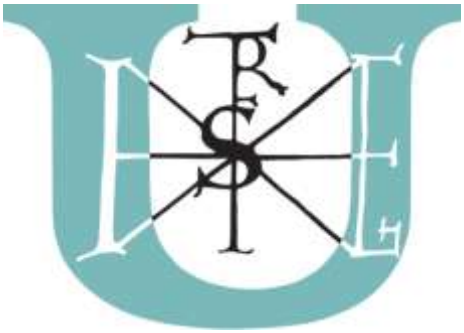


a Szent István Egyetem

INFORMÁCIÓBIZTONSÁGI SZABÁLYZATA

2012. október

Tartalomjegyzék

A Szent István Egyetem adatbiztonsága, az informatikai rendszerek védelme, illetve erősítése érdekében az alábbi utasítást adom ki:

1. ÁLTALÁNOS RENDELKEZÉSEK

Az Információ Biztonsági Szabályzat (továbbiakban: IBSZ) tárgya a Szent István Egyetem (továbbiakban: SZIE) tulajdonában vagy kezelésében lévő informatikai rendszerelemek, azaz tárgyak, eszközök, programok, adatok, adathordozók, dokumentumok és az informatikai rendszerekkel kapcsolatba kerülő kezelő, üzemeltető, kiszolgáló, karbantartó és felhasználó személyek.

1.1. Az IBSZ rendeltetése

Az IBSZ

- a hatályos jogszabályokkal (2.1. pont),
- az Informatikai Tárcaközi Bizottság (ITB) ajánlásaival,
- a Nemzeti Információs Infrastruktúra Fejlesztési Program (a továbbiakban NIIF) működtetéséről szóló 95/1999. (VI. 23*) Korm. rendeletben meghatározott, az NIIF keretében működtetett számítógép-hálózat használati szabályzatával,
- az MSZ ISO/IEC 27001:2006 szabvánnyal,
- valamint a SZIE működési és ügyrendi előírásaival

összhangban teremti meg a SZIE információinak biztonságát.

Az IBSZ kiadásának általános célja a SZIE rendszereiben kezelt adatok bizalmasságát, sértetlenségét és rendelkezésre állását illetve a rendszerek funkcionalitását fenyegető veszélyforrások elleni védelmi intézkedések szabályozása, ezáltal a SZIE alaprendeltetésből adódó célkitűzései és feladatai teljesítésének biztosítása.

1.2. Az IBSZ minősítése

A SZIE IBSZ **belső használatú dokumentum.** A belső használatú dokumentumot a SZIE informatikai területen, vagy informatikai rendszerekkel és alkalmazásokkal dolgozó munkatársai és szerződéses felei megismerhetik és birtokolhatják, de illetéktelenek részére nem adhatják tovább.

A hallgatókra vonatkozó jogokat és kötelességeket az Informatikai Szabályzat (is) tartalmazza. A SZIE hallgatói a ***„Felhasználói nyilatkozat”***-on keresztül ismerhetik meg, és aláírásukkal fogadják el az IBSZ-ből származtatott, hallgatókra vonatkozó jogokat és kötelességeket.

1.3. Az IBSZ hatálya

Az IBSZ végrehajtását a hatályba lépésnek megfelelően, kihirdetéstől kezdődően meg kell kezdeni. Az IBSZ a biztonságos információ ellátás érdekében utasításokat tartalmaz, amelyek hatálya kiterjed a SZIE informatikai rendszereinek teljes életciklusára (tervezés, fejlesztés, beszerzés, bevezetés, üzemeltetés, kivonás).

1.3.1. Személyi-szervezeti hatály

Az IBSZ személyi-szervezeti hatálya kiterjed:

- A SZIE valamennyi informatikát alkalmazó vagy az informatika környezetében működő szervezeti egységére.
- A SZIE informatikát alkalmazó vagy az informatika környezetében dolgozó valamennyi alkalmazottjára.
- A SZIE-vel szerződéses kapcsolatban álló informatikai vagy informatikához kapcsolódó munkát végző természetes és jogi személyekre. Valamint,
- Más szervezetek képviseletében a SZIE informatikai eszközeit használó munkahelyein vagy ezek környezetében tartózkodó személyekre.
- A SZIE-vel hallgatói jogviszonyban levő regisztrált, informatikát használó hallgatójára.

1.3.2. Tárgyi hatály

Az IBSZ tárgyi hatálya kiterjed:

- A SZIE tulajdonában lévő, illetve a munkatársak által használt valamennyi informatikai berendezésre (számítógépek, nyomtatók, külső háttértárolók, stb.), a számítástechnikai eszközre (aktív hálózati elemek, adathordozók, stb.).
- A SZIE területén ideiglenesen használt, a SZIE informatikai infrastruktúrájához bármilyen módon kapcsolódó, más szervezetek tulajdonát képező informatikai berendezésekre.
- A SZIE teljes számítástechnikai infrastruktúrájára (szerverek, kliensek, nyomtatók, rackszekrények, számítógépes vezetékes illetve vezeték nélküli hálózatok, hálózati aktív eszközök, szünetmentes áramforrások, stb.).
- A SZIE karai és központi szervezeti egységei által használt szoftverekre (rendszerprogramok, segédprogramok, alkalmazások, adatbázis kezelők, fejlesztő eszközök, operációs rendszerek, firmware-ek, stb.).
- A SZIE informatikai folyamataiban használt összes dokumentációra (tervezési, fejlesztési, üzemeltetési, szervezési, műszaki, informatika biztonsági, fizikai biztonsági dokumentációk stb.).

A papír alapú információk kezelését a SZIE Iratkezelési Szabályzata rögzíti.

1.3.3. Területi hatály

Az IBSZ területi hatálya kiterjed a Szent István Egyetem minden Karára, valamint a Rektori Hivatalára és Gazdasági Főigazgatóságára, területi elhelyezkedéstől függetlenül.

1.3.4. Az IBSZ további hatálya

Az IBSZ további hatálya kiterjed:

- A védelem körébe vont adatok és információk teljes körére, felmerülésüktől, feldolgozási helyüktől és az adatok fizikai megjelenési formájától függetlenül.

1.4. Az adminisztratív biztonsági intézkedések életciklusa

1.4.1. Utasítások készítése

Az utasításokat az érvényben levő szakmai, ügyviteli folyamatokra, a folyamatokban résztvevő informatikai rendszerekre és fizikai környezetükre vonatkozó nemzetközi és hazai szakmai szabályok, normák, szabványok előírásait, ajánlásait figyelembe véve és követve kell kialakítani, melyért az IK felelős.

1.4.2. Érvényesítés

- Az IBSZ-ben előírt eljárások és szabályok érvényesítése hagyományos vezetési eszközökkel történik, melynek elemei:
  - Irányítás (tervezés, feladatszabás, előírások, stb.)
  - Ellenőrzés
  - Felelősségre vonás

2. AZ INFORMÁCIÓ BIZTONSÁGI RENDSZER MŰKÖDTETÉSE

2.1. Megfelelés a jogszabályoknak és a belső szabályzatoknak

A SZIE működése követi a rá vonatkozó törvényi előírásokat és jogszabályokat, valamint a jelen IBSZ-en túl a következő belső szabályzatokat:

- A Szent István Egyetem Szervezeti és Működési Szabályzata
- A Szent István Egyetem Informatikai Szabályzata

- A Szent István Egyetem Iratkezelési Szabályzata
- A Szent István Egyetem Adatvédelmi Szabályzata
- SZIE Leltározási Szabályzata

2.2. Helyesbítő-megelőző intézkedések rendszere

Azokra a fenyegetettségekre, amelyekre szabályzatban nem rögzített eljárások, előírások, illetve a technikai eszközök nem adnak megoldást, az alábbi eljárásrend érvényes:

Az információbiztonsági rendszerrel kapcsolatos nem megfelelő működésekről, észrevételekről, javaslatokról a SZIE bármely dolgozója köteles tájékoztatni az adott kampusz rendszergazdáját vagy az Informatikai Központ[1] (továbbiakban: IK) illetékes informatikusát, illetve az információbiztonsági felelőst.

A bejelentésekről a kampusz rendszergazda vagy IK illetékes informatikusa tájékoztatja a kari információbiztonsági felelőst, illetve az informatikai igazgatót.

Az információbiztonsági felelős kari érintettség esetén, az informatikai igazgató SZIE központi probléma esetén az igényeket, bejelentéseket megvizsgálja, azokra intézkedési terveket dolgoz ki, amelyeket az egyetemi információbiztonsági felelős (főtitkár[2]) elé terjeszt jóváhagyásra. Jóváhagyás esetén az információbiztonsági rendszer fejlesztése, módosítása az kari információbiztonsági felelős és az informatikai igazgató felügyelete mellett történik.

3. VÉDELMI INTÉZKEDÉSEK MEGHATÁROZÁSA

3.1. Az adatok és eszközök biztonsági besorolása és ellenőrzése

3.1.1. Számadási kötelezettségek az informatikai eszközökkel kapcsolatban

A SZIE minden informatikai eszköze nyilván van tartva. A leltár elkészítéséről a SZIE Leltározási Szabályzata rendelkezik.

3.1.2. Az adatok osztályozása

Az adatok osztályozásának célja, hogy a különböző osztályozási kategóriába sorolt adatokhoz, illetve a kezelésüket megvalósító eszközökhöz különböző szintű védelmi intézkedéseket, eljárásokat lehessen rendelni.

3.1.3. Az adatok osztályozásának irányelvei

A SZIE-nél kezelt adatok osztályba vannak sorolva, annak érdekében, hogy az egyes adattípusokhoz különböző védelmi intézkedéseket lehessen rendelni.

Az információk osztályozását bizalmasság, sértetlenség, és rendelkezésre állás szempontjából osztályozni kell, amelyet az alábbi három szinten kell megvalósítani. Az osztályozási szinteket a táblázat foglalja össze (részletesebben lásd: ***1. számú melléklet***).

Osztályozási szintek	Bizalmasság	Sértetlenség	Rendelkezésre állás
1. Nyilvános	Nyilvános	Nem védett	Általános
2. Bizalmas	Bizalmas (belső használatra)	Védett	Fontos

[1] Korábbi szabályzatokban Informatikai Hivatal megnevezéssel azonos szervezeti egység.

[2] Az egyetem információbiztonsági felelőse a főtitkár, aki az informatikai és a papír alapú információk felügyeletét is ellátja.

3. Titkos	Titkos	Fokozottan védett	Kritikus

Az egyes adatcsoportok (rendszerek, alkalmazások) osztályba sorolási kategóriáját az határozza meg, hogy az adatok bizalmasságának, sértetlenségének, és rendelkezésre állásának sérüléséből a SZIE-nek milyen hátránya, anyagi kára származhat.

Az egyes biztonsági osztályba sorolt adatokhoz, és az adatokhoz tartozó adatkezelő- rendszerekhez, infrastrukturális elemekhez különböző szintű védelmi intézkedések vannak hozzárendelve.

Az adatok osztályozását az adatgazdák végezik. Az adatgazda szerepét annak a szervezeti egység (pl. egy osztály) egy alkalmazottja tölti be, aki az adott belső funkcionális részfolyamatot (pl. egy osztály vezetője vagy egy osztály adminisztrátora, stb.) végzi.

Az adatok osztályozása után meg kell határozni az osztályba sorolási szintnek megfelelően az adatok elvárt rendelkezésre állását is. Ennek alapján a helyi, illetékes kampusz rendszergazdával közösen, meg kell határozniuk azokat az információ-kezelő eszközöket is, amelyek szükségesek az adatok rendelkezésre állásához (szerverek, tárolók, aktív eszközök, adathordozó médiák, stb.). Ha az eszközök különböző rendelkezésre álló adatokat kezelnek, akkor azok közül a legszigorúbb követelményt kell figyelembe venni.

3.1.4. Adatok nyilvántartása

A SZIE adatait nyilván kell tartani. A nyilvántartásnak az alábbiakra kell kiterjedni:

- Az adat, vagy adatcsoport megnevezése
- Az adatosztályozási szint bizalmasság, sértetlenség, és rendelkezésre állás szerint
- Az adatgazda megnevezését
- Az adatokat kezelő eszközök megnevezését

A nyilvántartás vezetéséért az adatgazdák felelősek.

Az adatok nyilvántartási követelményei az ***1. számú mellékletben*** találhatók.

3.2. Az adathordozók biztonságos kezelése

Az adathordozók biztonságos kezelésének kialakításával megakadályozható a SZIE magasabb szintű adatbiztonsági kategóriákba besorolt adatainak illetéktelen kézbe való kerülése.

A SZIE tulajdonában lévő, a magasabb szintű adatbiztonsági kategóriákba besorolt adatok tárolására használt adathordozókat, amennyiben az a kockázati értékelésen egy előzetesen meghatározott értéket elér, azt egyedi azonosítóval kell ellátni, nyilvántartást kell vezetni róla. Az adathordozóra tett címkén, **az adattal dolgozó** SZIE **alkalmazottnak** fel kell tüntetnie az adott tartalomra vonatkozó bizalmassági kategóriákat. Kezelését ennek megfelelően kell megvalósítani.

3.2.1. Adathordozók tárolására vonatkozó szabályok

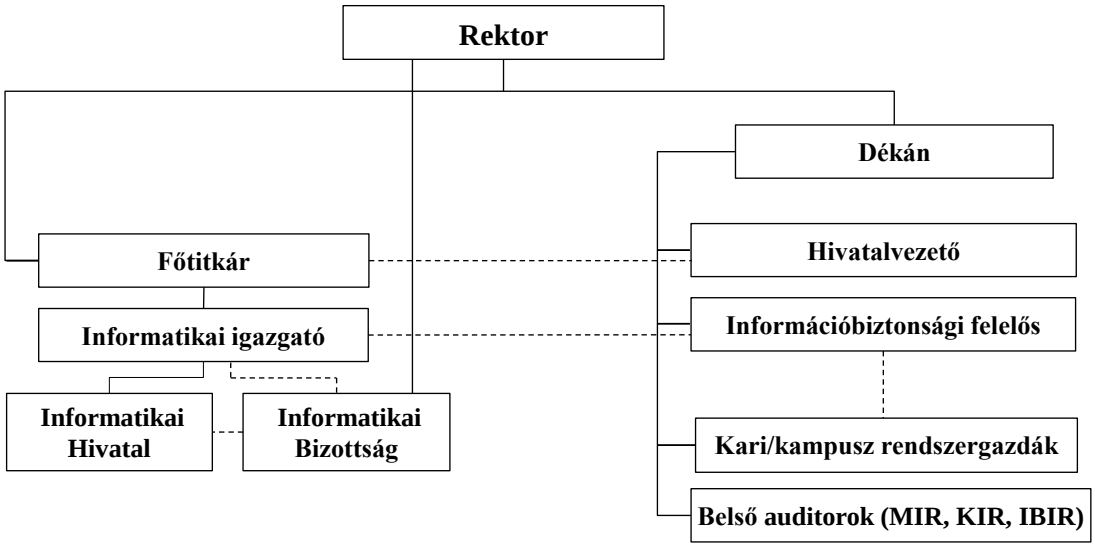
- Figyelembe kell venni a gyártó által meghatározott tárolási környezetre vonatkozó paramétereket, a tároló helynek tűzbiztos, elektromágneses hatásoktól védett helynek kell lennie,
- az adatbiztonsági kategóriákba besorolt adatokat tartalmazó adathordozók tárolásánál figyelembe kell venni a szabályzat adatok kezelésével kapcsolatos előírásaiban megfogalmazottakat.
- két példányban való tárolás esetében a tároló helyet úgy kell kiválasztani, hogy szükség esetén az arra jogosult akadálytalanul és viszonylag gyorsan hozzáférhessen, de célszerűen, viszonylag távol. Ezzel megakadályozva mindkét példány egyidejű megsemmisülését természeti katasztrófa esetén.

Az adatok osztályozása után meg kell határozni az osztályba sorolási szintnek megfelelően az adatok elvárt rendelkezésre állását is. Ennek alapján a helyi rendszergazdáknak az információbiztonsági felelőssel közösen, meg kell határozniuk azokat az információ-kezelő eszközöket is, amelyek szükségesek az adatok rendelkezésre állásához (szerverek, tárolók, aktív eszközök, adathordozó médiák, stb.). Ha

az eszközök különböző rendelkezésre-állású adatokat kezelnek, akkor azok közül a legszigorúbb követelményt kell figyelembe venni.

3.3. Az információ biztonsági szervezet működései rendje

3.3.1. Az információbiztonsági szervezet felépítése



Információbiztonsági szervezet felépítése

3.3.2. Információbiztonsági feladatkörök

Az *egyetemi információbiztonsági felelős (főtitkár)* feladatait a Főtitkári Hivatal ügyrendje szabályozza.

Informatikai igazgató feladatai:

- Felelős a kockázatkezelési feladatok rendszeres végrehajtásáért, a feltárt kockázatok csökkentésére vonatkozó akciótervek végrehajtásának ellenőrzéséért SZIE központi egységek szintjén.
- Gondoskodik a SZIE biztonsági alapdokumentumainak (stratégia, politikák, szabályzatok, utasítások, vészhelyzeti tervek, stb.) kidolgozásáról. Felelős az alacsonyabb szintű, eljárás- vagy eszköz/technológia specifikus biztonsági dokumentumok elkészítéséért, vagy illetékes felelős kijelöléséért központi szinten.
- Felügyeli a kockázatmenedzselési folyamatokat.
- Együttműködik a kari információbiztonsági felelősökkel, a kari rendszergazdákkal az informatikai rendszerek védelmére megvalósítandó rendszer biztonsági követelmények kialakításában, az információbiztonság fokozása, a biztonsági incidensek elhárítása érdekében.
- Ellenőrzi az informatikai rendszerfejlesztések, bővítések, beszerzések, ezekre vonatkozó szolgáltatási, rendelkezésre állási és más egyéb (pl. szállítási) szerződések egységes rendszer, hálózat és biztonsági szempontból való megfelelőségét központi szinten.
- Felügyeli a belső és külső informatika biztonsági ellenőrzések végrehajtását.
- Együttműködik az adatgazdákkal és a létesítmény biztonsági vagy műszaki felelősével az információ biztonsághoz kapcsolódó feladatokban központi szinten.
- Részt vesz a rendszer biztonsági oktatások tematikájának meghatározásában, szakmai felügyeletében központi szinten.

Információbiztonsági felelős feladatai:

- Felelős a kockázatkezelési feladatok rendszeres végrehajtásáért, a feltárt kockázatok csökkentésére vonatkozó akciótervek végrehajtásának ellenőrzéséért kari szinten.
- Javaslatot tesz az informatikai igazgatónak a felvállalható rendszer biztonsági kockázatokra, felhívja a figyelmét a nem felvállalható kockázatokra.
- Felelős az adatosztályozási folyamat fenntartásáért.
- Kezeli, és rendszeresen felülvizsgálja a SZIE és kar életbeléptetett biztonsági alapdokumentumait (stratégia, politikák, szabályzatok, utasítások, vészhelyzeti tervek, stb.). Kijelöli az alacsonyabb szintű, eljárás- vagy eszköz/technológia specifikus biztonsági dokumentumok.
- Együttműködik a SZIE IK, a kari rendszergazdákkal az informatikai rendszerek védelmére megvalósítandó rendszer biztonsági követelmények kialakításában, az információbiztonság fokozása, a biztonsági incidensek elhárítása érdekében.
- Ellenőrzi az informatikai rendszerfejlesztések, bővítések, beszerzések, ezekre vonatkozó szolgáltatási, rendelkezésre állási és más egyéb (pl. szállítási) szerződések egységes rendszer, hálózat és biztonsági szempontból való megfelelőségét kari szinten.
- Felügyeli a belső és külső informatika biztonsági ellenőrzések végrehajtását kari szinten.
- Együttműködik az adatgazdákkal és a létesítmény biztonsági vagy műszaki felelősével az információ biztonsághoz kapcsolódó feladatokban kari szinten.
- Részt vesz a rendszer biztonsági oktatások tematikájának meghatározásában, szakmai felügyeletében kari szinten.

Adatgazdák információbiztonsági feladatai

Az adatgazdák a SZIE ügyviteli és oktatási feladatait támogató folyamatok kijelölt tulajdonosai. Az adatgazdákat a szakmai (ügyviteli, oktatási) szervezetek állományából kell kijelölni. Feladatai az alábbiak:

- Részt vesz a Jogosultsági rendszer kidolgozásában, egységesítésében.
- Meghatározza az igényelt, kezelt, szolgáltatott strukturált és strukturálatlan adatok körének, formájának, biztonsági besorolását, aktualizálási gyakoriságát az ügyviteli és oktatási terület munkafolyamatainak megfelelően.
- Részt vesz a SZIE adatnyilvántartásainak kialakításában, naprakészen tartásában.
- Rendkívüli események esetére meghatározza a maximális átállási időt (sebezhetőségi ablakot).

Rendszergazdák

Feladataik az alábbi öt fő terület szerint csoportosíthatók:

Vírusok

- Folyamatosan figyeli a megjelenő vírusokról és sérülékenységekről szóló jelentéseket, szükség esetén javaslatokat tesz az információbiztonsági felelősnek, informatikai igazgatónak a védelmi szint emelésére.
- Szükség esetén értesíti a vírusvédelmi rendszert szállító vagy támogató céget, a vírusvédelmi rendszer felmerült üzemeltetési problémáinak, illetve vírusvédelmi vészhelyzet elhárítása miatt.
- Napi rendszerességgel ellenőrzi a vírusvédelmi rendszer állapotát, a vírusvédelmi eszközök vírusadatbázisát.
- Statisztikákat készít a vírusvédelmi incidensekről, és azokat háromhavonta jelenti az információbiztonsági felelősnek.

- Szükség esetén beavatkozik, illetve végrehajtja a vírusmentesítést.
- Elvégzi a SZIE-nél használt szoftverek, alkalmazások biztonsági frissítéseit.
- Javaslatokat tesz a szabályzat vírusvédelmi fejezeteinek módosítására.

Határvédelem

- Folyamatosan figyeli a megjelenő sérülékenységekről szóló jelentéseket, szükség esetén javaslatokat tesz az információbiztonsági felelősnek, az informatikai igazgatónak a védelmi szint emelésére.
- Végzi a tűzfal- és egyéb határvédelmi eszköz napi, rutinszerű üzemeltetési, és ellenőrzési feladatait.
- Szükség esetén értesíti a tűzfal-, és egyéb határvédelmi eszközt szállító vagy támogató céget az üzemeltetési problémáinak elhárítása miatt.
- Elvégzi vagy külső szolgáltató esetén ellenőrzi a tűzfal, és egyéb határvédelmi eszköz biztonsági frissítéseit. Gondoskodik a frissítések végrehajtásához szükséges licencek megfelelő számáról, illetve meghosszabbításáról.
- Információbiztonsági felelős/ informatikai igazgató jóváhagyása esetén végzi a tűzfalon és egyéb határvédelmi eszközön beállított szabályok szükséges módosításait, mentését, illetve gondoskodik azok rendszeres felülvizsgálatáról.
- Javaslatokat tesz a szabályzat határvédelmi fejezeteinek módosítására.

Adatmentés

- Részt vesz a mentési, archiválási rend kialakításában.
- Rendszeresen ellenőrzi a beállított automatikus mentések végrehajtását. Szükség esetén végrehajtja a mentéseket manuális módon.
- Az archiválási rendnek megfelelően végrehajtja az adatok archiválását, illetve a mentési, archiválási médiák biztonságos tárolását.
- Adatvesztés, vészhelyzeti terv aktiválása vagy felhasználói igény esetén végzi az adatok visszatöltését.
- Követi a mentési médiák életciklusát, szükség esetén másolással hosszabbítja meg az adatok visszaállíthatóságát.
- Gondoskodik a mentési médiák rotációjáról, újrahasznosításának szakszerű végrehajtásáról.

Jogosultságkezelés

- Részt vesz a jogosultsági rendszer kialakításában.
- Végrehajtja a szabályzatnak megfelelő jogosultság kezelési feladatokat (kiadás, módosítás, felfüggesztés, visszavonás).
- Végrehajtja a jogosultságok nyilvántartásával kapcsolatos adminisztratív feladatokat. Rendszeresen felülvizsgálja a kiadott jogosultságokat.

