Az informatikai biztonsággal kapcsolatos **szereplők hatáskörei, feladatai**:

Informatikai Biztonságért Felelős Felsővezető (IBFF)

Semmelweis Egyetemen az Informatikai Biztonságért Felelős Felsővezető (**IBFF**) a Stratégiai, Működésfejlesztési és Igazgatásszervezési Főigazgatóság (SMFI) főigazgatója, aki minden informatikai biztonsági tevékenységért felel.

Hatáskör:

- a fejlesztésekhez szükséges erőforrások biztosítása,
- biztonsági szabályzatok, utasítások jóváhagyatása,
- konfliktusos helyzetekben döntés az IBV javaslatai alapján,
- Semmelweis Egyetem szintű informatikai biztonsági oktatási terv jóváhagyása,
- a munkaköri érzékenységi kategóriák és a besorolások jóváhagyása,
- az informatikai kockázatkezelési terv jóváhagyása.

Informatikai Biztonsági Vezető (IBV)

Az informatikai biztonsággal kapcsolatos szakmai kérdések tekintetében az **Informatikai Biztonsági Vezető** (**IBV**) dönt, függelmileg az IBFF alá tartozik.

Az **IBV** informatikai biztonsági kérdésekben szakmai irányítási jogot gyakorol a rendszerbiztonsági felelősök felett.

Hatáskör:
- a központi rendszerekre vonatkozó rendszer-szintű biztonsági szabályzatok, utasítások elkészítése, vagy felelős kijelölése a szabályzatok elkészítésére,
- a helyi informatikai vezetők, illetve – szükség esetén – a rendszerbiztonsági felelősök informatikai biztonsági jellegű szakmai munkájának felügyelete,
- a központi rendszerekben történt módosítások informatikai biztonsági szempontú jóváhagyása,
- a központi biztonsági előírásoktól az eltérések jóváhagyása,
- javaslattétel a helyi rendszerbiztonsági felelősök kompetenciájára vonatkozóan,
- javaslattétel az informatikai biztonsági szabályzatok, utasítások jóváhagyására, az elkészült helyi szabályzatok véleményezése,
- javaslattétel az Informatikai Biztonsági Felelős Felsővezető felé a biztonsági szabályzatok, utasítások elfogadására vonatkozóan,
- Semmelweis Egyetem szintű éves informatikai biztonsági oktatási tervek kidolgozása,
- a munkaköri érzékenységi kategóriák meghatározása és a kategóriákba besorolás végrehajtása,
- az informatikai biztonsági előírások betartásának ellenőrzése.

Feladatok:
- éves ellenőrzési terv kidolgozása, végrehajtása,
- az informatikai kockázatkezelési rendszer folyamatos működtetése.

Informatikai Biztonsági Felügyelő (IBF)

Az informatikai biztonság Semmelweis Egyetemen belüli koordinációját az **Informatikai Biztonsági Felügyelő** (IBF) látja el. Az IBF feladatkörében az egész Semmelweis Egyetemre vonatkozóan informatikai biztonsági eljárások és szabályozások elkészítését koordinálja, ellenőrzi a szabályok betartását, illetve az ellenőrzések alapján jelentést tesz a rektornak.

Hatáskör:
- éves ellenőrzési terv kidolgozása,
- a biztonsági előírások betartásának ellenőrzése, a tervben szereplő ellenőrzéseken túl egyedi IT biztonsági ellenőrzések elrendelése, az ellenőrzések során valamennyi szervezeti egységtől, a rendszerbiztonsági felelősöktől tájékoztatást/információt kérhet, az ellenőrzés végrehajtása érdekében betekinthet dokumentumokba, rendszerekbe, helyszíni szemléket hajthat végre,
- éves ellenőrzési terv alapján informatikai biztonsági ellenőrzések végrehajtása,
- az ellenőrzések megállapításai alapján, indokolt esetben felelősségre vonásra tehet javaslatot,

- a helyi informatikai vezetők, illetve – szükség esetén – a rendszerbiztonsági felelősök biztonsággal összefüggő munkájának koordinálása, ellenőrzése,
- javaslattétel az informatikai kockázatkezelési tervre vonatkozóan az IBFF felé, a kockázatkezelési rendszer kialakítása.

Feladatok:

- a biztonsági tevékenységek Semmelweis Egyetemen belüli koordinálása,
- IT biztonsági ellenőrzések végrehajtása, az ellenőrzések eredményei alapján beruházási és egyéb, működéssel kapcsolatos módosítási javaslatok megfogalmazása (a rendszerbiztonsági felelősökkel egyeztetve),
- informatikai kockázatkezelési terv elkészítése,
- a rendszer-szintű biztonsági szabályzatok, utasítások elkészítésének koordinálása.

Helyi informatikai vezető

Feladatai az informatikai biztonság menedzselése kapcsán az alábbi hatáskörökkel/feladatokkal bővülnek:

Hatáskör:

- helyi (kari/intézeti) biztonsági szabályzatok jóváhagyása a nem központilag üzemeltett rendszerek esetében,
- függelmileg hozzá tartozó rendszerbiztonsági felelősök szakmai munkájának felügyelete, koordinálása,
- központi irányelvek alapján a rendszerbiztonsági felelősök által kidolgozott rendszer-szintű biztonsági szabályzatok, utasítások véleményezése, a szabályzatok elkészítése érdekében egyeztetés a többi rendszerbiztonsági felelőssel,
- biztonsági szabályok betartatása során felmerülő problémák esetén együttműködés a többi rendszerbiztonsági felelőssel, illetve az IBV-vel,

Feladatok:

- rendszerbiztonsági felelősök szakmai munkájának felügyelete, koordinálása,
- helyi rendszerszintű biztonsági szabályzatok kidolgozása.

Kari/informatikai szervezet IT rendszerbiztonsági felelős

A rendszerbiztonsági felelős egy-egy konkrét, központi, vagy helyi, karoknál/intézeteknél üzemeltetett rendszerek informatikai vagyontárgyainak védelme érdekében betartandó biztonsági előírásokat határozza meg, illetve felel ezen vagyontárgyak informatikai biztonságáért a területén lévő felhasználók vonatkozásában.

Informatikai Igazgatóság rendszerbiztonsági felelősei

A központi alkalmazásokra, a központi informatikai hálózatra vonatkozóan központi szabályozásokat dolgoznak ki, mely szabályok betartását a helyi rendszerbiztonsági felelősöknek kell a helyi sajátosságokat figyelembe véve, illetve a konkrét rendszerekre vonatkozóan biztosítani.

Helyi (intézeti) rendszerbiztonsági felelősök

A fentieken túl a helyben üzemeltetett rendszerekre vonatkozóan helyi biztonsági szabályozásokat dolgoznak ki, a központi rendszerbiztonsági felelősök iránymutatásai, sablonjai, mintái alapján.

A helyi rendszerbiztonsági felelősök munkáját az **informatikai szervezetek vezetői** fogják össze.

Hatáskör:

- a hatáskörébe tartozó informatikai rendszerek rendszerszintű biztonsági szabályzatának, utasításainak kidolgozása Semmelweis Egyetemre vonatkozó biztonsági stratégia (SE-IBPS) előírásai alapján, javaslattétel a rendszerszintű biztonsági szabályzatok tartalmára,
- a rendszer rendszerszintű biztonsági szabályzatában meghatározott biztonsági rendszer működtetése, utasításokban meghatározott szabályok betartása, betartatása,
- a rendszerek rendszergazdáinak szakmai irányítása/utasítása a biztonsági szabályzat betartása érdekében,
- informatikai biztonsággal kapcsolatos ellenőrzéseket kezdeményezhet,
- az informatikai biztonsággal kapcsolatos ellenőrzési vizsgálatok során információt ad,
- az ellenőrzési vizsgálatok megállapításai alapján intézkedéseket javasolhat a feltárt hiányosságok kiküszöbölésére,
- a rendszer változtatása esetén a változtatást informatikai biztonsági szempontból véleményezi.

Feladatok:

- a rendszer védelme rendszerszintű és általános biztonsági előírások betartásával,
- javaslatot ad a rendszerszintű biztonsági szabályzatok tartalmára az IBV felé, vagy közreműködik a szabályzatok, utasítások elkészítésében,
- vizsgálja a rendszer biztonsági előírásainak betartását, indokolt esetben jelentést tesz az IBF felé azok megsértéséről,
- a rendszerhez kapcsolódó fejlesztések során a biztonsági előírások betartásának ellenőrzése, biztonsági előírások betartatása,
- informatikai biztonsági ellenőrzés során együttműködik az ellenőrzés végrehajtójával,
- rendszer szintű biztonsági előírások felhasználók felé kommunikálása,
- rendszer kiesése esetén közreműködés a folyamatos működés helyreállítása érdekében,
- részt vesz az informatikai biztonsági oktatási terv kidolgozásában, elkészíti a rendszerszintű biztonsági oktatási anyagokat, illetve oktatóként részt vesz a belső informatikai biztonsági oktatásokon,
- egyéb feladatok: felügyelt rendszerhez kapcsolódó jogosultságállítás, rendszeres jogosultsági ellenőrzések végrehajtása, rendszerelemhez kapcsolódó rendszeres mentések biztosítása/végrehajtása, mentési médiák utasításoknak megfelelő tárolása,

rendszer-szintű biztonsági beállítások végrehajtása, biztonsági szoftverek telepítése / karbantartása, biztonsági események figyelése, stb.

4.1.3 Biztonsági felelősségek

Minden informatikai vagyontárgyat valamelyik rendszerbiztonsági felelős illetékességi köréhez kell rendelni.

A vagyontárgyak felelősségének meghatározása során a következőket kell szem előtt tartani:

- Egyértelműen **meghatározni, és azonosítani** kell, minden önálló rendszerhez hozzárendelt különböző vagyontárgyat, biztonsági intézkedést, és folyamatot,
- Minden egyes **vagyontárgyhoz** és biztonsági **folyamathoz rendszerbiztonsági felelőst** kell **kijelölni**, a felelősségeket a rendszerszintű biztonsági szabályzatban dokumentálni kell,
- Egyértelműen kell meghatározni, és dokumentálni a **jogosultsági szinteket**.
- A rendszerbiztonsági felelős **felel** az adott vagyontárgy védelmi intézkedéseinek kidolgozásáért, illetve azok betartásáért.

A rendszerszintű informatikai biztonsági szabályzatokban részletesen meg kell határozni a rendszerbiztonsági felelősök konkrét feladatait és hatásköreit. A rendszerszintű szabályzatok kidolgozását a rendszerbiztonsági felelősöknek kell elvégezni.

4.1.4 Feljogosítás informatikai rendszerek használatához

Új informatikai rendszerek üzembe helyezése az alábbi feltételekkel történhet:

- a felhasználó szervezeti egység a rendszer bevezetését engedélyezze,
- a rendszer felügyeletével megbízott rendszerbiztonsági felelős a rendszer használatát engedélyezze,
- ellenőrizni kell az új rendszer kompatibilitását az egyéb rendszerekkel,
- üzembe helyezésével kapcsolatos módosításokat át kell vezetni a rendszerszintű informatikai biztonsági szabályzatokban.

4.1.5 Biztonsági szaktanácsadás

Az informatikai biztonsági tevékenységek Semmelweis Egyetemen belüli felelőse az Informatikai Biztonsági Vezető (**IBV**), munkájához bizonyos speciális feladatok végrehajtására – igény szerint – külső szakértőket vonhat be.

4.1.6 Együttműködés külső szervezetekkel

Az Informatikai Biztonsági Vezető (**IBV**) feladata a jogalkalmazó hatóságokkal, szabályozó testületekkel, informatikai szolgáltatókkal, távközlő-hálózat üzemeltetőkkel a kapcsolattartás annak érdekében, hogy az informatikai biztonsági intézkedéseket be lehessen tartani és azokat betartatni.

4.1.7 A biztonság felülvizsgálata

Az informatikai biztonsági előírások betartását rendszeresen felül kell vizsgálni. A vizsgálatokat vagy az Informatikai Biztonsági Felügyelő (IBF), vagy külső, független szakértő végzi.

Informatikai Biztonsági Felügyelőnek (IBF) **éves ellenőrzési tervet** kell összeállítania, melyet az IBFF hagy jóvá.

Vizsgálatok eredményei alapján az Informatikai Biztonsági Felügyelő (IBF) javaslatot tesz a biztonsági gyakorlat módosítására.

4.2 Harmadik fél hozzáférési biztonsága

Célkitűzés: Fenntartani a harmadik fél számára hozzáférhető informatikai eszközök és információvagyon biztonságát, vagyis:.

- az Egyetem informatikai eszközeit **ellenőrizhető módon** kell a harmadik fél részére hozzáférhetővé tenni,
- **kockázatfelmérést** kell végezni annak meghatározására, milyen ezek biztonsági kihatása és milyen ellenőrzési követelményekre vezetnek.
- harmadik féllel kötött szerződésben az alkalmazott **óvintézkedéseket** meg kell határozni és az óvintézkedésekben meg kell egyezni.
- harmadik félnek adott hozzáférés **további résztvevőket is** magában foglalhat. A harmadik félnek szóló szerződés ezért magában foglalja a hozzájárulást más résztvevők kijelölésére és a számukra lehetséges hozzáférés feltételeit.
- e szabvány alapul szolgálhat **ilyen szerződésekhez**, amikor az információfeldolgozás alvállalkozásba adását fontolgatják.

MSZ ISO/IEC 17799:2002

4.2.1 Harmadik fél hozzáférésének kockázata

Külső, **harmadik félnek** (nem Semmelweis Egyetem) az informatikai vagyontárgyakhoz logikai és fizikai **hozzáférését kontrollálni** kell.

Rendszerszintű informatikai biztonsági szabályzatokban ki kell dolgozni harmadik félnek a rendszerekhez való hozzáféréssel kapcsolatos **előírásokat**. Ezek az előírások különösen az alábbiakat tartalmazzák:

- hozzáférés indoka,
- hozzáférés engedélyezőinek köre,
- harmadik félnek a vagyontárgyhoz hozzáférése során felmerülő kockázatok,
- a kockázatok csökkentése érdekében hozott óvintézkedések.

4.2.2 Harmadik féllel kötött szerződés biztonsági kitételei

Külső, harmadik féllel kötött **szerződéseknek,** különös tekintettel a fejlesztési, karbantartási szerződésekre, tartalmazniuk kell **biztonsági kitételeket** is. Ezek a kitételek konkrétan tartalmazzák, vagy utalnak minden az adott szerződés tárgyába tartozó informatikai biztonsági követelményre, illetve az ezzel kapcsolatos szabályozásra.

A **szerződésekbe** minimálisan bele kell foglalni **a következőket**:

- SE Informatikai Biztonsági Politika és Stratégia (SE-IBPS), illetve a szerződés által érintett rendszerszintű informatikai biztonsági szabályzat idevágó, lényeges részeit,
- Vagyonvédelem terén:
  - SE informatikai vagyonának a védelmét,
  - azokat az eljárásokat, amelyek segítségével meghatározható, vajon előfordult-e a vagyon olyan veszélyeztetése, mint pl. az adatvesztés vagy az adatmódosulás,
  - óvintézkedéseket, amelyek gondoskodnak az informatikai vagyon védelméről hogy a szerződés érvényességi idején belül, illetve annak lejárta után,
  - a sértetlenség és rendelkezésre állás, illetve
  - az információ másolásának és nyilvánosságra hozatalának korlátozásai.

- joganyagokra vonatkozó felelősség: (pl. adatvédelmi jogszabályok)
- hozzáférés-ellenőrzési megállapodások:
  - megengedett hozzáférési módokat, valamint az olyan egyértelmű azonosítókat, mint a használói azonosítók és jelszavak,
  - a használói hozzáféréssel és kiváltságokkal kapcsolatos feljogosítás folyamatát,
  - listát kell vezetni azokról, akiket feljogosítottak a rendelkezésre bocsátott szolgáltatások igénybe vételére,
  - a szerződésben rögzített felelősségek auditálásának joga, vagyis jog biztosítása ezen átvilágítás harmadik féllel elvégeztetésére.

- óvintézkedéseket, amelyek gondoskodnak a rosszindulatú szoftverek elleni védekezésről,
- a véletlen biztonsági eseményekről és a biztonság megsértéséről szóló jelentéseket, értesítések és kivizsgálások esetére vonatkozó rendelkezéseket,
- harmadik fél alvállalkozói szerződésbe vonása.

4.3 Erőforrás-kihelyezés (Outsourcing)

Célkitűzés: Fenntartani az informatikai biztonságot akkor is, ha az információfeldolgozás felelősségét más szervezeteknek alvállalkozásba adjuk.

Erőforrás-kihelyezés előkészületei során a felek közötti szerződésben célszerű kitérni az informatikai rendszerek, hálózatok és a számítógépes környezetek kockázataira, biztonsági óvintézkedéseire és eljárásaira.
MSZ ISO/IEC 17799:2002

Informatikai rendszerek, hálózatok, asztali számítógépes környezetek egészének, vagy egy részének menedzselését és ellenőrzését alvállalkozásba adó egyetemi szervezeti egység a felek közötti szerződésben ki kell térjen a biztonsági követelményekre is. Ezek egyrészt a harmadik fél 3.2 pontban részletezett feltételei, másrészt azokon túl:

- jogi követelmények kielégítésének eljárásai (pl. az adatvédelmi jogszabályozás),

- rendelkezések foganatosítása annak garantálására, hogy az erősforrás-kihelyezésben részt vevő valamennyi fél, (alvállalkozók is) tudatában van saját felelősségének,
- a szervezeti vagyon sértetlenségének, bizalmasságának, és titkosságának biztosítására vonatkozó előírások,
- fizikai és logikai óvintézkedéseket, hogy korlátozzák és behatárolják a jogosult felhasználóknak hozzáférését az Egyetem érzékeny információihoz, adataihoz,
- szolgáltatások fenntartására szolgáló biztosítékok katasztrófa esetében,
- betartandó fizikai biztonsági szintek meghatározása az erőforrás-kihelyezésben, alvállalkozásba adásban érintett informatikai vagyontárgyak esetében,
- auditálás végrehajtására vonatkozó jog.

5. Az informatikai vagyon osztályozása és ellenőrzése

Célkitűzés (**vagyoni felelősség szerint**): Fenntartani a szervezet vagyonának megfelelő **védelmét**.

Minden fontosabb informatikai vagyontárgyat **számba kell venni**, és valamennyinek legyen megnevezett tulajdonosa. Vagyontárgyakért a felelősségre vonhatóság segíthet a megfelelő védelem fenntartásában. Minden fontos vagyontárgynak legyen azonosított **tulajdonosa**, és a megfelelő **óvintézkedések felelőssége** is legyen kiosztva. Óvintézkedések megvalósításának felelősségét át lehet ruházni, de a felelősség akkor is a megnevezett tulajdonosé.

Célkitűzés (**információ osztályozása szerint**): gondoskodni az információvagyon megfelelő **védelmi szintjéről**.

Információkat a megfelelő védelem (védettségi szint) kialakítása érdekében **osztályozni** kell. Az információnak különböző érzékenységi foka és kritikussága lehet, egyes tételek kiegészítő védettségi szintet, illetve különleges kezelést igényelhetnek.
MSZ ISO/IEC 17799:2002

A Semmelweis Egyetem informatikai vagyontárgyairól **vagyonleltárt** kell készíteni és azt folyamatosan naprakész állapotban kell tartani. A leltárban szerepelnie kell minden jelentős vagyontárgynak, amely valamelyik informatikai rendszerrel kapcsolatban van.

Informatikai vagyontárgyak:
- **információ vagyontárgyak**: adatbázisok és adatállományok, rendszerdokumentáció, használói/kezelői kézikönyvek, oktatási anyagok, folyamatossági tervek, tartalékolási elrendezések,
- **szoftver vagyontárgyak**: alkalmazói szoftverek, rendszerszoftverek, fejlesztési eszközök és szolgáltatások,
- **fizikai vagyontárgyak**: számítógépek (és azok tartozékai, perifériás elemei), hálózati eszközök, adathordozók, egyéb műszaki berendezések (légkondicionálók, stb.).

Egyértelműen meg kell határozni, és **dokumentálni** kell a vagyontárgyak tulajdonjogát és biztonsági osztályát, valamint aktuális elhelyezését.

A vagyonleltárnak **összhangban** kell állnia a **Leltározási és Leltárkezelési Szabályzattal**.

Az informatikai rendszerek által kezelt adatokat **osztályozni kell,** vagyis a következő osztályok valamelyikébe be kell sorolni.

Alap biztonsági osztály:
- személyes adatok,
- üzleti titkok,
- pénzügyi adatok,

- egészségügyi adat,
- orvosi titoknak minősülő adat,
- az intézmény belső szabályozásában hozzáférés-korlátozás alá eső (pl. feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas rendszerek biztonsági osztálya,

Fokozott biztonsági osztály:
- a szolgálati titok,
- banktitkok,
- a nem minősített adatok közül: a különleges személyes adatok, nagy tömegű személyes adatok, egészségügyi adatok, orvosi titoknak minősülő adatok,
- közepes értékű üzleti titkok feldolgozására, tárolására is alkalmas rendszerek biztonsági osztálya.

Kiemelt biztonsági osztály:
- államtitok,
- katonai szolgálati titok,
- nem minősített adatok közül: a nagy tömegű, különleges személyes adatok és nagy értékű üzleti titkok feldolgozására, tárolására alkalmas rendszerek biztonsági osztálya.