Felhasználók támogatása

- Fogadja a kar/kampusz/SZIE informatikai rendszerével kapcsolatos incidens jellegű bejelentéseket.
- Végrehatja azoknak a biztonsági incidenseknek az elhárítását, amelyekhez kompetenciája van.
- A kompetenciáján kívül eső incidensek elhárítására, értesíti az incidensek kezeléséért felelős személyeket (rendszergazdák).
- Dokumentálja a biztonsági incidensek kezelésének teljes ciklusa alatt felmerült problémákat, tevékenységeket, megoldásokat.

- Valamennyi biztonsági incidensről jelentést tesz az információbiztonsági felelősnek, informatikai igazgatónak.

Az információbiztonsági auditor feladatai:

- Megtervezi, végrehajtja és dokumentálja a tervezett és a rendszeres belső informatika biztonsági, adatvédelmi, és fizikai biztonsági ellenőrzéseket az információbiztonsági felelős, és a létesítmény biztonsági vagy műszaki felelőse, illetve más szakértők bevonásával.
- Létrehozza, vagy megvizsgálja az általa észlelt, vagy szakértő által jelentett biztonsági eseményekről, visszaélésekről készített jelentéseket.
- Az általa észlelt, vagy szakértő által jelentett biztonsági eseményekről, visszaélésekről megfelelően tájékoztatja az érintett vezetőt, az ellenőrzésbe bevont személyt és az információbiztonsági felelőst/ informatikai igazgatót.

3.4. A személyekhez kapcsolódó biztonsági előírások

Az információbiztonság szintjének fenntartása, mint kiemelt feladat, a SZIE-ben a teljes személyi állomány felelőssége. Az információbiztonság minimálisan betartandó előírásait a ***„Felhasználói nyilatkozat”*** tartalmazza. A felhasználói nyilatkozat tudomásulvétele és aláírása a SZIE-nél az informatikai rendszer használatának a feltétele.

3.4.1. Fegyelmi eljárások, szankcionálások

Az információbiztonsági előírások súlyos megsértése esetén fegyelmi eljárást kell indítani a szabálysértő személyével szemben, ha:

- a szabálysértés valamely rendszer hozzáférési adatainak illetéktelen személynek történő tudomására hozatalával (pl.: személyes jelszó elmondása, vagy hozzáférhető helyre történő feljegyzése) kapcsolatos.
- a szabálysértés következtében a SZIE „Bizalmas”, vagy annál magasabb minősítésű adata, dokumentuma kerül illetéktelen kezekbe.
- a szabálysértés következtében a SZIE „Fontos” vagy annál magasabb minősítésű rendelkezésre állás szerint minősített adata, dokumentuma a rendelkezésre állási követelménynek nem tud eleget tenni.
- a szabálysértő a SZIE „Védett”, vagy annál magasabb sértetlenség szerint minősített adatát, dokumentumát szándékosan meghamisította.
- a szabálysértés következtében a SZIE biztonsági rendszerének védelmi megoldásai illetéktelenek kezébe jutottak.
- a szabálysértés következtében bekövetkezett vagyoni hátrány (vagyoni kár, többletköltség) eléri, vagy meghaladja a jogszabályban meghatározott alsó határt. A szabálysértővel kapcsolatban anyagi felelősséget is meg kell állapítani.
- Törvénysértés esetén:
  - a szabálysértés következtében súlyosan sérül a személyes adatok védelméről, és nyilvánosságra hozataláról szóló jogszabályok,
  - bűncselekmény gyanúja áll fenn.

Az információbiztonsággal kapcsolatos fegyelmi eljárás lefolytatását az alábbi személyekből álló bizottság hajtja végre a Kjt. 46§ előírásai alapján:

- Informatikai igazgató, vagy az általa delegált személy
- HR illetve munkaügyi vezető, vagy az általa delegált személy
- A szabálysértő személy közvetlen munkahelyi vezetője vagy hallgató esetében a hallgatói képviselet megbízottja

- kari információbiztonsági felelős, vagy rendszergazda.

Amennyiben a fegyelmi eljárás a felsorolt személyek valamelyikére irányul, új tagságot kell kijelölni, melyhez az érintett személy helyett a munkahelyi vezetője jelöl ki delegált személyt. Ha a felhasználó által okozott szabálysértés anyagi kárral is jár, anyagi felelősséget is meg kell állapítani, és az okozott kárt a törvényeknek megfelelően ki kell fizettetni a kár okozójával.

3.4.2. Információ biztonság tudatosítása

A személyi kockázatok csökkentése érdekében meg kell oldani a SZIE informatikai rendszerének üzemeltetőinek, használó alkalmazottainak és hallgatóinak a biztonsággal kapcsolatos tudatosítását.

Az üzemeltetői információbiztonság oktatása a SZIE-nél központilag kerül koordinálásra, az alábbiak szerint:

Az informatikai igazgató elkészíti a központi „Oktatási tematikát", melyet átad az információbiztonsági felelősöknek, akik kari szintű elemeket illeszthetnek hozzá minden év február 15-ig. Az oktatási tematika részletesen tartalmazza az oktatási témákat, amelyeket tárgyévben oktatni kell, illetve az **alkalmazottak és hallgatók részére** rendszeres biztonsági tájékoztatásokat.

Az informatikai igazgató, az információbiztonsági felelősök és rendszergazdák az oktatási tematika alapján elkészítik az „Információbiztonsági oktatási tervet", amely tartalmazza:

- Az oktatási napokat, naponként témákra lebontva
- Az oktatás biztosítási feltételeit (oktatás helye, vagy eszköze)

Az információbiztonság oktatásában az e-learning rendszert kell előnyben részesíteni, igény esetén hagyományos oktatást kell biztosítani. Az oktatási anyagból vizsgát kell tenni. Az oktatáson való részvételt minden vizsgázónak aláírásával kell igazolnia.

A rendszeres biztonsági tájékoztatást elektronikus eszközök felhasználásával kell megoldani (pl. tájékoztató e-mailek, portál, stb.).

3.4.3. Külső személyek általi hozzáférések

A SZIE informatikai rendszerein regisztrált, egyéni hozzáférési engedéllyel rendelkező felhasználók dolgozhatnak. Külső személy csak az adott szervezeti egység vezetőjének engedélyével és csak felügyelet mellett végezhetnek munkát. (Ez alól funkciójánál fogva kivételt képeznek a SZIE hallgatói által használt információs rendszerek, eszközök.)

Az informatikai rendszeren történő munkavégzéshez hozzáférést csak a szerződésben rögzített munkához szükséges, és elégséges jogosultságokkal kell biztosítani.

Külső személynek távoli elérés csak indokolt esetben, a külső személy (cég) megbízhatóságáról történő meggyőződés és titoktartási nyilatkozat tétele után biztosítható. (Ez alól funkciójánál fogva kivételt képez, kizárólag a SZIE vezetői számára szolgáltatott távoli rendszerhozzáférések és a távoli levelezési rendszer hozzáférés biztosítása.)

Az engedély kiadásában

- A SZIE központi informatikai rendszerei esetén az informatikai igazgatónk vétójoga van. A vétójog a jogosultság szerződésben rögzített tartalmára, illetve a jogosultság kiadására terjed ki. A vétójogot csak a főtitkár utasítására lehet feloldani, aki a kockázatokról a szükséges tájékoztatást megkapja. Ebben az esetben a jogosultsággal kapcsolatos kockázatokat a főtitkár felvállalja.
- A SZIE kari informatikai rendszerei esetén az információbiztonsági felelősnek és a rendszergazdának van vétójoga. A vétójogot csak a dékán utasítására lehet feloldani, aki a kockázatokról a szükséges tájékoztatást megkapja. Ebben az esetben a jogosultsággal kapcsolatos kockázatokat a dékán vállalja fel.
- Külső személyek hozzáférésének szabályozását a szerződésben kell rögzíteni.

- A hozzáférés csak támogatási szerződés időtartamára, illetve a munka elvégzésének idejére adható.

3.4.4. A felhasználók jogai

- A felhasználóknak joga van a rendelkezésükre bocsátott informatikai eszközök szabályszerű, rendeltetésszerű használatára a saját munkájuk támogatása érdekében.
- A felhasználóknak joga van a számítógépes tevékenységük során felmerült problémák, akadályok elhárításához támogatási kapni. A segítségnyújtáshoz az igényt a helyi informatikai szervezetnél kell bejelenteni.
- A felhasználónak joga van a reá vonatkozó törvények, és szabályzatok megismeréséhez.
- A felhasználónak joga van a munkájához szükséges információbiztonsági eljárások, ismeretek megismeréséhez.
- A felhasználóknak joga van megtagadni a számítógépes munkát, ha
  - A számítógépes munka súlyos törvénysértéshez, vagy bűncselekményhez vezet.
  - A tevékenység veszélyezteti az informatikai rendszer rendelkezésre állását.

A felhasználóknak joga van a számítógépes munkával kapcsolatos sérelmeinek jogorvoslati kezelésére. Jogorvoslati kérdésekben az információbiztonsági felelős, magasabb szinten az informatikai igazgató, végső esetben a főtitkár áll rendelkezésre.

3.4.5. Felhasználói felelősségek

A felhasználó általában felelősséggel tartozik:

- A hivatkozott törvények betartásáért,
- A SZIE szabályzataiban megfogalmazott előírások betartásáért,
- A „Felhasználói nyilatkozatban” felelősséget vállalt előírások betartásáért,
- A törvényekben, szabályzatokban megfogalmazott előírások bárki által történő megszegésének a jelentéséért,
- Az információbiztonságért felelős személyekkel való együttműködésért.

3.5. Az informatikai biztonság személyi vonatkozásai

Az informatikai biztonság a SZIE teljes személyi állományának felelőssége. A személyi kockázatok csökkentése érdekében:

- Biztosítani kell a felhasználók rendszeres információbiztonsági oktatását, tudatosítását, tájékoztatását.
- A felhasználóknak rendelkezniük kell a munkaköri kötelességük ellátásához szükséges számítógépes ismeretekkel. A szükséges kompetenciákat a munkaköri leírás tartalmazza.
- Amennyiben a felhasználó nem rendelkezik a munkakör betöltéséhez szükséges informatikai ismeretekkel, azt maximum három hónapon belül igazolható módon pótolnia kell.
- Valamennyi alkalmazott részletes munkaköri leírásában szerepeltetni kell az adott munkakörre vonatkozó biztonsági követelmények meghatározását.
- Tájékoztatni kell a felhasználókat az információbiztonsággal kapcsolatos feladataikról, és felelősségeikről.
- Minden felhasználónál tudatosítani kell a biztonsági szabályok megsértésével járó szankciókat, és azokat következetesen be kell tartatni.

3.6. Fizikai és környezeti biztonság

A SZIE-nél három biztonsági zónát különböztetünk meg a fizikai és környezeti biztonság szempontjából:

1. számú biztonsági zóna: Azok a helyiségek, ahol nincs informatikai eszköz elhelyezve, vagy azoknak folyamatos, állandó felügyelete (személy vagy kamera által) biztosított.
2. számú biztonsági zóna: Azok a helyiségek, ahol a felhasználói informatikai eszközök vannak elhelyezve.
3. számú biztonsági zóna: szerverszobák (kiszolgálók és hálózati aktív eszközök).

Ugyanezeket a kategóriákat alkalmazzuk a papíralapú információk biztonsági kezelésénél. Ebben az esetben az egyes zónák besorolásánál az alábbi meghatározások érvényesek:

1. számú biztonsági zóna: Azok a helyiségek, ahol nincs papíralapú bizalmas információ elhelyezve, vagy azoknak folyamatos, állandó felügyelete (személy vagy kamera által) biztosított.
2. számú biztonsági zóna: a bizalmas információkat tartalmazó zárható elemek helyiségei.
3. számú biztonsági zóna: a titkos adatok (személyiségi jogokat, gazdasági vagy üzleti titkos adatokat, vagyon leltárt, szigorú számadásra kötelezett nyomtatványok és dokumentumok) és a bizalmas események ténydokumentumainak tároló helye (lemezszekrények, zárható iratszekrény a SZIE Adatvédelmi szabályzata szerint).

A biztonsági zónákat a bennük folyamatosan tárolt, vagy rajta keresztül elérhető információk bizalmasságára, sértetlenségére és rendelkezésre állására vonatkozó osztályozási szintek alapján illetve az információkezelő eszközök kockázati besorolása alapján kell kialakítani.

A biztonsági zónákat, és a hozzájuk tartozó főbb követelményeket a 2***. számú melléklet*** tartalmazza.

3.6.1. Helyhez kötött eszközök kivitele

Az eszközök átmeneti kivitele

A SZIE irodahelységeiből kiszállítandó informatikai berendezésekre vonatkozó szabályok:

- minden informatikai eszköz épületből történő kivitele csak a munkahelyi vezető – távollétében helyettese – engedélyével lehetséges,
- a kivitt eszközért a kiszállítót anyagi és erkölcsi felelősség terheli,
- a ki- és beszállításokat minden esetben dokumentálni kell szállítólevél alkalmazásával, amelyen az adott informatikai eszköz egyedi azonosítóját fel kell tüntetni (típus, gyári szám, leltári szám), illetve nagy mennyiség esetén csatolt mellékletben kell felsorolni az egyedi azonosító adatait.
- a szállítólevelet a kiinduló és a fogadó helyen a szállítást engedélyező és a szállítmányt fogadó személynek kézjegyével ellen kell jegyeznie, ezáltal nyomon követhetővé válik az eszköz útja.

Az eszközök végleges kivitele

A SZIE tulajdonából véglegesen (pl. selejtezés miatt) kikerülő informatikai eszközökre vonatkozó szabályok:

- az informatikai eszközökön tárolt adatokat a **rendszergazdának** visszaállíthatatlanul törölnie kell vagy selejtezéskor használhatatlanná kell tenni az adattárolót,
- a kiszállítást dokumentálni kell szállítólevél alkalmazásával, illetve selejtezéskor – mivel az elektronikus eszközök és berendezések veszélyes hulladéknak minősülnek – a környezetvédelmi törvénynek és előírásoknak megfelelően dokumentáltan, az erre jogosítvánnyal rendelkező céggel kell elszállíttatni.
- a szállítólevél kiállításának feltétele a kiegyenlített számla, vagy a selejtezési jegyzőkönyv.

Külső szervezet által biztosított eszközök:

- Idegen eszközt csak szerződéses formában, az informatikai igazgató jóváhagyásával lehet elhelyezni.
- A szerződésben rögzíteni kell az információbiztonsági szempontokat az elhelyezésre, működtetésre és felügyeletre, illetve az elszállításra vonatkozóan.

4. INFORMÁCIÓTECHNOLÓGIAI FOLYAMATOK BIZTONSÁGA

4.1. Informatikai rendszerek tervezése és jóváhagyása

Az informatikai rendszerek, vagy egyes rendszerelemeinek tervezéskor a funkcionalitáson, a gazdaságosságon túl a biztonsági szempontokat is figyelembe kell venni.

A kari információbiztonsági felelősnek az informatikai központ kijelölt tagjával együttműködve a teljes tervezési ciklust felügyelni kell annak érdekében, hogy tervezéskor a biztonsági megoldások is hangsúlyt kapjanak.

A tervezés során általában az alábbi biztonsági szempontokat kell figyelembe venni:

- A rendszer együttműködése a meglévő rendszerelemekkel.
- Beépített biztonsági megoldások.
- Az informatikai rendszer hozzáférési megoldásai (jogosultság kezelés, titkosítás, stb.).
- Az informatikai rendszer rendelkezésre állást támogató megoldásai (karbantarthatóság, javíthatóság, van-e szupport, mentések végrehajthatósága, stb.).
- Az informatikai rendszer menedzselhetősége (központilag menedzselhető, vagy helyileg).
- Az informatikai rendszer ellenőrizhetősége (naplózhatók-e a kritikus folyamatok, távoli elérés biztosított-e, stb.).
- A SZIE szoftveres, hardveres illetve egyéb standardjainak való megfelelés.

4.2. Informatikai eszközök beszerzésének biztonsága

Az informatikai eszközök (hardver, szoftver) beszerzésének biztonsága érdekében a SZIE-re érvényes és központilag kidolgozott szabályokat, eljárásokat kell foganatosítani annak érdekében, hogy biztosítható legyen az eszközök funkcionalitása, homogenitása, a kari és intézeti rendszerek együttműködése, illetve a rendszer előírt biztonsága.

4.3. Az üzemeltetés biztonsága

A megbízható és biztonságos üzemeltetés érdekében intézkedési terveket kell kidolgozni az informatikai rendszerhez kapcsolódó folyamatok – javítások, karbantartások, szoftvertelepítések és beállítások, stb. – végrehajtására.

A szabályokat, eljárásokat össze kell hangolni az érvényben lévő információbiztonsági szabályokkal, eljárásokkal. Az üzemeltetési eljárásokat dokumentálni szükséges annak érdekében, hogy az elvégzett feladatok nyomon követhetőek legyenek.

Az informatikai rendszerterveket, és a biztonsági megoldásokat tartalmazó egyéb dokumentumokat „Titkos” információként kell kezelni.

Az üzemeltetési dokumentációk elkészítéséről az üzemeltetésért felelős rendszergazda gondoskodik. Az információbiztonsági felelős feladata a dokumentációk évenkénti felülvizsgálata.

4.4. A fejlesztés, bővítés biztonsága

A biztonságos fejlesztés és rendszerbővítés érdekében ki kell dolgozni a fejlesztési, bővítési folyamatot, a hozzátartozó feladatokkal, és felelősségekkel annak érdekében, hogy az információbiztonsági, homogenitási és központi menedzselhetőségre vonatkozó elvárások maximálisan érvényesíthetők legyenek a fejlesztés és bővítés folyamatában, és a fejlesztett, bővített rendszerekben.

A fejlesztés és bővítés folyamatait dokumentálni kell. Az információbiztonsági előírásokat érvényesíteni kell a fejlesztéssel, bővítéssel kapcsolatos szerződésekben, megállapodásokban. A fejlesztési, bővítési dokumentációk elkészítéséért a fejlesztésért felelős az informatikai igazgató által kijelölt személy gondoskodik. A fejlesztési és bővítési dokumentációkat „Bizalmas" minősítésű információnak kell tekinteni.

A fejlesztési, bővítési és egyéb rendszerdokumentációk biztonságos tárolásával kapcsolatos ellenőrzés az információbiztonsági felelős feladata

4.5. Rendszergazdai tevékenységek naplózása

A SZIE üzemeltetésű rendszereken végzett rendszergazdai (operátori) tevékenységként értelmezzük a SZIE alapfeladatát támogató informatikai rendszer üzemeltetetési, javítási, karbantartási tevékenységét.

Ezen tevékenységek megkezdését az információbiztonsági felelős/informatikai igazgató tudtával, beleegyezésével és szükség esetén koordinálásával/felügyeletével kell az arra kijelölt/megbízott rendszergazdáknak elvégeznie. Az elvégzett munkát vagy tevékenységet, amennyiben az elektronikusan a hardver eszközökön nem automatikusan rögzített naplózni kell írásos, vagy elektronikus formában (pl. szerver napló).

4.6. Biztonsági incidensek kezelése

A SZIE-nél biztonsági incidensnek számít minden, az informatikával kapcsolatba hozható rendellenes működés, fenyegetés, amely az adatok bizalmasságát, sértetlenségét, vagy rendelkezésre állását veszélyezteti.

A biztonsági incidensek kategóriájába az alábbi események tartoznak:

- Jogosulatlan hozzáférés (informatikai eszközhöz, alkalmazáshoz, adathoz, biztonsági zónához)
- Információs vagyon (eszköz, szoftver, adat, stb.) elvesztése, eltulajdonítása, vagy megrongálódása.
- Határincidensek, vírusfertőzések,
- A mentési feladatok végrehajtásának akadályoztatása,
- Működési rendellenességek (információ biztonságot veszélyeztető eszköz hiba, program hiba, információ rendelkezésre állásának elvesztése, hibás adatok, stb.),
- Az IBSZ-ben hivatkozott törvények, szabályzatok és előírások, vagy az IBSZ szabályzatának megsértésére utaló cselekmények.

4.6.1. Incidensek priorizálása

Magas prioritású incidensek: Az incidensek kivizsgálását és elhárítását azonnal meg kell kezdeni.

- Határsértés, és illegális tevékenység észlelése (behatolás).
- Vírus-vészhelyzet (tömeges fertőzés), vagy központi vírusvédelmi eszköz kiesése.
- Adminisztrátori jogosultságok sérülése.
- Kritikus rendszer, vagy rendszer elemek kiesése.
- „Titkos" információk bizalmasságának, sértetlenségének elvesztése.

Közepes prioritású incidensek: Az incidensek kivizsgálását azonnal meg kell kezdeni, ha az egy magas prioritású incidens elhárítása nem akadályozza.

- Ismétlődő vírusfertőzés, vagy vírusdefiníciós állomány nem frissülése.
- Felhasználói jogosultságok sérülése.
- Kiemelten fontos rendszer, vagy rendszer elemek kiesése.
- „Bizalmas" információk bizalmasságának, sértetlenségének elvesztése.

Alacsony prioritású incidensek: Az incidensek feldolgozását két órán belül meg kell kezdeni, ha az egy magasabb prioritású incidens elhárítása nem akadályozza.

- Egyszeri vírusfertőzés, vagy helyi vírusvédelmi eszköz kiesése. (Amennyiben a vírusvédelmi rendszerrel az eszköz kiesése a felhasználó részéről automatikusan megoldható, nem szükséges további intézkedés.)
- Fontos rendszer, vagy rendszer elem kiesése.
- Kisebb jogosultsági incidensek (felhasználó elfelejtette a jelszavát, vagy az lejárt, stb.).
- Vírusvédelmi menedzsment eszközök kiesése.
- Törvénysértések.

Egyéb incidensek: Az incidensek kivizsgálását lehetőleg még a bejelentés vagy az észlelés napján, a folyamatban levő magasabb prioritású incidensektől függően kell megkezdeni.

- Nem fontos rendszer, vagy rendszer elem kiesése.
- Munkaállomás működésével kapcsolatos működési hibák.
- Szabály-, és eljárássértések.
- Felhasználói hibák.

4.6.2. Biztonsági incidensek kezelésének folyamata

A SZIE informatikai rendszerét használója köteles értesíteni a rendszergazdát lokális probléma esetén vagy az információbiztonsági felelőst kiterjedt probléma esetén az általa észlelt biztonsági incidensekről.

Incidens bejelentés bármely SZIE informatikai eszközt használó, vagy üzemeltető SZIE munkatárstól illetve hallgatótól érkezhet munkaidőben.

Az incidensek bejelentésének módját az 6. ***számú melléklet*** tartalmazza.

Az incidensek kezeléséért felelős személyek az alábbiak:

- Kisebb incidensek: helyi rendszergazda
- Vírusvédelmi incidensek: helyi rendszergazda
- Határvédelmi incidensek: helyi rendszergazda és információbiztonsági felelős
- Jogosultsági incidensek: rendszergazda
- Rendelkezésre állási incidensek: adott rendszer/eszköz rendszergazdája,
- Törvény-, szabály-, és eljárássértések: főtitkár, információbiztonsági felelős

A biztonsági incidensek kezelése:

- A bejelentett incidensről szükséges minden rendelkezésre álló információt elkérni a felhasználótól/bejelentőtől. Minden vonatkozó információt rögzíteni kell. A bejelentéseket (pl. e-mail vagy telefon) minden esetben, a prioritásától függően minél hamarabb vissza kell igazolni.
- Amennyiben a rendszergazda saját hatáskörben meg tudja oldani a bejelentett incidenst, és a megoldott incidenssel kapcsolatban a bejelentő 5 napon belül nem jelzett vissza, az incidens megoldottnak tekinthető. A megoldott incidensről a felhasználót/bejelentőt értesíteni kell.
- Amennyiben a rendszergazda saját hatáskörben nem tudja megoldani a bejelentett incidenst, prioritástól függően azonnal értesíteni kell a helyi az információbiztonsági felelőst. Ebben az esetben a probléma megoldására az információ biztonsági felelős a rendszergazdákkal együttműködve, megpróbálja a megfelelő megoldást kidolgozni.
- A mennyiben a probléma továbbra sem oldódik meg, a probléma szélesebb eszkalálása szükséges. Ebben az esetben a probléma további megoldására az információbiztonsági felelős a

rendszergazdákkal együttműködve, külső szakértő vagy a rendszer szállítójának bevonásával megpróbálja a megfelelő megoldást kidolgozni.