A rendszerszintű biztonsági szabályozásoknak (**RIBSZ**) tartalmazniuk kell az informatikai rendszer és a benne tárolt adatok minősítését.

Minden rendszert minősíteni kell a rendszer által **kezelt adatok osztályba sorolása alapján**. Amennyiben egy rendszer több kategóriába tartozó adatot kezel, a legmagasabb kategóriát kell a rendszer minősítésének tekinteni. Az informatikai rendszerek védelme érdekében alkalmazott biztonsági **óvintézkedéseket** alapvetően a **rendszerek biztonsági osztálya szerint** kell meghozni.

A biztonsági óvintézkedések meghatározásakor másrészt **a költség-haszon elvet is** szükséges figyelembe venni, miszerint a védelmi intézkedések költsége - álljon arányban a védendő információ értékével.

Rendszerszintű biztonsági intézkedések kialakítása során figyelembe kell venni, hogy az információ érzékenysége, kritikussága az idő folyamán **változhat**.

6. A munkatársak biztonsága

6.1 Munkakörök meghatározása, a humán erőforrással ellátás biztonsága

Célkitűzés: **Emberi hibák**, lopás, csalás és visszaélés **kockázatának csökkentése**. Biztonsági **felelősséget** már a **munkaszerződésbe** bele kell foglalni, és az egyén foglalkoztatási ideje alatt figyelni kell. Leendő új **munkatársakról** megfelelően **tájékozódni** kell, különösen bizalmi munkakörökben. Informatikai eszközöket használó valamennyi alkalmazottat és a harmadik fél munkatársait célszerű **titoktartási megállapodás** kötésére kötelezni.
MSZ ISO/IEC 17799:2002

6.1.1 Biztonság és munkaköri felelősség

Az informatikai biztonság olyan felelősség, amelyet Semmelweis Egyetem vezetői, illetve munkatársai egyaránt viselnek.

Kiemelt felelősségek az informatikai biztonság területén:
- Informatikai Biztonsági Felelős Felsővezető (IBFF),
- Informatikai Biztonsági Vezető (IBV),
- Informatikai Biztonsági Felügyelő (IBF),
- Rendszerbiztonsági felelősök.

Fenti szereplők esetében javasolt munkaköri feladatokról és hatáskörökről részletes leírás a Szervezetbiztonság fejezetben található.

Informatikai Biztonsági Politika és Stratégia (SE-IBPS) személyi hatálya alá tartozó munkatársakkal szemben általánosan elvárt jelen stratégia alapelveinek megvalósítása és megtartása.

Jelen stratégia szerinti működés alapját a szabályzatnak az érintettekkel történő megismertetése jelenti.

Munkakörök meghatározásánál követendő alapelvek

Feladatmegosztás
Informatikai rendszereket használó és üzemeltető személyek feladatköreit úgy kell meghatározni, hogy azzal **minimalizáljuk** a mulasztások és szándékos visszaélések **kockázatát**, ugyanakkor **biztosítsuk** a minél teljesebb körű **helyettesítés**, vagy kiváltás lehetőségét.

Célja, hogy **minden folyamat végrehajtásába beépüljön a kontroll** – vagyis egyetlen személy se tudja szándékosan, vagy gondatlanságból megakadályozni valamely folyamat lefutását, illetve egy szervezetet károsan eltéríteni azt eredeti rendeltetésétől. A feladatmegosztás kialakítása biztonsági vezetői feladat.

Feladatelhatárolás
Az informatikai biztonság szempontjából **összeférhetetlen munkakörök** szétválasztása a szükséges tudás elve alapján, vagyis: a kiemelt biztonsági osztályba tartozó vagyon tulajdonosa a felhasználóknak **hivatali kötelezettségeik függvényében** határozza meg jogosultságaikat (az adatkezelésre, információkezelésre, rendszerek esetében ezek használatára vonatkozóan). A feladatelhatárolások kialakítása biztonsági vezetői feladat.

Munkakörök ilyen jellegű meghatározásából levezethető az egyes **munkakörök érzékenységi szintje**, a munkakörhöz kapcsolódó adatok, információk és rendszerek biztonsági osztályokhoz tartozása alapján.

A javasolt az érzékenységi szintek alapján **munkaköri kategóriák** felállítása, amelyekbe a munkakörök besorolásra kerülnek.

Kategóriákat, besorolási szempontokat, valamint a kategóriába sorolt munkaköröket / munkaköri csoportokat **dokumentálni** kell.

Kategóriák és a besorolások **felülvizsgálatát** szükséges elvégezni:
- ha a rendszerekben, működési folyamatokban, szervezeti felépítésben bekövetkező változások a korábbi munkaköri keretek módosítását követelik meg,
- évente egyszer, a megtervezett éves ellenőrzés keretében.

Az IBV javaslatot tesz az **IBFF** felé az érzékenységi kategóriákra, illetve az ezekbe a besorolásokra vonatkozóan. Informatikai Biztonsági Felelős Felsővezető (IBFF) jóváhagyja, véglegesíti a kategóriákat és besorolásokat.

Ezeket a munkaköri kategóriákat figyelembe kell venni az alkalmazás feltételeinek meghatározásakor, illetve a munkatársról az informálódáskor.

6.1.2 Informálódás a munkatársakról

Alkalmazotti állományba a felvételt megelőzően, a kiválasztási folyamat részeként **informálódni** kell a jelöltről. Ezek részletes szabályozása az Egyetem humánpolitikával kapcsolatos szabályzatának és politikájának része kell, hogy legyen.

Bizonyos informatikai biztonsági munkaköri kategóriák indokolhatják a **munkatárs megbízhatóságának** rendszeres **ellenőrzését,** egyéb esetekben a munkatárs megbízhatóságát elegendő felvételkor ellenőrizni.

Kiemelten hangsúlyos a **munkatárs közvetlen felettesének felelőssége**:
- az új munkatársaknál a betanulási időszakban, valamint a külső munkatársak felügyeletének biztosításában (különös tekintettel az kiemelt biztonsági osztályba sorolt adatokra, információkra és rendszerekre),
- a folyamatos munkavégzés során az alkalmazottak munkájának nyomon követése, az érzékelt (kedvezőtlen) változások értékelése és az okok – jogszerű – felderítése tekintetében (a különféle biztonsági problémák megelőzése érdekében).

6.1.3 Titoktartási megállapodás

A Semmelweis Egyetem felhasználói a közalkalmazottak, illetve a hallgatók. A titoktartásra vonatkozó megállapodások a Egyetem egészének biztonságos működését szolgálják, ezért ezek a **szervezeti szintű** személyügyi és jogi szabályozások keretében kerülnek rögzítésre. Titoktartás tekintetében a **közalkalmazottakra** a Munka Törvénykönyvéről szóló 1992. évi XXII. törvény, és a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény vonatkozik.

Az olyan szerződéses felek esetében, akik **kiemelt biztonsági osztályba** sorolt adatokhoz, információkhoz, rendszerekhez férnek hozzá, **titoktartási megállapodás** megkötése **előfeltétele** a szerződések megkötésének. Ez kiterjeszthető mind az informatikai tevékenységet végző, mind pedig a Semmelweis Egyetem által átadott, kiemelt biztonsági osztályba sorolt adatokat felhasználó cégekre és magánszemélyekre. A titoktartási megállapodás megkötéséért Semmelweis Egyetem részéről az alkalmazotti, vagy egyéb szerződést aláíró személyek egyetemlegesen felelősek. Megkötött titoktartási megállapodások **felülvizsgálatát** szükséges elvégezni minden olyan alkalommal, ha az alkalmazotti és egyéb szerződések módosulnak, illetve ha ezek lejárnak.

6.1.4 Az alkalmazás feltételei

Az alkalmazás feltételei között megállapításra kerülnek az adott **munkakörnek**, vagy munkaköri csoportnak **megfelelő informatikai biztonsági feladatok, hatáskörök** és felelősségek. A humánbiztonság megőrzése érdekében javasolt az olyan alkalmazotti és egyéb szerződések megkötése, melyekben az informatikai biztonsági felelősségek mind a jövőre vonatkozóan, mind pedig a Semmelweis Egyetemen kívül végzett munkákra, tevékenységekre vonatkozóan fennállnak.

A felelősségekhez kapcsolódóan rögzíteni kell azokat a **szankciókat, eljárásokat**, amelyek akkor lépnek életbe, ha szándékosan, vagy gondatlanul a követelményeket nem tartják be. Ennek részletes szabályozásáról – a megfelelő törvényekkel és egyéb belső szabályzatokkal összehangoltan – az Egyetem Kollektív Szerződésének a Fegyelmi Felelősség fejezete rendelkezik.

Az alkalmazás feltételei között továbbá meg kell határozni az **alkalmazottak egyéb jogait** is (pl. a szerzői jogok, és adatvédelmi jogok stb.).

6.2 Az informatikai biztonság oktatása és képzése

Célkitűzés: Gondoskodni arról, hogy a **felhasználók tudatában legyenek** az informatikai biztonság fenyegetettségével és el legyenek látva minden olyan feltétellel, hogy a szervezet biztonsági szabályzatában előírtakat, a szokásos napi munkájuk során betarthassák. A felhasználók legyenek oktatva a biztonsági eljárások és az informatikai eszközök helyes használatáról a lehetséges biztonsági kockázat minimalizálása érdekében.
MSZ ISO/IEC 17799:2002

Az informatikai biztonság **oktatás célcsoportja**: az Informatikai Biztonsági Politika és Stratégia (SE-IBPS) személyi hatályába tartozó személyek. Az oktatás belső tájékoztatást és belső, vagy külső képzést, illetve továbbképzést jelent.

Informatikai biztonság oktatásával kapcsolatban éves szinten – az egyéb oktatandó informatikai szakmai tartalmakkal együtt – az **éves informatikai oktatási terv** ad iránymutatást Semmelweis Egyetem egészére vonatkozóan. Az Informatikai Biztonsági Vezető (**IBV**) javaslatot készít az Informatikai Biztonsági Felelős Felsővezető (**IBFF**) részére az informatikai biztonsághoz kapcsolódó **felhasználói** és **informatikusokat** érintő oktatásokra. Az éves oktatási tervet a rendszerbiztonsági felelősök véleményét figyelembe véve, az egyéb oktatandó informatikai szakmai tervekkel és továbbképzésekkel **összehangolva** kell elkészíteni. Az Informatikai Biztonsági Felelős Felsővezető (**IBFF**) **jóváhagyja** az éves oktatási tervet, **biztosítja** a végrehajtáshoz szükséges **erőforrásokat**, valamint év végén **beszámoltatja** az Informatikai Biztonsági Vezetőt (**IBV**) ennek megvalósulásáról.

Rendszerbiztonsági felelősök kidolgozzák Semmelweis Egyetem szintű Informatikai oktatási terv alapján a saját egységükre vonatkozó területi informatikai oktatási tervek informatikai biztonságra vonatkozó részeit, valamint felügyelik ennek megvalósítását. Ennek kidolgozását a helyi informatikai és szervezeti vezetőkkel együttműködve kell végrehajtani.

- Informatikai Biztonsági Vezető (**IBV**) **támogatja, felügyeli** az oktatási tervek kidolgozását és megvalósítását. Az informatikai szakemberek IT biztonsági képzésére vonatkozóan összegyűjti a szervezeti egységek (saját keretekkel fedezett) javaslatait, összefogja, és véglegesíti Semmelweis Egyetem szintjén az informatikai szakemberek képzését.

A felhasználók oktatása két formában történhet:

- Informatikai Biztonsági Politika és Stratégia személyi hatályába tartozó személyek – a titoktartási nyilatkozat aláírását követően – az informatikai rendszerekkel a **munkavégzést megelőzően** úgynevezett **IT biztonsági tájékoztató dokumentumot** kapnak. Ez a dokumentum:
  - tudatosítja az informatikai biztonság alapvető szempontjait,
  - röviden bemutatja az Informatikai Biztonsági Politika és Stratégia (**SE-IBPS**) **főbb rendelkezéseit** – hangsúlyozottan a követelmények és jogi felelősségek vonatkozásában,
  - meghatározza az **általános óvintézkedéseket** és a biztonsági eseményekre adandó válaszokat (rendszer-specifikus tartalom nélkül).
  - fenti, Semmelweis Egyetem egészére érvényes, átfogó IT biztonsági tájékoztató elkészítéséért az **IBV**, annak átadásáért az alkalmazotti és egyéb szerződést aláíró személyek egyetemlegesen felelősek.

- Ennek a dokumentumnak az átadását-átvételét dokumentálni kell.

- **Betöltött munkakörtől**, illetve a szerződés tárgyától **függően -** a munkavégzést megelőzően - a személyek részére **rendszer-specifikus informatikai oktatás**t kell biztosítani.

- Ennek keretében oktatni kell az **adott rendszerekhez kapcsolódó** informatikai biztonsági ismereteket és követelményeket is. Az oktatás megtartását, a részvételt, az oktatási anyag átadását-átvételét **dokumentálni** kell.

- **A rendszerbiztonsági felelősök** az oktatások megtervezésében, a tartalom kidolgozásában, az oktatási anyagok elkészítésében és annak oktatásában is részt vesznek.
  - Az Informatikai Biztonsági Vezető (**IBV**) részt vesz **a rendszerbiztonsági felelősök koordinálásában**, valamint az oktatások informatikai biztonságra vonatkozó tartalmainak összehangolásában. Felelős azért, hogy a Semmelweis Egyetem **valamennyi rendszeréhez** – aktualizált – informatikai biztonsági oktatási anyag tartozzon.
  - **Új rendszerek bevezetésekor** a munka részének tekintendő az adott rendszerhez tartozó rendszer-specifikus informatikai oktatás kidolgozása. Ezért a rendszer bevezetésének Semmelweis Egyetem oldali irányítója a felelős.
  - **Felhasználóknak** rendszeres időközönként meg kell ismételni ezeket az oktatásokat, teljes körűen felújítandó ismereteiket. Ennek részletes megvalósítását az **éves informatikai oktatási tervben** kell részletezni.
  - Egy-egy rendszert érintő informatikai **biztonsági módosításokról** a rendszert felhasználóinak **tájékoztatást** kell adni, lehetőséget teremtve arra, hogy kérdéseikre, gyakorlati problémáikra is választ kapjanak. A tájékoztatásért, a változások egységes dokumentálásáért, az adott rendszer-specifikus oktatás aktualizálásáért a **szervezeti és a kari/intézeti IT biztonsági felelősök** felelnek.

Az informatikai szakemberek képzése két formában valósulhat meg:

- **Betöltött munkakörtől függően** - a munkavégzést megelőzően és a munkavégzés során rendszeresen - az informatikai szakembereknek **belső informatikai képzéseket** kell biztosítani.

- Ennek keretében oktatni kell magas szintű, **rendszer-specifikus**, illetve **általános informatikai** biztonsági ismereteket és követelményeket is.

- Az oktatás megtartását, a részvételt, az oktatási anyag átadását-átvételét **dokumentálni** kell. A belső informatikai képzések informatikai biztonsággal kapcsolatos tartalmának megtervezéséért, a jóváhagyott képzések részletes **kidolgozásáért**, az oktatási anyagok elkészítéséért az **IBV** felel.

- A **rendszerbiztonsági felelősök** az oktatások megtervezésében, a részletes tartalom kidolgozásában, és az oktatási anyagok elkészítésében vesznek részt, illetve **oktatnak**.

- **Új rendszerek bevezetésekor** a munka része kell legyen az adott rendszerhez tartozó belső informatikai képzés kidolgozása, illetőleg a már meglévő képzési tartalmak ki-

egészítése. Ezért a rendszer bevezetésének Semmelweis Egyetem oldali irányítója a felelős.

– Informatikai szakemberek képzésének **másik formája**: **külső tanfolyamon**, képzési programban a részvételének biztosítása.

6.3 Véletlen biztonsági események (zavarok)

Célkitűzés: Gondoskodni kell arról, hogy a biztonsági események, és zavarok okozta kár minimális legyen, továbbá meg kell figyelni, és tanulni kell az ilyen eseményekből.

A biztonságot érintő eseményeket, amilyen gyorsan csak lehet, a megfelelő menedzseri csatornákon **jelenteni** kell.

Valamennyi alkalmazott és szerződéses fél **ismerje** a különböző eseményekről szóló jelentések készítésére vonatkozó **eljárásokat**, (biztonság megsértése, fenyegetés, gyenge pontok és zavarok), amelyek hatással lehetnek az adott egyetemi szervezeti egység vagyonának biztonságára. Mindenkit fel kell kérni, hogy minden észlelt és feltételezett eseményt az előre kijelölt kapcsolaton keresztül a lehető legkorábban jelentse.

A szervezetnek rendelkeznie kell hivatalos **fegyelmi eljárással**, amely azokkal az alkalmazottakkal foglalkozik, akik a biztonsági szabályzatot **megsértették**. Azt, hogy a biztonsági eseményeket pontosan meg lehessen adni, szükség lehet arra is, hogy az esemény bekövetkezését követően a lehető legkorábban bizonyítékokat szerezzenek, gyűjtsenek.
MSZ ISO/IEC 17799:2002

6.3.1 Véletlen biztonsági események

Az **SE-IBPS** személyi hatálya alá tartozó **személyek**, az Informatikai Biztonsági Politika és Stratégia (**SE-IBPS**), valamint az informatikai biztonság független felülvizsgálatai során elfogadott **elvárások szerint kötelesek eljárni**.

Biztonsági esemény: a szabályszerű működés sérülése, olyan kedvezőtlen változás, amelynek hatására a biztonság állapota sérül. Fenyegetés a biztonságra nézve, illetőleg figyelmeztető jel a fenyegetésre, vagy annak lehetőségére.

Informatika értelemben: az adatok, információk bizalmasságának – titkosságának és / vagy sértetlenségének és / vagy rendelkezésre állásának megsérülése, vagy a sérülés lehetősége.

A biztonsági esemény **kezelése** akkor indulhat el, amikor az eseményt észlelők – a kedvezőtlen változás észlelését követően – **jelentik** a biztonsági eseményt. A felhasználók tájékoztatása a biztonsági eseményekkel kapcsolatos kötelezettségeikről az IT biztonsági tájékoztató része kell, hogy legyen, ezért az **IBV** felel. Az észlelt biztonsági eseményt, illetve annak gyanúját **jelenteni** kell a rendszerbiztonsági felelősöknek, a közvetlen munkahelyi felettesnek, valamint szükség esetén a jelentést készítők által végzett munkafolyamat-

tal kapcsolatban álló további személyeknek, akiket közvetlenül, vagy közvetetten érint a biztonsági esemény.

A rendszerbiztonsági felelősök **elérhetőségeit** az IT biztonsági tájékoztató átadásakor kell a felhasználók rendelkezésére bocsátani, továbbá Semmelweis Egyetem intranetén elérhetővé kell tenni az Egyetem teljes szervezetére vonatkozóan.

A biztonsági esemény **jelentéséhez** egyetemi szinten előre definiált, elektronikus dokumentum (**formanyomtatván**y) alkalmazása ajánlott.
Ennek tartalmaznia kell:

- biztonsági esemény fajtáját (az előre definiált kategóriák szerint, illetve biztonsági esemény meghatározásával),
- esemény rövid (1-2 mondatos) leírását,
- észlelő nevét, szervezeti pozícióját és elérhetőségeit,
- észlelés időpontját és helyét,
- értesített személyek (nevét, szervezeti pozícióját),
- ha szükséges: a biztonsági esemény részletes leírását,
- egyéb megjegyzéseket.

A kitöltött formanyomtatvány továbbításának ajánlott formája: **e-mail**. Amennyiben a biztonsági esemény, vagy egyéb körülmények nem teszik lehetővé az e-mailen történő továbbítást, akkor:

- formanyomtatványt kézi kitöltéssel, el kell eljuttatni (faxon, vagy személyesen) a rendszerbiztonsági felelősnek,
- ha nincs lehetőség a formanyomtatvány azonnali kitöltésére, akkor telefonon keresztül kell jelezni a problémát a helyi (a hiba által leginkább érintett) rendszerbiztonsági felelősnek.

A biztonsági eseményről **értesítettek** kötelesek a jelentés kézhezvételét követően a jelentés elküldőjének azonnal **visszajelezni**.

A rendszerbiztonsági felelősnek a biztonsági esemény által érintett teljes felhasználói kört **tájékoztatnia kell** a biztonsági esemény megszüntetésének várható idejéről, valamint a felhasználóktól elvárt további lépésekről. Ezek betartása mindkét fél irányában kötelező érvényű, ettől az eltérést egymás felé jelezni kell.

A biztonsági esemény **menedzseléséről** az informatikai rendszerek üzemeltetéséért felelős szakemberek gondoskodnak az üzemeltetési eljárások és felelősségek keretében meghatározottak szerint.

A biztonsági esemény **elhárítását követően** az abban közreműködők kötelesek **jelezni** a normál működés helyreállítását a jelentést készítők, illetve a teljes érintett kör felé. Szükség szerint tájékoztatniuk kell az érintetteteket a biztonsági esemény okáról, a jövőben alkalmazandó óvintézkedésekről.

6.3.2 A biztonság gyenge pontjai

A felhasználókat tájékoztatni kell a biztonság gyenge pontjaival kapcsolatos kötelezettségeikről. Ez az **IT biztonsági tájékoztató** része kell, hogy legyen, amiért az **IBV** felel.

Az informatikai rendszerekhez és szolgáltatásokhoz kapcsolódóan **jelenteni kell** az észlelt biztonsági gyengeséget, fenyegetettséget, illetve ezek gyanúját az adott szervezeti egység rendszerbiztonsági felelősének, valamint a közvetlen munkahelyi felettesnek.