- Ha eddig a pontig eljutva sem sikerül megoldást találni a problémára, akkor az információbiztonsági felelős a rendszergazdával az alábbi döntés előkészítő javaslatokat teszi a SZIE informatikai igazgató részére:

    1) A probléma súlyosságát mérlegelve vészhelyzetet kell elrendelni és a vészhelyzeti terveknek megfelelően a normál működésre történő visszaállítást végrehajtani.
    2) A probléma súlyosságát mérlegelve fejlesztések, vagy beszerzések elindítása.
    3) Az incidens okozta kockázatokat csak az informatikai igazgató/főtitkár vállalhatják fel az információbiztonsági felelős javaslata alapján.

Az incidensek elhárítására, a rendszergazda hatáskörén kívül tett intézkedéseket az információbiztonsági felelősnek jelenteni kell, aki a szükséges információkat dokumentálja.

A vészhelyzeti tervek kialakításának és megvalósítási rendjének leírása az ME-17 Az adat- és információbiztonság kockázatarányos megvalósítása eljárás 7. pontja határozza meg. A konkrét vészhelyzeti tervek és operatív tennivalók a tervezés során meghatározott helyen, formanyomtatványon vannak meghatározva. A vészhelyzethez tartozó általános adatok ***4. számú mellékletben*** vannak felsorolva.

4.7. Problémakezelés

A problémakezelés célja az elhárított incidensek okának feltárása, és a kiváltó ok megszüntetése ezen incidensek előfordulásának csökkentése, vagy megszüntetése érdekében. A keletkezett és lezárt incidensek hiba okának felderítése a kezelésében résztvevő kollegák feladata.

Eredménye lehet:

- hiba okának definiálása a hozzá tartozó megoldással,
- hiba okának definiálása megoldás nélkül,
- incidens vizsgálat folyamatossá tétele a kellő információ hiányában.

Amennyiben sikerült feltárni a hiba okát, azt rögzíteni kell a „tudásbázisban” illetve meg kell osztani a teljes informatikai szervezet körében (lásd: 3.4.2. pont). A hiba okát ismerve intézkedéseket kell tenni a kiváltó ok végleges megszüntetésére, illetve az általa okozott probléma előfordulási gyakoriságának csökkentésére.

5. ADATVÉDELMI ELJÁRÁSOK MENEDZSMENTJE

5.1. A határvédelem megvalósítása

A SZIE informatikai rendszere és az Internet között határvédelmi technikai megoldások biztosítják a biztonság megfelelő szinten tartását. A biztonsági szint fenntartása érdekében az alább felsorolt előírások szükségesek. Az ún. demilitarizált zónákban azokat az informatikai eszközöket (szervereket, védelmi eszközöket, stb.) helyezik el, amelyek az Internet felé is nyújtanak szolgáltatásokat.

A SZIE egységes és homogén határvédelmi eszközök alkalmazására törekszik (tűzfal, vírusvédelmi gateway-ek, appliance, stb.). A határvédelmi eszköz felülvizsgálatát évente kell elvégezni és szükség esetén fejlesztéseket kell végrehajtani (cseréje, upgrade-je, újra licencezése, stb.).

Az életcikluson belül a határvédelmi eszközök biztonsági frissítéseit rendszeresen, folyamatosan el kell végezni. A firmware frissítéseket legalább évente szükséges ellenőrizni illetve végrehajtani. A szignatúra-frissítéseket, amennyiben automatikusan beállítható az eszközön, napi rendszerességgel kell ütemezni; amennyiben manuális beavatkozást igényel, hetente kell elvégezni.

Biztosítani kell, hogy a határvédelmi eszközökhöz csak kiemelt felhasználók (erre a célra kijelölt és kiképzett rendszergazdák) férjenek hozzá. A SZIE egységes határvédelmi eszközein minden tevékenységet naplózni kell, a beállításokat minden változtatást követően menteni szükséges.

Az egységes határvédelmi eszközöket rendszeresen monitorozni kell. A monitorozás eredményét minden esetben vissza kell csatolni, ha szükséges fejlesztést, vagy szabályozást kell végrehajtani, bevezetni. Az egységes és homogén határvédelem dokumentációját úgy kell tárolni, hogy az indokolatlan hozzáférés, illetve az illetéktelen kezekbe jutásuk elkerülhető legyen.

5.2. Vírusvédelem

5.2.1. A vírusvédelem irányelvei:

A SZIE vírusvédelmi rendszere korszerű vírusvédelmi technológiák, összehangolt folyamatok és szabályok összessége, melyek alkalmazásának irányelvei az alábbiak:

- ***Megelőzés:*** a SZIE a rosszindulatú programkódok elleni védekezésben a megelőző folyamatokra koncentrál.
- ***Folyamatosság:*** a vírusvédelmi kockázatok csökkentése, valamint a fertőzések megelőzése érdekében a vírusvédelmi rendszert folyamatosan, ebben a szabályzatban megfogalmazott módon kell működtetni.
- ***Reagálás:*** A világban folyamatosan változó, vírusvédelemmel kapcsolatos kihívásokra a SZIE igyekszik rugalmasan, gyorsan, és hatékonyan reagálni.
- ***Tudatosság:*** A vírusvédelmi rendszer hatékony ága jelentős mértékben növelhető, ha a vírusvédelemben résztvevő személyek (informatikai dolgozók, felhasználók), felkészültsége, motivációja, illetve tudatos felelősségvállalása biztosított.

A SZIE-nél a vírusvédelem központilag irányított folyamat. A részletes vírusvédelmi előírásokat a 14. ***számú fejezet*** tartalmazza.

5.3. A jogosultsági rendszer megvalósítása

Az adatok bizalmasságának és sértetlenségének biztosítása érdekében a SZIE-nél egységes jogosultság kezelő és nyilvántartó rendszer működik, amely alapja az LDAP rendszer.

A jogosultsági rendszer a felhasználói csoportokon és ezek hierarchikus rendszerén keresztül biztosítja az adatok adatosztályozási szintjeinek megfelelő bizalmassági és sértetlenségi követelményeknek való megfelelést.

A jogosultságokkal és azok kezelésével kapcsolatos előírásokat a ***15. számú fejezet*** tartalmazza.

5.4. Mentés, archiválás, visszatöltés

Az adatok rendelkezésre állásának biztosítása érdekében a SZIE-nél egységes biztonsági alapokon nyugvó mentési, archiválási, illetve visszatöltési rendszert kell kialakítani, működtetni.

A mentési, archiválási, illetve visszatöltési rendszernek biztosítania kell az adatok adatosztályozási szintjének megfelelő rendelkezésre állási követelményeknek való megfelelést.

A mentési, archiválási, illetve visszatöltési rendszer eljárásait, előírásait, és a rendszer üzemeltetésével kapcsolatos feladatokat a ***15 számú fejezet*** tartalmazza.

6. INFORMATIKAI SZOLGÁLTATÁSOK BIZTONSÁGA

6.1. Alkalmazás-, és szoftvereszközök használatának szabályozása

A SZIE minden Kara és Intézete és hallgatója számára biztosítja a munkához, illetve a tanulmányokhoz szükséges jogtiszta szoftvert. A személyhez kötött munkaállomásokra, oktatótermekben lévő munkaállomásokra illetve az otthoni munkavégzéshez biztosított, egyetemi tulajdonban lévő munkaállomásokra csak azok az alkalmazások, és szoftver eszközök telepíthetők, amelyre az alkalmazottnak a munkájához szüksége van, és az adott alkalmazással a távoli elérés engedélyezett. A szoftverek telepítése a rendszergazdák feladata.

6.2. Az elektronikus adatok és a levelezés biztonságának irányelvei

A SZIE informatikai rendszerében kezelt (továbbított, tárolt) elektronikus adatok, így az elektronikus levelek is - a levelek feladójától, címzettjétől, tartalmától függetlenül-, a SZIE tulajdonát képezik.

A felhasználók a SZIE rendszereit és erőforrásait csak az engedélyezett módon és mértékben használhatják. A SZIE rendszerein, ily módon elhelyezett adatokért a felhasználót terhel minden jogi felelősség. A használatot a SZIE kijelölt szakemberei ellenőrizhetik, illetve korlátozhatják.

Az elektronikus levelezéssel kapcsolatos feladatokat, felelősségeket, és eljárásokat a ***SZIE Informatikai szabályzat*** tartalmazza.

6.3. Az Internet elérés biztonságának irányelvei

A SZIE az Internet elérést a SZIE ügyviteli és oktatási folyamataihoz, és az azokat támogató folyamatok fenntartásához az NIIF hálózatán keresztül biztosítja.

Az Internet eléréssel kapcsolatos feladatokat, felelősségeket, és eljárásokat a ***SZIE Informatikai szabályzat*** tartalmazza.

6.4. Fájlkezelés / Címtárkezelés

A SZIE informatikai rendszerében kezelt (továbbított, tárolt) elektronikus adatok így a fájlok is a SZIE tulajdonát képezik. A fájlok kezelése során törekedni kell, hogy a tároló rendszerben az adott fájlnak minél kevesebb példánya tárolódjon. Dokumentumok közzététele esetén célszerű a fájlt egy helyre letárolni, és a címzetteknek a fájl elérési útvonalát tartalmazó, a fájlra mutató linket megküldeni.

A felhasználók a fájljaikat a központilag kialakított helyen tárolják. Nyilvános mappában tilos elhelyezni „Bizalmas”, vagy ennél magasabb minősítésű dokumentumot. A felhasználóknak tilos megosztani az egyéni mappájukat, illetve a saját helyi tárolójuk bármely mappáját.

7. A BIZTONSÁGI SZINT MÉRÉSE, MONITOROZÁSA

7.1. A biztonsági szint mérésének feltételei

Az informatikai rendszer biztonsági szintjének hiteles méréséhez az alábbi feltételek biztosítása szükséges:

- A mérés függetlenségének biztosítása:
  1) A méréseket a mérésben érintettek előzetes értesítése nélkül kell végrehajtani, hogy ne tudjanak felkészülni, illetve ne tudják befolyásolni a mérés eredményét.
  2) Az informatikai rendszer biztonsági szintjének mérése a főtitkár vagy dékán általa hivatalosan megbízott külső megbízott feladata. A méréseket a felhasználóktól, az üzemeltetési területtől független személy végezi.
- A mérés hitelességének biztosítása
  1) Az informatikai rendszer elemeinek idő szinkronizálása szükséges a naplófájlok megbízható kiértékeléséhez
  2) A biztonsági szint mérésével megbízott személy rendelkezzen naplófájlok eléréséhez szükséges felhatalmazással.
  3) Biztosítani kell a naplófájlok sértetlenségét. A naplófájlokhoz csak olyan személyeknek legyen hozzáférése, akiknek a munkájához feltétlen szükséges

7.2. A biztonsági szint mérésének eszközei és módszerei

7.2.1. Technikai szintű auditok

A biztonság szintjének mérésének egyik leghatásosabb módszere a technikai audit jellegű felmérések, amelyek lehetnek:

- Az informatikai rendszer Internet felöli sérülékenységeinek vizsgálata.

- Az informatikai rendszer Intranet felöli sérülékenységeinek vizsgálata.

Technikai szintű auditot a SZIE-nél kétévente, a fenyegetettségek felmérésével egy időben kell elvégezni.

7.2.2. Személyi biztonság szintjének mérése

A személyi biztonság szintjének mérését a SZIE-nél kétévente, a fenyegetettségek felmérésével egy időben kell elvégezni. A vizsgálat célja feltárni a felhasználók magatartásában, szokásaiban, tudatosságában rejlő alapvető biztonsági hiányosságokat.

A vizsgálat az alábbi területekre terjed ki:

- A felhasználók adat-tárolási szokásaira
- A felhasználók levelezési szokásaira
- A felhasználók Internetezési szokásaira

7.3. Az informatikai rendszer monitorozása

Az informatikai rendszer kritikus elemeit, illetve biztonsági eszközeit folyamatosan kell monitorozni. A monitorozásnak minimálisan az alábbi témákra terjed ki:

- Határvédelmi incidensek, és hálózati illegális tevékenység
- Vírusvédelmi incidensek
- Jogosultság kezelési incidensek (pl.: 5-nél többszöri sikertelen belépések száma)
- Mentési feladatok sikeres/sikertelen végrehajtása
- Védett adatok hozzáférésének naplózása
- Hiba jellegű incidensek
- Külső vagy távoli felhasználók tevékenységei, távoli elérések naplózása
- Rendszergazdák tevékenységei
- Rendszer konfigurációjának megváltoztatása
- Biztonsági riasztórendszerek naplózása (UPS, Tűzvédelem, Behatolás/betörés védelem, stb.)

7.4. A mérési adatok feldolgozása, visszacsatolása

Az információbiztonság szempontjából kritikus pontokon mérési és ellenőrzési rendszert kell bevezetni. A mérések eredményéről az **információbiztonsági felelős** évente írásban számol be az **Informatikai Bizottságnak.**

A mérési rendszer kontroll pontjait összefoglaló táblázat a ***3. számú mellékletben*** található.

7.5. Ellenőrzési irányelvek

Az információ biztonság szinten tartása érdekében megfelelő kontrollokat kell kialakítani. A kontrollok kialakításánál elsődlegesen azt kell figyelembe venni, hogy azok által az információbiztonság szintje mérhető legyen. Ennek érdekében meg kell határozni az ellenőrzések területeit, és minden területhez külön- külön meg kell fogalmazni az ellenőrzési célkitűzéseket.

Az ellenőrzési célkitűzések ismeretében meg kell jelölni az ellenőrzés eszközeit (dokumentumok, naplók, szoftverek, adatok, amelyek a biztonsági rendszerről hiteles képet tudnak adni), azok tartalmi követelményeit.

Az ellenőrzés eredménye minden esetben kiértékelésre kerül, amelyből a megfelelő következtetések levonhatók, így a kapott eredmények visszacsatolhatóak a biztonsági folyamatra. Vagy szükség esetén felelősségre vonási eljárást is kezdeményezhető.

Az ellenőrzéseket dokumentumok, dokumentációk, személyes beszámoltatás és helyszíni szemlék alapján lehet végrehajtani.

Az információ biztonsággal kapcsolatos ellenőrzések területei az alábbiak lehetnek:

- ***Megfelelőségi vizsgálat.*** Célja felderíteni, hogy a SZIE hivatalai, szervezeti egységei, Karai és Intézetei rendelkeznek-e a törvényi előírásokban meghatározott személyi, eljárási, tárgyi feltételekkel, és azok megfelelően dokumentáltak-e.
- ***Az információ biztonság szintjére vonatkozó vizsgálat***. Célja felderíteni, hogy a SZIE hivatalainál, szervezeti egységeinél, Karainál és Intézeteinél az információ biztonság szintje megfelel-e a meghatározott védelmi szintnek.
- ***Az információ biztonsági szabályok betartásának ellenőrzése.*** Célja felderíteni, hogy a SZIE információ biztonsági szabályait az illetékes személyek ismerik-e, illetve betartják-e. Ez az ellenőrzés az információ biztonság egy-egy területére is leszűkíthető.

Az ellenőrzések során elsősorban az alábbiakat kell vizsgálni:

- Az információbiztonsági rendszer működése megfelel-e a törvényi előírásoknak.
- Az információbiztonsági rendszer felépítése, tartalma megfelel-e az ISO 27001 szabványnak.
- Az információbiztonsági szabályok érvényesítve vannak-e a folyamatokban.
- Az információbiztonsági rendszer előírt dokumentumai léteznek-e, illetve naprakészek-e.
- Az információszemélyzet, illetve a felhasználók rendelkeznek-e a megfelelő információbiztonsági ismeretekkel.
- Az adatokra és rendszerekre vonatkozó kezelési szabályok betartását.
- A naplózási rendszer megfelelő alkalmazását. A biztonsági események kezelésének, a szükséges mértékű felelősségre vonás gyakorlatát.
- A mentési rendszer megfelelő alkalmazását.
- Az informatikai rendszert üzemeltetők, és felhasználók információ biztonsággal kapcsolatos ismereteit.
- A hozzáférési jogosultságok nyilvántartásának naprakészségét, a kiadott jogosultságok szükségességét.
- A dokumentációk pontosságát - naprakészségét, változás követését, megfelelő kezelését/nyilvántartását.
- Az alkalmazott szoftverek jogtisztaságát.
- A szerződések megfelelőségét.
- A fizikai biztonsági előírások betartását.

Az információbiztonsági rendszer, illetve annak egyes elemeit rendszeresen felülvizsgálatra kerülnek. A biztonsági rendszerek felülvizsgálati idejét összefoglaló táblázat a ***3. számú mellékletben*** található.

8. A SZERVERTEREM KIALAKÍTÁSÁNAK KÖVETELMÉNYEI

8.1. A szerverterem elhelyezésének szempontjai

Az szerverterem elhelyezésének biztonsági szempontjai az alábbiak:

- A belmagasságot is figyelembe véve biztosítsa az egyes szerverek, vagy egyéb aktív eszközök számára szükséges levegő térfogatot.
- A helyiség aljzatának megfelelő statikai terhelhetősége az elhelyezett eszközök tömegét, és fizikai méretét figyelembe véve.
- A helyiség ajtajának mérete biztosítsa az elhelyezésre kerülő eszközök akadálytalan ki- és beszállítását.
- A helyiséghez vezető folyósok, lépcsők, liftek alkalmasak legyenek az elhelyezésre kerülő eszközök ki-, és beszállítására.

- A helyiség határoló falai és nyílászárói alkalmasak legyenek a fizikai betörések megakadályozására.
- A helyiség elhelyezését úgy kell megválasztani, hogy a felette elhelyezkedő helyiségekben ne legyen vizes blokk (mosdó, WC, konyha, stb.). Ellenkező esetben a födém vízzárásának kialakítása szükséges.
- Ha a szerverszoba szintjén vízkár veszélye forog fenn (árvíz, belvíz, csőtörés, stb.), akkor az alábbi védőmechanizmusok bevezetése szükséges:
  - Állpadló, a berendezések mennyezetről való táplálása.
  - Falak, nyílászárók vízbehatolás elleni védelme.
  - Ún. védőtálcák alkalmazása a berendezések elhelyezésére.

8.2. A szerverterem behatolás védelme

A bizalmas adatok tárolását végző szerverek esetében a szerverterem behatolás-védelmének biztosítása érdekében az alábbi szempontokat kell érvényesíteni:

- Belépést regisztráló rendszer kialakítása (A munka befejezését is célszerű rögzíteni)
- Automatán záródó ajtó, mely kifelé kézzel nyitható (a menekülés biztosítása érdekében).
- Betörés-riasztó rendszer alkalmazása.

8.3. A szerverterem tűzvédelme

A szerverterem tűzvédelmének biztosítása érdekében az alábbi szempontok figyelembe vétele szükséges:

- A tűz-, vagy füstriasztó rendszer alkalmazása.
- Kézi tűzoltó-berendezések elhelyezése a bejárat közvetlen közelében.

8.4. A szerverterem áramellátása

A szerverterem illetve a szervertermen kívüli zárt rack-szekrényben elhelyezett hálózati aktív eszközök áramellátásának biztosítását az alábbi szempontok szerint kell végrehajtani:

- A teljes épület villámvédelmének biztosítása.
- A szerverterem független betáplálásának biztosítása.
- A szerverteremben illetve az azon kívül zárt rack-szekrényben üzemeltetett eszközök túlfeszültség elleni biztosítása.
- A főkapcsolók biztonságos helyen való elhelyezése (lehetőleg a bejárat közelében). A főkapcsolók legyenek védve illetéktelen beavatkozás ellen.
- Az eszközök szünetmentes tápellátása (központi UPS vagy helyi UPS-ek).
- A helyiség betáplálásának terhelés elosztása fázisonként.
- Az UPS-ek betáplálásának elosztása fázisonként.
- A szerverteremben illetve az azon kívül zárt rack-szekrényben elhelyezett eszközök részére minimálisan 30 perc tartási időre méretezett UPS-t kell alkalmazni.
- Az UPS-ek akkumulátorait legalább évente egyszer (pl. a tervszerű megelőző karbantartás alkalmával) tesztelni kell és szükség esetén gondoskodni kell azok haladéktalan cseréjéről).
- Érintésvédelem kialakítása, rendszeres felülvizsgálata.

8.5. A szerverterem klimatizálása

A szerverterem üzemi hőmérsékletének szabályozásának érdekében az alábbi szempontok figyelembe vétele szükséges:

- A szerverteremben klíma-berendezéseket kell üzemeltetni, a megfelelő üzemi hőmérséklet szabályozására.
- A klímarendszer független legyen az épület egyéb klíma rendszereitől.
- A klíma berendezések darabszámát, típusát, teljesítményét úgy kell tervezni, hogy a szerverteremben elhelyezett eszközök hődisszipációs mutatói mellett, még egy klímaberendezés meghibásodása esetén is biztosítani tudják a megfelelő szabályozást.
- A klíma-berendezések automatikus újraindítását biztosítani kell az esetleges áramszünet megszűnése esetén.
- A csapadékos évszakokban, különösen alagsori helységek esetén a megnövekedett pára kártékony hatása ellen páramentesítő alkalmazása célszerű.

8.6. Zavarvédelem

A szerverterem zavarálló képességének biztosítására az alábbiakat kell megfontolni: gépészeti eszközök (víz-, gáz-, fűtés vezetékek, stb.) eltávolítása javasolt.

9. A SZERVERTEREM HOZZÁFÉRÉSI KÖVETELMÉNYEI

9.1. A szerverterem nyitásának, és zárásának szabályai

A szervertermet folyamatosan zárva kell tartani még akkor is, amikor a helyiségben éppen munkavégzés folyik. Amennyiben a fenti követelmény valamilyen ok miatt nem követhető (pl.: meghibásodás, vagy beszállítás) a szerverterem bejáratának felügyeletét meg kell oldani.

9.2. A szerverterembe történő belépés, kilépés rendje

Kerülni kell a szerverteremben indokolatlan belépést. Azokat az üzemeltetési feladatokat, amelyek távoli eléréssel elvégezhetők, távoli menedzsment alkalmazásával kell elvégezni. A szerverterembe csak az arra felhatalmazott személyek léphetnek be. A SZIE-nél a szerverterembe a következő személyek belépése engedélyezett:

- informatikai igazgató,
- munkaköri leírása alapján arra jogosult munkatársak,
- az információbiztonsági felelős,
- a fentiek valamelyikének jelenlétében megbízott vagy felkért auditor,
- a fentiek valamelyikének jelenlétében és felügyelete alatt telepítést, karbantartást végző vállalkozó.

A szerverterembe történő belépéseket dokumentálni kell. A dokumentáció tartalmazza:

- a belépő nevét,
- a belépés célját,
- a belépés idejét,
- a kilépés idejét.

9.3. A szerverteremben történő munkavégzés rendje

A szerverteremben csak a folyamatban lévő munkavégzéshez szükséges eszközöket, szerszámokat szabad tartani. A helyiségben tartózkodás ideje alatt az elrendelt munkavégzéstől eltérő tevékenységet folytatni (evés, ivás, stb.) tilos.

A szerverterem más irányú hasznosítása (pl. raktározás, stb.) tilos. Ha olyan tevékenységet kell a szerverteremben végezni, amely veszélyeztetheti az egyes eszközök rendelkezésre állását, akkor a feladat végrehajtását az informatikai vezetőnek engedélyeznie kell.

Az elvégzett tevékenységet (telepítés, konfigurálás, javítás, karbantartás, stb.) minden esetben dokumentálni kell. A dokumentáció tartalmazza:

- A feladatot végző személy(ek) nevét
- A tevékenység leírását
- A tevékenység időtartamát

A dokumentáció lehet azonos a szervernaplóval.

10. A BESZERZÉSI FOLYAMATRA VONATKOZÓ BIZTONSÁGI ELŐÍRÁSOK

A beszerzésekre vonatkozó felhasználói és egyéb rendszerbővítési igényeket a lokális informatikai vezető specifikálja, melynek során figyelembe veszi:

- Az oktatási intézményekre vonatkozó közbeszerzési eljárás lefolytatására vonatkozó előírásokat.
- Az oktatási intézmények által alkalmazható speciális szoftverlicencezési lehetőségeket.
- A SZIE teljes informatikai rendszerére vonatkozó informatikai fejlesztési és bővítési terveket, a homogén rendszer kialakítására és megtartására irányuló előírásokat és standardokat valamint az információbiztonsági követelményeket.
- Az adott piaci kínálatot.

Az eszközök (hardver, szoftver) kiválasztásánál a fentiekben részletezett általános és gazdasági tényezők mellett figyelembe kell venni az adott eszköz által nyújtott biztonsági funkciókat, megoldásokat is.

A hardver eszközök beszerzéséhez még az alábbi tényezők figyelembevétele szükséges:

- A hardver funkcionalitása, erőforrásai
- A hardver várható rendelkezésre állása (megbízhatóság)
- A hardver garanciális feltételei (garancia idő, tartalom)
- A hardver szakértői és technikai támogatottsága (tanácsadás, alkatrész biztosítás)
- Támogatja-e a hardver a SZIE homogenitási és standardizálási törekvéseit

A szoftver megoldásoknál még az alábbi tényezők figyelembevétele szükséges:

- A szoftver funkcionalitása
- Illeszkedés a platform szabványokhoz (kompatibilitás)
- Támogatja-e a szoftver a SZIE homogenitási és standardizálási törekvéseit
- A szoftver biztonsági megoldásai (jogosultság kezelés, titkosítás, AD integrálhatóság, stb.)
- A szoftver menedzselhetősége
- A szoftverhez biztosított szupport és rendelkezésre állás

A teljes beszerzési folyamatot, feladatokat, és felelősségeket a ***SZIE Gazdálkodási Szabályzata*** rögzíti.

10.1. Az eszközök átvételével kapcsolatos előírások

A beszerzett eszközöket a beszállítás után ellenőrizni kell, hogy mennyiségre és minőségre azonos-e a megrendelésen szereplő tételekkel, illetve meg kell győződni arról, hogy a beszállított eszközök sértetlenek-e (nincs-e a szállításból adódó fizikai sérülés).

A szállítólevelet vagy az átadás-átvételi jegyzőkönyvet csak akkor szabad aláírni, ha a fenti ellenőrzés során nem merült fel mennyiségi, minőségi vagy más kifogás.

10.2. Szolgáltatások minőségének ellenőrzése

A szolgáltatások minőségének ellenőrzésére szolgáltatásonként kontrollokat kell felállítani. Minimális kontrollok az alábbiak:

- Szolgáltatás minőségére vonatkozó kontrollok:
  1) A szolgáltatás rendelkezésre állása (PL: Internet esetén kiesett órák száma, vagy a hiba elhárításának megkezdése, stb.).
  2) A szolgáltatás minősége (Pl.. Internet esetén sávszélesség, vagy a hiba gyors és szakszerű elhárítása, stb.).
- A szolgáltató megbízhatóságára vonatkozó kontrollok:
  1) A szolgáltató rendelkezésre állása.
  2) A szolgáltató együttműködési készsége.
  3) A szolgáltató szakmai kompetenciája.

A szolgáltatások minőségének ellenőrzését a rendszergazda végzi.

10.3. Szerződésekre, dokumentumokra vonatkozó előírások

10.3.1. A beszállítói szerződésekre vonatkozó előírások

A beszállító szerződésekben az alábbiak szerint kell érvényesíteni a biztonsági szabályokat:

- A beszállítónak titoktartási nyilatkozatot kell tennie a szerződésben, vagy különálló dokumentumban, amelyben a beszállító felelősséget vállal arra, hogy az általa szállított megoldásokról, illetve a SZIE-ről tudomására jutott egyéb információkról nem ad tájékoztatást harmadik félnek.
- A beszállítói szerződésekben meg kell határozni a garancia és a szupport pontos tartalmát, és idejét. Szükség esetén ki kell térni a szellemi tulajdonjogok tisztázására.

10.3.2. A szolgáltatói szerződésekre vonatkozó előírások

A szolgáltatói szerződésekben az alábbiak szerint kell érvényesíteni a biztonsági szabályokat:

A beszállítónak kollektív titoktartási nyilatkozatot kell tennie a szerződésben, vagy különálló dokumentumban, amelyben a beszállító felelősséget vállal arra, hogy az általa szállított megoldásokról, illetve a SZIE-ről tudomására jutott egyéb információkról nem ad tájékoztatást harmadik félnek.

Igény esetén a szolgáltatói szerződésekben meg kell határozni a hozzáférések követelményeit, valamint a szolgáltató részére bocsátott erőforrások körét. Ebben az esetben a külső szolgáltatókra vonatkozó biztonsági szabályokat a munka megkezdése előtt meg kell ismertetni a szolgáltatóval.

Meg kell határozni az incidensek bejelentésével, kezelésével kapcsolatos elvárásokat

A szolgáltatói szerződésekben meg kell határozni a szolgáltatói fél rendelkezésre állásának követelményeit, illetve a szolgáltatás tárgyát képező eszközökkel kapcsolatos rendelkezésre állási követelményeket.

A szolgáltatásokkal kapcsolatos rendelkezésre állási előírásoknak követnie kell a SZIE teljes informatikai rendszerére vonatkozó, az egységes üzemvitel kialakítására és megtartására irányuló előírásokat és standardokat valamint az információbiztonsági követelményeket.

10.4. A dokumentumokkal kapcsolatos követelmények

A beszerzések során, az alábbi dokumentációk átadását kell a beszállítóktól, illetve a szolgáltatóktól megkövetelni:

- Titoktartási nyilatkozat: a beszállítást, illetve szolgáltatást végző alkalmazottaktól
- A beszállítás tárgyát képező eszköz eredeti gyártói specifikációkat és licenceket, felhasználói segédleteit, üzemeltetési és üzembe helyezési (installációs) dokumentumokat.

- A szolgáltatással kapcsolatos elvégzett feladatokról (javítás, karbantartás, stb.) munkalap.

11. AZ ÜZEMELTETÉSHEZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEK

11.1. Az üzemeltetési folyamathoz tartozó biztonsági előírások

Az üzemeltetési folyamatokhoz ki kell alakítani a tevékenység-felelősség mátrixot, amelyben az alábbi felelősségeket kell megállapítani:

- Döntési felelősség.
- Koordinálási / felügyeleti felelősség.
- Végrehajtási felelősség.
- Ellenőrzési felelősség

A feladatkörök leosztásánál lehetőség szerint biztosítani kell, hogy az adott feladat végrehajtását, és ellenőrzését ne végezze ugyanaz a személy.

Az informatikai rendszer, vagy rendszerelemek változása (verzióváltás, frissítések) csak előzetesen sikeres tesztelés után történhet meg. Abban az esetben, amikor tartalékeszköz nem áll rendelkezésre, a visszaállíthatóság érdekében gondoskodni kell a mentésről. Több, azonos funkciót ellátó eszköz vagy eszközcsoport esetében (pl. hallgatói számítógépes labor) előbb egy tesztcsoporton kell a változtatásokat végrehajtani és csak pozitív teszteredmények esetén szabad csak a változtatásokat a rendszer többi elemén is végrehajtani.

Kritikus eszközöknek tekintjük azokat a kiszolgáló, illetve hálózati aktív eszközöket, amelyek segítségével illetve melyeken keresztül a SZIE kifejti informatikát igénybevevő, normál ügyviteli, oktatási, kutatási és egyéb feladataihoz kötődő folyamatait.

A kritikus eszközökön történő változás esetén, amely veszélyeztetheti az eszköz rendelkezésre állását, a változás előtt mentést kell végrehajtani a visszaállíthatóság érdekében. A javítási, karbantartási és szolgáltatási szerződésekben az eszközök által kezelt adatok rendelkezésre állási követelményeihez igazodó rendelkezésre állási időket kell érvényesíteni.

Az informatikai rendszert folyamatosan monitorozni kell. A monitorozás eredményéből, valamint az incidensek kezeléséből származó információkból statisztikákat, kimutatásokat kell készíteni, hogy a rendszerek megbízhatósága, rendelkezésre állása mérhető legyen.

12. INFRASTRUKTURÁLIS RENDSZERFEJLESZTÉSEKKEL KAPCSOLATOS KÖVETELMÉNYEK

12.1. Szakmai követelmények meghatározása

A SZIE-n-ben egységes fejlesztési tervet kell kidolgozni, amely meghatározza az egységes és homogén infrastruktúra kialakításának alapelveit és standardizálja az alkalmazott hardver és szoftver eszközök körét, típusait és ezek jellemző paramétereit. Az egységes fejlesztési terv kidolgozásáról a SZIE Informatikai Bizottsága (IB) dönt.

Az infrastrukturális rendszerfejlesztések tervezésekor az alábbi szempontokat kell figyelembe venni:

- A rendszerek egységesítése, funkcionalitása, platformfüggősége, illetve annak homogenitása.
- A rendszer teljesítmény, és kapacitás adatai.
- A rendszer biztonsági megoldásai (pl.: jogosultság kezelés, titkosítás, stb.).
- Alkalmazott szabványok, interfészek.
- A rendszer (központi) menedzselhetősége.
- A rendszerhez nyújtott garanciák, és szupport tevékenységek.
- A megoldást szállító cég referenciái.

A rendszer tervezésének és bevezetésének folyamatát az információbiztonsági felelősnek végig kell kísérni. A fejlesztéssel kapcsolatos szerződéseket az információbiztonsági felelősnek véleményezni szükséges.

12.2. Infrastrukturális fejlesztéssel kapcsolatos szerződések tartalmi követelményei

Az infrastrukturális rendszerfejlesztésekkel kapcsolatos szerződések tartalmazzák az alábbi követelményeket:

- A vállalkozóval szemben támasztott titoktartási követelményeket.
- A rendszerrel kapcsolatos garanciális-, és szupport-megegyezéseket.
- Az rendszerrel átadandó dokumentumok listáját, és azok tartalmával kapcsolatos esetleges követelményeket.

13. DOKUMENTÁCIÓVAL KAPCSOLATOS KÖVETELMÉNYEK

Az infrastrukturális rendszerfejlesztések alkalmával az alábbi dokumentációkat kell elkészíteni:

- Rendszerterv, amely tartalmazza:
  1) A bevezetésre kerülő rendszer leírását, funkcióit
  2) A bevezetésre kerülő rendszer logikai, és fizikai moduljainak funkcionális felépítését, leírását
  3) A bevezetésre kerülő rendszer illeszkedését a jelenlegi rendszerhez, az alkalmazott interfészek, szabványok leírása
- Üzemeltetési és karbantartási utasítás, amely tartalmazza:
  1) A rendszer elhelyezésével kapcsolatos követelményeket
  2) A rendszer üzemelési paramétereinek leírását (áramellátás, hőmérséklet, stb.)
  3) A rendszer installálásával kapcsolatos instrukciókat
  4) A rendszer karbantartásával kapcsolatos követelményeket
  5) Hibajelzési, és javítási alapinstrukciókat

14. A NEM KÍVÁNT PROGRAMOK (VÍRUS, SPAM, SPYWARE, STB.) ELLENI VÉDELEM

14.1. Rosszindulatú programok elleni védekezés alapjai

14.1.1. Vírusvédelmi események

A fertőzés nagyságától függően az alábbi területeket különböztetjük meg:

- **Elszigetelt:** ha a SZIE területén, 24 órán belül legfeljebb 2-3, egy intézményben legfeljebb 1-2 fertőzés fordul elő, és egy védendő eszközön sem ismétlődött meg a fertőzés.
- **Ismétlődő:** ha egy bizonyos eszköz egy nap többször, vagy több egymás utáni napon, hasonló módon megfertőződik.
- **Sorozatos:** ha 24 órán belül a SZIE területén 10-20, egy intézményen belül 5-10 fertőzés történt.
- **Tömeges:** fentieknél nagyobb 24 órán belüli fertőzésszám.
- Fertőzés az is, amit nem a vírusvédelmi eszközök jeleznek, hanem ami a felhasználók és rendszergazdák jelzései alapján valószínűsíthető.

14.1.2. Események szintjei:

1. szintű vírusvédelmi eseménynek minősül, ha a víruskereső elszigetelt fertőzést észlelt, és az előírt vírusmentesítést elvégezte.

2. szintű vírusvédelmi eseménynek minősülnek a következők:

- A vírusvédelem elszigetelt fertőzést észlel, de nem tudja a vírusmentesítést elvégezni.
- A vírusvédelem sorozatos vagy ismétlődő vírust észlelt, és a vírusmentesítést elvégezte.
- A vírusvédelmi menedzsment alkalmazás azt észleli, hogy valamelyik kiemelt eszközön nem fut a vírusvédelem.
- A vírusvédelmi menedzsment alkalmazás azt észleli, hogy valamelyik munkaállomáson 2 napja nem fut a vírusvédelem.
- A vírusvédelmi eszköz jelzi, hogy egy számítógépen 5 napnál régebbi a szignatúra. Kivételt képez az az eset, amikor a menedzsmentfelület a saját adatbázisa alapján azért mutat régi szignatúrákat, mert az adott számítógép több napja nincs bekapcsolva vagy nem elérhető, illetve már nem a hálózat része.
- A központi vírusvédelmi eszközök valamelyikének 1 napnál hosszabb üzemképtelensége.
- Itt fel nem sorolt egyéb esetek, amikor a vírusvédelmi rendszerbe bármi okból illetéktelenül beavatkoznak.

3. szintű vírusvédelmi eseménynek (vírusriadó) minősül:

- Tömeges vírusfertőzés
- Sikertelen vírusmentesítés sorozatos vagy ismétlődő fertőzés esetén.

14.2. A valósidejű védelem kialakítása

A SZIE-nél a védendő eszközök hatékony védelmének érdekében valósidejű védelmet kell kialakítani.

A szervereken és munkaállomásokon a valósidejű védelemnek folyamatosan bekapcsolva kell lennie, hogy biztosítsa a felhasználói munka során igénybevett állományok (adatok, programok) használat előtti vírusellenőrzését. Olyan központi kliens szerver megoldáson alapuló megoldást kell alkalmazni, mely automatikusan ellenőrzi:

- A teljes lokális és távoli fájlrendszert.
- A hálózati (vezetékes és vezeték nélküli) kapcsolatokat.
- Az adatbeviteli perifériákat (floppy, USB tárolók, CD és DVD meghajtók).
- Levelezési rendszer.

Biztosítani kell, hogy a munkaállomásokon a valósidejű védelmet a felhasználók ne tudják kikapcsolni.

Amennyiben a valósidejű védelem a detektált vírus eltávolítására nem képes, a vírusvédelmi rendszer automatikus értesítést küld a felhasználó és a helyi rendszergazda számára, és a fertőzés gyanús állományt a rendszer automatikusan karanténba helyezi.

A vírusfertőzésről vagy annak gyanújáról a felhasználó köteles értesíteni a helyi rendszergazdát.

14.3. Manuálisan indított/időzített teljes fájlrendszer átvizsgálása

A védendő kiszolgáló eszközökön a teljes állományrendszer vírusellenőrzését legalább heti egy alkalommal végre kell hajtani. A vírusellenőrzést ütemezve minden szerveren el kell indítani.

A helyi vírusvédelmi eszközöknél biztosítani kell, hogy a felhasználók a távolról indított vagy ütemezett feladatokat ne tudják leállítani vagy megváltoztatni.

A munkaállomásokon talált vírusgyanú esetén a teljes fájlrendszer ellenőrzésének elindítása kötelező. A teljes fájlrendszer átvizsgálásának manuális elindítása a vírusvédelemi rendszergazda feladata.

Szükség esetén a manuális átvizsgálás történhet a telepített vírusvédelmi eszközöktől független, hiteles forrásból származó, jogtiszta vírusvédelmi keresőprogramok segítségével is).

14.4. A vírusveszély csökkentésének hardveres és szoftveres lehetőségei

14.4.1. Egyéb hálózati eszközök alkalmazása a vírusvédelemben

A SZIE-nél a vírusfertőzés veszélyének csökkentése érdekében ki kell használni azokat a rendelkezésre álló technikai eszközöket, amelyek nem vírusvédelmi feladatokat látnak el, de egyes funkcióik alkalmas a vírusok elleni védekezésre, mint például:

- A hálózati aktív eszközök nem használt – fizikai és szoftveres – portok letiltása.
- A tartalomszűrő eszközökkel letöltések vagy levélben való küldésének blokkolása (vírusok jellemző karakter sorozatainak kiszűrése, veszélyes fájltípusok tiltása: exe, bat, com, stb.).
- A határvédelmi tűzfalakon a nem használt illetve nem támogatott protokollok és szoftver portok letiltása.
- Szervereken a nem használt applikációk és szervizek leállítása, eltávolítása.
- Szervereken kizárólag a működésükhöz és üzemeltetésükhöz szükséges programok telepítése.

14.4.2. Korlátozások operációs rendszer szinten

A vírusvédelmi kockázatok csökkentése érdekében lehetőség szerint az operációs rendszerek szintjén korlátozásokat kell bevezetni. A korlátozások terjedjenek ki az alábbiakra:

- A munkaállomásokon és szervereken meg kell akadályozni a nem használt távdiagnosztikai portok, távoli hozzáférést biztosító szolgáltatások elérését.
- A munkaállomásokon és szervereken meg kell akadályozni a nem használt szervizek, beépített alkalmazások hozzáférését.

A korlátozásokat a telepítő image-ben, illetve a csoportos és helyi házirendben is alkalmazni kell.

14.4.3. Szoftverek biztonsági frissítése

A vírusfertőzések kockázatainak csökkentése érdekében a SZIE-nél központilag menedzselt szervert kell üzemeltetni a Microsoft rendszerek automatikus biztonsági frissítésére. Továbbá biztosítani kell a többi alkalmazott szoftver folyamatos biztonsági frissítését is. A frissítéseket úgy kell ütemezni, hogy egy sérülékenység nyilvánosságra hozatala és a biztonsági frissítése között a legkevesebb idő teljen el.

A nem dobozos szoftverek esetében kötött szerződésekben ki kell térni a szoftver biztonsági frissítéseiről szóló utógondozási feladatokra.

14.4.4. Vírusvédelmi szignatúrák frissítése

A helyi vírusvédelmi eszközök vírusadatbázis (szignatúra) elosztása három szinten, automatikusan történik:

Felső szint: központi CMS (Central Manager System)

A vírusvédelmi eszközök műszaki dokumentációjában rögzített időpontokban (de legalább naponta) Internetről frissíti a vírusadatbázist a szoftver gyártója által leírt módon, elérhetővé teszi azokat más számítógépek számára és/vagy átmásolja a másodlagos vírusvédelmi szerverekre.

Második szint: Területi CMS (Central Manager System)

A szignatúra frissítésével kapcsolatos hálózati terhelés csökkentését szolgálják. A lokális vírusvédelmi szerverek az elsődleges központi vírusvédelmi szerverről frissítik az adatbázisukat. A frissítés az eszközök műszaki dokumentációjában rögzített időpontokban (de legalább naponta) történik.

Alsó szint: a védendő eszközök, ezek lehetnek munkaállomások és szerverek

A SZIE munkaállomásai, szerverei, amelyeken vírusvédelmi szoftver üzemel. A lokális vírusvédelmi szerverről frissítik az adatbázisukat.

14.5. Előírások felhasználók részére a vírusveszély csökkentésére

14.5.1. Általános előírások

A felhasználóknak tilos a munkaállomásukon, hordozható számítógépükön alkalmazott vírusvédelmi szoftver aktív védelmének kikapcsolás, vagy a védelmi beállításának megváltoztatása.

A szerverekhez tilos nem SZIE tulajdonú perifériát csatlakoztatni.

A vírusvédelem humán kockázatainak csökkentése érdekében a felhasználóknak meg kell ismernie, és alá kell írnia a ***„Felhasználói nyilatkozatot***".

Levelezés biztonsága: 19.1. pont.

14.5.2. Internetezés biztonsága

Tilos az ügyvitellel és az oktatási, kutatási feladatokkal össze nem függő fájlok megnyitása, letöltése az Internetről. A SZIE munkatársai a fájlletöltő oldalak tekintetében kizárólag az informatikai központ ajánlati listája szerinti letöltéseket végezhetnek.

14.5.3. Adathordozók kezelése

A szerverek és munkaállomások adatmeghajtó eszközeibe illetve csatlakozó felületeihez tilos ismeretlen eredetű vagy nem biztonságos adathordozót behelyezni (CD, DVD) vagy csatlakoztatni (pen-drive, memóriakártya olvasó).

14.5.4. Vírusvédelmi incidensek jelentése

A felhasználóknak jelenteniük kell a rendszergazdának a normális működéstől eltérő eseményeket. Vírusvédelmi incidens esetén a felhasználónak a rendszergazda útmutatásai szerint kell eljárnia.

14.6. A vírusvédelemi felelősségek, feladatok

A SZIE-nél a vírusvédelmet egységesen kell kezelni. A vírusvédelmi feladatok végrehajtása kétszintű:

14.6.1. Felső szint: IK

Háttérfeladatok

- Rendszeresen felülvizsgálja jelen vírusvédelmi folyamatot, szükség esetén módosítja azt.
- Elkészíti a vírusvédelmi rendszer műszaki dokumentációját, szükség esetén elvégzi a szükséges módosításokat.
- Részt vesz a vírusvédelmi eszközök kiválasztásában, felügyeli azok rendszeresítését, és telepítését.
- Részt vesz a vírusvédelemmel kapcsolatos oktatási és tudatosítási feladatok szervezésében, és lebonyolításában.

Védelmi feladatok

- Folyamatosan ellenőrzi a vírusvédelmi folyamatok betartását, szükség esetén javaslatot tesz a hiányosságok megszüntetésére, vagy felelősségre vonás kezdeményezésére.
- Jóváhagyja a vírusvédelmi eszközök Vírusvédelmi szakértő által meghatározott beállításait.
- Rendszeresen értékeli a vírusvédelmi események emlékeztetőit, szükség esetén javaslatot tesz fegyelmi vizsgálat lefolytatására.
- Felügyeli a vírusvédelmi eszközök működőképességét.

Feladatok sorozatos vagy tömeges vírusfertőzés esetén

- Információkat gyűjt a vírusfertőzés főbb jellemzőiről (fertőzés módja, mértéke, stb.).
- Meghatározza a vírusmentesítéshez szükséges mentesítési eljárásokat, megbecsüli azok erőforrásigényét, idejét.
- Felügyeli a vírusmentesítés folyamatát, szükség esetén kapcsolatot tart fenn a vírusvédelmi cégek tanácsadóival.
- Folyamatosan tájékoztatja a szervezeti egységek vezetőit.
- Felügyeli a visszaállítás folyamatát.
- Kivizsgálja a fertőzés okait, szükség esetén javaslatokat tesz a vírusvédelmi rendszer módosításaira, illetve a fegyelmi eljárások végrehajtására.

14.6.2. Technikai szint: rendszergazda

Háttérfeladatok

- Folyamatosan tájékozódik az újabb vírusfenyegetettségekről, és vírusvédelmi eszközökről.
- Rendszeresen felülvizsgálja a vírusvédelmi eszközök beállításait, szükség esetén javaslatokat tesz azok módosítására.
- Elvégzi a vírusvédelmi eszközök rezidens keresési, időzített keresési, frissítési, és riasztási beállításait.
- Végrehajtja a vírusvédelmi eszközök telepítését, végrehajtja a jóváhagyott és standardizált beállításokat.
- Tájékoztatás vagy oktatás tart a felhasználóknak a vírusvédelemről.
- Tartja a szakmai kapcsolatot a vírusvédelmi szoftverek szállítójával. Ha indokoltnak látja, tanfolyam elvégzését javasolja a vírusvédelemben résztvevő szereplőknek.
- Tervezi és nyomon követi vírusvédelmi eszközök optimális életciklusát, szükség esetén javaslatokat tesz az eszközök fejlesztésére, cseréjére.