A **felhasználóknak tilos**, hogy maguk akarják bizonyítani a feltételezett biztonsági gyengeség, fenyegetettség meglétét, vagy kezelni ezeket, mivel ez a rendszerrel kapcsolatos visszaélésnek minősülhet.

A biztonsági gyengeség, fenyegetettség **jelentéséhez** egyetemi szinten előre definiált, elektronikus dokumentum (**formanyomtatvány**) alkalmazása ajánlott.
Ennek tartalmaznia kell:

- gyengeség, fenyegetettség rövid leírását,
- észlelő nevét, szervezetét és elérhetőségeit,
- észlelés időpontját és helyét,
- értesített személyek nevét, szervezetét,
- szükség esetén: részletes leírást,
- egyéb megjegyzéseket.

A kitöltött formanyomtatvány továbbításának ajánlott formája: belső, **hivatalos levél.**
Az átadott dokumentum **központi megőrzésre** kerül.

A gyengeségről, fenyegetettségről **értesítettek** kötelesek a jelentés kézhezvételét követően 1 munkanapon belül a jelentés elküldőjének az üzenet megérkezéséről **visszajelezni**. A **rendszerbiztonsági felelősök** a gyengeség, fenyegetettség által érintett teljes felhasználói kört – a szakmai érvek alapján döntve – **tájékoztatják** a jelenség természetéről, kezelés módjáról, valamint a felhasználóktól elvárt lépésekről. (Amennyiben a szakmai érvek úgy indokolják, e tájékoztatás elmaradhat.)

A gyengeség, fenyegetettség **menedzseléséről** az informatikai rendszerek üzemeltetéséért felelős szakemberek gondoskodnak az üzemeltetési eljárások és felelősségek keretében meghatározottak szerint.

A gyengeség, fenyegetettség **kezelését követően** az abban közreműködők – a szakmai érvek alapján döntve – **jelzik** a normál működés helyreállítását, a jelentést készítők, illetve az érintettek felé. A szakmai érvek indokolhatják a tájékoztatás elmaradását. Tájékoztatásnak tartalmaznia kell a felmerült gyengeség, fenyegetettség okait és a jövőben alkalmazandó várható óvintézkedéseket.

6.3.3 A szoftverzavarok

A felhasználók tájékoztatása a szoftverzavarokkal kapcsolatos kötelezettségeikről az IT biztonsági tájékoztató része kell, hogy legyen, ezért az IBV felelős.

A szoftverzavarok biztonsági kezeléséhez szükséges rögzíteni azt, hogy melyek azok a kiemelt szoftverzavarok, amelyek esetében a felhasználók kötelesek minden egyéb tevékenységet azonnal beszüntetni, és a hiba elhárításáig nem folytathatják a munkavégzést gépeiken.

Jelenteni kell az észlelt szoftverzavarokat az adott szervezeti egység, illetve a rendszer **rendszerbiztonsági felelősének**, valamint a közvetlen munkahelyi felettesnek.

A szoftverzavarok **jelentéséhez** az egész Semmelweis Egyetem szintjén előre definiált, elektronikus dokumentum (**formanyomtatvány**) alkalmazása ajánlott, melynek tartalmaznia kell:

- szoftverzavar rövid leírását,
- részletes leírását: szimptómáit, a képernyőn megjelenő valamennyi üzenetet (javasolt a mentése és csatolása),
- észlelő nevét, szervezeti pozícióját és elérhetőségeit,
- észlelés időpontját és helyét,
- értesítettek nevét, szervezeti pozícióját,
- egyéb megjegyzéseket.

A kitöltött formanyomtatvány továbbításának ajánlott formája: belső, **hivatalos levél.**
Az átadott dokumentum központilag **megőrzésre kerül**.

A szoftverzavar által érintett gépeket le kell kapcsolni az Egyetem hálózatáról, és használatát lehetőség szerint be kell szüntetni. A szoftverzavar által érintett gépekről tilos állományok átmozgatása más gépekre (pl. floppyn, CD-n). A szoftverzavarról értesítettek kötelesek a jelentés kézhezvételét követően azonnal a jelentés elküldőjének az üzenet megérkezéséről visszajelezni.

Felhasználóknak tilos, hogy maguk akarják kezelni az észlelt szoftverzavart, vagy eltávolítani a hibás szoftvert.

Rendszerbiztonsági felelősöknek a szoftverzavar által érintett teljes felhasználói kört **tájékoztatniuk kell** a biztonsági esemény megszüntetésének időbeli kereteiről, valamint a felhasználóktól elvárt további lépésekről. Ezek betartása mindkét fél irányában kötelező érvényű, ettől való eltérést egymás felé jelezni kell.

A szoftverzavar **menedzseléséről** az informatikai rendszerek **üzemeltetéséért felelős szakemberek** gondoskodnak, az üzemeltetési eljárások és felelősségek keretében meghatározottak szerint.

A szoftverzavar **elhárítását követően,** az abban **közreműködők** kötelesek **jelezni** a normál működés helyreállítását, a jelentést készítők, és a teljes érintett kör felé. Szükség szerint tájékoztatniuk kell az érintett kört a szoftverzavar okáról, a jövőben alkalmazandó óvintézkedésekről.

6.3.4 A biztonsági események tanulságai

A **biztonsági események**, (a feltárt gyengeségek, fenyegetések, valamint a szoftverzavarok) **okainak elemzése**, a **menedzselés** folyamatának értékelése, valamint a tanulságok összefoglalása és **fejlesztése** az egyetemi, kari/intézeti biztonsági vezetők feladata. Ezt részben önállóan végzik el – év közben, részben közösen – az éves ellenőrzés keretében.

Az éves ellenőrzés során a **rendszerbiztonsági felelősök** az **IBF** vezetésével:

- **értékelik** a saját szervezeti egységük, és Semmelweis Egyetem szintjén a felmerült biztonsági események, gyengeségek, fenyegetések, valamint szoftverzavarok fajtáját, mennyiségét és költségét,
- **meghatározzá**k ezek közül azokat, melyek gyakoriságuk és/vagy költségvonzatuk alapján kiemelt figyelmet és kezelést igényelnek, ennek alapján:
  - **javaslatot** készíthetnek az Informatikai Biztonsági Politika és Stratégia (**SE-IBPS**) célszerű módosításaira,
  - **indítványozhatják** a szállítókkal, szolgáltatókkal kötött megállapodások felülvizsgálatát,
  - **fejlesztési programokat** terjeszthetnek elő a következő évre vonatkozóan.

Semmelweis Egyetem Informatikai Biztonsági Vezetője (**IBV**) **véglegesíti** a módosításokat, elindítja a szükséges felülvizsgálatokat, fejlesztési programokat és **meghatározza** a szükséges személyi, anyagi feltételeket, melyeket jóváhagyásra **felterjeszt** az **IBFF** felé.

Az **IBV** feladata, hogy az életbe léptetett **új szabályokat átvezesse** az IT biztonsági tájékoztatóban és gondoskodjon az **aktuális tájékoztató** eljuttatásáról az Informatikai Biztonsági Stratégia hatálya alá tartozó természetes és jogi személyeknek.

A rendszerbiztonsági felelősök feladata, hogy az életbe léptetett **új szabályokat beillesszék** a következő évre tervezett rendszer-specifikus informatikai oktatásokba.

6.3.5 A fegyelmezés folyamata

Az informatikai rendszereket használó és üzemeltető személyek feladatköreit úgy kell meghatározni, hogy azzal **minimalizáljuk** a **mulasztások** és szándékos **visszaélések kockázatát**, ugyanakkor biztosítsuk a minél teljesebb körű helyettesítés, vagy kiváltás lehetőségét.

Az Informatikai Biztonsági Politika és Stratégia (**SE-IBPS**) keretében meghatározott szabályok és eljárások **megsértőit** fegyelmi és kártérítési **felelősség terheli**. A közalkalmazottak fegyelmi és kártérítési felelőssége részletesen szabályozásra kerül a hatályos törvényekben (a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény és a Munka Törvénykönyvéről szóló 1992. évi XXII. törvény). A bizonyítékok gyűjtése, tárolása, bemutatása és megőrzése kapcsán Semmelweis Egyetem Fegyelmi Szabályzatában (Kollektív Szerződés, Fegyelmi Felelősség fejezet) rögzítetteknek megfelelően kell eljárni.

Külön kiemelendő, hogy a **Fegyelmi Tanács** felállításakor figyelemmel kell lenni arra is, hogy a tanácsnak nem lehet tagja, sem jegyzőkönyv vezetője olyan személy, akit az adott kérdéskörben tanúként, vagy szakértőként kívánnak meghallgatni.

7. A fizikai és környezeti biztonság

7.1 Általános óvintézkedések

Célkitűzés: **Megvédeni** az információt és az informatikai eszközöket a veszélyeztetéstől és a lopástól.

Az informatikai vagyontárgyakat (információt és informatikai eszközöket) ajánlatos védeni a jogosulatlan személyek által elkövetett nyilvánosságra hozataltól, a módosítástól, a lopástól. A veszteséget és a károsodást minimalizáló óvintézkedéseket kell alkalmazni.
MSZ ISO/IEC 17799:2002

7.1.1 "Üres asztal – tiszta képernyő" szabály

- A **papíranyagokat és adathordozókat** alkalmasan zárható szekrényben kell őrizni/tárolni, amikor éppen nincsenek használatban, főként a munkaidőn kívüli időszakban.
- Amennyiben **ISO előírások** vannak érvényben egy szervezeti egységnél, akkor a dokumentumokat azon előírások alapján kell tárolni.
- Személyi számítógépeket, munkaállomásokat nem szabad **felügyelet nélkül** hagyni úgy, hogy azok a szokásos bejelentkezési procedúra nélkül használhatók legyenek. A munkahely átmeneti elhagyásának esetén biztosítani kell, hogy a berendezést illetéktelen személy ne használhassa (pl. lock-olás).
- **Bizalmas információ** kinyomtatására elkülönült nyomtatót kell használni, a kinyomtatott anyagokat a nyomtatás befejezése után azonnal el kell távolítani a nyomtatóból.

7.1.2 A tulajdon eltávolítása

- Bármiféle hardvert, szoftvert, vagy információt, csak megfelelő **engedélyezés** alapján szabad házon kívülre juttatni, elvinni.
- Helyszíni **ellenőrzéseket** ajánlatos végezni annak érdekében, hogy a vagyontárgyak illetéktelen eltávolítását észre lehessen venni. Mindenkiben tudatosítani kell, hogy időnként helyszíni ellenőrzéseket fognak lefolytatni.

7.2 Biztonságos környezet

Célkitűzés: **Megvédeni az üzleti helyszíneket** és információt a jogosulatlan hozzáféréstől, a sérüléstől, valamint az illetéktelen beavatkozástól.

Kritikus, vagy érzékeny üzleti informatikai eszközöket biztonságos körletekben kell elhelyezni, meghatározott biztonsági sávval, megfelelő biztonsági akadályokkal és beléptető rendszerrel kell védeni.

Informatikai eszközöket fizikailag is védeni kell a jogosulatlan hozzáférés, a sérülés, valamint az illetéktelen beavatkozás ellen.

A kialakított biztonság arányos kell legyen a megállapított kockázattal. Célszerű az „üres asztal – tiszta képernyő” szabály alkalmazásával csökkenteni a papírokhoz, adathordozókhoz, informatikai eszközökhöz a jogosulatlan hozzáférés és sérülés kockázatát.
MSZ ISO/IEC 17799:2002

Fizikai biztonság védősávja
A Semmelweis Egyetem minden telephelyén a belépést kontrollálni, a forgalmat naplózni kell. A telephelyek minden bejáratánál, illetve a kritikus egységeket (pl. szerverszoba) magukba foglaló épületek bejáratánál lehetőség szerint személyi védelem szükséges, aki a forgalom naplózását is elvégzi, továbbá ellenőrzi a telephelyről elszállított informatikai eszközök elszállításának jogosságát (pl. jóváhagyott szállítólevél).

Fizikai beléptetési óvintézkedések
A kritikus helyszíneken a munkatársakat el kell látni mások által jól látható, az illető személy fényképét tartalmazó azonosító címkével, melynek viselése kötelező. A munkatársaknak kötelessége kíséret nélkül a telephely területén tartózkodó idegent, illetve azonosítót nem viselő személyt megszólítani, tartózkodásának céljáról kikérdezni, illetve indokolt esetben a személyi védelemnek átadni.

7.2.1 Irodák, helyiségek és az eszközök biztonsága

Semmelweis Egyetemen használt szerverek közül a fokozott és kiemelt biztonsági osztályba tartozó rendszerek hardverelemeit szerverszobában kell elhelyezni. Egyéb rendszerek esetében szerverszobában elhelyezés nem kötelező.

Szerverszobákra vonatkozó **követelmények**:

- Álmennyezet és antisztatikus álpadló kiépítése. Az álpadló alsó része fémborítású, egymással, a vezetéktálca rendszerrel, és az épület EPH (egyen potenciálú hálózat) pontjával galvanikusan össze van kötve.
- Szerverszobák falai nem készülhetnek könnyűszerkezetes technológiával, nem lehetnek üvegből, gipszkartonból vagy más könnyen áttörhető anyagból.
- Ajtók megerősített kivitelűek, több ponton záródóak, az ablakok fixen beépített, zárt ablakok betörésvédő fóliázással, vagy fém ráccsal és árnyékoló (sötétítő) fóliázással ellátva. Ablak nélküli helyiségek is megfelelőek.
- A szerverszobákat klímaberendezéssel kell ellátni, és olyan teljesítményűeknek kell lenniük, hogy a szerverszoba maximális teljesítményénél és 35C° külső hőmérséklet esetén is 20C° környezeti hőmérsékletet biztosítható legyen. A klímaberendezés duplikált, illetve redundáns, esetleges meghibásodás esetén maximum 27 C°-ra emelkedhet a szerverszoba hőmérséklete. A relatív páratartalomnak szabályozhatónak kell lennie (50-80% között). Klímaberendezéseket porszűrővel szükséges ellátni, és enyhe túlnyomást kell létrehozni a helyiségben a nagy értékű berendezések porszennyeződésének elkerülésére. A klímaberendezésnek az automata tűzoltó rendszerrel összhangban kell működnie.
- A szerverszobákat el kell látni automatikus tűzérzékelő, riasztó és oltó berendezéssel, a riasztó jelzéseknek a biztonsági munkatársakhoz kell befutniuk.
- A szerverszobákba megfelelő számú mozgás-, és nyitásérzékelőket kell felszerelni.

- Az álpadlóban megfelelő számú nedvességérzékelőt kell elhelyezni. Az érzékelőknek az épület, illetve telephely biztonsági rendszerébe kell becsatlakozniuk.
- Önálló riasztó-, és beléptető rendszert kell kiépíteni, különös figyelemmel arra, hogy a helyiségbe belépőket utólag is bármikor azonosítani lehessen. A szerverszoba biztonsági rendszerének az épület meglevő rendszerével összhangban kell működnie.
- Szerverszobákban a szünetmentes tápláláson kívül szükséges kiépíteni nem szünetmenetes energia elérési lehetőséget is (pl. takarításhoz).
- Szerverszobákat EMC (Elektro Magnetic Compatibility) védelemmel kell ellátni az IEC 61000 és a CISPR 22-IT szabványok előírásainak megfelelően.
- Szerverszobák elhelyezkedésére utaló jelzéseket az épületben, illetve a telephelyen nem szabad elhelyezni.
- A szobák, irodák ajtaját munkaidőn kívül, illetve ha abban nem tartózkodik egyetlen ott dolgozó munkatárs sem, be kell zárni, a kulcs nem maradhat a zárban.

7.2.2 Munkavégzés biztonságos környezetben

- A szerver szobákban, az érvényben levő Munkavédelmi, Tűzvédelmi, Vagyonvédelmi és Adatvédelmi szabályzatokat be kell tartani.
- Szerverszobákba belépés szigorúan szabályozott, a mozgásokat a szerverszoba naplóban rögzíteni kell. Meg kell határozni, és a bejáratnál ki kell akasztani a belépésre jogosultak névsorát. A listán nem szereplő személyek csak felügyelet mellett léphetnek be a helyiségbe.
- Idegenek a szerverszobákban kizárólag felügyelet mellett tartózkodhatnak.
- A szerverszobákban tartózkodni kizárólag indokolt esetben, (pl.: más helyszínen el nem végezhető munkavégzés) szabad, ott más munkát végezni, szerelni, tárgyalni, valamint mobiltelefont használni stb. tilos.
- Szerverszobákban ételt, italt bevinni, étkezni, valamint ott dohányozni tilos. Nyílt láng, vagy egyéb nagyteljesítményű hőforrás használata ugyancsak tilos.
- Szerverszobákban nem tárolhatók idegen berendezések, alkatrészek és anyagok (pl. dokumentációk, festékpatronok, összerakásra váró számítógépek).
- Szerverszobák takarításának, valamint az esetlegesen felmerülő rovar, és rágcsálóirtásnak felügyelet mellett kell megtörténnie.
- Szerverszobákban elhelyezett berendezések (szerverek, hálózati eszközök) tisztítása, pormentesítése, illetve a gyártó által előírt tervszerű karbantartása rendszeresen meg kell, hogy történjen.
- Takarítás során nedves ruhával a feltörlés, porszívózás elvégzése szükséges. A takarítás során a géptermekben elhelyezett berendezésekbe nedvesség nem juthat.
- Takarításhoz a szünetmentes áramforrásokat nem szabad használni. A takarítás megtörténtét a szerverszoba naplóban rögzíteni kell. Fel kell tüntetni a takarítást és a felügyeletet végző személy nevét, a takarítás időpontját és időtartamát.
- Tisztaságra és a rendre ügyelni kell, a szerverszoba ajtaja mindig zárva tartandó!
- Szerverszobákban fénykép, videó-, audió-, illetőleg más felvétel készítése tilos.
- Hálózatba kapcsolt munkaállomások adattároló eszközein bizalmas információ nem tárolható, ezek csak a központi szervereken szerepelhetnek.
- A hálózatba nem kapcsolt munkaállomások esetén a bizalmas információk csak kizárólag titkosítva tárolhatók.

7.2.3 Elkülönített kiszállítási és rakodási helyszínek

A telephelyekre beérkező informatikai berendezéseket már a beérkezéskor nyilvántartásba kell venni, használatba vételükig biztonságos, zárható raktárhelyiségben kell tárolni őket.

7.3 A berendezések biztonsága

Célkitűzés: Megelőzni a vagyon elvesztését, sérülését, vagy veszélyeztetését, valamint az üzleti tevékenységek megszakadását.

Berendezéseket fizikailag védeni kell a biztonsági fenyegetésektől és a környezeti veszélyektől. Berendezések védelme azért szükséges, hogy csökkentsük az illetéktelen adathozzáférés kockázatát, valamint, hogy védekezzünk adatvesztés és adatsérülés ellen. Ennek során figyelembe kell venni a berendezések elhelyezését és a velük kapcsolatos rendelkezést. Különleges óvintézkedésekre lehet szükség ahhoz, hogy bizonyos veszélyek és jogosulatlan hozzáférés ellen védekezzünk, megóvjuk az olyan támogató eszközöket, mint a villamosenergia-ellátás, vagy a kábelezési infrastruktúra.
MSZ ISO/IEC 17799:2002

7.3.1 A berendezések elhelyezése

- Semmelweis Egyetemen használt szerverek közül a fokozott és kiemelt biztonsági osztályba tartozó rendszerek hardverelemeit szerverszobában kell elhelyezni. Az egyéb rendszerek esetében a szerverszobában az elhelyezés nem kötelező.
- A szobákban a munkahelyeket úgy kell kialakítani, hogy a monitorokra a rálátás lehetősége minimális legyen.
- Közösen használt nyomtatókat, vagy a közösen használt helyiségekben, vagy olyan folyosószakaszokon kell elhelyezni, amelyet a nyomtató használóin kívül mások nem használnak.
- Bizalmas anyagok nyomtatására elkülönített nyomtatókat kell használni. Ezekhez a nyomtatókhoz hozzáférést mind fizikailag, mind logikailag korlátozni kell, csak a bizalmas anyagokhoz egyébként is hozzáférő munkatársak használhatják őket.
- Hordozható gépeket munkaidőben megfelelő eszközzel a munkaasztalhoz kell rögzíteni, munkaidőn kívül a telephelyen maradókat pedig elzárva kell tartani.
- Munkaállomások, amelyek helyi adathordozójukon más számára titkos, illetve bizalmas információkat tartalmaznak, hozzáférés védelmet biztosítani kell. Ezeket a gépeket csak zárható helyiségekben szabad elhelyezni, ezen túlmenően ezeket a gépeket több szintű BIOS jelszóvédelemmel (boot password, setup password), valamint operációs rendszer szintű jelszóvédelemmel kell ellátni. A Windows 95/98 operációs rendszerrel működő gépeken a jelszóvédelem nem tekinthető semmilyen védelmi szintnek sem. Ezeken a gépeken át kell térni a követelményeket kielégítő más operációs rendszerre, illetve más segédprogrammal kell megoldani a védelmet.
- Informatikai eszközök közelében az étel és italfogyasztás, valamint a dohányzás tilos.