Védelmi feladatok

- Megoldja a vírusvédelemben előforduló váratlan vagy tisztázatlan technikai problémákat. Együttműködik az információbiztonsági felelőssel azoknak a vírusforrások minimalizálására, amelyek többször is fertőzést okoztak, vagy okozhatnak.
- Szükség esetén az Internetről előírt rendszerességgel letölti a vírusszignatúrákat a kijelölt tároló helyre.
- 2. szintű vírusvédelmi eseménykor indokolt esetben, 3. szintű eseménykor minden esetben végrehajtja a vírusmentesítést.
- Rendszeresen, de legalább hetente minden védendő eszközön ellenőrzi vírusvédelem működőképességét, illetve a vírusszignatúrák frissességék.
- 1. szintű eseménynél kivizsgálja a vírus eredetét, és amennyiben lehetséges, akkor végrehajtja vírusmentesítést. Amennyiben a fertőzést emberi mulasztás okozta, vagy a jelenséget trójai vagy kémprogram okozta, azt jelenti az információbiztonsági felelősnek.
- A 2. vagy magasabb szintű eseményekről emlékeztetőt készít, mely tartalmazza
  - az esemény fajtáját,
  - az elhárítással foglalkozók nevét,
  - az érintett eszközöket,

- az esemény észlelésének és az elhárítás befejezésének az idejét,
- az esemény valószínű okát.

Feladatok sorozatos vagy tömeges vírusfertőzés esetén

- Végzi a vírus szignatúrák soron kívüli frissítését.
- Végzi a fertőzött rendszerek vírusmentesítését.
- Közreműködik a visszaállításánál.
- A visszaállítás után a kivizsgálja a fertőzés okát, lokalizálja annak forrását, majd jelenti az információbiztonsági felelősnek.

14.7. A vírusvédelemi[3] eszközök üzemeltetése

A vírusvédelmi eszközök üzemeltetéséért a SZIE IK, illetve rendszergazdák a felelősök. Az üzemeltetési feladatokat a következő pontok figyelembe vételével kell végrehajtani a SZIE vírusvédelmi szabályzata szerint.

14.7.1. A vírusvédelmi eszközök javítása

Meghibásodott központi vírusvédelmi eszközök javítása idejére, a rendelkezésre álló tartalék vagy a javítást végző szakszerviz által biztosított egyéb vírusvédelmi eszközzel meg kell oldani a helyettesítést. Ellenkező esetben az adott szolgáltatást (Internet, E-mail) a javítás idejére szüneteltetni kell.

14.7.2. A vírusvédelmi eszközök karbantartása

A vírusvédelmi eszközök karbantartását (pl.: frissítések), amennyiben lehetséges úgy kell elvégezni, hogy a vírusvédelmi eszköz működőképessége biztosítható legyen. A verzióváltásokat munkaidőn kívül célszerű végrehajtani.

14.7.3. A vírusvédelmi eszközök mentése

A vírusvédelmi eszközöket rendszeresen menteni kell annak érdekében, hogy:

- Szükség esetén a vírusvédelmi képesség visszaállítható legyen,
- A vírusvédelmi eszközök által jelentett vírusvédelmi incidensek visszakereshetők legyenek.

14.8. Ellenőrzés

Minden három hónapban az IK kijelölt munkatársa kötelessége vírus statisztikákat elkészíteni és az informatikai igazgató részére eljuttatni. Az informatikai igazgató kötelessége, hogy háromhavonta feldolgozza a kapott statisztikát meghatározva:

1) a vírusvédelmi eszközök által felismert és sikeresen elhárított vírustámadásokat,
2) a vírusvédelmi eszközök által felismert és sikeresen elhárított, de további emberi beavatkozást kívánó vírustámadásokat,
3) a vírusvédelmi eszközök által felismert, de el nem hárított támadásokat,
4) a vírusadatbázis frissítésekkel kapcsolatos riasztásokat szerverenként, a vírustámadások eloszlását, telephelyek, vírusfajták szerint.

15. A JOGOSULTSÁGI RENDSZER ELŐÍRÁSAI

15.1. A hozzáférési rendszer kialakítása

15.1.1. A hozzáférés követelményrendszere

A SZIE-nél a hozzáférési jogosultságok kialakítását szabályozó követelmények a következők:

[3] Beleértve az alábbiakat: vírus, spam, kémprogramok, stb.

- A hozzáférési jogosultságokat az adatcsoportok osztályozásával összhangban kell megállapítani.
- Az optimális hozzáférési rendszer kialakításához minél kevesebb, a feladathoz kapcsolódóan minimális jogokkal rendelkező felhasználói csoport kialakítása szükséges. A csoportok kialakítását a SZIE szervezeti felépítéshez és oktatási tevékenységéhez igazodva kell elvégezni. A csoportokhoz rendelt jogosultságoknak összhangban kell lenniük a csoport tagjai által kezelt adatok osztályozásával.
- A felhasználói csoportok jogosultsági körét az általuk végzett feladatokhoz képest úgy kell minimalizálni, hogy a felhasználónak csak a munkaköri feladataik elvégzéséhez szükséges minimális hozzáférési jogok álljanak rendelkezésre.
- A felhasználókat minden általuk használt rendszerben egyedileg azonosítani kell, és informálni kell őket az illető rendszerben fennálló korlátozásokról.
- A felhasználók azonosítását egyedi, titkos információval kell hitelesíteni (felhasználói azonosító és jelszó).
- A jogosultsági rendszer kialakításánál figyelembe kell venni a védelemre vonatkozó szerződésszerű kötelezettségeket, melyben az adatokhoz, vagy alkalmazásukhoz való hozzáférésről esik szó.
- Egyedi, személyre szóló hozzáférési jogokat kell alkalmazni, a felhasználói azonosítókat nem lehet megosztani a felhasználók között.
- Ideiglenes jogok meghatározása külső személyek számára csak a tevékenységükhöz szükséges mértékben történhet, kizárólag korlátozott időtartamig aktiválható, a szerződésükben meghatározott rendszerekhez. Ennek hiányában külső személynek hozzáférés nem adható a SZIE informatikai rendszereihez. A munkajogviszony megszűnését követően vagy a munkavégzés alóli mentesítés kezdetétől, amennyiben a munkáltatós és a közalkalmazott úgy állapodnak meg, hogy a mentesítési idő egy időtartamban és nem megosztva kerül kiadásra, vagy az előre meghatározott időtartam lejárta után a jogokat inaktiválni kell.

A követelményrendszert évente felül kell vizsgálni, és javított formában a rendszergazdák számára át kell adni. A felülvizsgálatot az információbiztonsági felelős végzi.

15.1.2. A hozzáférési rendszer kialakításának részfeladatai

A hozzáférési jogosultságok kialakításának részfeladatai a következők:

- a tárolt adatok különböző szervereken és ezeken belül különböző megosztásokba való csoportosítása,
- a tárolt adatok besorolása biztonsági szempontból
- felhasználói csoportok definiálása,
- az egyes megosztások és az azokon belül található almappákhoz és adatokhoz történő csoportok és azok jogosultságainak hozzárendelése,
- a rendszergazdák feladat megosztási rendszerének és az ennek megfelelő hozzáférési jogainak kidolgozása
- a hozzáférés nyilvántartásának kialakítása és folyamatos karbantartása.

15.1.3. Felhasználói csoportok létrehozása

A SZIE egyes szervezeti egységeinél használatos munkakörök (felhasználói csoportok) kialakítása:

- Az adott alkalmazás vagy szervezeti egység adatgazdája meghatározza az adott alkalmazást, illetve központi erőforrást használók általános és speciális felhasználói csoportjait.
- A SZIE adott karához vagy intézetéhez tartozó informatikai szervezet nyilvántartja, és a SZIE számára közzéteszi az aktuális felhasználói csoport listát

15.1.4. Jogosultságok felhasználói csoporthoz rendelése

A SZIE egyes szervezeti egységeinél használatos informatikai alkalmazások által létrehozott, illetve kezelt biztonsági szempontok szerint besorolt és rendszerekhez hozzárendelt adatok felhasználói csoporthoz rendelése.

- A hozzárendelés során egy adathoz több felhasználói csoport is rendelhető.
- A hozzárendelés során egy felhasználói csoporthoz több jogosultság is rendelhető.

15.2. Hozzáférési jogosultságok nyilvántartása

A SZIE dolgozói számára a rendszerhez való hozzáférési jogosultságot elektronikus vagy papír alapon, a SZIE iktatási és dokumentum -kezelő rendszerében rögzítetten, munkáltatói jóváhagyás mellett kell igényelni.

A központi jogosultságigénylés menete a következő:

1) A központi rendszerekhez jogosultságot a 3. mellékletben található Jogosultságigénylő lapon lehet igényelni. A munkavállaló részére a közvetlen felettese igényli a hozzáférést, az érintett rendszer adatgazdájától. A különböző rendszer adatgazdái megtalálhatóak a 4. mellékletben. A jóváhagyott igénylést az adatgazda továbbítja beállításra az IK-hoz.

2) A jogosultságokat úgy kell meghatározni, hogy a felhasználó minden, a munkájához szükséges, és csak a szükséges adatokhoz, funkciókhoz férjen hozzá.

3) Nem a szabályozott csatornán és formában érkező igényeket az IK nem hajthatja végre.

A kari üzemeltetésben lévő szolgáltatásokhoz jogosultságok igénylése az érintett kar Dékáni Hivatalában történik.

A hallgatói hozzáférés SZIE azonosító (Neptun kód) alapján, automatikusan, egységesen történik a központi azonosítást használó rendszerekben. A hozzáférést külön igényelni nem kell. A hozzáférés a hallgatói jogviszony létrejöttétől annak megszűntéig érvényes.

15.3. Felhasználói jogosultságok aktiválása, inaktiválása

- Új munkatárs hozzáférési rendszerbe való illesztését, vagy jogosultsággal rendelkező munkatárs jogosultság változási igényét a ***„Jogosultság kezelő lap”*** űrlap kitöltésével és elküldésével, az adott szervezeti egység vezetője írásban (elektronikusan vagy hagyományos módon) igényeli a rendszergazdájának való megküldésével. A „Jogosultság kezelő lap” űrlap lefűzésre kerülhetne a személyi dossziéban is.
- A SZIE informatikai rendszeréhez kizárólag olyan munkatárs kaphat hozzáférést, akinek adatai az Egyetem munkaügyi rendszerében rögzítésre kerültek, emellett az Egyetemmel aktív jogviszonnyal rendelkezik.
- Új hallgató hozzáférési rendszerbe való illesztését, vagy jogosultságának felfüggesztését (hallgatói jogviszony szüneteltetése) illetve megszüntetését (hallgatói jogviszony megszűnése) külön kérvényezni nem kell, mivel ezek az Egyetem tanulmányi rendszerében tárolt adatok alapján automatikusan átvezetésre kerülnek a jogosultságkezelő rendszerbe. aA jogosultság aktiválása és nyilvántartásba vétele előtt az adott rendszer adatgazdája ellenőrzi az igény jogosságát, a kitöltött Jogosultságigénylő űrlapon Annak jogosultságát aláírásával igazolja és elektronikusan archiválja azt. A jóváhagyott igénylést beálításra továbbküldi az érintett rendszer üzemeltetőjének. A jogosultság elbírálásának eredményéről, valamint a beállítás megtörténtéről az igénylőt tájékoztatni kell.
- Minden felhasználó (alkalmazott és hallgató) definiálásánál biztosítani kell az 1 természetes személy = 1 felhasználói azonosító, egy-egy értelmű megfeleltetést, azaz nem lehet közösen használt felhasználói azonosító. Kivételt képeznek ez alól az oktatási célra, hallgatók által használt informatikai eszközök.
- Az alkalmazotti jogviszony megszűnésének, megszüntetésének esetében a felhasználói hozzáférés zárolása automatikusan történik az alkalmazott kilépésekor. Ennek biztosítására:

1) Azonnali felmondás esetén, illetve ha a kilépő alkalmazott vezetője úgy ítéli meg, a jogosultság azonnal visszavonásra kerül. A kilépő alkalmazott vezetője ebben az esetben értesíti a rendszergazdát. A telefonos vagy szóbeli értesítést írott formában (e-mail vagy papír) is meg kell erősíteni.

2) Munkaviszony megszűnése esetén a jogosultság visszavonása a „Leszámolási lap" aláírásával egy időben történik. Ehhez az IK-t tájékoztatni kell a munkaviszony megszűnéséről.

- Alkalmazott esetében a kari információbiztonsági felelős köteles rendelkezni a felhasználó adatairól, dokumentumairól (archiválás, törlés, 3. személy általi hozzáférhetőség). A felhasználói fiók törlésére az adatok sorsának rendezése után kerülhet sor. A szervezeti egység vezetőjének a szóban forgó adatokkal kapcsolatban rendelkeznie kell arról, hogy az adatokhoz a továbbiakban ki férhet hozzá, illetve archiválni, törölni kell-e az adatokat.
- Amennyiben a felhasználó (alkalmazott és hallgató) jogviszonyában változások következnek be, de a munkáltatói jogviszony (áthelyezés más osztályra, munkakör vagy munkaköri leírás megváltozása) vagy a hallgatói kapcsolat valamilyen formája (pl. öreg diák) továbbra is a SZIE-hez köti, a felhasználót a felhasználói és hozzáférési jogosultságokat az új jogviszony szerint (az új jogviszonyhoz tartozó vezető kérelmének megfelelően) kell beállítani.

15.4. A jelszavas védelem felépítése, fajtái

A SZIE informatikai rendszereinek elérésére használható hozzáférés szintjei:

1) **Névre szóló rendszergazdai hozzáférés** esetén, a rendszergazdai jogosítványt a rendszergazda a saját nevére szóló, kizárólagosan általa használt, megfelelő rendszergazdai jogkörrel felruházott felhasználói azonosító segítségével lehet használni.

2) **A beépített** (root, administrator, rendszergazda, stb.) rendszergazdai accountokat biztonsági okokból el kell távolítani a rendszerből. Bármilyen operációhoz használni ezeket tilos. (Abban a rendszerben, ahol ez nem távolítható el, ott le kell tiltani.) Minden rendszergazdának rendelkeznie kell felhasználói hozzáféréssel is, amelyet egyébként használ.

3) **Speciális esetek** számára (pl., vészhozzáférés) létre lehet hozni a kétemberes szabály alkalmazásával egy rendszergazdai jogosítványt. Egyéb esetben amennyire technikai és egyéb szempontok lehetővé teszik, a csoportos rendszergazdai hozzáférést használni **Tilos.**

4) **Névre szóló felhasználói** hozzáférés keretében a felhasználó külön, saját névre szóló, más által nem használt, kizárólag a munkája ellátása miatt elengedhetetlen jogosítványokkal rendelkezik az informatikai és telekommunikációs rendszerekhez és azok erőforrásaihoz, az üzleti folyamatok ellátásához kapcsolódó feladatok elvégzéséhez.

5) **Csoportos felhasználói hozzáférés** keretében több felhasználó azonos, a munkája ellátása miatt elengedhetetlen felhasználói hozzáférést használ az informatikai és telekommunikációs rendszerekhez és azok erőforrásaihoz, az üzleti folyamatok ellátásához kapcsolódó feladatok elvégzéséhez. Amennyire technikai és egyéb szempontok lehetővé teszik, a csoportos felhasználói hozzáférést csak a védelmet nem igénylő adatokat tartalmazó rendszerek esetén szabad alkalmazni, minden más esetben **Tilos.** A csoportos felhasználói hozzáférést csak igen különleges és indokolt esetekben szabad csak alkalmazni (pl. technikailag elavult könyvtári rendszer).

15.5. Illetéktelen hozzáférés elleni védelem

15.5.1. Jelszómenedzsment

A SZIE informatikai rendszereihez való illetéktelen logikai hozzáférés megakadályozására jelszavas védelmet kell alkalmazni.

A SZIE informatikai hálózatába, illetve az alkalmazások rendszerébe bejelentkezési névvel (accounttal) rendelkező felhasználó köteles a bejelentkező nevéhez tartozó jelszó megőrzésére. A saját bejelentkező névhez tartozó jelszót elárulni, mások által is elérhető módon feljegyezni tilos.

Bejelentkező névhez tartozó jelszó beállításának megtörténtét és a jelszót a jogosultság kezelő rendszergazda telefonon közölheti abban az esetben, ha

- új felhasználó felvétele, vagy egyéb ok (pl. elfelejtés) miatt a felhasználó előtt még ismeretlen új belépési jelszót definiált,
- a beszélgető partner azonosítására az elvárható gondossággal járt el, és
- figyelmezteti a felhasználót arra, hogy a beszélgetést követő első bejelentkezésekor a rendszer a közölt jelszó megváltoztatására fogja kényszeríteni.

Valamennyi informatikai rendszer esetén a hozzáférésekhez rendelt jelszavaknak, a hozzáférés szintjétől függetlenül az alábbi alapkritériumoknak feleljenek meg:

- A jelszavak tartalmazzanak numerikus és alfabetikus karaktereket.
- Ne tartalmazzon ékezetes betűket és szóközöket.
- Ne tartalmazzon bármilyen nyelvű szót szótári alakban.
- Ne egyezzen meg a felhasználó nevével, felhasználói azonosítójával, egyik telefonszámával sem, engedélyének számával, személyi számával vagy dolgozói kódjával, valamint a felhasználóhoz kötődő bármely karaktersorozattal (pl. születési dátum, lakcím, gépkocsi rendszám, stb.).
- Ne egyezzen meg személynévvel.
- Ne egyezzen meg irodalmi, színházi, televíziós, közéleti személyek nevével és egyéb közismert szavakkal, kifejezésekkel.
- Ne tartalmazzon azonos, vagy ismert logika szerint egymást követő karaktereket (pl. 11111, asdfg, stb.).
- Ne utaljon a felhasználóra, munkakörére, munkahelyére.

A helyes jelszóhasználatról és az alap kritériumokról a felhasználókat – saját érdekükben – tájékoztatni kell. A jelszavak módosításának szükségességéről a rendszergazda e-mailen értesíti a munkatársakat.

15.5.2. Felhasználói hozzáférések

Azon informatikai rendszerek esetén, melyek rendelkeznek a megfelelő technikai feltételekkel, a hitelesítéshez használt felhasználói hozzáféréshez rendelt jelszavaknak az alábbi kritériumoknak kell megfelelni:

- Az utolsó 4 jelszót nem lehet újra használni.
- A felhasználói jelszavak minimális hossza 7 karakter.
- A felhasználóknak be kell jelentkezni a jelszó megváltoztatásához.
- A felhasználóknak meg kell változtatniuk a jelszavukat, amikor első alkalommal használják felhasználói azonosítójukat.
- A rendszer tagadja meg a hozzáférést 6 hibás jelszó megadása után.
- A hibás próbálkozásokat követően a rendszer 30 percre blokkolja az accountot.
- Mind a sikeres, mind a sikertelen belépési és kilépési kísérleteket naplózni kell.
- .
- Hálózatba kötött, vagy bizalmas adatok tárolására használt informatikai eszközök esetében félévente a jelszó változtatása kötelező.

A fenti követelményekről minden felhasználót tájékoztatni kell, munkájának megkezdése előtt.

15.5.3. Rendszergazdai, alkalmazásgazdai hozzáférések

Azon informatikai rendszerek esetén, melyek rendelkeznek megfelelő technikai megoldásokkal, az azonosításhoz használt **rendszergazdai** hozzáféréshez rendelt jelszavaknak az alábbi kritériumoknak kell megfelelni:

- A rendszergazdai jelszavak minimális hossza 8 karakter.
- Az utolsó 12 jelszót nem lehet újra használni.
- A rendszergazdának be kell jelentkezni a jelszó megváltoztatásához.
- Szabályozni és szűrő segítségével biztosítani kell a jelszavak összetettségét: szükséges nagybetűk, kisbetűk, számok és speciális karakterek együttes használata.
- Mind a sikeres, mind a sikertelen belépési és kilépési kísérleteket naplózni kell.
- Vészhozzáférések: a rendszergazdai hozzáféréseket a rendszerüzemeltetés számára nem ismert tartalommal, kinyomtatott formában, zárt borítékban el kell helyezni a SZIE adott szervezetének vezetője által használt tűzálló páncélszekrényben.
- Félévente a jelszó változtatása kötelező.

A **bejelentkező** névhez tartozó jelszót meg kell változtatni,

- a felhasználói név rendszerbe történt felvételét követő első bejelentkezéskor,
- ha a jelszó illetéktelen személy tudomására jutott, vagy bármilyen módon nyilvánosságra került.

A vészhozzáférést biztosító jelszavakat tartalmazó borítékok felbontását a központilag a főtitkár/informatikai igazgató, kari szinten a dékán/információbiztonsági felelős rendelheti el. A felbontásnál meg kell határozni a felbontás elrendelésének okát, és a felbontás bekövetkeztéről írásos feljegyzést kell készíteni, és értesíteni kell az információbiztonsági felelőst. A rendszergazda gondoskodik a vészhozzáférést biztosító jelszavak megváltoztatásáról és a zárt boríték páncélszekrénybe történt elhelyezéséről.

Az alkalmazói rendszerekben a jelszavak biztonságos tárolásánál az operációs rendszerek jelszó tárolási elvét kell alapul venni. A felhasználó rendszerek biztonságos jelszó tárolási mechanizmusát, módszerét a rendszergazda ellenőrzi.

15.6. Alkalmazotti munkaállomásokra vonatkozó előírások

A munkaállomások monitorait úgy kell elhelyezni, hogy a monitorokon megjelenésre kerülő adatokat illetéktelen személyek ne tudják leolvasni.

"Üres asztal – tiszta képernyő" szabály:

- A papíranyagokat és adathordozókat zárható szekrényben kell őrizni/tárolni, amikor éppen nincsenek használatban, főként a munkaidőn kívüli időszakban.
- Amennyiben sajátos információbiztonsági előírások vannak érvényben egy szervezeti egységnél, akkor a dokumentumokat azon előírások alapján kell tárolni.
- Munkaállomást csak abban az esetben szabad felügyelet nélkül hagyni, ha a munkaállomáson jelszó védelemmel rendelkező képernyő-védőt alkalmaznak, vagy a munkaállomást zárolják.

.

.

„Rendszergazda” jogosultságú felhasználóval csak az ilyen jogosultságú feladat elvégzésének idejére szabad bejelentkezni a munkaállomásra, ezután ki kell vele jelentkezni. A feladat elvégzése alatt a munkaállomást felügyelet nélkül hagyni, vagy a munkaállomáson egyéb tevékenységet folytatni szigorúan tilos.

15.7. Felhasználók bejelentkezése

A SZIE számítógépes hálózatába és rendszereibe bejelentkezni csak a rendszerben definiált bejelentkező név és a hozzátartozó jelszó ismeretében lehet.

A több felhasználós informatikai rendszerek elérésénél a felhasználók megkülönböztetésére, illetve a bizalmasság és sértetlenség megőrzésére bejelentkezési és kijelentkezési eljárásokat kell definiálni.

A bejelentkezési eljárások definiálásánál az alábbi biztonsági követelményeket kell figyelembe venni:

- Egyéni felhasználói azonosítók használata, amely felhasználóhoz köthető és az ő műveleteiért felelős.
- Ellenőrizni kell, hogy a felhasználónak van-e engedélye az informatikai rendszer, vagy alkalmazás használatára.
- A felhasználó a hozzáférési jogairól, annak változásairól kapjon írásos értesítést.
- A hozzáférés igénylés jóváhagyásáig nem lehet ideiglenes hozzáférést biztosítani.
- Listát kell tudni készíteni az alkalmazásokat használó regisztrált személyekről (vagy az alkalmazás menüjéből lekérdezhető módon, vagy külön vezetett lista segítségével).
- Biztosítani kell, hogy a feleslegessé vált felhasználói azonosítók minél hamarabb törlésre kerüljenek, és ne kerüljenek ismét felhasználásra.