7.3.2 Tápáram-ellátás

- Bizonyos központi géptermeknek, szerverszobáknak **többutas erősáramú betáplálással** kell rendelkezniük, kiemelt berendezések (pl. szerverek) tápáramellátását szünetmentes áramforrásokon keresztül kell biztosítani.
- **Kritikus berendezéseknél** tartalék áramforrás (pl. dízelgenerátor) biztosítása is szükséges lehet. Megfelelő szoftverek telepítésével biztosítani kell a külső áramforrások és a gépek közötti biztonságos kommunikációs kapcsolatot.
- **Szünetmentes és tartalék áramforrások** karbantartását és tesztelését havonta el kell végezni, az elvégzett munka megtörténtét naplózni kell. Lehetőség szerint olyan szünetmentes áramforrások használatát kell preferálni, melyeknél az akkumulátorok rendszeres karbantartása, formázása, illetve állapotának lekérdezése megoldható. Tartalék áramforrás működtetéséhez folyamatosan biztosítani kell a megfelelő mennyiségű üzemanyagot.

7.3.3 A kábelezés biztonsága

- Az energetikai és informatikai kábelezést úgy kell kialakítani, hogy a mechanikai sérülésektől és az elektromágneses zavaroktól megfelelőképen védettek legyenek (pl. föld alatti kábelvezetés, védőcsövek alkalmazása, stb.).
- Zavarok hatásának minimalizálása érdekében az erősáramú és az informatikai kábeleket elkülönítetten kell vezetni, az optikai kábelek kivételével.
- Illetéktelen rácsatlakozás elkerülése érdekében a kábelezés végpontjait és esetleges vizsgálati pontjait zárható helyiségekben kell elhelyezni.
- Kritikus rendszerek kábelezését redundáns módon kell kialakítani, ez esetben a kábelezéseket elkülönült nyomvonalon kell bevezetni, vagyis az áramellátást más rendszerektől elkülönült áramkörökről kell megoldani.
- Villamos kapcsolószekrényekben a fenti áramkörökhöz tartozó kismegszakítókat, biztosítókat egyértelműen jelölni kell, illetve ezeket a véletlen kikapcsolás ellen védeni kell.

7.3.4 A berendezések karbantartása

- A berendezéseket a gyártójuk által megadott eljárásnak és időszaknak megfelelően kell karbantartani.
- Karbantartási és javítási tevékenységet csak arra feljogosított személy végezheti.
- Minden feltételezett és tényleges meghibásodásról, valamint minden karbantartási tevékenységről feljegyzést kell készíteni.
- Külső helyszínen végzett karbantartás/javítás esetén gondoskodni kell arról, hogy a kiszállított berendezések adathordozóin bizalmas adatok ne szerepeljenek.

7.3.5 Berendezések házon kívüli biztonsága

- Semmelweis Egyetem telephelyein kívül elhelyezett/szállított berendezések és adathordozók nem hagyhatók felügyelet nélkül. A szállítást lehetőség szerint rejtetten kell megvalósítani különösen az adathordozók és a hordozható gépek tekintetében. A szállítások időpontját és a szállítási útvonalat dokumentálni kell.

- Szállításkor és idegen helyen történő elhelyezéskor a gyártók berendezés-védelmi utasításait be kell tartani (pl. mágneses adathordozók esetén elektromágneses mezőben tartás tilalma.)
- Otthoni munkavégzés esetén a fellépő kockázattal arányos védelmi intézkedéseket kell tenni (pl. használaton kívüli, hordozható gép zárt szekrényben elhelyezése).

7.3.6 A berendezések biztonságos átadása, újrahasznosítása

- Bizalmas információkat tartalmazó adathordozók, illetve adathordozókat tartalmazó berendezések továbbadása, illetve selejtezése előtt az azokon tárolt információt alkalmas módon meg kell semmisíteni. Nem adattovábbítási céllal adathordozó csak akkor adható át, ha arról az adatok törlése visszaállíthatatlan módon megtörtént.
- Átadás előtt az átvételi jogosultságot minden esetben ellenőrizni, az átadás/átvételt pedig írásban rögzíteni kell.
- Átadásra kerülő adathordozókat úgy kell előkészíteni, hogy azokon csak az átadásra szánt információk szerepeljenek.

8. Kommunikáció és üzemeltetés menedzselése

8.1 Informatikai folyamatok és felelősségek

Célkitűzés: Gondoskodni kell az informatikai eszközök biztonságos működéséről.

Informatikai **eszközök menedzselésének** és **üzemeltetésének felelősségeit** és **eljárásait** meg kell határozni. Ebbe ajánlatos belefoglalni az üzemeltetési utasításokat és a véletlen eseményekre adandó válaszokat. Ahol lehetséges, ott meg kell valósítani a felelősségek és feladatok szétosztását, annak érdekében, hogy csökkentsük a rendszerrel a hanyag, vagy szándékos visszaélés lehetőségét.
MSZ ISO/IEC 17799:2002

8.1.1 Dokumentált üzemeltetési eljárások

Az üzemeltetési folyamatokat és az ezekhez kapcsolódó felelősségeket teljeskörűen egy **központi üzemeltetési szabályzatban** kell dokumentálni. Minden informatikai **rendszer csak a szabályzatban foglaltak szerint üzemeltethető**. Az üzemeltető munkatársak a szabályzatban foglaltaktól csak kivételes esetekben (pl. biztonsági események) az üzemeltetés vezető jóváhagyásával térhet el. Az elkészült dokumentáció hivatalos dokumentumnak minősül, melynek fizikai és elektronikus tárolásáért az adott szervezeti egység informatikai rendszerének üzemeltetés-vezetője felelős. Dokumentumokban bárminemű változtatás csak az üzemeltetés-vezető jóváhagyásával lehetséges.

Üzemeltetési szabályzatnak tartalmaznia kell a következőket:

- A munkafolyamatok részletes leírását.
- Végrehajtáshoz szükséges időütemezést, figyelembe véve a kapcsolódó rendszerek tulajdonságait és azokra gyakorolt hatásokat.
- Munkafolyamatok során fellépő hibák és más kivételes helyzetek esetére vonatkozó utasításokat, megszorításokat.
- Váratlan meghibásodások és üzemeltetési problémák esetére vonatkozó utasításokat, illetve az ezek esetén rendelkezésre álló támogatási konstrukciókat. (Szerződések, kapcsolatok, alternatívák, stb.)
- Rendszer leállításának, újraindításának menetét meghibásodások esetén.

8.1.2 Az üzemeltetés változásainak ellenőrzése

Az üzemeltetési folyamatok, és rendszerek változását szigorú ellenőrzési és engedélyezési folyamatnak kell megelőznie, az alábbiak szerint:

- Meg kell vizsgálni a felmerült igény szükségességét és kivitelezhetőségét, különös tekintettel a változás lokális és kapcsolódó rendszerekre, más alkalmazásokra gyakorolt hatásaira.
- Tervezett változások csak a rendszer üzemeltetéséért felelős munkatárs, az alkalmazás gazdája, illetve a rendszerbiztonsági felelős együttes hozzájárulásával valósíthatók meg.

- Meg kell határozni a változások kivitelezéséért felelős személyeket, illetve a sikertelen változások esetén megvalósítható visszaállítási eljárásokat.
- Változások minden lényeges részletét az érintett illetékes személyekkel hivatalos úton közölni, és tudomásul vétetni kell.
- Változással kapcsolatos dokumentációkat meg kell őrizni, és a változás sikeres végrehajtása után az üzemeltetési szabályzat megfelelő részeit ezeknek megfelelően aktualizálni kell.
- Dokumentációban az összes sikeres és sikertelen változást rögzíteni, naplózni kell.

8.1.3 Biztonsági eseményt menedzselő eljárások

Ki kell dolgozni a biztonsági események minden ismert lehetséges fajtája esetén alkalmazandó eljárásokat, különös tekintettel a következőkre:

- meghibásodások, illetve az ezekből származó szolgáltatás-kiesések,
- véletlen, vagy szándékos mulasztásból adódó szolgáltatás-kiesés,
- pontatlanul, hibásan, vagy hiányosan bevitt és feldolgozott adatokból eredő hibák,
- adattitok megsértése, külső behatolás, vagy szabotázs útján,
- rosszindulatú szoftverek, vírusok bejutása a rendszerbe.

Ilyen esetekben alkalmazandó általános eljárásrendet a következő prioritások szerint kell felépíteni:

- az eseményt kiváltó tényezők mielőbbi lokalizálása, megszüntetése, vagy elhatárolása,
- érintettek értesítése,
- adatintegritás, illetve a szolgáltatások mielőbbi helyreállítása,
- helyreállítás, illetve a hibák kijavításának folyamatát hivatalosan és szigorúan ellenőrizni kell, különös tekintettel arra, hogy:
  - kizárólag a feljogosított és azonosított munkatárs kaphat engedélyt az adatok és szolgáltatások üzemben tartására,
  - valamennyi vészhelyzetben végzett tevékenységet részletesen dokumentálni, illetve a vezetőség felé rendszeresen jelenteni, szükség szerint felülvizsgálni, és módosítani kell,
  - helyreállítás, illetve a szükséges óvintézkedések megtörténtét a lehető legrövidebb időn belül az érintettekkel közölni kell.
  - az eljárások során keletkező dokumentumokat meg kell őrizni, mivel ezek alapjául szolgálhatnak az eseményt érintő további eljárásoknak,
  - tevékenységek jelentése az illetékes szerveknek.
  - szerződésszegés, szabályzatok megsértése, vagy visszaélések esetén bizonyítékok szolgáltatása polgári peres, vagy büntetőjogi eljárásokhoz.
- esemény elemzése, szükséges óvintézkedések meghozatala,
- szállítók, szolgáltatók részére segítség a további fejlesztésekhez, hibák javításához,
- információk biztosítása további belső problémák elemzéséhez.

8.1.4 A feladatkörök meghatározása, feladatok megosztása

- Az informatikai rendszereket használó és **üzemeltető személyek feladatköreit** úgy kell meghatározni, hogy azzal minimalizáljuk a mulasztások és szándékos visszaélések kockázatát, ugyanakkor biztosítsuk a minél teljesebb körű helyettesítés, vagy kiváltás lehetőségét.
- A feladatköröket lehetőség szerint **úgy kell meghatározni**, hogy egy feladatot ellátó, valamint azt ellenőrző, vagy felülvizsgáló személy ne legyen azonos.
- Elvégzett feladatokat, tevékenységeket a szervezeti egység üzemeltetés-vezetőjének rendszeres időközönként a rendelkezésre álló dokumentumok (pl. üzemeltetési napló) alapján **ellenőriznie** kell.
- Olyan területeken, ahol összejátszás, vagy korrupció lehetősége áll fenn, a feladatokat úgy kell meghatározni, hogy azokban egyidejűleg **több személy** vegyen részt.
- Ha lehetséges, meg kell oldani, hogy a **kritikus feladatokat** időnként más-más személy lássa el. Nem fordulhat elő, hogy kritikus feladatokat ellátó személy nem veszi ki szabadságát.

8.1.5 Fejlesztési és üzemeltetési eszközök szétválasztása

A fejlesztések, tesztelések és bevizsgálások mindig csak az üzemi környezettől lehetőség szerint maximálisan elkülönített környezetben történhetnek.

Ezek során a következő óvintézkedéseket célszerű betartani:

- Fokozottan kell figyelembe venni és alkalmazni a **feladatszétosztás** szabályait. A fejlesztési és tesztelési feladatokat, tevékenységeket szét kell választani, amennyire csak lehetséges.
- Fejlesztő, tesztelő és produktív rendszerekhez ugyanazon felhasználók **különböző felhasználónevekkel** és/vagy **jelszavakkal** férjenek hozzá az esetleges hibák kockázatának csökkentése érdekében.
- Amennyiben elkerülhetetlen a teszt és a produktív környezetbe az egyidejű bejelentkezés, az erre a célra kiadott jogosultságokat és jelszavakat a lehető legszigorúbb **biztonsági szabályozások szerint** kell kialakítani (pl. minimális jogosultságok, időkeretek, rövid lejáratú jelszavak).

8.2 Rendszerek tervezése és üzemeltetésre átadása

Célkitűzés: Minimalizálni a rendszer-meghibásodások kockázatát.

Modern tervezési és előkészítési módszerekre van szükség ahhoz, hogy szavatolni tudjunk, hogy a **kellő rendszerkapacitás** és **erőforrás-kapacitás** rendelkezésre álljon. **Előre jelezni** kell a jövőben várható kapacitáskövetelményt annak érdekében, hogy csökkentsük a rendszer túlterhelésének kockázatát. Már az átvétel és a **használatba vétel előtt** meg kell állapítani, dokumentálni kell, és be kell vizsgálni az új rendszerek üzemeltetési követelményeit.
MSZ ISO/IEC 17799:2002

A rendszer-**meghibásodások** és **túlterhelések** kockázatának csökkentése, valamint a kellő rendszer-, és erőforrás-kapacitás rendelkezésre állásának biztosítása érdekében folyamatosan figyelni kell a rendszer jelenlegi, illetve várható kapacitásigényét.

Különös figyelmet kell fordítani a **szervergépek** fejlesztésére és a feldolgozási **folyamatok** során keletkező **szűk keresztmetszetek** felszámolására, mivel ezek fejlesztése általában csak hosszabb távon oldható meg, viszont nagymértékben befolyásolják a szolgáltatások minőségét.

Az új rendszerek, korszerűsítések, új változatok átvétele és bevezetése előtt alapos **megfelelőségi-, és hatásvizsgálatot** kell végezni, a következők figyelembevételével:

- A fejlesztés **megfelel-e** a tervezett teljesítmény és kapacitás elvárásoknak.
- Az új rendszer **nem lehet negatív hatással** a meglévő környezet kapacitására és teljesítményére, különösen bizonyos csúcsidőszakokban (pl. hónap végi zárás, hétfő reggel).
- **Elemezni** és dokumentálni kell az új rendszer üzembe helyezésének hatását a Egyetem informatikai és általános biztonságára.
- **Tervet** kell készíteni a fellépő hibák esetén alkalmazandó visszatérési és újraindítási eljárásokról, valamint a rendelkezésre álló tartalékokról.
- Üzemeltetési eljárásokat, azok változásait a megfelelően **dokumentálni** kell.
- Meg kell határozni, és/vagy megfelelően módosítani kell az **üzletmenet** (üzemelés) f**olytonosságát** biztosító intézkedéseket, eljárásokat.
- Szoftverek támogatására, módosítások, upgrade-k végrehajtására **szerződést** kell kötni külső féllel (különös tekintettel a biztonsági szoftverekre).

8.3 Védelem rosszindulatú szoftverek ellen

Célkitűzés: **Megvédeni a szoftver** és az **információ sértetlenségét**.

Elővigyázatossági intézkedésekre van szükség ahhoz, hogy a rosszindulatú szoftver betelepülését megelőzzük és észleljük. Szoftver és az informatikai eszközök igen sérülékenyek az olyan rosszindulatú szoftverek betelepülésével szemben, mint a számítógépvírusok, a hálózati férgek, a trójai falovak és a logikai bombák.

A felhasználóknak tudatában kell lenniük, hogy a jogosulatlan és a rosszindulatú szoftverek milyen veszélyesek, a menedzsereknek, ahol lehet, különleges **óvintézkedéseket** kell bevezetniük, hogy **észleljék** azokat és **megakadályozzák** betelepülésüket. Különösen az a lényeges, hogy a személyi számítógépek esetében óvintézkedéseket tegyünk a számítógépvírusok észlelése és betelepülésüknek megelőzésére.
MSZ ISO/IEC 17799:2002

A rosszindulatú szoftverek által jelentett fenyegetéseket teljes mértékben megszüntetni nem lehet, de minden lehetséges eszközzel **csökkenteni kel**l ezek bekerülésének lehetőségét.

Emellett rendszeresen **azonosítani** és **védeni** kell az általuk támadható területeket.

Ennek érdekében a következő **intézkedések, illetve szabályozások** szükségesek:

- Az SE Informatikai Üzemeltetési Szabályzatban (**SE-IÜSZ**) szabályzatában rögzítésre került, hogy az egyetemi számítógépekre az Egyetem által központilag beszerzett, illetve ettől eltérően kizárólag az Informatikai Igazgatóság által engedélyezett és **jogosan licenszelt szoftver** telepíthető, tilos az illegális, vagy magáncélú szoftverhasználat.

- Gondoskodni kell arról, hogy a stratégiát/**szabályzatot** mind az újonnan belépő, mind a meglévő munkatárs írásos formában **tudomásul vegye**.

- A vírusvédelemmel foglalkozó szabályokat, a védelmi rendszerek használatát ismertető eljárásokat, a részletes üzemeltetés folytonossági terveket rögzíteni kell az **üzemeltetési szabályzatban**.

- **A vírusfertőzés**, vagy más rosszindulatú program bejutása **biztonsági eseménynek** minősül, kezelésekor az erre vonatkozó szabályok szerint kell eljárni. A szabályozások kialakításakor a feladatokat és felelősségeket az alábbiak figyelembevételével kell meghatározni.

- Rendszerbe külső forrásból érkező adathordozókat **csak vírusellenőrzés után** szabad használni. Hálózati kommunikációs csatornákon beérkező állományok (levélmellékletek, internetről letöltött állományok stb.) vírusellenőrzését is minden esetben el kell végezni.

- A vírusokat és rosszindulatú programokat detektáló, valamint azokat semlegesítő szoftverek, céleszközök telepítését és frissítését napi rendszerességgel **ellenőrizni** kell.

- A kiszolgáló (szerver) és munkaállomás számítógépekre csak megfelelően kiképzett és feljogosított munkatárs **telepíthet szoftvert**. Munkaállomásoknál, ahol ez lehetséges helyi, vagy központi biztonsági beállításokkal meg kell akadályozni annak a lehetőségét, hogy illetéktelenek szoftvert telepítsenek a számítógépekre. A telepítés csak előzetes vizsgálatot követően hajtható végre.

- Rendszeresen figyelni kell, és majd csak a tesztelés és hatásvizsgálatok elvégzése után lehet telepíteni a szoftvergyártók által kibocsátott operációs rendszer és az alkalmazások **biztonsági frissítéseit**.

- Az **ellenőrzés rendszere** lehetőleg többszintű legyen. A felhasználó munkaállomása mellett a szervereken – levelezés, fájlszerverek – is működjön vírusellenőrzés.

- Rendszeresen **figyelni** kell különböző megbízható, **minősített források információit** (biztonságtechnikai szervezetek – pl. CERT -, szoftvergyártók), melyek figyelmeztetéseket adnak közre a megjelenő veszélyekről: vírusok, férgek, trójai programok, megtévesztések). Ezek figyelembe vételével esetleges **rendkívüli óvintézkedéseket** kell

foganatosítani. (pl. a szükséges védelmi frissítés kiadásáig a levélmellékletek blokkolása.)

8.4 A mentések

Célkitűzés: Fenntartani az információfeldolgozás és a hírközlési szolgáltatások sértetlenségét és rendelkezésre állását.

Az egyeztetett mentési stratégia végrehajtására rutineljárást kell megállapítani az adatok biztonsági másolatának készítésére, az adatok időben történő visszaállítására, a berendezéskörnyezet eseményeinek megfigyelésére és meghibásodásainak naplózására.
MSZ ISO/IEC 17799:2002

Az informatikai rendszerekben tárolt adatokról és szoftverekről rendszeres időközönként **biztonsági másolatokat** kell készíteni annak érdekében, hogy bármely biztonsági esemény, vagy katasztrófa esetén az **adatállományok** és a **működés helyreállítható legyen**. A rendszerekre vonatkozó mentési eljárásokat, feladatköröket és felelősségeket úgy kell meghatározni, hogy összhangban legyenek az üzemelés folyamatossági tervekkel.

A mentési eljárásokat a következők szerint kell kialakítani:

- **Szervereken** tárolt adatokról, információkról rendszeres biztonsági mentéseket kell készíteni. A mentések gyakoriságát az adatok fontossága és változásának gyakorisága alapján kell meghatározni. Ajánlott a fokozott és kiemelt minősítésű adatokról naponta, vagy – amennyiben ezt az infrastruktúra lehetővé teszi – akár naponta több alkalommal mentést készíteni.

- **Statikus adatokról** (rendszerkörnyezet, szoftverek, információs adatbázisok stb.) a változtatások alkalmával, és ezen kívül hosszabb időközönként is (pl. havonta) rendszeres mentéseket kell készíteni. Egyszerűen installálható szoftverek esetén az installációs anyag mentésként elfogadható.

- Különböző területek mentési **eljárásait** (gyakoriság, médiatípus, médiaforgatási rendszer stb.) az **üzemeltetési szabályzatban** kell rögzíteni.

- A mentések elvégzése, figyelése, naplózása, a **rendszergazdák feladata** és felelőssége. A mentések bármilyen okból bekövetkező meghiúsulása biztonsági eseménynek minősül, és a továbbiakban a biztonsági eseményekre vonatkozó rendelkezések szerint kezelendő.

- A mentés céljára szolgáló infrastruktúra (eszközök, adathordozók, kapcsolatok) kialakítása és méretezése, úgy kell, hogy történjen, hogy **bizonyos** mértékű **redundanciát** tartalmazzon, azaz valamely egység meghibásodása esetén a mentést a rendelkezésre álló időszegmensen belül el lehessen végezni.

- Adatmentésekről **naplót** kell vezetni, ebbe fel kell jegyezni minden olyan rendes és rendkívüli eseményt, amely az adatmentésekkel kapcsolatos.

- Az adatmentések adathordozóit a sérülésektől és az illetéktelen hozzáférésektől védett, **biztonságos helyen** kell tárolni. Erősen ajánlott megfelelően védett és tűzbiztos helyiség, vagy tűzbiztos páncélszekrény használata.