15.8. Felhasználók logikai hozzáféréssel kapcsolatos kötelességei, felelősségei

A **felhasználóknak** ismerniük kell a jelszavak, illetve a felhasználó kezelésében lévő berendezések használatára vonatkozó előírásokat.

A SZIE informatikai rendszerének használatával kapcsolatos felhasználói feladatok:

- A felhasználói jelszavak titkosan kezelendők.
- A jelszó elfelejtése esetén a felhasználó a rendszergazdától vagy a jogosultság kezelő rendszergazdától igényelhet új jelszót. Az új jelszót az első bejelentkezés alkalmával kötelező megváltoztatni.
- A jelszó megválasztására vonatkozó szabályokat jelen szabályzat tartalmazza.
- A jelszót a felhasználó semmilyen körülmények között nem jelenítheti meg a különböző adathordozókon, képernyőn, papíron stb.

Szándékos jogosulatlan hozzáférés kísérlete esetén – a sikerességre vagy sikertelenségre való tekintet nélkül – a felhasználót felelősségre vonás terheli. Minden, az informatikai rendszerek hozzáférésével kapcsolatos visszaélési kísérletet jelenteni kell az információbiztonsági felelősnek.

15.9. Felügyelet nélkül hagyott alkalmazotti munkaállomások

Ha a felhasználó szünetelteti a munkaállomáson végzett tevékenységét, ki kell jelentkeznie, *vagy* zárolnia kell a számítógépet, *vagy* automatikus képernyővédőt kell alkalmazni a domain policy-ban, melynek időzített aktiválása a munkaállomás kihasználatlansága esetén nem lehet több 10 percnél. A rendszernek ez után újra kell indítania az azonosítási és a jogosultság ellenőrzési folyamatot, a felhasználó csak az újbóli bejelentkezés, illetve jelszó megadás után folytathatja a munkát.

A megnyitott alkalmazásokat, a használatot követően a felhasználónak be kell zárnia.

A felügyelet nélkül hagyott felhasználói munkaállomások védelme érdekében a munkaállomások beállításait a rendszergazdák végzik. A felhasználóknak tilos a rendszergazdák által beállított paraméterek törlése, megváltoztatása.

15.10. Belépési kísérletek korlátozása

A felhasználók és rendszergazdák pontos azonosításának megőrzésének érdekében, a felhasználói jelszavak bizalmasságát biztosítani kell. Az azonosításra fennálló 30 perces időtartam túllépése esetén

a folyamatot, lehetőség szerint, le kell állítani. Amennyiben technikailag lehetséges, biztosítani kell, hogy felhasználói azonosító hat egymást követő sikertelen bejelentkezési kísérlet után felfüggesztésre kerüljön. A felfüggesztést automatikus módon, 30 perc elteltével a rendszer is visszaállíthatja, illetve a rendszergazdák állíthatják vissza a felhasználó személyes kérésére. (Az oktatás folytonossága érdekében az oktatótermekben az oktató csak az oktatói gépen léphet be a rendszerbe.)

Az operációs rendszerhez, illetve az alkalmazói rendszerekhez való hozzáférés esetén, ahol lehet, az utolsó sikeresen bejelentkezett felhasználói azonosítónak rejtve kell maradnia.

15.11. A hozzáférés ellenőrzése

A SZIE jogosultsági rendszerét meghatározott időközönként, de legalább évente felül kell vizsgálni, melynek felelőse az információbiztonsági felelős.

Az ellenőrzések megkezdése előtt információkat kell gyűjteni:

- az egyes alkalmazások személyes biztonsági követelményeiről,
- az alkalmazások ki és bemenő adatairól,
- az adatok bizalmassági/sértetlenségi szintbe sorolásáról,
- az adott bizalmassági/sértetlenségi szinten meghatározott adatkezelésről,
- a különböző rendszerek és hálózatok összefüggéseiről,
- a vonatkozó törvényi, hatósági és szervezeti szabályozásokról, stb.

Az ellenőrzés során felmerülő feladatok:

- Felülvizsgálni a felhasználók jogosultságait, illetve jogosultság változást előidéző eseményekkor (pl.: a felhasználó kilépésekor, áthelyezésekor, új munkatárs felvételekor). A vizsgálat során figyelni kell arra, hogy a felhasználónak csak olyan alkalmazásokhoz, rendszerekhez legyen hozzáférési joga, amiket valójában használ.
- Szúrópróbaszerűen ellenőrzi, hogy a jogosultságok adminisztrációja a szabályzatban foglaltak szerint történik-e, a rendszerek felhasználására és az adatok meghatározott mértékű elérésére csak a dokumentációban rögzített személyek jogosultak.
- A vizsgálat során ki kell térni különös tekintettel a páncélszekrényben tárolt rendszergazdai jelszavak vizsgálatára is. A vizsgálatot végző ellenőr a páncélszekrényben található borítékok felbontása után meggyőződik, hogy az ott tárolt jelszavak használhatóak, valamint gondoskodik arról, hogy a vizsgálat után a rendszergazda a rendszergazdai jelszót megváltoztassa, és leellenőrzi, hogy ez nem egyezik a vizsgálat elején a borítékban talált jelszóval. A felbontott borítékokat és tartalmukat, a vizsgálatot követően meg kell semmisíteni, és a rendszergazdának gondoskodni kell arról, hogy az új jelszó elhelyezésre kerüljön a páncélszekrényben.
- A feltárt hiányosságokról jegyzőkönyvet kell készíteni, és a megfelelő eljárásokról saját hatáskörében intézkedni, valamint szükség esetén hatáskörét meghaladó eljárások megindítását kezdeményezi.

15.12. Mentés, archiválás, és visszatöltés

A dokumentum célja, hogy meghatározza a SZIE informatikai rendszerén elektronikusan tárolt adatok mentési és archiválási rend alapelveit.

A mentési rend alapelveinek célja, hogy kialakítsa azokat az eljárásokat, feladatokat és felelősségeket, amelyekkel biztosítani lehet az üzleti szempontból „fontos”, vagy annál magasabb adatosztályba sorolt adatok előírt rendelkezésre állását.

15.13. Felelősségek

15.13.1. Az információbiztonsági felelős elektronikusan tárolt adatok mentésével kapcsolatos feladatai és felelőssége:

1) Felelős a SZIE adott karának vagy intézetének mentési, archiválási rendjének kidolgozásáért.

2) Felelős a mentési, archiválási rend rendszeres ellenőrzéséért.
3) Felelős a mentési rendet érintő változások követéséért, illetve a mentési rendről szóló dokumentációk felülvizsgálatáért.
4) Felelős a mentési feladatokkal megbízott rendszergazda által jelentett incidensek kezelésére vonatkozó intézkedések foganatosításáért, illetve szükség esetén a kezeléshez szükséges erőforrások biztosításáért.
5) Felelős a helyi mentések visszatöltéssel történő ellenőrzéséért.
6) Felelős a helyi archívumban elhelyezett médiák rendszeres ellenőrzéséért.
7) Felelős a helyi mentéssel, archiválással, illetve visszatöltéssel kapcsolatos dokumentálások ellenőrzéséért.

15.13.2. A mentésért felelős rendszergazda felelőssége:

1) Felelős a kezelésére bízott informatikai rendszerben tárolt elektronikus adatok mentésének, archiválásának rendszeres, előírásszerű végrehajtásáért.
2) Felelős a mentések, archiválások végrehajtása során feltárt incidensek jelentéséért, , illetve ebben a dokumentumban meghatározott követelmények alapján az incidensek kezeléséért.
3) Felelős a mentések visszatöltéssel történő ellenőrzések végrehajtásáért.
4) Felelős az archívumban elhelyezett médiák rendszeres ellenőrzéséért, időszakonként történő átcsévéléséért, vagy átmásolásáért.
5) Felelős a mentéssel, archiválással, illetve visszatöltéssel kapcsolatos dokumentálások elvégzéséért.

15.14. Mentés irányelvei

A mentések megtervezésekor az alábbi szempontokat kell figyelembe venni:

- Minden olyan adat mentésre kerüljön, amely az adatosztályozás során „fontos”, vagy annál magasabb besorolást kapott.
- Minden mentésnek biztosítani kell az adatok kezeléséhez szükséges szoftverkörnyezet következetes helyreállíthatóságát (operációs rendszer, adatbázis-kezelő, stb.).
- Minden olyan adat mentésre kerüljön, amely az auditálás, ellenőrzés eszköze lehet (naplófájlok, riportok, stb.).
- Minden olyan eszköz konfigurációja mentésre kerüljön, amely részt vesz „fontos”, vagy annál magasabb besorolású adat kezelésében (tárolásában, továbbításában, stb. pl.: hálózati aktív eszközök).
- Minden mentés alkalmas legyen olyan környezet helyreállítására, mely lehetővé teszi valamely igazolható állapothoz való visszatérést.
- A kritikus rendszerek mentése legalább két példányban készüljön, a két példányt elkülönítetten kell tárolni

15.14.1. A mentések tartalma

Szerverek mentése

A szerverek mentését a mentendő eszközök listáját, a mentési eljárást (mentés gyakorisága, típusa) a mentendő állományok specifikációját (image, tároló területek, fájlok, adatbázisok, konfigurációs fájlok, rendszer területek, jelszó fájlok, profil fájlok, stb.) a mentések időpontját és gyakoriságát a ”***Mentési Rend”*** tartalmazza.

Adatkommunikációs eszközök mentése

Az adatkommunikációs eszközök mentését az alábbi esetekben kell elvégezni

- Új eszköz rendszerbeállítása esetén,
- Az adatkommunikációs eszközök konfigurációjában történő bármilyen változás esetén.
- Félévente egy alkalommal

Mentendő állományok:

Router, Tűzfal, Switch esetében: az NVRAM-ban található startup-config file,

Az adatkommunikációs eszközök konfigurációit a kijelölt szerveren a rendszergazdai könyvtárba kell lementeni, valamint a lementett konfigurációs fájlok archiválását legalább 6 havonta, a gyors visszaállíthatóság érdekében külső adathordozóra is kell elvégezni.

15.15. Az archiválások rendje

Archiválásnak nevezik azt, amikor a rendszerből az adatok kikerülnek és csak az adathordozón léteznek tovább.

15.15.1. Kiszolgálók archiválásának rendje

Archiválást kell biztosítani az alábbi állományikra:

- Fájlszerveren tárolt fájlok dokumentumok, melyeket régóta nem használnak, jelentős tárterületet foglalnak és a felhasználó, vagy az adatgazda kéri az archiválást.
- A felhasználók postaládájában található régi levelek, amelyek a méretkorlátozások miatt akadályozzák a kommunikációt, és a felhasználó kéri az archiválást.

Az archiválások által keletkezett adathordozók tárolását jelen szabályzatnak megfelelően kell tárolni, illetve dokumentálni.

15.15.2. Az egyéni archiválások igénylésének rendje

Ha az információk rendelkezésre állási követelményei miatt szükséges, vagy a központi archiválási eljárásban nem szerepel, a felhasználó kérheti adatainak renden kívüli archiválását.

Az archiválási igényeket az informatikai igazgatónak kell benyújtani. A mentésre adatokat tartalmazó média tárolásáról, megőrzéséről a felhasználó gondoskodik.

Amennyiben a felhasználó jogosan igényel, vagy eleve rendelkezik archiválási eszközzel saját munkaállomásán, úgy a helyi informatikai szervezet segítséget nyújt a helyes archiválási eszköz kiválasztásához, elvégzi annak installálását és segíti a felhasználót az archiválás elsajátításában.

15.16. A mentések visszatöltése

15.16.1. A mentések visszatöltése ellenőrzési céllal

A mentési médiákat a mentési eljárás sikeres lefutásától függetlenül a ***"Mentési rend***'-ben előre meghatározott terv alapján szúrópróba-szerűen minimum félévente minden mentési feladat esetén, és évente az archív mentések esetében ellenőrizni kell. Az ellenőrzés lefolytatása az alábbi feladatok végrehajtását jelentik:

- Média kiválasztása (véletlenszemen)
- Visszatöltés teszt-célú rendszerbe átmeneti helyre
- A sikeresség ellenőrzése mintavételezéses eljárással
- Média visszahelyezése, teszt elvégzésének dokumentálása

Az ellenőrzések lefolytatását, dokumentálását a mentésért felelős rendszergazda hajtja végre. Az információbiztonsági felelős évente egy alkalommal ellenőrzi a visszatöltések dokumentáltságát.

15.16.2. Mentések visszatöltése visszaállítási céllal

Az adatok visszatöltési idejét az adatok rendelkezésre állása szerinti osztályba sorolásnak védelmi követelményei alapján kell meghatározni.

Az adatok visszatöltését a katasztrófa vagy más létező vészhelyzeti tervek aktualizálása esetén, az abban foglaltak szerint kell végrehajtani.

Egyéb esetben adatok visszatöltését az illetékes munkahelyi vezető kérheti a helyi informatikai vezetőtől.

A visszaállítás tényét a visszatöltést végző rendszergazdának dokumentálni kell.

15.17. Mentési médiák kezelése

15.17.1. Cserélhető mentési médiák használatba vétele

Az adathordozót használatba vétel előtt külsőleg is fel kell címkézni. A címkén kötelező jelleggel szerepelnie kell – választott ciklikus mentési rendnek megfelelő – a sorozat és napi azonosítónak. A mentési folyamatokban a szalag belső elektronikus azonosítója használható.

15.17.2. Mentési médiák tárolása

Munkapéldányok tárolása

A napi és heti mentések egyes számú példányait a gépteremben vagy az informatikusi szobában elhelyezett tűzbiztos dobozban kell tárolni, hogy szükség esetén a hozzáférés azonnal biztosítható legyen.

Biztonsági másolatok tárolása

A biztonsági mentési kazettákat a jelen szabályzatban előírt módon, biztonsági besorolásától függően tűzbiztos dobozban vagy tűzálló páncélszekrényben kell tárolni. A másolat elhelyezéséért a mentésért felelős rendszergazda a felelős.

Archív mentések tárolása

A biztonsági mentési kazettákat a jelen szabályzatban előírt módon, biztonsági besorolásától függően tűzbiztos dobozban vagy tűzálló páncélszekrényben kell tárolni. Az archívum elhelyezéséért az archiválást kérő szervezeti egység adatgazdája a felelős. A hozzáférésükről naplót kell vezetni.

15.17.3. Mentések, archiválások dokumentálása

A mentések végrehajtását mentési naplóban (automatikusan készül, vagy egyedileg vezetett) kell rögzíteni. Ha külön szabályozás nincsen a mentési rendre, akkor a naplónak a következőket kell tartalmaznia:

1) Szervezeti egység megnevezése
2) Rendszer megnevezése
3) Mentés azonosítója
4) Mentés ideje
5) Mentés tartalma
6) Mentés végrehajtója és aláírása
7) Mentés státusza (sikeres, sikertelen)

A mentési napló ellenőrzését az információbiztonsági felelős végzi.

A mentési médiák rotálására, selejtezésére illetve megsemmisítésére vonatkozó táblázatokat a ***4. számú melléklet*** tartalmazza.

16. VÉDELMI INTÉZKEDÉSEK

16.1. Hardver eszközök fizikai hozzáférése

16.1.1. Szerverek fizikai hozzáférése

A SZIE szervereit az erre a célra kialakított szerverszobákban kell elhelyezni. A szerverszoba kialakítási, és hozzáférési követelményeiről jelen szabályzat ***2. számú melléklete*** rendelkezik.

16.1.2. Munkaállomások fizikai hozzáférése

A munkaállomások elhelyezési követelményeiről, fizikai védelméről jelen szabályzat rendelkezik.

Felhasználóknak tilos a munkaállomás hardver konfigurációját megváltoztatni, a hardver eszköz belsejébe bármilyen okból belenyúlni, burkolatukat megbontani. A csatlakozó külső perifériák csatlakozását megszüntetni.

A munkaállomásokat az üzembe helyezés alkalmával zárjeggyel lehet ellátni annak érdekében, hogy meg lehessen állapítani, ha a hardver eszköz konfigurációját valaki megbontotta.

Az irodán belül a munkaállomást úgy kell elhelyezni, hogy a normál munkavégzés során biztosítva legyen, hogy a munkaállomás képernyőjét csak annak használója láthassa.

16.1.3. Nyomtatók fizikai hozzáférése

A SZIE nyomtatóit úgy kell elhelyezni, hogy a kinyomtatott anyagok illetéktelen kezekbe ne kerülhessenek.

Ennek érdekében:

- A megosztott nyomtatókat úgy kell elhelyezni, hogy az állandó felügyelet, vagy a hozzáférés egyedisége és naplózása biztosított legyen. Elszeparált „nyomtatóhelység” használata tilos!
- A megosztott nyomtatókon „Belső használatra”vagy „Bizalmas”, illetve annál magasabb minősítésű információt csak abban az esetben szabad nyomtatni, ha a nyomtatóhoz hozzáférő valamennyi személynek az ilyen információkba betekintési joga van.
- Azokat a nyomtatókat, amelyeken „Titkos” anyagok nyomtatása történik, névhez kell kötni, és a munkaállomás közvetlen környezetében, ahhoz közvetlen módon csatlakoztatva (soros, párhuzamos vagy USB port) kell elhelyezni.

16.2. Hálózati eszközök fizikai hozzáférése

A hálózati eszközöket úgy kell elhelyezni, hogy az illegális tevékenységből adódó kockázatok minimálisak legyenek.

Ennek érdekében az alábbi elhelyezési körülmények közül kell választani:

- Központi rendezés esetén a szerverszobában
- Osztott rendezés esetén zárható, vagy felügyelhető helyiségben, illetve zárt rack- szekrényben.

16.3. Hardver eszközök fizikai biztonsága

A hardver eszközök fizikai biztonságának biztosítása érdekében minimálisan az alábbi védelmeket kell kialakítani:

- **Tűzvédelem:** A tűzvédelmi szabályzatban kell kitérni az egyes biztonsági zónák tűzvédelmi minősítéséről, és tűzvédelmi megoldásairól.
- **Villámvédelem:** A SZIE épületeit villámvédelemmel kell ellátni, melyeket rendszeresen felül kell vizsgáltatni.
- **Túlfeszültség-védelem:** Túlfeszültség-védelmet kell telepíteni azoknak az eszközöknek a betáplálásához, amelyek kritikusak a meghibásodás szempontjából (szerverek, aktív eszközök, stb.)

A fentieken túl biztosítani kell, hogy a hardver eszközök közelében ne folyjon olyan tevékenység, amely veszélyeztetheti az eszköz működőképességét. Tilos az alábbi tevékenységek folytatása:

- A hardver eszközökön tilos tárolni olyan anyagokat, amelyek veszélyeztethetik a hardver eszközt (virág, élelmiszer, ital, mágneses tárgyak, stb.)
- Tilos a hardver eszközök közvetlen környezetében étkezni, és bármilyen italt fogyasztani.

16.4. Hardver eszközök üzemeltetési környezetének paraméterei

A hardver eszközök üzemeltetése során figyelembe kell venni a hardver gyártójának üzemeltetésre vonatkozó előírásait.

Általában az alábbi környezeti feltételeket kell biztosítani a hardver eszközök számára:

- A munkaállomások üzemeltetési hőmérséklet tartomány 15 Celsius foktól 35 Celsius fokig terjedjen. Szerverek esetében ez az érték 21 Celsius környékén stabilizált (klíma). Kerülni kell a hirtelen hőmérsékletváltozást, ügyelni kell a fokozatosságra.
- A hardver eszközöket óvni kell a fröccsenő víztől, illetve a levegő magas portartalmától.
- A hardver eszközöket óvni kell az erős mágneses, vagy elektromágneses tértől.
- A hardver eszközök számára biztosítani kell a gyári specifikációban előírt betáplálást. Ez hazánkban 230 V / 60 Hz.

A fenti követelményeknek való megfelelésért a szerverszobában elhelyezett eszközök esetén az eszközök üzembe helyezéséért felelős rendszergazda, munkaállomások esetében a felhasználó felelősek.

16.5. Hardver eszközök teljesítmény-, és kapacitásmenedzsmentje

A hardver eszközök előírt rendelkezésre állási követelményeknek való megfelelősége érdekében a kiszolgáló hardver eszközök teljesítményét, és egyéb kapacitását (pl.: tároló kapacitás, memória kapacitás, processzor teljesítmény, nyomtató kapacitás, stb.) rendszeresen monitorozni kell.

A tapasztalatok alapján eszközönként meg kell határozni azokat a teljesítmény és kapacitás korlátokat, amelyek elérése esetén a hardver eszközök fejlesztése szükséges.

A kapacitástervezésnél figyelembe kell venni azokat az időkorlátokat is, amelyek az eszközök fejlesztéséhez szükséges beszerzésekhez szükséges.

A kapacitás menedzsment végrehajtásáért az adott hardver eszköz üzemeltetéséért felelős rendszergazda felelős.

16.6. Hardver eszközök rendeltetésszerű használata

A munkaállomások rendeltetésszerű használatához az alábbiakat kell figyelembe venni:

- A munkaállomás be-, és kikapcsolásához a hardver eszköz erre a célra kialakított kapcsolóját kell használni. Lehetőség szerint a kikapcsolásra az operációs rendszer kikapcsolás funkcióját kell használni.
- Az adatvesztés elkerülése érdekében a munkaállomás kikapcsolását kerülni kell, amikor az, lemezműveletet végez (munkaállomás indítása, fájlhozzáférés, stb.)
- Ha a munkaállomás a művelet végzése közben „lefagy” elsősorban az újraindítással kell próbálkozni (Ctr+Alt+Del többszöri próbálkozása), kikapcsolás akkor kell kezdeményezni, ha az újraindítás sikertelen volt.
- A perifériákat (billentyűzet, egér, nyomtató, stb.) csak kikapcsolt állapotban szabad a munkaállomáshoz csatlakoztatni, vagy onnan leválasztani (kivéve USB eszközök).
- A munkaállomás adatbeviteli egységeibe csak szabványos a munkaállomáshoz illeszkedő adathordozókat szabad behelyezni.

16.7. Hardver eszközök kezelési rendjével kapcsolatos óvintézkedések

16.7.1. Hardver eszközök üzembe helyezése

A hardver eszközök üzembe helyezését csak az informatikai üzemeltetés munkatársai végezhetik. A felhasználóknak tilos az üzembe helyezéssel kapcsolatos bármilyen tevékenységet (telepítés, installálás) folytatni.

Az informatikai eszközöket az üzembe helyezés során aláírással ellátott zárcímkével lehet ellátni. A felhasználóknak a zárcímkét tilos eltávolítani, vagy megrongálni.

16.7.2. Hardver eszközök cseréje, módosítása

A felhasználóknak tilos a hardver eszközök konfigurációjának megváltoztatása. Erre csak az informatikai üzemeltetés kijelölt munkatársai jogosultak.

A felhasználók nem csatlakoztathatnak idegen, vagy magántulajdonú perifériákat a munkaállomásaikhoz.

16.7.3. Hardver eszközök javítása, karbantartása

A hardver eszközök rendelkezésre állási követelményeinek való megfelelés érdekében „***Karbantartási tervben***” tervszerű megelőző karbantartási, valamint javítási eljárást kell kialakítani.

A hardver eszközök karbantartására évente „***Karbantartási tervet***” kell készíteni. A tervben szerepeltetni kell minden eszközt (vagy eszközcsoportot), amelynek karbantartásával számolni kell.

A karbantartási tervben minimálisan szerepelnie kell az alábbi eszközcsoportoknak:

- Szerverszoba klíma berendezései
- Szerverek
- Hálózati aktív és passzív eszközök
- UPS-ek
- Központi nyomtatók

A hardver eszközök javításával, karbantartásával kapcsolatos szerződésekben szerepeltetni kell azokat a rendelkezésre állási követelményeket, amelyek az eszköz által kezelt adatok minősítési osztálya megkövetel.

A rendelkezésre állási követelményeknek ki kell térnie:

- A cég szakembereinek rendelkezésre állásának meghatározására
- A karbantartás, vagy javítás tárgyát képező eszközök rendelkezésre állási követelményeinek meghatározására

A karbantartási, javítási szerződésekben ki kell térni a titoktartás felelősségekre, vagy a már meglévő szerződéseket ún. „Titoktartási nyilatkozatot kell kiegészíteni.

A fenti karbantartási, javítási feladatok végrehajtásáért a helyi informatikai vezető a felelős.

A felhasználók szükség esetén az alábbi karbantartásokat végezhetik:

- Monitor képernyőjének tisztítása arra alkalmas tisztító eszközökkel.
- A billentyűzet tisztítása, portalanítása alkalmas tisztító eszközökkel.
- Az egér tisztítása alkalmas tisztító eszközökkel.

16.7.4. Hardver eszközök tárolása

A használaton kívüli hardver eszközöket raktáron kell tárolni. A raktári tárolás közben is biztosítani kell a gyári specifikációban előírt tárolási környezeti paramétereket. A szerverhelységeket tilos raktárként használni.

A raktári eszközök esetén biztosítani kell az eszközök fizikai védelmét.

16.7.5. Hardver eszközök szállítása

A hardverek eszközök szállítása közben biztosítani kell:

- A munkavédelmi törvények betartását
- A hardverek fizikai védelmét
- A káros környezeti hatásoktól való védelmet (hősugárzás, erős sztatikus kisülés, mágneses tér, folyadék, stb.)

A hardver eszközök szállítása közben biztosítani kell a folyamatos felügyeletet.

16.7.6. Hardver eszközök selejtezése, megsemmisítése, továbbértékesítése

A hardver eszközök selejtezése, megsemmisítése, vagy továbbértékesítése előtt a hardver eszköz adathordozóját visszaállíthatatlanul törölni kell.

A törlési eljárás kiválasztásáról és végrehajtásáról a rendszergazda gondoskodik. Minden más tevékenységet a jelen szabályzatban megfogalmazottak, illetve az érvényben levő selejtezési eljárás szerint kell lefolytatni.

16.7.7. Hardver eszközök nyilvántartása

A törvényben előírt analitikus nyilvántartáson (Leltár) kívül a hardver eszközök nyilvántartására az alábbi nyilvántartást kell vezetni:

- Szerverek legalább domain béli névvel és IP címmel való azonosítása
- Hálózati eszközök legalább IP-címmel (külső- és belső interfész egyaránt ha mindkettő van) való azonosítása
- Raktárnyilvántartások
- Eszközkiadási bizonylatok
- Szállítólevél

A szerverhelységekben és rack-szekrényekben elhelyezett szervereket és hálózati aktív eszközöket, az azonosítás megkönnyítése végett fel kell címkézni. A címkéken minimálisan a következő információkat kell feltüntetni:

- Szerverek esetében domain béli név és IP cím
- Hálózati eszközök esetében a külső- (és belső) interfész IP-címmel való azonosítása.

17. A MOBIL ESZKÖZÖK KEZELÉSI RENDJE

17.1. Mobil eszközök kezelése

17.1.1. A hordozható eszközök használatba adása-vétele

A hordozható számítógépek és eszközök (notebook, PDA, stb.) szoftvereit, operációs rendszerét az üzemeltetésért felelős helyi informatikai szervezet, kijelölt rendszergazdái telepítik az előre kidolgozott szabványos eljárás és paraméterezés szerint.

Ugyancsak az üzemeltetésért felelős szervezet jogosult az alkalmazói szoftverek telepítésére, verziófrissítésre, a beállítások megváltoztatására.

Használatba adás előtt az alábbi védelmi eszközöket kell telepíteni, konfigurálni:

1) Helyi biztonsági házirend
2) Vírusvédelmi szoftver
3) Személyi tűzfal

4) Szükség esetén titkosító szoftvert és/vagy hardver megoldás

A felhasználónak a használatba vétel során ellenőrizni kell:

1) A mobil eszköz és tartozékainak meglétét.
2) A telepített védelmi eszközök meglétét (vírusvédelmi eszköz, személyi tűzfal)

Az átadás-átvétel tényét dokumentálni kell.

17.1.2. A hordozható eszközök használata

A hordozható eszközök konfigurációjának, beállításainak, paramétereinek megváltoztatására kizárólag az üzemeltetésért felelős szervezet kijelölt rendszergazdája jogosult.

Amennyiben az eszköz hosszabb ideig (1-2 hét) nem csatlakozik a helyi hálózathoz, a vírusvédelmi szoftver szignatúrájának frissítését a felhasználónak kell megoldani. Ehhez szakmai segítséget a helyi rendszergazdától kaphat.

A felhasználó köteles a hordozható eszközt a hivatali munkával kapcsolatos feladatokra, rendeltetésszerűen használni.

A mobil eszközön tilos a „Titkos” minősítésű, valamint magánjellegű adatok tárolása, feldolgozása.,.

A szükséges frissítések, illetve konfigurációs változtatások végrehajtására, legalább havi rendszerességgel, az üzemeltetésért felelős helyi informatikai szervezet kérésére a felhasználó köteles a hordozható eszközt a beavatkozás idejére. biztosítani.

17.1.3. Az eszköz tárolása

A SZIE-ben hordozható eszközöket használaton kívül zárható szekrényben kell tárolni, amelyhez a mobil eszköz használójának kizárólagos joga van.

17.1.4. A hordozható személyi számítógépek épületéből való kivitele

A hordozható eszközök az arra jogosultak mobilitását szolgálják, így az épületből való kivitelhez külön engedély nem szükséges.

17.2. Mobil eszközök védelmi előírásai

17.2.1. Mobil eszközök fizikai védelme

A hordozható eszközök mobilitásuknál fogva fokozott veszélynek vannak kitéve a fizikai biztonságukkal kapcsolatos fenyegetettségekkel szemben. A hordozható eszközök fizikai biztonsága érdekében az alábbi szabályokat kell betartani:

A mobil eszközöket csak az arra rendszeresített vízlepergetős, bélelt táskában szabad szállítani. A szállítás során biztosítani kell, hogy az eszköz ne legyen kitéve erős rázásnak, vagy ütésnek. A mobil eszközt tilos felügyelet nélkül hagyni.

Repülőn, autóbuszon, vagy vasúton történő szállítás esetén a hordozható eszközöket kézipoggyászként kell szállítani. A folyamatos felügyeletet ez alatt is biztosítani kell.

A hordozható eszközöket általában tilos kitenni:

1) Erős fizikai behatásnak
2) Sugárzó hőnek
3) Erős mágneses, vagy elektromágneses térnek
4) Fröccsenő víznek
5) Poros környezetnek

A perifériákba csak szabványos adathordozók használhatók.

A megjelenítő eszköz fokozottan érzékeny a fizikai behatásoknak, ezért annak tisztítását csak erre a célra alkalmas törlőkendőkkel, és tisztítóanyagokkal szabad elvégezni.

17.2.2. Mobil eszközökön tárolt adatok védelme

Titkosítás

A hordozható eszközökön külön engedéllyel tárolt a „Titkos” minősítésű adatok védelmére hardveres és/vagy szoftveres titkosító eszközök használata szükséges.

Ebben az esetben a titkosító kulcsokat külső eszközön kell tárolni (PEN drive, SmartCard, Security Key, stb.). A titkosító kulcsokat tartalmazó eszközt a hordozható eszköztől külön kell kezelni (tárolni, szállítani, stb.).

Teendő, ha a számítógépet eltulajdonították

Amennyiben a számítógépet eltulajdonították, az alábbiakat kell tenni:

- Értesíteni kell a rendőrséget, aki kiállítja a bejelentésről szóló jegyzőkönyvet. Értesíteni kell az információbiztonsági felelőst, illetve a helyi rendszergazdát, aki intézkedik a felhasználó jelszavának megváltoztatására.
- Az információbiztonsági felelős illetve a helyi rendszergazda intézkedik az esemény kivizsgálására annak érdekében, hogy megállapítható legyen a felhasználó esetleges felelőssége.
- Ha a rendőrségi nyomozás nem jut eredményre a nyomozás befejezéséről szóló jegyzőkönyvet, és a bejelentésről szóló jegyzőkönyvet át kell adni az adott szervezet gazdasági vezetőjének.

17.3. Távoli hozzáférések, távmunka

17.3.1. Hozzáférések szabályozása

A távoli hozzáféréseket illetve távmunkával kapcsolatos jogosultság kezelését a jelen szabályzatban leírt módon kell végrehajtani.

Eszközök hálózatra csatlakoztatása

Távoli hozzáférés a SZIE Internet kapcsolatain az Internet kapcsolaton keresztül üzemeltetett biztonságos virtuális magánhálózat kialakításával (VPN).

A kifejezetten belső használatra konfigurált hordozható eszközök nem csatlakoztathatók idegen hálózatra.

17.3.2. A távoli munkavégzés szabályai

A távoli elérés csak működő személyi tűzfal, illetve vírusvédelmi szoftver mellett kezdeményezhető.

A távoli elérés alatt tilos más - nem az aktuális munkával kapcsolatos - tevékenységek folytatása.

A távoli elérés alatt használt erőforrásokat csak szükséges időtartamra szabad foglalni. A nem használt hozzáféréseket be kell zárni.

17.4. Mobil eszközök vezeték nélküli hozzáférése

A belső ügyviteli hálózatra kapcsolódó vezeték nélküli hozzáféréséhez a SZIE szabványos (wifi) vezeték nélküli hozzáférést biztosít kizárólag alkalmazottai számára, SZIE tulajdonban levő mobil eszközökhöz. Vezeték nélküli kapcsolódás esetén gondoskodni kell az illetéktelen használat, megelőzéséről az alábbi előírások egyidejű betartásával:

- WPA Enterprise (vagy ennél erősebb, illetve hatékonyabb) titkosítással,
- amennyiben az eszköz nem alkalmas WPA Enterprise kommunikációra: MAC address szűréssel,
- a broadcast tiltása (amennyiben a hozzáférési ponton ez konfigurálható).

Kivételt képez konkrét eseményhez (pl. konferencia) kötötten az informatikai igazgató engedélyével.

17.5. Ellenőrzések

A mobil eszközök használata szabályainak betartását a helyi rendszergazda rendszeresen ellenőrzi.

A távoli hozzáféréseket naplózni kell, a log-állományokat rendszeresen elemezni, és kiértékelni szükséges.

18. A SZOFTVEREKHEZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEKNEK

18.1. Szoftverek erőforráskönyvtárainak védelme

A SZIE-nél használt szoftverek védelmének érdekében a szoftverek erőforráskönyvtárait védeni kell az illetéktelen hozzáférésektől az illetéktelen installációtól és az abban található fájlok nem rendeltetésből adódó megváltoztatásától.

18.2. Szoftverek nem használt funkcióinak tiltása

A SZIE-nél használt szoftverek védelmének érdekében a szoftverek (különösen az operációs rendszer) nem használt funkcióit, szolgáltatásait (szervizeit) le kell tiltani.

Az operációs rendszerek nem használt távdiagnosztikai portjait szintén le kell tiltani, hogy csökkentsük a távoli elérésből származó kockázatokat.

18.3. Szoftverek biztonsági frissítése

A helyi rendszergazdának rendszeresen figyelni kell a megjelenő sérülékenységekről szóló jelentéseket

Ki kell dolgozni a SZIE-ben használt szoftverek biztonsági frissítésével kapcsolatos:

- Letöltési folyamatokat
- Disztribúciós folyamatokat
- Tesztelési folyamatokat
- Implementációs folyamatokat

A biztonsági frissítéseket, a megjelenésüket követően a lehető legrövidebb idő alatt kell telepíteni.

18.4. „Dobozos” szoftverek tárolása

A „dobozos” szoftvereket a helyi informatikai rendszer üzemeltetéséért felelős szervezeti egység, központi helyen kell tárolni. A rendszertelepítésekhez lehetőleg az eredeti példányról készült másolatot kell használni.

Egy időben maximálisan egy másolt példány létezhet.

18.5. Szoftverek nyilvántartása

A SZIE-nél használt szoftverekre és szoftver licencekre nyilvántartást - a tárgyi eszköz nyilvántartásától függetlenül - kell vezetni. A nyilvántartások vezetéséért a helyi informatikai vezető felelős.

A nyilvántartás tartalmazza:

- A szoftver pontos megnevezését
- A szoftver verziószámát
- Nyelvi verzióját
- A szoftver regisztrációs kódját (nem azonos az installációs kóddal)
- A szoftverhez tartozó licence szerződés számát
- A licenc jellegét vagy típusát
- A szoftver licence hány telepítésre ad lehetőséget (felhasználó szám)

- A beszerzés idejét
- A szállító nevét

A szoftverek informatikai nyilvántartásánál figyelembe kell venni a mindenkor érvényben lévő számviteli törvény előírásait, a BSA (Business Software Alliance) ajánlásait. Az informatikai szoftver nyilvántartásának összhangban kell lennie az ügyviteli rendszerek (tárgyi eszköz) nyilvántartásával.

19. A KOMMUNIKÁCIÓHOZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEK

19.1. Az elektronikus levelezés biztonsága

19.1.1. Az elektronikus levelezés biztonsági követelményei

Az elektronikus levelezés a SZIE informatikai rendszerében az egyik fő fenyegetettség forrása. Az elektronikus levelezés biztonsága érdekében az alábbi előírásokat kell betartani:

Az elektronikus levelezéssel kapcsolatos tiltórendelkezések az alábbiak:

- Szigorúan tilos a közízlést, a SZIE jó hírnevét veszélyeztető, erkölcstelen, vagy politikai tartalmú e-mail elküldése.
- Tilos a levelező rendszert „Titkos” minősítésű fájlok, dokumentumok kijuttatására használni.
- Tilos a SZIE hivatalos ügyeket nem egyetemi levélcímen intézni. Tilos olyan levelek továbbítása a SZIE levelező rendszerében, amelyek bármilyen nyelven arra szólítanak fel, hogy a levelet minél több címre kell továbbítani (lánclevél).
- Tilos feliratkozni nem szakmai jellegű illetve nem az ügyviteli vagy oktatási munkát segítő hírlevél küldő szolgáltatásra.
- Tilos válaszolni olyan levelekre, amelyek arra szólítanak fel, hogy a SZIE biztonsági rendszeréről, vagy a felhasználó saját hozzáférési adatairól (felhasználónév, jelszó) adjon tájékoztatást.
- Tilos az elektronikus levelező rendszeren „Titkos”, információt titkosítás nélkül továbbítani.
- A levélszűrésen fennakadt levelekről automatikus üzenet csak a SZIE alkalmazottjának küldhető. Ezzel kapcsolatos automatikus üzenet küldése a SZIE-en kívülre tilos.

19.1.2. Az elektronikus levelezés korlátozásai

Az elektronikus levelezés biztonsága érdekében az alábbi korlátozások vannak érvényben:

A dolgozói postafiók mérete általában: 1Gb, a hallgatói fiók 100Mb. Szükség esetén ettől eltérő kapacitást az informatikai igazgató engedélyezhet, de ennek mérete sem haladhatja meg a 8Gb-ot.

A fogadható és küldhető levelek maximális megengedett mérete általában: 20 Mb.

19.1.3. Elektronikus levelezés magáncélú használata

Mivel minden levelezést a SZIE tulajdonát képező infrastruktúra és erőforrások biztosítanak, ezért a magán célú levelezésre a SZIE által biztosított postafiók nem használható.A fentieken túl kerülni kell az Interneten található ingyenes levelezési portálok belülről történő használatát.

19.1.4. Elektronikus levelezés jogosultsága

A SZIE valamennyi aktív jogviszonnyal rendelkező alkalmazottja és hallgatója hozzáférést kap az elektronikus levelezési rendszerhez.

19.1.5. Elektronikus levelezés ellenőrzése

A SZIE fenntartja a jogot a levelezés méretének, gyakoriságának, korlátozására a levelező szerver és az Internet csatlakozás kapacitásának hatékonyabb kihasználása, valamint a SZIE informatikai rendszerének biztonsága érdekében.

19.2. Az internet biztonsága

19.2.1. Az Internet hozzáférés biztonsági előírásai

Az Internet hozzáférés a SZIE informatikai rendszerében az egyik fő fenyegetettség forrása. Az Internet hozzáférés biztonsága érdekében az alábbi előírásokat kell betartani:

Az Internet hozzáférést csak az ügyviteli folyamatokkal, illetve azok támogatásával kapcsolatos ügyintézésre, szabad használni.

Az Internet böngésző beállításaiban tilos az Internet zóna biztonsági szintjét közepesnél alacsonyabbra állítani.

Az Internetezés közben el kell utasítani azokat a felbukkanó párbeszéd ablakokat, amelyek segédprogramok telepítésére, vagy egyes funkciók kikapcsolására ösztönöznek.

Tilos az Internetes web helyek eléréshez szükséges jelszavakat úgy megválasztani, hogy abból a SZIE-nél használt jelszóra következtetni lehessen. Erről a felhasználót tájékoztatni kell.

19.3. Korlátozások az Internet használatában

19.3.1. Tiltott Internetes alkalmazások

A SZIE-nél csak a rendszeresített Internetes alkalmazások használhatók

A SZIE-nél a felhasználóknak szigorúan tilos olyan internetes alkalmazások használata:

1) Melyekkel a SZIE, vagy más személyek információinak, alkalmazásainak bizalmasságának, sértetlenségének, rendelkezésre állásának megsértésére irányul.
2) Melyekkel a SZIE erőforrásainak illegális megosztására irányul.
3) Melyek licenc szerződéseivel a SZIE nem rendelkezik.

19.3.2. Tiltott Web helyek

Szigorúan tilos a SZIE érdekeit sértő, erkölcstelen oldalak látogatása, bővebb szabályozást a SZIE Informatikai Szabályzat tartalmaz, amely hivatkozik a Nemzeti Információs Infrastruktúra Fejlesztési Program Felhasználói Szabályzatára (http://www.niif.hu/niif_intezet/aup).

19.3.3. Tiltott Internetes tevékenységek

Szigorúan tilos internetes illegális tevékenységek folytatása, amelyek más jogi személyek adatainak, alkalmazásainak bizalmasságát, sértetlenségét, vagy rendelkezésre állását sértheti (hack, crack, flood, stb.).

Szigorúan tilos minden, a közízlést sértő, erkölcstelenállomány letöltése. Bővebb szabályozást a SZIE Informatikai Szabályzat tartalmaz, mely hivatkozik a Nemzeti Információs Infrastruktúra Fejlesztési Program Felhasználói Szabályzatára (http://www.niif.hu/niif_intezet/aup).

A SZIE fenntartja a jogot, hogy biztonsági okokból technikai szűréseket és korlátozások rendeljen el az informatikai igazgató által.

19.4. Az Internet hallgatói hozzáférése vezetékes illetve vezeték nélküli módon

A SZIE a tanulmányi és ehhez kapcsolódó adminisztrációs feladatok ellátásához az NIIF hálózaton keresztül, Internet hozzáférést biztosít a hallgatói számára. Az Internet hozzáférés az alábbi három módon biztosított:

1) Hallgatói géptermekben, a SZIE tulajdonában levő hardver eszközök használatával.
2) Kollégiumi fizikai port csatlakozás biztosításával, amelyen keresztül a hallgatói eszközök csatlakoztathatók.
3) A SZIE területén felszerelt vezeték nélküli hozzáférési pontok segítségével (Wifi), amelyen keresztül hallgatói mobil eszközök csatlakoztathatóak.

A hozzáférést minden hallgatói jogviszonnyal rendelkező, a Tanulmányi Hivatal által regisztrált hallgató automatikusan megkapja.

A központi azonosítást használó hallgatói géptermekben való géphasználat illetve Internet hozzáférés a hallgatói nyilvántartásba vételt és a hallgatói account (felhasználói név és jelszó) kiadását követően minden további nélkül használható.

A hallgatói mobil eszközök csatlakoztatására és az Internet eléréséhez a SZIE wifi elérést biztosít az egyetem közösségi területein.

19.5. Az Internet hozzáférések ellenőrzése

A SZIE fenntartja a jogot az Internetezés gyakoriságának, és ha szükséges tartalmának ellenőrzésére, korlátozására az Internet csatlakozás kapacitásának hatékonyabb kihasználása, valamint a SZIE informatikai rendszerének biztonsága érdekében.

19.6. A Nemzeti Információs Infrastruktúra fejlesztési Intézet (NIIF) előírásai

A SZIE informatikai rendszere több ponton kapacsolódik a NIIF tagintézmények és felhasználók számára üzemeltetett hálózati infrastruktúrához és szolgáltatásainak egy részét ezen keresztül biztosítja. Ebből következően minden SZIE felhasználó egyben NIIF felhasználó is. így minden SZIE felhasználó köteles betartani a NIIF működtetéséről szóló 95/1999. (VI. 23.) Kormányrendeletben (a továbbiakban Kormányrendelet) meghatározott, az NIIF keretében működtetett számítógép-hálózat használati szabályait (a továbbiakban NIIF Szabályzat).

Az NIIF hálózat használati szabályzat teljes szövege megtalálható az Informatikai és Hírközlési Közlönyben illetve az IHM és a NIIF (http://www.niif.hu/aup) internetes honlapján. Kivonatolt formájában a SZIE Informatikai Szabályzatban olvasható.

20. ZÁRÓ RENDELKEZÉSEK

A szabályzat által hivatkozott biztonsági dokumentumokat a hatálybalépéstől számított folyamatosan kell kidolgozni és a folyamatokba beilleszteni.

Jelen szabályzatot elfogadta a Szenátus 30/2012/2013 SZT számú határozatával a 2012. október 24. napi ülésén.

Gödöllő, 2012. október 24.

Dr. Solti László
rektor

1. SZÁMÚ MELLÉKLET: AZ ADATOK MINŐSÍTÉSÉNEK ÉS KEZELÉSÉNEK RENDJE

Az adatok osztályozása

A bizalmasság, sértetlenség, és rendelkezésre állás sérüléséből, vagy elvesztéséből vagyoni, erkölcsi, és jogi hátrány származhat. Az egyes kritikusnak tetsző vagy annak tapasztalt vagyontárgyak besorolását egy vagyonleltár tartalmazza, melyben az alábbi értékeléseket végzi el a kar informatikához értő, megbízott munkacsoportja. A besorolásokat évről évre felül kell vizsgálni és fejleszteni kell a tapasztalatok alapján. A hátrány mértéke az alábbi besorolás szerint határozható meg:

Vagyonleltár																
Vagyontárgy	**Folyamat**	**Vagyontárgy típus**	**Vagyonelem felelőse**	**Vagyontárgy értéke**	**Vagyonelem biztonsági besorolása**	**Rendelkezésre állás szerinti besorolás**	**Feldolgozás kritikus időszakai**	**Tolerálható kiesési idő**	**Információt feldolgozó alkalmazás**	**Fenyegető tényező(k)**	**Rendelkezésre állásuk kritikussága**	**Lehetséges kár**	**Függőség**	**Védelmi elem?**	**Futtató hardver**	**Használatra vonatkozó útmutató elérhetősége**

A táblázat három jelentős oszlop értékelési lehetőségét bontottuk le.

Besorolás a keletkezett lehetséges kár alapján

Az osztályozás alapját a bizalmasság, a sértetlenség, és a rendelkezésre állás sérüléséből, vagy elvesztéséből keletkező, a SZIE számára kimutatható lehetséges hátrány nagysága képezi.