- A biztonsági mentések adathordozóit rendszeres időközönként **tesztelni** kell, illetve meg kell győződni a rajtuk tárolt adatok visszaállíthatóságáról.

- Bizonyos rendszeres időközönként ún. „offsite-készleteket" kell létrehozni, melyeket egy t**ávoli biztonságos helyen kell tárolni** arra az esetre, ha az adott egyetemi szervezeti egység telephelyén bekövetkező katasztrófa (pl. tűzeset, vagy egyéb természeti csapás) következtében az ott tárolt információk és mentések megsemmisülnének.

  Ezeknek a készleteknek a következőket kell tartalmazniuk:
  - a biztonsági másolatok adathordozóit, melyek a szervezetben tárolt összes adatot, illetve használatos szoftvert tartalmazzák,
  - a visszaállítási eljárások teljes dokumentációját,
  - a visszaállításhoz szükséges szoftverek adathordozóit,
  - visszaállításhoz szükséges egyéb információkat (jelszavak, titkosítási kulcsok stb.)

- A kezelő munkatársnak **mentési naplót** kell vezetnie, melybe az üzemeltetés során előforduló minden rendes és rendkívüli eseményt, illetve az ezek kapcsán végzett tevékenységeket fel kell jegyezni.

- A naplókat a felelős helyi vezetőnek (alkalmazásgazda, üzemeltetés vezető) rendszeresen **ellenőriznie** kell és bizonyos időközönként – az érvényes üzemeltetési szabályzattal összevetve – **független ellenőrzésnek** is alá kell őket vetni.

8.5 Az infrastruktúra védelme - hálózatmenedzsment

Célkitűzés: Megóvni a hálózaton áthaladó információt, és megvédeni az infrastruktúrát.

Különös figyelmet igényel az olyan hálózatok biztonsági menedzselése, amelyek túlnyúlhatnak a szervezeti határokon. Kiegészítő óvintézkedésekre lehet szükség nyilvános hálózatokon áthaladó érzékeny adatok megvédéséhez.
MSZ ISO/IEC 17799:2002

A hálózaton áthaladó információ és az infrastruktúra védelme, valamint a terhelés optimális elosztása érdekében az informatikai vezetőknek és a hálózatmenedzsereknek a következő intézkedéseket kell megvalósítaniuk:

- Amennyire lehetséges, alkalmazni kell a **feladatszétosztást**, vagyis hálózatmenedzselést külön kell választani a számítógépek üzemeltetésétől.

- A szolgáltatások optimalizálása és a különböző óvintézkedések egész infrastruktúrára kiterjedő betartása érdekében az informatikai **menedzserek tevékenységét** az egész szervezetre vonatkozóan **össze kell hangolni**.

- A távoli berendezések menedzselésének eljárásait és felelősségeit a **központi üzemeltetési szabályzatban** rögzíteni kell.

- A hálózati infrastruktúra menedzselésével kapcsolatos feladatokat és felelősségeket a hozzáférés ellenőrzés részben leírtak vonatkozó rendelkezéseivel **összhangban** kell meghatározni.

8.6 Adathordozók védelme

Célkitűzés: Megvédeni a vagyontárgyakat a sérüléstől és az üzleti tevékenységeket a megszakításoktól.

Az adathordozókat ellenőrizni, és fizikailag védeni kell. Megfelelő üzemeltetési eljárásokat kell bevezetni, annak érdekében, hogy a dokumentumokat, a számítógépes adathordozókat, a kimenő/bemenő adatokat és a rendszerdokumentációkat a sérüléstől, a lopástól és a jogtalan hozzáféréstől megvédjük.
MSZ ISO/IEC 17799:2002

Hordozható számítógépek adathordozóinak, illetve ezek miatt bizalmas információk megsérülésének, vagy illetéktelen kezekbe kerülésének megakadályozása érdekében az adathordozók kezelésére és tárolására **hivatalos eljárásokat** kell kialakítani a következők szerint:

- Minden adathordozót biztonságos és **védett környezetben** kell tárolni, a gyártó előírásainak figyelembevételével.

- **Hordozható adathordozók** – különösen a felhasználói adathordozók kategóriájába tartozó eszközök, pl. floppy, CD-lemez, USB pendrive – csak indokolt esetben használhatók, ha a körülmények más biztonságosabb eszköz (hálózati átvitel, mágnesszalag stb.) alkalmazását nem teszik lehetővé.

- Az adathordozóknak a szervezeti egységektől az elvitelhez, feljogosítás szükséges, melyekről naprakész **nyilvántartást** kell vezetni. A nyilvántartásokat a rendszerbiztonsági felelősöknek időközönként ellenőrizniük kell, a feltárt mulasztások esetén a szükséges intézkedéseket meg kell tenni.

- A **hordozható adathordozón** kivitt adatokat azok kritikusságától, bizalmas mivoltától függően kriptográfiai eljárással **titkosítani** kell. A titkosítás szükségességét a kivitel engedélyezőjének kell elbírálnia, szükség szerint elrendelnie.

- Ha adathordozók tartalmára már nincs szükség, az **újrafelhasználható eszközök** tartalmát törölni kell, a nem törölhető adathordozókat meg kell semmisíteni. A meg-

semmisítésekről naplót kell vezetni. A megsemmisítésért az adat tárolására szolgáló informatikai rendszer rendszerbiztonsági felelőse felel.

- **Kerülni kell** az adathordozók törlés nélküli raktározását, mivel a felgyülemlő nagy mennyiségű, osztályozatlan információ komoly biztonsági kockázatokat jelent.

8.7 Az információcsere biztonsága

Célkitűzés: Megvédeni a szervezetek közötti információcserét az elvesztéstől, módosulástól és a visszaéléstől.

A szervezetek közötti információ- és szoftvercsere legyen jól kontrollált, és feleljen meg a vonatkozó jogszabályoknak. Minden adatcserét **megállapodás alapján** kell végezni. A szállítás alatti információnak és adathordozóknak védelmét ellátó eljárásokat és szabályokat rögzíteni kell. Megfontolás tárgyává kell tenni az elektronikus adatcserével (EDI), az elektronikus kereskedelemmel, valamint az elektronikus levelezéssel összefüggő **üzleti és biztonsági** kérdéseket, továbbá a vonatkozó **óvintézkedések** követelményeit.
MSZ ISO/IEC 17799:2002

Semmelweis Egyetem külső intézményekkel, állami szervezetekkel az együttműködés kereteit a vonatkozó jogszabályok határozzák meg. Egyéb esetekben, illetve a jogszabályok által nem szabályozott kérdésekben a biztonsági stratégia/szabályzat szerint kell eljárni.

Az információcsere – akár elektronikus, akár manuális – **csak előzetesen megkötött megállapodás alapján** jöhet létre.

A megállapodásoknak **tartalmazniuk kell** az alábbiakat:
- az információ minősítését (adatszolgáltatás, tájékoztatás, bizalmas információ stb.),
- az adattovábbítás és adatátvétel módjának meghatározását, eljárásait (pl. hálózati átvitel, vagy fizikai adathordozó, adathordozó típusa, alkalmazott titkosítási eljárás stb.).
- az adatátvitel műszaki követelményeit, vagyis az információ rögzítéséhez, feldolgozásához, olvasásához szükséges műszaki feltételeket,
- az adattovábbításban résztvevők megnevezését és az azonosításukra szolgáló eljárásokat,
- az adatvesztés esetén felmerülő feladatokat, felelősségeket,
- az adatátvitel kezdetének időpontját, határidejét, várható időtartamát,
- egyéb óvintézkedéseket, melyet a szigorúan bizalmas, vagy nagy érzékenységű információk védelme tehet szükségessé.

Az adattovábbítás folyamata alatt – legyen az fizikai, vagy elektronikus – az információ fokozottan érzékeny a sérüléssel, jogtalan hozzáféréssel és visszaélésekkel szemben. Ezért a továbbítás megszervezésekor lehetőség szerint a **következők szerint kell eljárni**:

Fizikai adathordozó továbbítása esetén általánosan a korábbiakban leírtak az irányadóak, de emellett gondoskodni kell a következőkről:

- megbízható kézbesítőt kell alkalmazni,
- az adathordozókat a gyártó előírásai szerint kell csomagolni, a csomagolásnak meg kell védenie a tartalmat az esetleges sérülésektől.
- nagy érzékenységű információk esetén további óvintézkedések alkalmazása szükséges.

Elektronikus adattovábbítás esetén:
- Online átvitel esetén az adattovábbítás **védett csatornán** történjen. Adatátvitel, csak a küldő, és fogadó fél egyértelmű **azonosítása után** kezdhető meg, az azonosítás módját előzőleg megállapodásban kell rögzíteni.
- **Fokozott, vagy kiemelt biztonsági osztályba tartozó adatokat** – különösen, ha azok nem titkosított csatornákon kerülnek továbbításra (pl. email) – kriptográfiai eljárással **titkosítani** kell.

Bármely továbbítási eljárás során **egyéb hitelesítési eljárások** (digitális aláírás, hash-kód stb.) használata javasolt.

Elektronikus levelezés jelentősen gyorsítja a kommunikációt, ugyanakkor a hozzá kapcsolódó szolgáltatások növekedésével és nagymértékű, gyors elterjedésével komoly biztonsági és üzemeltetési kockázatokat hordoz magában.

Egyetem **levelezési szabályzatának** kialakításakor ezért rendkívüli gondossággal kell eljárni. Felhasználókat alaposan tájékoztatni kell az elektronikus levelezés használatának kockázatairól:
- az üzenetek kézbesítése és a kézbesítés időtartama nem garantálható,
- az üzenetek sérülékenyek a módosításokkal és jogtalan hozzáférésekkel szemben,
- címzések helyessége nem, vagy csak korlátozottan ellenőrizhető, ily módon bizalmas információk kerülhetnek illetéktelen személyekhez,
- kéretlen, zaklató tartalmú üzenetek érkezhetnek ismeretlen és azonosíthatatlan feladóktól, melyek mellékletként akár rosszindulatú programokat is tartalmazhatnak,
- ismert feladóktól és forrásokból is érkezhetnek olyan levelek, melyek akár rosszindulatú programokat hordoznak magukban – az esetek túlnyomó többségében a feladó tudta nélkül.
- Levelezési címek meggondolatlan kiadásával, illetve azok illetéktelen kezekbe kerülésével a felhasználó kéretlen reklámlevelek tömegét zúdíthatja magára, melyek amellett hogy rendkívül megnehezítik az értékes információ kiszűrését, korlátozhatják és akár meg is akadályozhatják a levelező szerverek működését (SPAM).

Elektronikus levelezés szabályzata a következőket kell, hogy tartalmazza:
- A **levelezőszervereket** hatékony **védelemmel kell ellátni** az illetéktelen hozzáférések és egyéb biztonsági események ellen.

- Az elektronikus levelezést **vírusvédelemmel,** és lehetőség szerint **tartalomszűréssel** kell védeni a rosszindulatú programok, SPAM-ek, egyéb veszélyforrások ellen. Ez történhet a levelezőszerverre telepített szoftverrel, vagy a kommunikációs vonalba beiktatott hardver eszközzel.

- **A felhasználók** csak **megfelelő hitelesítés után** férhetnek hozzá a levelező rendszerekhez. Olyan rendszerek esetén, ahol a levelek a felhasználó munkaállomására letöltődnek, gondoskodni kell arról, hogy a hitelesítés **a munkaállomáson is** megtörténjen.

- Az érzékeny, vagy bizalmas tartalmú üzeneteknél **kriptográfiai titkosítást** és/vagy **hitelesítési eljárást** (pl. digitális aláírás) kell alkalmazni, melyek használatára a felhasználókat megfelelően ki kell képezni.

- Meg kell határozni a felhasználók felelősségét és jogosultságát az egyetemi **szervezeti egység nevében elküldhető üzenetek** tekintetében.

- A felhasználókkal írásban tudomásul kell vetetni, hogy az egyetemi **szervezeti egység** nevében jogosulatlanul feladott, esetleg rágalmazó, vagy lejárató tartalmú üzenetek **szankciókat,** súlyosabb esetben polgári, vagy büntetőjogi **pereket** vonhatnak maguk után.

9. Hozzáférés ellenőrzése

9.1 Hozzáférés-ellenőrzés követelményei

Célkitűzés: Az információhoz hozzáférést ellenőrizni kell.

Az információhoz, és az üzleti folyamatokhoz a hozzáférést az **üzleti és biztonsági követelmények alapján** kell ellenőrizni. A hozzáférés-ellenőrzés vegye figyelembe az információterjesztés és a felhatalmazás szabályzatait.
MSZ ISO/IEC 17799:2002

Valamennyi szervezeti egységre, felhasználócsoportra és szükség szerint egyedi felhasználóra vonatkozóan meg kell határozni a **rendszerszintű hozzáférés-ellenőrzési szabályokat** a jelen stratégiában/szabályzatban meghatározott keretek alapján. A szabályok kidolgozása a rendszerszintű biztonsági felelősök feladata.

9.1.1 A hozzáférés ellenőrzés szabályozása

Alapvető szempontok a szabályok meghatározásához:
- az információ besorolási szintje, minősítése,
- információ védelmére vonatkozó törvények és szerződésekben vállalt kötelezettségek,
- az alkalmazások biztonsági követelményei,
- közös munkaterületek, tevékenységek felhasználói hozzáférési igényei,
- az informatikai és kommunikációs infrastruktúra lehetőségei a hozzáférések ellenőrzésére, naplózására,
- az idevágó belső szabályozások.

A szabályokat a következő **irányelvek szerint** kell kialakítani:
- a legszigorúbb **korlátozásokat** kell kialakítani, melyek azért a megfelelő munkavégzést már lehetővé teszik (lásd: a szükséges minimális jogosultság elve),
- alapértelmezés: **minden hozzáférés tiltott**, csak a szükséges szolgáltatások használata engedélyezett,
- ha ez lehetséges, gondoskodni kell a szabályok és óvintézkedések **kikényszerítéséről** (pl. az operációs rendszer beállításaival),
- **minimalizálni** kell az opcionális szabályokat és intézkedéseket, mivel ezek fokozottan magukban hordozzák a mulasztások és visszaélések lehetőségét.

9.2 A felhasználói hozzáférés menedzselése

Célkitűzés: Megvédeni az informatikai rendszereket a jogosulatlan hozzáféréstől.

Hivatalos eljárásokat kell érvényesíteni az informatikai rendszerekhez és szolgáltatókhoz a hozzáférési jogoknak a kiosztására.

A felhasználói hozzáférés minden részét eljárásokkal kell lefedni, az új felhasználók első nyilvántartásba vételétől a felhasználónak a végső törléséig. Gyakoroljunk ellenőrzést az olyan kiváltságos hozzáférési jogok felett, amelyek lehetővé teszik, hogy a felhasználó a rendszervezérlést hatástalanítsa.
MSZ ISO/IEC 17799:2002

9.2.1 A felhasználók nyilvántartásba vétele, jogosítása

A felhasználók nyilvántartásba vétele, jogosultságaik kiosztása, rendszeres felülvizsgálata, illetve megszüntetése **biztonsági szempontból kritikus** fontosságú, ezért a rendszerszintű szabályozásokban **részletesen rögzíteni** kell az ezekkel kapcsolatos **tevékenységeket**, **felelősségeket**:

- **Szükséges minimális jogosultság** alapelve szerint az alkalmazásgazdáknak és a rendszerbiztonsági felelősöknek meg kell határozniuk **a feladatok elvégzéséhez** szükséges jogosultságokat. Ellenőrizni kell, hogy a meghatározott jogosultságok valóban alkalmasak az elvárt munkafeladatok elvégzésére, illetve nem ellentmondóak egyéb üzemeltetési szabályzatokkal (pl. feladatszétosztás).

- Olyan felhasználó-azonosítókat kell kiosztani, melyekkel a **felhasználó** kiléte könnyen és egyértelműen **azonosítható**, ezáltal a feladatok hozzárendelése és számonkérése áttekinthető.

- **Csoportos felhasználói azonosítók** (olyan azonosítók, melyeket több személy is használhat) használatát csak ott szabad alkalmazni, ahol ez a feladat elvégzéséhez feltétlenül szükséges, vagy a rendszer nem teszi lehetővé a felhasználók és jogosultságaik elkülönítését. Ezen azonosítók használatát az **IBV-nek engedélyeznie** kell.

- A felhasználók mindaddig nem kaphatják meg a felhasználó-azonosítójukat és jogosultságaikat, amíg azok egyértelmű meghatározása, dokumentálása és engedélyezése meg nem történt. Az engedélyezési folyamat során **minden lépést írásban** kell rögzíteni, majd azokat az engedélyező aláírásával hitelesíteni.

- **Kerülni kell az ideiglenes**, vagy „vendég” **azonosítók használatát**. Amennyiben a jogosultságokban sürgős módosítás szükséges, ki kell jelölni az engedélyezésre jogosult és az adott területet jól ismerő személyt, aki **indokolt esetben** (pl. helyettesítés) utasíthatja a jogosultságok állítását végrehajtó munkatársat a megfelelő jogosultságok beállítására. Az ilyen eseményekről jegyzőkönyvet kell készíteni, melyet a normális engedélyezési folyamatban résztvevőknek felül kell vizsgálniuk. A jegyzőkönyvet az **IBV** őrzi. Az ilyen azonosítókat azonnal vissza kell vonni, amikor azok indokoltsága megszűnik.

- A felhasználóknak azonosítójukról, hozzáférési jogaikról és az ezekhez kapcsolódó szabályokról, korlátozásokról **írásos tájékoztatót** kell átadni, melynek tudomásulvételét egy nyilatkozatban aláírásukkal hitelesítik.

- Az alkalmazási **területet elhagyó felhasználók** (pl. kilépés, áthelyezés, szerződéses viszony megszűnése) azonosítóit a jogviszony megszűnésekor a lehető legrövidebb időn belül meg kell szüntetni.

- Lehetőséget kell biztosítani arra, hogy indokolt esetben a **felhasználói azonosító azonnal visszavonásra** kerülhessen. Ennek elrendeléséről a munkahelyi vezető rendelkezik.

- **Naprakész nyilvántartást** kell vezetni a kiadott felhasználó-azonosítókról és az azokhoz rendelt jogosultságokról. Minden, a **felhasználó-azonosítókat érintő tevékenységről** (létrehozás, a jogosultságok változtatásai, illetve a megszüntetés) a rendszerszintű szabályozásokban foglaltaknak megfelelően **naplót** kell vezetni, a napló aktualitásáért a felelősséget is a rendszerszintű szabályzatokban kell meghatározni. Dokumentált és a tényleges helyzet azonosságát meghatározott időközönként a rendszerbiztonsági felelősöknek ellenőrizniük kell.

9.2.2 A központilag üzemeltett rendszerek jogosultságkezelése

Központilag üzemeltetett rendszerek jogosultságkezelésével kapcsolatosan az alábbi alapelvek érvényesek:

- A Humánerőforrás-Gazdálkodási Igazgatóság felelőssége, hogy az alkalmazások jogosultságkezelése kapcsán szükséges dolgozói törzs naprakész legyen.
- A jogosultság-nyilvántartás központilag történik, a jogosultságok és szerepkörök nyilvántartásáért és naprakészségének biztosításáért az Informatikai Igazgatóság felel.
- A jogosultságok állítását az Informatikai Igazgatóság végzi, a meghatározott jóváhagyások után.

9.2.3 A kiváltságok menedzselése

Kiváltságos felhasználóknak a rendszer üzemeltetéséhez, illetve különböző kritikus rendszer-, és alkalmazási feladatok elvégzéséhez szükséges jogosultságokkal felruházott felhasználók (pl. rendszergazdák) minősülnek.

Mivel ezek a feladatkörök az átlagos felhasználóknál szélesebb körű jogosultságokat (kiváltságokat) igényelnek, ezért a kezelésük során a következőket fontos figyelembe venni:

- Pontosan **meg kell határozni** a különböző feladatok elvégzéséhez, illetve a rendszer-felügyeleti eszközök üzemeltetéséhez **szükséges kiváltságokat**. Itt is a szükséges minimális jogosultság alapelvét kell szem előtt tartani.

- A magasabb vezetői pozíciók nem feltétlenül igényelnek kiváltságos felhasználói jogokat.

- A kiváltságokat, lehetőség szerint ne a felhasználó általánosan használt azonosítójához rendeljük hozzá, hanem ehhez másik felhasználói azonosítót hozzunk létre, így a felhasználó csak akkor használja a kiváltságos azonosítót, amikor ez a munkájához szükséges.

- Különösen veszélyes, és probléma esetén nehezen ellenőrizhető, ha bizonyos kulcsfontosságú azonosítók (pl. a beépített adminisztratív azonosítók) jelszavait több személy ismeri. Az ilyen azonosítók osztott használatát lehetőség szerint feltétlenül kerülni kell.

9.2.4 A jelszavak kezelése

Az Egyetem egészére **szigorú jelszókezelési szabályokat** kell meghatározni, a következő elvek alkalmazásával:

- **Felhasználó-azonosítók létrehozásakor** egy ideiglenes, véletlenszerűen generált jelszót kell megadni, és a felhasználót írásban és/vagy a megfelelő rendszerbeállítások segítségével arra kötelezni, hogy az első bejelentkezés alkalmával változtassa meg. Amennyiben az adott rendszer lehetővé teszi, az ideiglenes jelszó érvényességének lejártát is minimális időtartamra kell beállítani. Ideiglenes jelszót lehetőleg biztonságos módszerrel, biztonságos helyen kell átadni a felhasználónak, (pl. lepecsételt, zárt boríték) hogy harmadik személy ahhoz ne férhessen hozzá.

- Meg kell határozni a **jelszavak komplexitásának** követelményeit. Ajánlott: minimum 6 karakter, kis- és nagybetűk, számok vegyesen. Amennyiben lehetséges, megfelelő rendszerbeállításokkal gondoskodni kell ennek betartásáról.

- Gondoskodni kell a felhasználói jelszavak **rendszeres karbantartásáról**. Ahol a rendszer lehetővé teszi, ott be kell állítani a meghatározott időszakonként **kötelező jelszóváltást**. Célszerű 30-60 napos, de maximum 6 hónapos időszakot meghatározni.

- **A felhasználókkal** nyilatkozatban, aláírásukkal hitelesítve **tudomásul kell vétetni**, hogy jelszavaikat titokban tartják, más részére ki nem adják.

- **A jelszavakat tilos** a számítógépeken titkosítás nélkül, vagy egyéb módon védtelen formában tárolni (pl. egy füzetben). Amennyiben ez szükséges, (pl. vészhelyzet) a különleges azonosítók jelszavait egy titkosított adatbázisban, vagy fizikailag védett helyen (pl. páncélszekrényben, lepecsételt borítékban) kell tárolni.

- Ha felhasználó elfelejtette jelszavát, akkor azt az új felhasználók létrehozásának szabályaival megegyezően egy ideiglenes jelszóval kell helyettesíteni, majd a fentiekben ismertetett eljárások szerint gondoskodni annak rövid időn belüli megváltoztatásáról.

9.2.5 A hozzáférési jogok felülvizsgálata

A hozzáférési jogosultságokat (adatokhoz és informatikai rendszerekhez) rendszeresen ellenőrizni és felül kell vizsgálni. Az ellenőrzés során a rendelkezésre álló dokumentumok (jogosultság-nyilvántartás, változási naplók, stb.) mellett meg kell vizsgálni az üzemeltetett rendszerek sajátosságait, igényeit, illetve ezek változásait.

A felhasználók hozzáférési jogosultságait bizonyos időközönként, illetve a rendszert érintő jelentősebb változásokat követően felül kell vizsgálni.

Ilyen jelentős változásnak minősülnek az alábbiak:
- új kiszolgálók, szolgáltatások üzembe helyezése,
- új alkalmazások bevezetése,
- az alkalmazások verzióváltása,
- alkalmazások, adatok áthelyezése más kiszolgálóra, vagy tárterületre,
- kiszolgálók, illetve szolgáltatások megszüntetése,
- alkalmazások, illetve adatok használatának megszüntetése,
- szervezeti változások.

Kiváltságos jogosultságokra szóló felhatalmazásokat, és azok kiosztását rövid időközönként kell ellenőrizni és felülvizsgálni. Amennyiben a vizsgálat mulasztást, vagy hibát tár fel, azt **biztonsági eseménynek** kell minősíteni, és az ennek megfelelő intézkedéseket kell végrehajtani.

9.3 A felhasználó felelőssége

Célkitűzés: Megakadályozni illetéktelen felhasználó hozzáférését.

A biztonság megteremtésének lényeges eleme a jogosult használók együttműködése. Felhasználókban tudatosítani kell saját felelősségüket a hatékony hozzáférés-ellenőrzés fenntartásában, különösen a jelszóhasználatban és a használói berendezések biztonságában.
MSZ ISO/IEC 17799:2002

9.3.1 A jelszó-használat

Felhasználókat tájékoztatni kell a jelszavak használatával kapcsolatos kockázatokra:
- A jelszavakat **titokban** kell tartani, azokat más személynek kiadni **tilos**.
- Lehetőség szerint kerülni kell a jelszavak papírra rögzítését, azokat minél előbb memorizálni kell.
- A felhasználókat a jelszavak önálló **megváltoztatására** oktatni kell, és arra is, hogy minden esetben cseréljék le a jelszavukat, ha bármi jel utalna arra, hogy a jelenlegi jelszó nem biztonságos, pl. ha valaki megfigyelhette a billentyűzeten a jelszó begépelését.
- A felhasználókat figyelmeztetni kell a **„kitalálható jelszavak”** veszélyeire és azok használatnak kerülésére.
- Ha a rendszerben nincs rendszeres **jelszóváltoztatás** kikényszerítve, vagy ahol erre nincs lehetőség, akkor is célszerű bizonyos rendszerességgel a jelszavakat megváltoztatni.
- Törekedni kell a **komplex, „minőségi” jelszavak** használatára akkor is, ha a rendszerben erre bármilyen okból nincs szabályozás.

- Biztonsági szempontból különösen veszélyes és kerülendő az **automatikus bejelentkezési folyamatok**, szolgáltatások használata. Bizonyos operációs rendszerekben és alkalmazásokban lehetőség van a **beírt jelszavak** tárolására, majd ennek alapján a következő bejelentkezések alkalmával a felhasználó automatikus beléptetésére. Ezek használatát rendszergazdai eszközökkel **meg kell akadályozni**, amennyiben ez technikailag lehetséges.

9.3.2 Felügyelet nélküli felhasználói eszközök

Felügyelet nélkül hagyott felhasználói berendezések (munkaállomások, hordozható számítógépek stb.) kellő védelme hiányában illetéktelenek férhetnek hozzá az azokon tárolt adatokhoz, súlyosabb esetben az informatikai rendszer további részeihez.

Ezek megelőzése érdekében a **következő óvintézkedéseket** kell megvalósítani:

- A felhasználóknak munkájuk végeztével a hálózati szolgáltatásokból, illetve munkaállomásokból **ki kell jelentkezniük**.
- Amennyiben a munkaállomásokon végzett munkafolyamatok nem követelik meg a folyamatos üzemelést, a munkaállomásokat a munka végeztével **ki kell kapcsolni**.
- Ha a felhasználó munkahelyét, munkaállomását munkaidőben hosszabb időre elhagyja, gondoskodnia kell a munkaállomás manuális, vagy automatikus **védelméről**.
- A rendszerbiztonsági felelős javaslata alapján a rendszergazdáknak gondoskodniuk kell **a fentiek kikényszerítéséről** (pl. automatikus kiléptetés, bizonyos időtartalmú inaktivitás után).
- **A hordozható számítógépeken** lehetőség szerint csak a munkavégzéshez szükséges minimális adatokat szabad tárolni, mivel ezek sokkal inkább ki vannak téve az illetéktelen hozzáférés veszélyeinek. Amennyiben lehetséges, érdemes további védelmekkel (chip-kártyás azonosítás, titkosított fájlrendszer, stb.) ellátni ezeket.
- A munkaállomásokat, hordozható számítógépeket amennyiben nincsenek használatban, megfelelő **fizikai védelemmel** kell ellátni a jogosulatlan hozzáférések megakadályozása érdekében (pl. kulccsal lezárás, vagy biztonságos helyen tárolás).

9.4 Hozzáférés a hálózathoz

Célkitűzés: A hálózatra telepített szolgáltatások védelme

Ellenőrizni kell mind a belső, mind a külső hálózatra telepített szolgáltatásokat. Erre azért van szükség, hogy szavatolhassuk, azok a használók, akiknek hozzáférésük van a hálózatokhoz és a hálózati szolgáltatásokhoz, ne veszélyeztethessék ezeket a hálózati szolgáltatásokat.
Ezt elérhetjük:

- az adott szervezet hálózata és bármely más szervezet hálózata közé, valamint a nyilvános hálózatok közé egy alkalmas interfész telepítésével,
- felhasználókhoz és a berendezésekhez hitelesítő mechanizmus alkalmazásával,
- az informatikai szolgáltatások használói hozzáféréseinek ellenőrzésével.

MSZ ISO/IEC 17799:2002

A hálózati biztonság kidolgozását, a szabályzatban foglaltak szerinti működtetését és az abban meghatározott policy-k betartatását az **Informatikai Igazgatóság** végzi.

Az egyetemi hálózat részletes biztonsági szabályait az SE Informatikai Hálózati Szabályzata (**SE-IHSZ**) tartalmazza, melyből egy-két lényeges elvet a következőkben ismertetünk:

- A hálózati szolgáltatásokra vonatkozó szabályok kialakításakor is elsősorban a **szükséges minimális jogosultság** alapelvét kell szem előtt tartani.

- A felhasználó munkaállomásáról **elérhető hálózati szolgáltatásokat** pontosan meg kell határozni, és csak ezek elérését szabad lehetővé tenni.

- A hálózatok terhelésének optimális elosztása, illetve a hálózati adatbiztonság növelése érdekében minden lehetséges hálózati szolgáltatás eléréséhez a **lehetséges útvonalak korlátozása** – ily módon ún. kényszerpályák kialakítása – szükséges.

- **Csak kapcsolt** (switch) **rendszerű aktív eszközökkel** szabad a végpontok (pl. kiszolgálók és felhasználók) kommunikációját megvalósítani, így megakadályozható illetéktelenek a kommunikáció „lehallgatása" és analizálása.

- A szervezeten belüli szolgáltatások és felhasználói csoportok kezelésére – amennyiben a fizikai elhelyezkedés és a hálózat kialakítása lehetővé teszi – **különálló logikai tartományokat** (subnetek) kell létrehozni. Indokolt esetben a tartományok közötti adatforgalmat csak szükséges hitelesítések után, **biztonsági átjárók** közbeiktatásával kell megvalósítani.

- A forgalomirányítókat (ROUTER-ek) úgy kell beállítani, hogy **a felhasználók** a hálózatnak csak a kiszolgáló, illetve egyéb szolgáltatás használatához **szükséges szegmenseit, tartományait, végpontjait** érhessék el. Ezzel megakadályozható a hálózaton belüli „barangolás", esetleg jogosulatlan hozzáférés adatokhoz és szolgáltatásokhoz.

- Gondoskodni kell arról, hogy külső hálózati szolgáltatásokat a felhasználók csak **szükséges hitelesítések után, biztonsági átjárókon keresztül** érhessenek el (pl. az internet elérés csak proxy-autentikáció után, tűzfalon keresztül, opcionálisan tartalomszűrés és vírusellenőrzés közbeiktatásával legyen lehetséges.).

- **A külső hálózati használóknak** – a megfelelő hitelesítési folyamatok és biztonsági átjárók mellett – fokozott figyelemmel kell a **legszigorúbb kényszerpályákat** kijelölni és ellenőrizni, így jelentősen lassítható, vagy bizonyos mértékben megakadályozható a bejutó rosszindulatú programok hálózaton belüli elterjedése. **Külső összeköttetésnek** minősül, ha a felhasználó az egyetemi hálózathoz, annak infrastruktúráján és fizikai **határain kívül eső helyről** kapcsolódik, valamilyen ideiglenes kapcsolat (pl. modemes-betárcsázás) segítségével. A külső összeköttetések **fokozott biztonsági kockázatokat** és veszélyforrásokat jelentenek, ezért kialakításuk és használatuk során **maximális körültekintéssel** kell eljárni.

- **Távoli hozzáférés csak biztonságos hitelesítés útján** jöhet létre. A hagyományos jelszóvédelem helyett ajánlatos valamilyen **magasabb biztonsági fokozatú rendszer** (pl. SecurId token, SmartCard) alkalmazása.

- A kommunikáció – különösen, ha az valamilyen publikus csatornán keresztül (pl. internet) történik – **védett csatornán** valósuljon meg.

- A rosszindulatú programok bejutásának megakadályozása céljából **vírusvédelmet és tartalomszűrést** kell alkalmazni.

- **A külső összeköttetésekkel kapcsolatos tevékenységeket** (be- és kijelentkezés, sikertelen próbálkozások, egyéb rendkívüli események) lehetőség szerint **naplózni** kell. Amennyiben a hitelesítést végző rendszer arra lehetőséget nyújt, be kell állítani, hogy bizonyos számú sikertelen próbálkozás után riasztást küldjön a rendszergazdáknak, illetve a felhasználói azonosítót – ezzel egyidejűleg – tiltsa le.

- A rendszerbiztonsági felelősöknek rendszeresen (legalább félévente**) felül kell vizsgálniuk** a meglévő külső kapcsolatok által jelentett **kockázatokat**, esetleges biztonsági hiányosságokat, ezek ismeretében kezdeményezniük kell a szükséges módosításokat.

- A felhasználók – különösen az Egyetem határain túlmutató – kommunikációs lehetőségeinek kialakításakor az **elérhető végpontokat és szolgáltatásokat** megfelelő módon **korlátozni** kell a következő szempontok figyelembe vételével:
  - adatforgalom optimalizálása, túlterhelések csökkentése, megakadályozása.
  - rosszindulatú programok bejutásának megakadályozása.
  - az Egyetem működési szabályzatának keretében nem megengedett programok, információk bejutásának megakadályozása.
  - ellenőrizetlen levelezés, illetékteleneknek adattovábbítás megakadályozása.

  Ennek érdekében a **következő intézkedéseket** célszerű foganatosítani:
  - **adatok letöltésének korlátozása** (pl. programfájlok, tömörített állományok letöltésének megakadályozása),
  - a **kimenő adattovábbítás korlátozása** oly módon, hogy arra csak az engedélyezett végpontok felé, a vonatkozó szabályok szerint kialakított csatornákon keresztül legyen lehetőség,
  - közismerten illegális tartalmat szolgáltató **helyek elérésének megakadályozása**,
  - az Egyetem működésével és profiljával nem összeegyeztethető tartalmú szolgáltatások és **szolgáltatók elérésének megakadályozása** (pl. fájlcserélő programok, pornográf weboldalak),
  - az Egyetem levelezőrendszerén **kívüli levelezés** megakadályozása.

9.5 Hozzáférés-ellenőrzés az operációs rendszerekben

Célkitűzés: Megakadályozni az illetéktelen hozzáférést a számítógéphez.

Operációs rendszer szintjén elérhető biztonsági eszközöket arra kell használni, hogy korlátozzuk a hozzáférést a számítógépi erőforrásokhoz.

Ezek az eszközök a következő képességekkel rendelkezzenek:
- jogosult használók azonosságának, és szükség esetén termináljának vagy telephelyének az azonosítására és igazolására,
- sikeres és sikertelen rendszer-hozzáférések rögzítésére,
- hitelesítés alkalmas eszközzel, ha jelszógondozó rendszert alkalmaznak, akkor ezt szavatolja ennek ellátását minőségi jelszavakkal,
- ahol alkalmazható, a használók összeköttetési tartásidőnek korlátozására.

Egyéb hozzáférés-ellenőrző módszerek, mint a kérdés-válasz, rendelkezésre állnak olyan esetekre, amelyekben ezt üzleti kockázatra alapozva igazolni lehet.
MSZ ISO/IEC 17799:2002

Bizonyos esetekben (pl. hordozható gépek használatakor) szükséges lehet, hogy a hozzáférés hitelességének ellenőrzése érdekében ne csak a felhasználót, hanem a csatlakozó számítógépet is egyértelműen azonosítani lehessen. Ehhez szoftver és hardver alapú megoldások egyaránt rendelkezésre állnak. Az ilyen azonosítások kiépítésekor gondoskodni kell az azonosítást végző elemek fizikai és logikai védelméről.

A hálózati szolgáltatások mellett **a munkaállomást is védeni kell** a jogosulatlan hozzáférésektől, ezek védelmét a következő szempontok figyelembevételével kell kialakítani:
- A **bejelentkezés előtt** a munkaállomás lehetőleg jelenítsen meg egy figyelmeztető üzenetet, hogy a rendszert csak az arra feljogosított személyek használhatják, a jogosulatlan, illegális hozzáférés eljárást von maga után.
- **A beléptető eljárá**s előtt és alatt a rendszer csak annyi információt jeleníthet meg, amennyi a bejelentkezés lebonyolításához feltétlen szükséges. Kerülni kell a rendszer vagy munkaállomás azonosítójának, illetve az alkalmazás verziójának kijelzését.
- **A bejelentkezési eljárás** alatt csak minimális hiba- és egyéb rendszerüzeneteket szabad kijelezni, hogy a rendszer vagy alkalmazás ezzel ne segíthesse az illetéktelen hozzáférést.
- **A rendszer** ne jelenítse meg a begépelt jelszót és úgy kell beállítani, hogy a képernyőn megjelenő „maszk karakterek” száma ne egyezzen meg a beírt karakterekkel.
- **Hibás bejelentkezés esetén** a rendszer csak a hiba tényét közölje, ne részletezze, hogy az azonosítás mely komponense volt hibás. **Korlátozza** a bejelentkezési kísérletek számát, bizonyos számú sikertelen kísérlet után **tiltsa le** a hozzáférést, illetve a felhasználó azonosítóját úgy, hogy azt csak a rendszergazda tudja feloldani. Ez biztonsági eseménynek számít, amiről a rendszerbiztonsági felelősöket értesíteni kell.
- A bejelentkezést **időkorláttal** kell ellátni, illetve a sikertelen bejelentkezési kísérletek között néhány másodperc várakozási időt kell beiktatni.

- A sikertelen bejelentkezési kísérleteket **rögzíteni kell**, ha lehetséges, a bejelentkezéshez használt azonosítót, illetve jelszót is. A nagyszámú, rendszeresen előforduló sikertelen bejelentkezési kísérletek okait ki kell vizsgálni.

9.6 Mobil számítástechnika és távmunka

Célkitűzés: Gondoskodni az informatikai biztonságról a mobil számítástechnikai és a távmunkát végző eszközök használata esetén.

A megkívánt biztonság legyen összemérhető azzal a kockázattal, amelyet az ilyen munkavégzési mód hordoz. Amikor mobil számítástechnikát alkalmazunk, meg kell fontolni a védetlen környezetben elvégzett munka kockázatát és a megfelelő védelem használatát. Távmunka végzése esetében a szervezet védelmet fog alkalmazni a távmunka-végzés helyszínén és gondoskodni arról is, hogy az ilyen munkavégzésnek megfelelő legyen az alkalmazott elrendezés.
MSZ ISO/IEC 17799:2002

9.6.1 Mobil számítástechnika

A mobil számítástechnikai eszközök (notebook számítógépek, palmtopok, mobiltelefonok) fokozottan ki vannak téve az illetéktelen hozzáférés veszélyének, ezért ezek alkalmazásakor szigorú biztonsági követelményeket és szabályokat kell meghatározni:

- Mobil eszközökön **csak olyan programok** használhatók, melyeket az alkalmazásgazdák és a rendszerbiztonsági felelősök előzőleg megvizsgáltak, minősítettek és engedélyeztek.
- Csak olyan mobil eszközöket szabad használni, melyek bekapcsoláskor **hardver szintű** lehetőséget biztosítanak a felhasználó **jogosultságának ellenőrzésére**. (pl. notebook gépeknél „Power-On password”.)
- A hordozható számítógépeken amennyiben lehetőség van a merevlemez tartalmának **hardver szintű jelszóvédelmére**, a rendszergazdáknak be kell kapcsolni, ha erre nincs lehetőség, vagy az adatok minősítése ezt szükségessé teszi, egyéb **titkosítási eljárással** is kell az adatokat védeni.
- Gondoskodni kell a hordozható eszközök megfelelő szintű **vírusvédelméről**. A hordozható eszközöket kiadó és felügyelő rendszergazdáknak rendszeresen ellenőrizniük kell, hogy a vírusvédelem adatállományának frissítése rendben megtörtént-e, és erre a felhasználót is figyelmeztetni kell.
- Amennyiben az eszköz, illetve rendszerszoftvere lehetővé teszi, megfelelően **szabályozni** kell **a hálózatra csatlakozás** lehetőségeit, különös tekintettel a szervezeten kívüli, vagy nyilvános hálózatokhoz kapcsolódás lehetőségeire.
- A hordozható eszközök hálózati kapcsolatait megfelelő módon (rendszergazdai beállítások, tűzfal telepítése stb.) **védeni** kell az illetéktelen hozzáférésekkel, és behatolási kísérletekkel szemben.
- Gondoskodni kell a hordozható eszközök megfelelő **fizikai védelméről** (pl. zárható táska, lopásvédelmi biztonsági zár, zárható szekrény).

- Biztosítani kell a mobil **eszközök mentésének lehetőségét**. Bár az eszközök jellege miatt a rendszeres napi mentés általában nem megoldható, ajánlatos legalább havonta, minimálisan a rendszerkörnyezet mentése.
- A felhasználókat fel kell készíteni a mobil eszközök használatának szabályaira és kockázataira.

Minden felhasználóval írásban, aláírásával hitelesítve **tudomásul kell vetetni** a következőket.

- Mobil eszközöket munka végeztével nem lehet őrizetlenül hagyni, azokat megfelelően el kell zárni.
- Eszközök konfigurálása, bármilyen – különösen kommunikáció – jellegű beállítása, azokra szoftverek telepítése csak a rendszergazda által, vagy az ő tudtával és irányításával lehetséges.
- Mobil eszközökön csak a munkavégzéshez szükséges minimális mennyiségű adat tárolható. A teljesítmény optimalizálása és az adatbiztonság érdekében kerülni kell az adatok szükségtelen felhalmozását.
- Mobil eszközökön létrehozott, vagy módosított adatokat amilyen hamar csak lehetséges, valamilyen biztonságos környezetbe (pl. az Egyetem belső informatikai rendszerébe) át kell helyezni, ahol védettek az illetéktelen hozzáférésekkel szemben, illetve rendszeres mentésük megoldott.
- Fel kell hívni a felhasználók figyelmét a mobil eszközök nyilvános helyen a használatának veszélyeire és az ilyen esetekben alkalmazandó eljárásokra (pl. illetéktelenek általi betekintés, hálózati behatolás, lopás).

9.6.2 Távmunka

A távmunka végzés lehetőségét csak az illetékes munkahelyi vezető engedélyezheti. Ennek körülményei csak a rendszerbiztonsági felelősök által meghatározott, illetve az üzemeltetés-vezető által jóváhagyott eljárások szerint alakíthatók ki.

A távmunka biztonsági szabályok kidolgozásáért, a szabályzatban foglaltak szerinti működtetéséért, a szükséges VPN-ek létrehozásáért, valamint az abban meghatározott policy-k betartatásáért az **Informatikai Igazgatóság a felelős**.

Az egyetemi hálózat a távmunkával kapcsolatos biztonsági szabályait részletesen az SE Informatikai Hálózati Szabályzata (**SE-IHSZ**) tartalmazza.

10. Rendszerfejlesztések és azok karbantartása

10.1 Rendszerek biztonsági követelményei

Célkitűzés: Gondoskodni, hogy a **biztonságot építsük be az informatikai rendszerekbe**.

Ebbe beleértjük az infrastruktúrát, az üzleti alkalmazásokat, valamint a felhasználók által kifejlesztett alkalmazásokat. A biztonság szempontjából az alkalmazást, illetve a szolgáltatást támogató üzleti és informatikai folyamat tervezése és megvalósítása egyaránt kritikus lehet. A biztonsági követelményeket már az informatikai rendszerek kifejlesztését megelőzően azonosítani és egyeztetni kell. Minden biztonsági követelményt, a szükséges elrendezéseket is beleértve, már a projekt követelményeinek a felállítása során az informatikai rendszer általános **üzleti terv részeként** kell azonosítani, igazolni, egyeztetni és dokumentálni.
MSZ ISO/IEC 17799:2002

A biztonsági követelményeknek már **a tervezési fázisban** meg kell jelenniük. Az új rendszerek rendszerbeállítása, illetve meglevő rendszerek bővítése esetén a fejlesztési tervnek tartalmaznia kell a kapcsolódó biztonsági követelményeket is. Feltétlenül szükséges, hogy a biztonsági követelmények meg legyenek határozva már a fejlesztést megelőzően valamennyi informatikai rendszerhez kapcsolódó összetevő esetén (infrastruktúra, alkalmazások, informatikai fejlesztések stb.).

A **fejlesztési projektek során** a biztonsági követelményeket érvényesíteni kell. A projekt alapító okiratokban a projekt célja mellett rögzíteni kell a **mérvadó biztonsági követelményeket is**. Hasonlóképpen rögzíteni kell minden létrehozandó, fejlesztendő, átalakítandó informatikai rendszer fizikai, logikai és adminisztratív védelmi rendszerének **tervezési és megvalósítási lépéseit, költségeit és felelőseit**.

Minden informatikai rendszerhez kapcsolódó **beruházás előkészítő fázisában** ki kell dolgozni és dokumentálni szükséges a következőket:

- Az informatikai rendszer **védelmi céljainak** meghatározása, a kezelendő adatok elemzése (információvédelem és a megbízható működés szempontjából),
- Az informatikai rendszer informatikai **biztonsági osztályba sorolása**.
- A fizikai és logikai **védelem** rendszerszintű leírása és a szükséges feltételrendszer meghatározása.
- A megvalósítandó biztonsági rendszer **becsült költségének** összevetése a **lehetséges károkkal**.
- A projektek költségvetésében szerepeltetni kell a biztonsági rendszer tervezési és megvalósítási **költségeit** is.
- A jogszabályokból és a belső szabályozásokból származó **kötelezettségek**.

Fentiekben megfogalmazott feltételek nem teljesítése esetén a projekt nem indítható el.

Minden jelentősebb informatikai fejlesztéssel járó projekt során kötelező az **IBV bevonása** a projektbe. Az informatikai biztonsági követelmények betartásáért a **projektvezető felelős**.

10.2 Az alkalmazói rendszerek biztonsága

Célkitűzés: Megvédeni az alkalmazói rendszerekben lévő felhasználói adatokat az elvesztéstől, azok módosulásától, illetve a visszaéléstől.

Az alkalmazói rendszerekbe - beleértve a használó által írt alkalmazásokat is - **be kell tervezni a megfelelő óvintézkedéseket**, az ellenőrzést és a tevékenységek naplózását, valamint magukba foglalják a bemenő, a folyamatközi és kimenő adat ellenőrzését is.
MSZ ISO/IEC 17799:2002

Az alkalmazói rendszerek biztonsága kiterjed a rendszerekben tárolt **adatok** illetéktelen hozzáférésére, módosítására, törlésére, illetve a nem megfelelő felhasználásának megelőzésére. A rendszertervek készítése során meg kell fontolni a rendszerbe beépítendő automatikus **ellenőrző eszközök**, valamint a biztonságot támogató manuális ellenőrző eszközök szükségességét.

Bizalmas adatok kezelését végző rendszerek esetén **kockázatelemzést** kell végezni, és ezt felhasználva kell meghatározni, hogy van-e szükség további ellenőrző eszközökre. A lépéseket és eredményeket részletesen dokumentálni kell.

A felhasználói rendszerekben meg kell tervezni, és dokumentálni kell a megfelelő **ellenőrző eszközöket** és eseménynaplókat, valamint a tevékenységek naplózását. Ezeknek tartalmazniuk kell a bemenő adatokra, a belső adatfeldolgozásra, az üzenetek hitelesítésére valamint a kimenő adatokra vonatkozó kontrollokat:

Bemenő adatok ellenőrzése

- ismételt adatbevitel és az ebből származó adat-karbantartási anomáliák elkerülésére írt eljárások,
- időszakos adatmező és adatállomány-vizsgálat, valamint a felvitt adatok hitelességének és integritásának ellenőrzése és igazolása,
- az adatbevitel alapját képező nyomtatott input dokumentumok ellenőrzése, illetve ezek engedély nélküli módosításának megakadályozása,
- az adathitelesítési hibák kiküszöbölését elősegítő eljárások,
- az adatbevitel során, a mezőtípus kompatibilitást biztosító, illetve adattartalom helyességét ellenőrző és kikényszerítő eljárások,
- az alkalmazási hozzáférések naplózása,
- a feldolgozásban részt vevő munkatársak feladatkörének és felelősségének rögzítése a munkaköri leírásokban.

Az adatfeldolgozás ellenőrzése (pl. szoftver meghibásodások kezelése):

- az adatfeldolgozás rendszerébe **ellenőrzési, hitelesítési pontok** beépítése, különös tekintettel az adatmódosító-, törlő funkciók helyére,

- az **adatfeldolgozási hibák** esetére vonatkozó hibadetektáló, és a további rendszerfutást leállító eljárások beépítése a rendszerbe,
- **korrekciós programok** alkalmazása a feldolgozás során felmerülő hibák korrigálására,
- a folyamatba épített ellenőrzés ellátásáért **felelős** személy megjelölése,
- az üzenetek hitelesítése (pl. kriptográfiai módszerek),
- az azonosítás és hitelesítés keretében a **hozzáférést jelszavakkal** kell ellenőrizni, a jelszavak kezelésére a vonatkozó fejezetben részletezett általános szabályokat kell alkalmazni,
- **a hitelesítést** a felhasználó és a rendszer között egy, a felhasználó kezdeményezésére létrehozott **védett csatornán** keresztül kell biztosítani,
- a kimenő adatok ellenőrzése.

Kimenő adatok biztonsága érdekében a következő védelmi eljárásokat kell alkalmazni:
- az adatok integritásának ellenőrzése (cél: hiánytalan, teljes adatok),
- az adattartalom meglétének, értékének ellenőrzése,
- a megfelelő minősítés meglétének ellenőrzése,
- a kimenő adatok értékelésében és hitelesítésében részt vevő munkatársak feladatainak és felelősségének meghatározása.

10.3 Kriptográfiai óvintézkedések

Célkitűzés: Megvédeni az információ titkosságát, hitelességét és sértetlenségét.

Kriptográfiai rendszereket és technikákat kell alkalmazni mindazon információ védelmére, amelyet kockázatosnak tekintünk, és amelyet más óvintézkedések nem látnak el kellő védelemmel.
MSZ ISO/IEC 17799:2002

Semmelweis Egyetem bizalmas adatainak, illetve olyan adatok esetében, **ahol más védelmi eszközök nem nyújtanak kellő biztonságot**, rejtjelező eszközökkel és technikákkal kell gondoskodni a védelemről. **Kriptográfiai eszközöket** kell használni minden olyan esetben, amikor az adatokat illetéktelen személyek által is hozzáférhető csatornán, illetve helyen kell továbbítani, vagy tárolni, illetve minden olyan esetben, amikor fennáll az adatok kompromittálódásának veszélye. Kriptográfiai eljárásként, vagy eszközként kizárólag a Magyar Köztársaság Információs Hivatala Országos Rejtjelfelügyelet által engedélyezett változat alkalmazható. A rejtjelező algoritmusok kiválasztását, illetve a rejtjelező kulcs hosszúságát **kockázatelemzés alapján** kell meghatározni.

A **rejtjelkulcsok menedzseléséről** (kiadás, megszemélyesítés, visszavonás stb.) jól definiáltan kell gondoskodni. A kulcsmenedzsment konkrét eljárásait és módszereit a megfelelő rendszerszintű informatikai biztonsági szabálytatok tartalmazzák. A rejtjelezés konkrét kialakításakor a feldolgozás első pontjától az utolsóig át kell tekinteni a rendszert, egy-egy elem rejtjelezése önmagában nem elegendő.

Semmelweis Egyetem bármely rendszeréhez nyilvános hálózaton keresztül , kriptográfiai eszközt nem tartalmazó hozzáférés nem megengedett. A **távoli hozzáférés** kizárólag a távmunkához kialakított **VPN-en keresztül** valósulhat meg.

A rendszerszintű informatikai biztonsági szabályzatoknak ki kell térniük az adott rendszerben alkalmazott kriptográfiai alkalmazás konkrétumaira.

Digitális aláírást kell alkalmazni a **külső partnerekkel folytatott adatcsere** eljárások esetén (pl. elektronikus pénzátutalások, megállapodások, szerződéskötések), ahol azonosítani kell a kötelezettségvállalásokat aláíró személyét, illetve bizonyítani kell az aláírt dokumentum integritását. Az elektronikus aláírás kulcsa és a rejtjelező kulcs nem lehet azonos.

A kriptográfiai óvintézkedésekhez kapcsolódóan konkrét felelősségi köröket, felelős személyeket kell kijelölni. A kulcsok kezelését végző személyek fontos és bizalmas munkakört betöltő személynek minősülnek.

A letagadhatatlanság bizonyítására automatikus, a titkosításon és digitális aláíráson alapuló, a felhasználó által nem befolyásolható eszközöket kell kialakítani.

10.4 A rendszerállományok / fájlok biztonsága

Célkitűzés: Gondoskodni kell az IT projekteket és az azokat segítő tevékenységek biztonságos vezetéséről. A rendszerállományokhoz a hozzáférést ellenőrizni kell. A rendszersértetlenség fenntartásának felelősségét a felhasználó, az a funkcionális, vagy fejlesztő csoport viselje, akihez az alkalmazási rendszer, vagy szoftver tartozik.
MSZ ISO/IEC 17799:2002

Bármely rendszer **bevezetése/frissítése** csak megfelelő, pozitív eredménnyel járó **tesztelési eljárások után** történhet meg, a fejlesztési, tesztelési és éles rendszerek nem lehetnek azonosak. A tesztelésnek bizonyítania kell, hogy a változtatás a működőképességgel és a biztonsággal nem ütközik. Amennyiben a tesztelés éles adatbázis alapján történik, úgy biztosítani kell az éles adatbázis olyan módú konvertálását, amely biztosítja, hogy az éles adatok ne legyenek kinyerhetők. Az éles rendszerbe a beillesztés előtt a változtatásokat az alkalmazásokkal együtt kell tesztelni.

A **programok forráskönyvtáraihoz** a hozzáférést korlátozni kell. Amennyiben lehetséges, a forráskódot az operációs rendszer állományaitól **elkülönítetten** kell tárolni. Minden alkalmazáshoz ki kell jelölni egy **felelős személyt**, aki az alkalmazás forráskódjának biztonságáért felel. Az illető alkalmazás forráskódjához kizárólag a felelős személy férhet hozzá. Forrásprogram aktualizálását és programozóknak rendelkezésére bocsátását csak a felelős személy végezheti, az alkalmazásgazda írásos engedélyével. A forrásprogramok minden változását naplózni, a forrásprogramok korábbi verzióit archiválni kell.

Minden telepítés, illetve frissítés előtt **mentést** kell végezni, a szoftverek telepítését, frissítését, illetve törlését naplózni kell.

Szoftvert kizárólag a **rendszergazdák** telepíthetnek a gépekre, illetve megfelelő szerződés esetén csak a garanciát vállaló szolgáltató.

Külső fejlesztők által fejlesztett szoftverek esetén a szerződésnek tartalmaznia kell, hogy maga a szoftver **kinek a tulajdona**. Az egyedileg fejlesztett szoftverek forráskódjai is átadásra kell, hogy kerüljenek. Független harmadik félnél végzett (pl. közjegyző) tárolás is elfogadható.

Az informatikai rendszerek által biztosított **naplózási** lehetőségeket be kell kapcsolni. A naplózás konkrét konfigurálása a rendszerszintű informatikai biztonsági szabályzatok alapján történik. A rendszergazdáknak az operációs rendszer napló bejegyzéseit rendszeresen ellenőrizniük kell, és az ellenőrzés eredményeiről havonta összefoglaló jelentést kell készíteniük.

A **központi erőforrások** (szerverek, tűzfalak) naplóállományaihoz az informatikai biztonságért felelős szervezeti egységnek hozzáférést (pl. távoli elérést) kell biztosítani, olvasási jogosultsággal.

10.5 A fejlesztő és támogató folyamatok biztonsága

Célkitűzés: Fenntartani az alkalmazási rendszerhez tartozó szoftver és információ biztonságát.

Mind a projekt-környezetet, mind a támogató környezetet szigorúan ellenőrizni kell. Ajánlatos, hogy azok a vezetők, akik felelősek az alkalmazási rendszerekért, legyenek ugyancsak felelősek mind a projekt-környezet, mind a támogató környezet biztonságáért. Ők gondoskodjanak arról, hogy minden javasolt rendszerváltoztatás felülvizsgálaton menjen át, amelyben ellenőrzik, hogy sem magának a rendszernek, sem az üzemeltetési környezetnek a biztonságát nem veszélyeztetik.
MSZ ISO/IEC 17799:2002

Az informatikai rendszer veszélyeztetésének minimalizálása érdekében folyamatosan **kontrollálni** kell **a rendszert érintő változásokat**:

- A változással járó munka elkezdése előtt részletes, formalizált **elfogadási eljárásra** van szükség.
- Szabályozni kell a változást **végrehajtó személyek** körét.
- A szükséges módosítás érdekében az összes szoftver, információ, adatbázis és hardver **azonosítást** el kell végezni.
- A rendszer és üzemeltetési dokumentációkban a változásokat át kell vezetni, a régi dokumentációkat archiválni kell.
- A változásmenedzsment segítségével karban kell tartani az összes **szoftverfrissítést**.
- Gondoskodni kell arról, hogy minden változás **ellenőrizhető** legyen.
- Biztosítani kell, hogy a változtatások a kellő időben és a folyamatok minimális zavarásával legyenek megvalósítva.

Szoftverbeszerzés esetén a következő szempontokat kell figyelembe venni:

Semmelweis Egyetemen **kizárólag jogtiszta szoftverek** használhatók. Ha a vásárlási (fejlesztési, licence) szerződés másképpen nem rendelkezik, a **szerzői jogról** szóló törvény szerint kell eljárni. Ennek megfelelően a megszerzett szoftver nem többszörözhető, nem dolgozható át, nem dolgozható fel, nem fordítható le más nyelvre, nem módosítható (még hibajavítás érdekében sem).

Külső partner szoftver fejlesztési megbízása esetén a megbízási szerződésben rögzíteni kell, hogy a fejlesztést vállaló cég figyelembe veszi és betartja Semmelweis Egyetemben érvényes informatikai biztonsági szabályokat.

Ebben az esetben **biztosítani kell** a következőket:
- Biztosítani, hogy a program a fejlesztőtől függetlenül is továbbfejleszthető legyen.
- A fejlesztő a fejlesztési munka során az üzemelő éles rendszerhez nem férhet hozzá, az éles rendszerből származó olyan adatokkal, amelyekből bizalmas információ kinyerhető, tesztelést nem folytathat.
- Biztosítani kell, hogy az Egyetem a fejlesztőre vonatkozó biztonsági előírásokat ellenőrizhesse.

11. Üzletmenet (üzemeltetés) folytonosság

11.1 Az üzletmenet folytonosság és a menedzselési szempontok

Célkitűzés: Megvédeni a kritikus üzleti folyamatokat a nagyobb meghibásodások és a katasztrófák hatásaitól.

Üzletmenet folyamatosságát **menedzselő folyamatot** kell kialakítani annak érdekében, hogy megelőző és helyreállító óvintézkedések alkalmazásával elfogadható szintre lecsökkentsük a katasztrófák és az olyan biztonsági hibák hatására előálló üzleti (üzemeltetési) folyamatok kieséseit, melyek a természeti katasztrófák, balesetek, a berendezések meghibásodásai, illetve akár szándékos emberi tevékenységek következményei lehetnek.

Katasztrófák, biztonsági hibák, hiányosságok és a szolgáltatások kiesésének következményeit **elemezni** kell. **Terveket** kell kidolgozni és azokat megvalósítani a váratlan események kezelése érdekében, hogy biztosítsuk az üzleti folyamatoknak az elvárt időn belüli helyreállíthatóságát. Ezeket a terveket karban kell tartani és gyakoroltatni kell, hogy a többi menedzselési folyamat szerves részévé válhassanak.

Üzletmenet folyamatosságának menedzselése foglalja magában a kockázatokat azonosító és csökkentő, a károkozó véletlen események következményeit korlátozó, valamint a fontos működés időben újraindítását szavatoló **óvintézkedéseket**.
MSZ ISO/IEC 17799:2002

11.1.1 Az üzletmenet (üzemeltetés) folytonosság menedzselés folyamata

Az üzemeltetés kialakítása során kiemelten kell figyelembe venni a Semmelweis Egyetem **kritikus folyamatainak** kiesésmentes működését. E célból a kritikus folyamatokat támogató rendszerek beszerzésekor a magas minőségi követelményeket kielégítő **megoldásokat** kell választani és gondoskodni kell a kezelő munkatársak megfelelő szintű kiképzéséről.

A beszállítói support **szerződésekben** a folytonos működés biztosíthatóságára nagy hangsúlyt kell fektetni. Kritikus folyamatok kiesésmentességét **redundáns megoldások** alkalmazásával kell biztosítani. Erre kevésbé összetett rendszerek esetén akár papír alapú **alternatív megoldás** is elfogadható. Olyan menedzselt folyamatokat kell tervezni és működtetni, amellyel az **egész Egyetemre** vonatkozóan lehet az üzletmenet folyamatosságot fejleszteni és karbantartani.

Üzletmenet folytonosság menedzselése

- Fel kell mérni Semmelweis Egyetem folyamatait érintő mérvadó **fenyegetéseket**, ezek bekövetkezési valószínűségeit és hatásaikat, illetve az ezekből eredő **kockázatokat**.
- Meg kell határozni a működés szempontjából a **kritikus folyamatokat**.
- **Megoldásokat** kell kidolgozni a váratlan események kezelésére, amelyek az egyetem, illetve szervezeteinek folyamatos működését veszélyeztetik.

- Semmelweis Egyetem definiált tevékenységeivel és céljaival konzisztens **üzletmenet folyamatossági stratégia** megfogalmazása, dokumentálása és jóváhagyása olyan módon, hogy azok feleljenek meg a Egyetem stratégiai céljainak.
- A **tervek és a folyamatok** szabályos időközönkénti **vizsgálata** és napra késszé tétele. Biztosítani kell, hogy az üzletmenet folytonosságának menedzselése szervesen integrálódjon az Egyetem folyamataiba.
- Az üzletmenet folytonosság menedzselési folyamatok **koordinálásának felelősségét** hozzá kell rendelni egy szervezeti egységhez, illetve munkatárshoz (pl. IBV).

11.1.2 Az üzletmenet (üzemeltetés) folytonosság elemzése

Fel kell mérni azokat a **fenyegető tényezőket**, amelyek Semmelweis Egyetem működési folyamatainak tekintetében mérvadónak tekinthetőek. Meg kell határozni, hogy a fenyegető tényezők bekövetkezésekor milyen **kárkövetkezményekre** lehet számítani.

Meg kell határozni, hogy a kiesések bekövetkezésekor mekkora **költséget** jelenthet a folyamat helyreállítása és az milyen időtartam alatt valósulhat az meg. A dokumentált és jóváhagyott üzletmenet folytonossági stratégiát mindezek figyelembe vételével kell elkészíteni.

11.1.3 Az Üzletmenet (üzemeltetés) folytonossági terv és megvalósítása

Dokumentált és jóváhagyott üzletmenet folytonossági **tervet** kell készíteni **a működés fenntartására** és a kritikus folyamatok **meghibásodására**, vagy a megszakadását követően az előre meghatározott időn belüli **visszaállítására**, és a helyreállítására vonatkozóan. Részletesen meg kell határozni a szükséges megelőző, helyettesítő, illetve visszaállító/helyreállító intézkedések megvalósításához **szükséges feltételeket**, szervezeti és szervezési **lépéseket** és a megvalósítás módját.

A terv elkészítéséért az Informatikai Biztonságért Felelős Felsővezető (**IBFF**) **felel**.

Az üzletmenet folytonossági **terv tartalma**:

- A felelősségek és a vészhelyzeti eljárások **azonosítása**.
- A **vészhelyzeti eljárások** kidolgozása abból a célból, hogy ezzel lehetővé a tegyük kívánt időn belüli visszaállítást és helyreállítást. Különleges figyelmet igényel a külső üzleti kapcsolatok és az érvényben lévő szerződések felmérése.
- A munkatársak krízishelyzetekkel, vészhelyzeti eljárásokkal és folyamatokkal kapcsolatos **kiképzése**.
- A tervek **tesztelése** és naprakészségük biztosítása.

11.1.4 Az üzletmenet (üzemeltetés) folytonosság tervezés

Az üzletmenet (üzemeltetés) folytonosság tervekben a vizsgálatokhoz és a karbantartáshoz prioritásokat lehessen megadni. Az üzletmenet folytonosságának terve írja elő a hatálybalépés feltételeit, valamint a terv összetevőinek végrehajtásáért felelős személyeket. Új követelmények fellépése esetén módosítani kell a korábban felállított vészhelyzeti eljárásokat, terveket, vagy bármelyik tartalékra áttérés terveit.

Az üzletmenet folytonossági **terv kidolgozásának szempontjai**:

- A terv **kidolgozásának folyamatai** (vizsgálatok, prioritás, hatályba lépés feltételei).

- **Krízis/vészhelyzeti eljárásokat**, amelyek olyan tevékenységeket definiálnak, amelyek azonnali válaszlépést igényelnek bizonyos folyamatos működést, vagy emberéletet veszélyeztető véletlen eseményekre. Ezeknek magába kell foglalniuk a közhivatali kapcsolatok menedzselését is, mint pl. a rendőrséggel, a tűzoltósággal, stb.

- **A tartalék megoldásra áttérés** eljárásait, melyek azokat a tevékenységeket írják le, amelyeknek megfelelően a lényeges tevékenységeket, vagy a támogató/kisegítő szolgáltatásokat ideiglenesen áthelyezik alternatív helyekre, megoldásokra és a folyamatokat az elvárt/kívánt időn belül ismét elindítják.

- **Az újrakezdés/folytatás eljárásait**, amelyek a normál működés újbóli elérése érdekében megtett tevékenységeket írják le.

- **A terv karbantartásának összetevőit**, a tesztelések ütemezését és azok megvalósításának módját, illetve a karbantartás folyamatait.

- A **tudatosítás és az oktatás tevékenységeit**, melyeknek céljuk, hogy az érintettek megértessék az üzletmenet folyamatosság menedzselési folyamatát, és biztosítsa, a folyamat hatékonyságát.

- Az **egyéni felelősségeket**, amelyek megadják az érintettek felelősségét, a terv összeállítása és annak a végrehajtása során.

- Valamennyi **tervhez tulajdonost** kell rendelni, annak érdekében, hogy a vészhelyzeti eljárások, manuális tartalék, átkapcsolási és újraindulási tervek, illetve az erőforrások és folyamatok egyértelmű felelősségi köre biztosítható legyen.

11.1.5 Az üzletmenet folytonossági tervek vizsgálata, karbantartása

Üzletmenet folytonossági terveket **időszakonként tesztelni** szükséges. A tesztelés **célja**, hogy a tervekben előforduló hibás feltételezések, a figyelmetlenségek, a nem, vagy hiányosan átvezetett eszközök/berendezések, vagy szervezeti/személyi változások, illetve felkészülésbeli hiányosságok kiderüljenek. Az üzletmenet folytonosság tesztelési terveinek tartalmaznia kell a tesztelések **ütemezését és módját**.

A tesztelés **javasolt tartalma**:

- A különböző **forgatókönyvek elvi értékelése**, melyek a feltételezett kiesésekből kiindulva a visszaállításokat modellezik, vagyis gondolják végig.

- **Szimulációs gyakorlatok:** ennek keretében a kijelölt munkatársak felkészültsége ellenőrizhető, illetve az is kiderül, hogyan viselkednek váratlan események tényleges bekövetkezésekor.

- **Műszaki visszaállítási vizsgálatok:** melyek alapján ellenőrizhető, hogy az informatikai rendszerek működése milyen hatékonysággal állítható vissza.

- **Alternatív** helyszíneken telepített **rendszerek működőképességének**, illetve az átkapcsolás / áttelepítés lebonyolíthatóságának **ellenőrzése**.

- **Beszállítói szolgáltatások** és **eszközök** vizsgálatát annak érdekében, hogy a külső felek nyújtotta szolgáltatások és termékek kielégítsék a szerződéses kötelezettségként vállaltakat.

- **A teljes értékelés / beszámoltatás:** annak érdekében, hogy az érintett szervezetek, a munkatársak, a berendezések, az eszközök és a szolgáltatások alkalmasak-e, illetve képesek-e megbirkózni az üzemeltetési megszakításokkal.

Az üzletmenet (üzemeltetés) folytonossági terveket **folyamatosan naprakész állapotban** kell tartani. Valamennyi üzletmenet folyamatossági terv szabályos időközönkénti **felülvizsgálatának felelősségét személyekhez** kell rendelni, a felelős személy feladata, hogy a bekövetkezett változásokat a tervek megfelelő pontosítása/kiegészítése kövesse.

A v**áltozások átvezetése** után az aktualizált tervek megfelelő kiosztása, illetve az elavult változatok begyűjtése szükséges.

A tervek aktualizálására a következők tényezők változása esetén van **szükség**:
– Új berendezések használatba vétele,
– Egyetemi stratégia,
– a munkatársak,
– elérhetőségi címek és telefonszámok,
– elhelyezés, eszközök, erőforrások,
– szerződő felek, (szállítók, illetve kiemelt ügyfelek),
– új, vagy a visszavont folyamatok,
– jogi környezet,
– az üzemeltetői rendszer, illetve az üzemetetés változása.

Jelen Informatikai Biztonsági Politika és Stratégia a Szenátus 95/2007. (IX. 27.) számú határozatával az elfogadás napján lép életbe.

Budapest, 2007. szeptember 27.

Dr. Tulassay Tivadar s.k.
rektor

Dr. Stubnya Gusztáv s.k.
főigazgató

12. Mellékletek

12.1 1. sz. melléklet: A biztonsági osztályok minimális követelményei

Alap biztonsági osztály

Információvédelem:
- Az azonosítás és hitelesítés keretében a hozzáférést jelszavakkal kell ellenőrizni.
- A hozzáférés-jogosultság menedzselés, az elszámoltathatóság és az auditálhatóság biztosítása logikai védelmi funkció kialakításakor az ITSEC F-C2 funkcionális követelményszintnek megfelelően kell eljárni. A hitelesítés, az azonosítás, valamint a hozzáférés szabályozás rendszerét a hálózati alapú osztott rendszerek esetén az ITSEC F-C2 funkcionális szinttel azonos egyenszilárdsággal kell megvalósítani.
- Ki kell dolgozni az informatikai rendszerhez a hozzáférések illetékességi, jogosultsági rendszerét. A jogosultsági rendszernek támogatnia kell a jogosultságokhoz kapcsolódó adminisztrátori alapműveleteket (pl. a módosítás, törlés, stb.). Egy rendszeren belül a különböző adattípusokat olyan mértékben kell elkülönítetten kezelni, hogy megállapítható legyen a hozzáférések jogossága. On-line tranzakció kezdeményezésének jogosultságát minden esetben ellenőrizni kell.
- Intézkedési tervet kell kidolgozni arra vonatkozóan, mi történjék illetéktelen hozzáférések, illetve jogosultságokkal visszaélések esetén, amely során a lehető legnagyobb mértékben meg kell tudni határozni a felelősséget.
- Ki kell alakítani a biztonság belső ellenőrzésének rendszerét, amely során meg kell határozni a felügyeleti és megelőzési tevékenységek eljárásrendjét.
- Az informatikai rendszer üzemeltetéséről nyilvántartást kell vezetni, amelyet az arra illetékes személynek rendszeresen ellenőriznie kell.

Megbízható működés:
- Az informatikai rendszer megbízhatóságát az MM-A osztály szintjén jó minőségű és megfelelő számú referenciával rendelkező hardver és szoftver termékek beszerzésével kell biztosítani.
- A szállítóval és a szerviz cégekkel olyan garanciális, illetve garancián túli szerviz szerződést kell kötni, amely garantálja az MM-A osztályra definiált rendelkezésre állási szint betarthatóságát. A szerviz szerződésben legalább a 12 órás reakcióidő kikötése ajánlott.
- Az informatikai rendszer tervezésénél betartandók a funkcionalitást meghatározó lépések.
- Az informatikai rendszer beszerzési, vagy fejlesztési folyamatának dokumentációs rendszerét ki kell alakítani.
- A fontosabb számítástechnikai eszközöket tartalmazó helyiségeket (pl. szerverszoba, hálózati központi elosztó helyiség) a MABISZ és a Rendőrség által jóváhagyott biztonsági zárral zárni kell, a kulcskezelést szabályozottan kell végezni.
- A számítástechnikai eszközöket tartalmazó helyiségekben az országos és az intézményi szintű tűz- és munkavédelmi rendszabályokat be kell tartani és tartatni.
- A fontosabb számítástechnikai erőforrások (pl. szerverek) legyenek ellátva szünetmentes tápegységgel.

- A rendszerbe kívülről bekerülő adathordozókat felhasználás előtt vírusellenőrzésnek kell alávetni. A vírusdetektálás és eltávolítás is biztonsági eseménynek számít, ezért a biztonsági naplózásnál leírtaknak megfelelően kell eljárni.
- A megbízható működéssel kapcsolatos eseményekre (rendszer indítás/leállás, nagyobb üzemzavarok, alap- és felhasználói szoftverekkel kapcsolatos, a megbízható működést érintő események) gépi, illetve manuális biztonsági naplózásokat kell végezni.
- A rendszer- és adatmentéseket az üzemeltetési előírásoknak megfelelő rendszerességgel el kell végezni, a mentésekről biztonsági másolatot kell készíteni. A primer és a biztonsági mentések adathordozóit külön-külön, tűzbiztos helyen kell tárolni.
- 100-nál nagyobb számú felhasználót kezelő hálózatnál az egyszerűsített SNMP szintű hálózat menedzsment alkalmazása szükséges.
- A hálózati elemek rongálás és tűz elleni védelmét biztosítani kell.
- Az informatikai rendszer üzemeltetéséhez és karbantartásához biztosítani kell az MM-A osztály követelményeinek megfelelő szaktudású és tapasztalatú munkatársakat.

Fokozott biztonsági osztály:

Információvédelem:
- Az azonosítás és hitelesítés logikai védelmi funkció kialakításánál az ITSEC F-B1 funkcionális követelményeknek megfelelően kell eljárni.
- A hozzáférés-szabályozás logikai védelmi funkció kialakításánál az ITSEC F-B1 funkcionális követelményeknek megfelelően kell eljárni.
- Az adatok minősítését és a feljogosítás műveletét a vonatkozó és hatályos törvények szerint kell elvégezni, illetve engedélyezni.
- Az elszámoltathatóság és az auditálhatóság logikai védelmi funkciót az ITSEC F-B1 funkcionális követelményeknek megfelelően kell kialakítani.
- Minősített adatokat kezelő alhálózatot az osztott rendszer más alhálózatával a 4.3. pontban leírt összekapcsolási szabályok betartásával szabad csak megvalósítani. Ha ez a feltétel nem biztosítható, a különbözőképpen minősített adatokat csak fizikailag teljesen elkülönített rendszeren szabad kezelni.

Megbízható működés:
- A szerverszobában ki kell építeni a technikai védelmi rendszert. A riasztásoknak az épület biztonsági szolgálatánál meg kell jelenniük.
- Az informatikai rendszer legyen ellátva másodlagos villámvédelemmel.
- A központi egység rendelkezzen egy laza csatolású (pl. hálózaton keresztül biztosított) melegtartalékkal vagy egy hideg tartalék egységgel. A mágneslemez egységek és kritikus hálózati elemek, illetve kapcsolatok tartalékolása szintén biztosított legyen. Az adatbázis kezelő szoftver rendelkezzen automatikus adatállomány mentési és visszaállítási funkciókkal.
- A szállítóval és a szerviz cégekkel olyan garanciális, illetve garancián túli szerviz szerződést kell kötni, amely garantálja az MM-F osztályra definiált rendelkezésre állási szint betarthatóságát. A szerviz szerződésben minimálisan 8 órás reakcióidő kikötése ajánlott.
- A kritikus hardver és hálózati elemekről olyan szintű dokumentációval kell rendelkezni, hogy az üzemeltető munkatársak az egység, vagy kártya szintű hibaelhárítást el tudják végezni.

Kiemelt biztonsági osztály:

Információvédelem:
- Az azonosítás, hitelesítés és hozzáférés-szabályozás logikai védelmi funkció kialakításánál az ITSEC F-B2 funkcionális követelményeknek megfelelően kell eljárni.
- Az adatok minősítését és a feljogosítás műveletét a vonatkozó és hatályos a törvények szerint kell elvégezni, illetve engedélyezni.
- A hozzáférési jogok egyedi, vagy csoport szintű megkülönböztetésénél az ITSEC F-B3 osztály biztonsági követelményeinek a rendszeradminisztrátor, az operátor és a biztonsági felügyelő szerepkörére, valamint a felhasználói jogok odaítélésére, módosítására és visszavonására vonatkozó részét szükséges figyelembe venni.
- A biztonsági napló adatait heti rendszerességgel kell ellenőrizni és archiválni.

Megbízható működés:
- A számítóközpontok, a szerverszobák, és az egyéb "központi" jellegű informatikai helyiségek legyenek ellátva intelligens beléptető rendszerrel, amely a mozgásokat két irányban regisztrálja és több ezer eseményt képes naplózni.
- A szerverszobában vízhűtéses klíma nem üzemeltethető.
- A számítóközpontok, a szerverszobák, és az egyéb "központi" jellegű informatikai helyiségek legyenek ellátva automatikus működtetésű oltórendszerrel.
- A központi egység rendelkezzen egy szoros csatolású melegtartalékkal és megfelelő automatikus áttérés menedzsment megoldással. A mágneslemez egységek és kritikus hálózati elemek, illetve kapcsolatok tartalékolása az MM-K osztály rendelkezésre állási követelményeinek megfelelő szinten legyen biztosítva.
- A szállítóval és a szerviz cégekkel olyan garanciális, illetve garancián túli szerviz szerződést kell kötni, amely garantálja az MM-K osztályra definiált rendelkezésre állási szint betarthatóságát. A szerviz szerződésben minimálisan 4 órás reakcióidő kikötése ajánlott.
- A teljes hardver/szoftver rendszerről és a hálózati elemekről olyan szintű dokumentációval kell rendelkezni, hogy az üzemeltető munkatársak az egység vagy a kártya szintű hibaelhárítást el tudják végezni.
- A munkatársak összetétele és kiképzettsége olyan legyen, hogy erre a biztonsági osztályra meghatározott 16 perces kiesési időt tartani tudja a kiemelt fontosságú alkalmazások, illetve a teljes rendszer kiesése esetén.

12.2 2. sz. melléklet: Rendszerszintű Biztonsági Szabályzat (RIBSZ) - sablon

1. Általános rendelkezések
   1.1. Rendszerszintű Informatikai Biztonsági Szabályzat (RIBSZ) kiadásának célja
   1.2. RIBSZ hatálya
      1.2.1. Személyi hatály
      1.2.2. Szervezeti hatály
      1.2.3. Tárgyi hatály
      1.2.4. Időbeni hatály

   1.3. RIBPSZ kezelése, frissítése, (ezzel kapcsolatos felelősségi-, és szerepkörök

2. Rendszer átfogó ismertetése
   2.1. Rendszer feladata
   2.2. Rendszer főbb elemei, (azok közötti adatkapcsolatok, összefüggések)
   2.3. Rendszer kapcsolatai
   2.4. Rendszer fizikai környezete

3. Biztonsági osztályba sorolás

4. Feladat-, felelősség- és hatáskörök
   4.1. Szervezeti feladat-, és felelősségelhatárolás
   4.2. Személyi feladat-, és felelősségelhatárolás

5. Rendszerrel kapcsolatos folyamatok
   5.1. Biztonságmenedzsment
      5.1.1. A védelmi dokumentáció struktúrája, kezelése, aktualizálása
      5.1.2. Biztonsági események
      5.1.3. Biztonsági felülvizsgálatok
      5.1.4. Eltérések kezelése
      5.1.5. Jelentési rendszer

   5.2. Működési folyamatok
      5.2.1. A rendszer kapcsolódása a működés folyamataihoz
      5.2.2. A rendszer által támogatott, implementált folyamatok

   5.3. Dokumentumokkal kapcsolatos folyamatok
      5.3.1. A rendszer dokumentációja
      5.3.2. A rendszer be- és kiviteli dokumentumai
      5.3.3. A rendszer adathordozói

   5.4. Személyekkel kapcsolatos folyamatok
      5.4.1. Oktatás
      5.4.2. Jogosultságok kezelése
      5.4.3. Azonosító konvenciók
      5.4.4. Jogosultságok igénylése és engedélyezése
      5.4.5.Jogosultságok módosítása

12.3 3. sz. melléklet: Éves ellenőrzési terv (példa)

Szervezetek ellenőrzése
Ellenőrizendő terület, érintett szervezeti egység
Ellenőrzés végrehajtásának időpontja (negyedév)
Ellenőrzés időtartama
Ellenőrzés végrehajtója
Ellenőrzés végrehajtásába külső szakértőt be kell-e vonni?

Funkcionális ellenőrzések
- Szerverszobák, géptermek ellenőrzése,
- Szerverek biztonsági beállításai,
- Fizikai biztonság ellenőrzése,
- Rendszerek jogosultságkezelési gyakorlatának ellenőrzése, stb.

12.4 4. sz. melléklet: SE-IBPS megvalósítás projekt terv (minta)

A következőkben – mintaként - az **Informatikai Biztonsági Politika és Stratégiában** megfogalmazott alapelvek, elvárások megvalósítása érdekében kidolgozandó **Informatikai Biztonsági Szabályzat megvalósításának projekt tervét** mutatjuk be.

Feladat prioritások:
1 – magas prioritású
2 – közepes prioritású
3 – alacsony prioritású

Terület / Akció	Prioritás	Felelős
Informatikai Biztonsági Stratégia (IBS) jóváhagyása	1	Rektor
Informatikai kockázatkezelés Kockázatkezelési rendszer kialakítása, Folyamatos működtetése a stratégiai elvek szerint	2	IBV
Szervezetbiztonság		
Informatikai biztonság menedzselése Szervezeti keretek kialakítása.	1	IBV - IT Biztonsági Vezető
Munkaköri leírások módosítása, új munkatársak felvétele	1	Humánerőforrás-Gazdálkodási Igazgatóság
Informatikai vagyon teljes felmérése, osztályozása (Semmelweis Egyetem telephelyein teljes felmérés, osztályozása, biztonsági felelősségek kiosztása.)	1	IBV, Informatikai vezetők IT biztonsági vezetők
Rendszer szintű Biztonsági Szabályzatok kidolgozása a kockázatkezelés eredményeit is figyelembe véve.	1	IBV
Munkatársak biztonsága Munkaköri leírások pontosítása, HR tevékenységek biztonsági stratégiának megfeleltetése	1	Humánerőforrás-Gazdálkodási Igazgatóság
Általános IT biztonsági oktatási terv elkészítése, oktatások megtartása a szabályzatban rögzített körnek.	2	Humánerőforrás-Gazdálkodási Igazgatóság

Terület / Akció	**Prioritás**	**Felelős**
Fizikai és környezeti biztonság		
Az Informatikai Biztonsági Politika és Stratégiának megfelelő: - biztonságos körletek kialakítása, - a berendezések biztonságának megvalósítása, - általános óvintézkedések bevezetése.	3	IBV, INFORMATIKAI IGAZGATÓSÁG, kari informatikai vezetők
A kommunikáció és üzemeltetés menedzselése Üzemeltetési szabályzatok teljes körűvé tétele.	2	INFORMATIKAI IGAZGATÓSÁG
Rosszindulatú szoftverek ellen védelmi szabályzat elkészítése.	3	INFORMATIKAI IGAZGATÓSÁG
Adathordozók kezelése és biztonsága Tárolási feltételek kialakítása (pl. zárható szekrények), hordozható számítógépes adathordozók védelme.	2	INFORMATIKAI IGAZGATÓSÁG
Információcsere Információcsere megállapodásainak megkötése a biztonsági stratégiában meghatározottak szerint (rendszerszintű biztonsági szabályzatokban kell szabályozni).	3	Rektor
Információcsere nyilvántartására szolgáló rendszer kialakítása.	3	IBV
Elektronikus levelezés szabályzatának elkészítése	2	INFORMATIKAI IGAZGATÓSÁG
Hozzáférés ellenőrzés szabályzata Hozzáférés-kezelési és ellenőrzési szabályzat elkészítése az IBPS biztonsági stratégia tartalmát alapul véve.	2	Humánerőforrás-Gazdálkodási Igazgatóság
Üzletmenet folytonosság		

Üzletmenet folytonossági stratégia kialakítása, katasztrófavédelmi terv elkészítése.	1	Informatikai Igazgatóság, informatikai szervezetek