	A hátrány mértéke (Vagyontárgy értéke)		
	Elhanyagolható	**Jelentős**	**Súlyos**
Vagyoni hátrány			
Vagyoni kár, vagy többletköltség,	A kár nagysága meghaladja a szabálysértési értékhatárt.	A kár nagysága meghaladja az 500.000 forintot.	A kár nagysága meghaladja a 1.000.000 forintot.
Erkölcsi hátrány			
Bizalomvesztés a hallgatók körében	A SZIE megítélése lényegesen nem változik.	Bizalomvesztés a SZIE 1-2 alkalmazottjával szemben	Bizalomvesztés a SZIE egy szervezetével szemben.
Bizalomvesztés a dolgozók körében (Munkahelyi hangulat).	A SZIE alkalmazottai körében legfeljebb kisebb, átmeneti elégedetlenség (családottság) áll fenn.	Bizalomvesztés a SZIE egy szervezetének vezetőjével szemben.	Bizalomvesztés a SZIE felső vezetésével szemben.
Jogi hátrány			
A törvényesség megsértése	A SZIE-fel szemben nem indul jogi eljárás.	A SZIE-fel vagy a SZIE egy alkalmazottjával szemben jogszabálysértés elkövetése miatt indul eljárás.	A SZIE-fel, vagy a SZIE egy alkalmazottjával szemben vétség vagy bűncselekmény elkövetése miatt indul eljárás.
Jogi és oktatási kötelezettségek	A kár a SZIE jogi, szerződéses és oktatási kötelezettségeinek teljesítését zavarja (kisebb, incidens jellegű fennakadásokat okoz).	A kár a SZIE jogi, szerződéses és oktatási kötelezettségeinek teljesítését gátolja (a teljesítés, és annak minősége csak újabb erőforrás bevonásával biztosítható).	A SZIE csak jelentős késéssel, esetleg nem megfelelő minőséggel tudja teljesíteni a jogi, szerződéses és oktatási kötelezettségeit.

	A hátrány mértéke (Vagyontárgy értéke)		
	Elhanyagolható	**Jelentős**	**Súlyos**
Információk bizalmasságának, sértetlenségének sérülésével kapcsolatos incidensek	Nyilvános információk, dokumentumok illetéktelen személy által történő megváltoztatása, az információk pontosságának, és teljességének sérülésével.	„Bizalmas" vagy „Belső használatú" minősítésű információk illetéktelen kezekbe, vagy nyilvánosságra kerülése, vagy illetéktelen személy által történő megváltoztatása, az információk pontosságának, és teljességének sérülésével.	„Titkos" minősítésű információk illetéktelen kezekbe, vagy nyilvánosságra kerülése, vagy illetéktelen személy által történő megváltoztatása, az információk pontosságának, és teljességének sérülésével.
Üzletmenet (ügyvitel, iktatás)			
Az üzletmenet minősége és folytonossága	Az üzletmenet folyamatos, kisebb incidens jellegű fennakadások észlelhetők.	A kár az üzletmenetet gátolja (az üzletmenet folytonossága, vagy minősége csak újabb erőforrások bevonásával biztosítható).	A kár a SZIE-et az üzletmenet folytonossági terv aktiválására vagy ezzel egyenrangú intézkedésekre kényszeríti.

Az adatok kezelésének követelményei

A következő táblázat az adatok kezelésével kapcsolatos követelményeket foglalja össze **bizalmasság** és **sértetlenség** szerint (**Vagyonelem biztonsági besorolása**):

	„Nyilvános" illetve „Nem védett"	**„Bizalmas" illetve „Védett"**	**„Titkos" illetve „Fokozottan védett"**
Tárolás	Központi tároló helyen kell tárolni.	Személyes, vagy korlátozott hozzáférésű mappában/ dossziéban kell tárolni.	Titkosított mappában/ dossziéban kell tárolni.
Adatátvitel	Nincs követelmény.	A SZIE-en kívülre jelszó védett állományban (pl.: ZIP vagy jelszóval védett Office dokumentum) kell küldeni.	A fájl titkosításával kell küldeni (pl.: PGP).
Adatmegosztás	A központi nyilvános tároló helyeken megosztható.	A központi tároló helyen a betekintésre jogosultak körében megosztható.	Nem megosztható, szükség esetén több példányban kell tárolni.
Megsemmisítés, törlés	Nincs követelmény.	Csak az adatgazda engedélyével törölhető/semmisíthető meg.	Csak az adatgazda engedélyével törölhető/semmisíthető meg. Az elektronikus adathordozón lévő adatokat törölni kell, a papír alapú dokumentumokat a SZIE Iratkezelési szabályzata szerint kell kezelni. A hibás adathordozókat fizikailag meg kell semmisíteni.
Felülvizsgálat	Nincs követelmény.	Minimálisan kétévente.	Minimálisan évente.

Az adatok kezelésének követelményei **rendelkezésre állásuk** szerint:

	„Általános”	**„Fontos”**	**„Kritikus”**
Tárolás	Elégséges a központi tároló helyen való elhelyezés.	Kötelező a kétpéldányos tárolás (egy online elérésű és egy rendszeres napi mentésű off-line példány). Az off-line példány esetében adatok tárolási helyét rögzítő nyilvántartás (back-up lóg, lista, stb.) kíséretében.	Kötelező a kétpéldányos tárolás (egy online elérésű és egy rendszeres napi mentésű off-line példány). Az off-line példány esetében adatok tárolási helyét rögzítő nyilvántartás (back-up lóg, lista, stb.) kíséretében.
Adatátvitel	Nincs követelmény.	A forráshelyen és a nyilvántartásban megjelölt tárolási helyen maradjon egy példány az adatból.	Tartalék vagy redundáns eszközt, csatornát kell biztosítani.

2. SZÁMÚ MELLÉKLET: INFORMÁCIÓ BIZTONSÁGI ZÓNÁK

Zóna követelmények	1. számú biztonsági zóna	2. számú biztonsági zóna	3. számú biztonsági zóna
Általános követelmények			
Természeti katasztrófák kockázatainak csökkentése	-	-	A zóna kialakításánál figyelembe kell venni az árvíz, belvíz, villámcsapás és egyéb természeti katasztrófák kockázatait.
Hozzáférési követelmények			
Belépés, beléptetés	Információbiztonsági szempontból nincsen előírás.	Az irodákba történő belépés kulccsal történik.	A zónába történő belépés egyedi azonosítással (mágneskártya, kód, stb.) történik.
A belépés engedélyeztetése	Külön engedély nem szükséges.	A fogadó szervezet vezetőjének szóbeli engedélye szükséges.	Írásbeli engedély szükséges.
Környezeti követelmények			
Klimatizálás	-	-	Klimatizálás szükséges.
Páratartalom mérése	-	-	A páratartalom mérése szükséges.
Áramellátás szabályozása	-	-	Az áramellátás szabályozása, és a működés redundanciája szükséges.
Tűzvédelem	Kézi tűzoltó készülékek kihelyezése szükséges a folyósón.	Kézi tűzoltó készülékek kihelyezése szükséges a folyósón.	Tűzvédelmi füstérzékelő és a közelben kézi riasztó szükséges. A helységben vagy annak bejáratánál kézi tűzoltó készülék kihelyezése szükséges.
Kontroll követelmények			
Biztonsági felügyelet	-	-	Felügyeleti (riasztó) eszközökkel kell ellátni.
Behatolás-védelem	Passzív behatolás védelmi eszközök szükségesek az alagsori, földszinti, és 1. emeleti ablakokra.	Passzív behatolás védelmi eszközök szükségesek az alagsori, földszinti, és 1. emeleti ablakokra.	Passzív behatolás védelmi eszközök szükségesek az alagsori, földszinti, és 1. emeleti ablakokra, valamint aktív behatolás-védelmi eszközök felszerelése szükséges a helységbe vagy a folyosókra.
Dokumentálási követelmények			
A beléptető rendszer naplózásával vagy a kulcs felvételénél kell dokumentálni	-	A kulcs felvételnél kell dokumentálni.	A belépések naplózása.
Biztonsági események	-	-	A felügyeleti eszközök jelentéseit naplózni kell.

3. SZÁMÚ MELLÉKLET: KONTROLL ÉS FELÜLVIZSGÁLAT

Biztonsági rendszerek kontroll pontjai

A minimálisan szükséges kontroll pontok az alábbiak:

Mérendő terület	Mérendő mennyiség	Beszámolóban szerepel
IT tevékenység	Szerverszobába való belépések naplózása	-
	Hozzáférések (logikai) naplózása	-
Illegális informatikai tevékenység	Észlelt behatolási kísérletek száma	X
	Nem SZIE dolgozó/hallgató által végzett tevékenység teljes körű naplózása	-
Vírusvédelem	Beérkezett vírusok, SPAM-ek száma	X
	Hatástalanított vírusok és blokkolt SPAM-ek száma	X
	Nem Internetről beérkezett vírustámadások száma, ezek módja	X
Mentési rendszer	A teszt visszatöltések eredményei	X
Rendelkezésre állás	Rendszerek kieséseinek száma, ezek oka, időtartama, javítási költsége	X
Kapacitás információk	Kritikus rendszerekre vonatkozó teljesítményadatok jelentős változása	kivonat
	Tárolási kapacitásokra vonatkozó információk	X
Ellenőrzések eredményei	Feltárt hiányosságok, és azok megszüntetésére vonatkozó intézkedések	X
Oktatás helyzete	Az információbiztonsági oktatásban részt vett személyek száma, a beszámoltatás eredményei	X
Az információbiztonsággal kapcsolatos fegyelemsértések	Az információbiztonságot megsértő személyekre vonatkozó fegyelmi statisztikák	X
Az információbiztonsági rendszer összesített értékelése	Az informatikai rendszer technikai és biztonsági szintjére vonatkozó megállapítások, javaslatok	X
Javaslatok	Javaslatok kidolgozása a hiányosságok megszüntetésére, a biztonsági és rendelkezésre állási szint emelésére	X

Biztonsági rendszerek felülvizsgálata

A szükséges felülvizsgálatok és gyakoriságuk a következő:

A felülvizsgálat tárgya	A felülvizsgálat ciklikussága
Kockázatfelmérés	2 évente
IT biztonsági szabályzat	2 évente
IT biztonsági folyamatok	2 évente
Határvédelem	1 évente
Vírusvédelem	1 évente
Mentés, archiválási rend	1 évente
IT biztonsági oktatás	1 évente

4. SZÁMÚ MELLÉKLET: VÉSZHELYZETI TERVEK TENNIVALÓI ÉS FELELŐSEI

1. Vészhelyzeti elérhetőségek

Név	Érintett terület	Elérhetőség
Mezei Tibor	papír alapú információk	30/256 0313
Gál György	informatika alapú információk	30/894 8178
Lajber Zoltán	informatikai alapú információk	20/491 6580

2. Vészhelyzeti értesítési lánc

<table>
<tr><th></th><th colspan="3">Nappal</th><th colspan="2">Éjszaka / munkaidőn túl</th></tr>
<tr><td rowspan="2">1.</td><td colspan="3" rowspan="2">észrevételező</td><td colspan="2">észrevételező</td></tr>
<tr><td colspan="2">portaszolgálat</td></tr>
<tr><td>2.</td><td>rendszergazda / informatikai központ munkatársa</td><td>informatikai igazgató / főtitkár</td><td rowspan="2">kari információbiztonsági felelős</td><td>informatikai igazgató / főtitkár / dékán</td><td>kari információbiztonsági felelős</td></tr>
<tr><td>3.</td><td colspan="2">dékán/ rektor (szükség esetén)</td><td colspan="2"></td></tr>
</table>

3. A kritikus területek meghatározása

A kritikus információbiztonsági területek meghatározása az információbiztonsági kockázatértékelés során történik.

4. Vészhelyzet elrendelése

Aszerint, hogy a kialakult hiba milyen hatáskörzetben észlelhető, megkülönböztethető:

- a folyamatban résztvevők jelentései alapján,
- külső jelzés útján előforduló rendkívüli eseményeket.

Minden olyan esetben, amikor a munkatársba felmerül a gyanú, hogy az egyetem/ kar. bármely folyamata során az információbiztonsági szempontokat veszélyeztető esemény várható vagy az már be is következett, akkor köteles jelenteni azt **közvetlen felettesének** és/vagy a **információbiztonsági felelősnek, rendszergazdának**. Amennyiben az észrevétel külső féltől ered, a kapcsolattartó kötelessége az információ továbbítása.

A vészhelyzetnek megfelelő minősítést, valamint a vészhelyzeti terv alkalmazását

- főtitkár,
- informatikai igazgató,
- dékán,
- kari információbiztonsági felelős rendelheti el.

5. Az irányítási feladatok

Amennyiben a vészhelyzet kezelése az egyetem/ kar egységein túli szervezetek bevonását is jelenti a vészhelyzet kezelésének összehangolása, koordinálása a **főtitkár** feladatköre. A kari **információbiztonsági felelősök** feladata a hatáskörük alá tartozó területek esetén az intézkedések közvetlen irányítása, a munkatársa koordinálása, kapcsolattartás a **főtitkárral, informatikai igazgatóval,** és szükség szerint más **területek vezetőivel**. Amennyiben a vészhelyzet az üzem területi egységein belül jelentkezik a vészhelyzet irányítása a **területi vezető** feladatköre.

6. Veszélyhelyzeti tevékenységek

Tevékenység		*Felelős*
1.	Riasztás, vezetők kiértesítése az értesítési láncnak (0. pont) megfelelően	észrevételező
2.	Információk pontosítása, a vészhelyzeti állapot elrendelése	irányításért, minősítésért felelős személy
	Szükség szerint külső szervek bevonása (pontosítani: pl. Rendőrség, Kárelhárítás stb.)	főtitkár, informatikai igazgató
	Az információbiztonságot veszélyeztető tényező következtében jelentkező személyi és tárgyi erőforrások biztonságának szükség szerinti kezelése a Katasztrófa- és polgári védelmi szabályzat/Tűzvédelmi szabályzat szerint	területi vezető
3.	Biztonsági eljárások, kárelhárítás (Katasztrófa- és polgári védelmi szabályzat, Tűzvédelmi szabályzattal összhangban) – Szükség szerint a további információs rendszerek eltávolítása, veszélyes és veszélyessé váló területek kiürítése. – Védelmi szakaszolások, elhatárolások. – Szükség szerinti adatmentések. – Szükség szerint külső felek azonnali tájékoztatása.	egyetemi, kari információbiztonsági felelős, rendszergazda
4.	Kivizsgálás, elhárító intézkedések A folyamat leállítása után ki kell vizsgálni, hogy mekkora információbiztonság megsértésének hatása, egyedi intézkedések. Amennyiben az információbiztonság sérülése az egyetem/ kar kompetenciáján túlmutat, hatáskörének megfelelően a **főtitkár/ dékán** értesíti az illetékes hatóságokat. Helyreállítási lépések.	egyetemi, kari információbiztonsági felelős, rendszergazda
5.	A vészhelyzet feloldása, dokumentálás A vészhelyzet feloldását ugyanaz a személy rendelheti el, aki azt kezdeményezte, de csak abban az esetben, ha az információbiztonsági problémát megszüntették, és az elhárító intézkedés dokumentáltan megtörtént. A vizsgálat befejezésekor jegyzőkönyv megírásával dokumentálni kell.	egyetemi, kari információbiztonsági felelős, rendszergazda
6.	A vészhelyzet típusától függően bejelentés további külső szervek felé.	főtitkár/ dékán
7.	Helyreállítás, újraindítási feltételek és ezek meglétének ellenőrzése	főtitkár, informatikai igazgató/ dékán

7. Helyreállítási lehetőségek

Veszély	Megoldás	Jellegzetes helyreállítási lehetőségek	Megjegyzések
Informatikai szempontból, üzletmenet folytonosság szempontjából kritikus helyiségek (pl. szerverszoba) megrongálódása vagy megközelíthetetlensége	Kisegítő helyiségek keresése és biztosítása. A helyreállítás gyorsabb, ha a helyiség előre el van látva árammal, telefonnal, és hálózati végponttal	A karon belüli, vagy kívüli megfelelő kisegítő helyiségek találása, és rendelkezésre állásuk figyelmen kísérése	Helyiségeket lehet felszabadítani, de valószínűleg fel kell szerelni őket, mielőtt használhatóak lesznek
		Kijelölt kisegítő helyiség az karon / csoporton belül	A kar felügyelete alatt megfelelően fel lehet szerelni előre
		Külső helyreállítási szolgáltatás: Mobil helyiségek	Megfelelő hozzáférést és elhelyezést igényel
		Külső helyreállítási szolgáltatás: Szolgáltató telephelyén biztosított helyiségek	Az alkalmazottaknak a szolgáltató telephelyére kell utazniuk
		Kisegítő egyezmény egy harmadik féllel	Harmadik félre is hatással van
		Otthonról dolgozó alkalmazottak	Kommunikációs nehézségek. Megvalósítható lehet, de csak rövidtávon.
		Rugalmas munkafolyamatok, vagyis a pótolhatatlan alkalmazottak elosztása több helyszínre	Költséges lehet
Számítógépes eszközök megsemmisülése, vagy végzetes meghibásodása (pl. tanulmányi hivatal)	Csereeszközök keresése, és biztosítása, amelyek rövid idő alatt beszerezhetőek	Hardverek használata kevéssé fontos szervezeti folyamatokból	Más szervezeti folyamatokat is befolyásolhat
	A helyreállítás gyorsabb, ha a csereeszközt előre telepítik a megfelelő programokkal és kiegészítő eszközökkel, és ennél is gyorsabb, ha az adatokat is rendszeresen karbantartják rajtuk		
	Végül, ha az adatokat valós időben tükrözzük tartalék gépekre, akkor lehetséges a szinte azonnali helyreállítás		
Számítógép szoftver végzetes hibája	Eszközök, amelyek lehetővé teszik a munkafolyamatok alternatív módon való működtetését	Régebbi változatok mentése	Mentési példányokat védeni kell a szándékos károkozástól
		Visszatérés a manuális feldolgozásra a javítások elvégzéséig	Olyan kockázatcsökkentési módszerek, mint a szigorú tesztelés és az új szoftverek szakaszos feltöltése
Számítógépes rendszerek műszaki hibája	Gyors hibajavítás biztosítása, vagy ahol megszakítás nélküli működés szükséges, ott hibatűrő szerkezetek biztosítása	Helyi, vagy gyors reagálású karbantartó személyzet, pótalkatrészekkel és megfelelő szakértelemmel	Fenn áll a veszélye, hogy a helyreállítási célkitűzések nem teljesülnek. Fennáll a veszélye, hogy a szoftver vészhelyzeti javítása veszélyezteti a folyamatos üzemvitelt vagy a biztonságot
		Hibatűrő szerkezetek, úgymint több processzor és / vagy meghajtó	Költséges lehetőség, de megszakítás nélküli működést biztosít
		Szoftver mentése	Mentési példányokat védeni kell a szándékos károkozástól
Adatvesztés	Olyan rendszerességgel végzett mentések, ahogy azt az adatvesztésből eredő szervezeti hatás indokolja. A mentéseket védeni kell, és a működő példányoktól különböző helyen tárolni	Cserélhető adathordozó, mint a szalagos egység, hajlékonylemez, dobozos szalag, CD lemez	Idő szükséges az adatok visszatöltéséhez. Nem teljesen naprakész
		Távoli (naplózás/ elektronikus védelem	Költséges lehet, de gyors helyreállítást tesz lehetővé
		Valós idejű lemeztükrözés	Költséges lehetőség, korlátozva van a meghajtók közötti távolság, de szinte azonnali helyreállítást biztosít
Létfontosságú papír alapú iratok megsemmisülése	Biztosítani kell, hogy az adatok más módon is rendelkezésre álljanak	Másolat készítése, és külső tárolás	Költséges lehet
		Mikrofilm vagy dokumentum beolvasó használata	Költséges lehet, vagy nehézkes az alkalmazása
		Igényli a szállítók / harmadik felek adatduplikálását	Jelentős biztonsági kérdéseket vet fel
Kulcsfontosságú alkalmazottak elérhetetlensége	Kerülni kell a kulcsfontosságú alkalmazottaktól függést, és gondoskodni kell helyettesítő személyzetről	Hasonló szakterületű szakemberek továbbképzése	Naprakészen kell tartani

5. SZÁMÚ MELLÉKLET: MENTÉSI MÉDIÁK ROTÁLÁSA, SELEJTEZÉSE

4.1. Mentési médiák újrahasznosítása, rotálása

A mentési adathordozókat, vagy az adathordozókon tárolt adatokat az alábbiak szerint kell rotálni:

Típus	Rotálási ciklus
Napi	7 nap
Heti	5 hét
Havi	1 év
Éves	5 év

4.2. Mentési médiák selejtezése, megsemmisítése

Az alábbi táblázat a mentési médiák számításba vehető maximális élettartamát tartalmazza. (Az egyes gyártók az itt megadott értékektől eltérhetnek. Amennyiben a gyártói előírások szigorúbbak, úgy azokat kell alkalmazni.)

Média	**Max. élettartam**
LTO-x	3 év
CD-R	5 év
CD-RW	5 év
DVD-R	5 év
DVD-RW	5 év

A maximális élettartamuk lejárta után az adathordozókat át kell másolni új adathordozóra, majd a régi adathordozót le kell selejtezni, és meg kell semmisíteni. Megsemmisítéskor az adathordozót fizikailag kell megsemmisíteni.

Az adathordozót le kell selejtezni akkor is, ha vélhetően az adathordozó hibája miatt az adatmentés sikertelen volt, illetve ha a katasztrófa vagy visszatöltési próbák során az adatvisszatöltés sikertelenné vált.

6. SZÁMÚ MELLÉKLET: A BIZTONSÁGI ESEMÉNYEK KEZELÉSE

A SZIE alkalmazottainak és hallgatóinak az általuk észlelt, a SZIE informatikai rendszerében keletkező biztonsági incidenseket be kell jelenteniük a helyi információbiztonsági rendszergazdáknak.

A bejelentésre az alábbi információs csatornák állnak rendelkezésre:

Elsődlegesen

- helpdesk@ih.szie.hu
- Központi HelpDesk telefonszám: 28/ 522-924 vagy 28/522 000 és 1291 mellék

Lokális probléma kezelésére:

SZIE Kar vagy Intézet	Telefon	e-mail
SZIE IK	28/ 522-000 mellék: 1911 mobil: 30 894 8178	gal.gyorgy@fh.szie.hu
SZIE IK	28/ 522-000 mellék: 1290 mobil: 20 4916580	lajber.zoltan@ih.szie.hu
SZIE GK	66/ 524-700 mellék: 1024	toth.janos@gk.szie.hu
SZIE GK	66/ 524-700 mellék: 1017	unyatinszki.zoltan@gk.szie.hu
SZIE GK	66/ 524-700 mellék: 1016	streit.janos@gk.szie.hu
SZIE GK	66/ 311-511 mellék: 2230	otta.endre@gk.szie.hu
SZIE GK	66/ 561-620 mellék: 122	sandor.papp@gk.szie.hu
SZIE ABPK	66/ 311 511 mellék: 3137	liszkai.lorant@abpk.szie.hu
SZIE ABPK	57/ 502-444	bagi.zsolt@abpk.szie.hu

7. SZÁMÚ MELLÉKLET: FOGALOMTÁR

Adat: A hivatalos küldemények azon része, amelynek elektronikus eszköz az információ hordozója (pl.: floppy, e-mail üzenet a képernyőn), függetlenül attól, hogy az információ szöveges vagy számszerű.

Adatkezelés: Az adatok tárolásával, továbbításával, megsemmisítésével, nyilvántartásával és feldolgozásával kapcsolatos tevékenységek összessége.

Adatállomány: Valamely informatikai rendszerben lévő adatok logikai összefogása, amelyet egy névvel jelölnek. Ezen a néven keresztül lehet hozzáférni a rendszer által tartalmazott adatokhoz.

Adatgazda: Az ügyviteli, működési folyamatokhoz tartozó adatok kezeléséért felelős személy.

Adatátvitel: Elektronikus adatok szállítása összeköttetéseken, összekötő utakon keresztül. (Például számítógépek között hálózaton keresztül, e-mail-ben, Interneten.)

Adatbiztonság: Az adat bizalmasságának, integritásának és rendelkezésre állásának biztonságos megőrzése.

Adatbiztonsági szint: Az adat sértetlenségét és bizalmasságát jellemző minőségi (kvalitatív) osztályozás.

Adathordozó: Az adat tárolására és terjesztésére alkalmas eszköz.

Adatvédelemi szint: Az adat rendelkezésre állását jellemző minőségi (kvalitatív) osztályozás. Az osztályozás meghatározza, hogy a szóban forgó adat rendelkezésre állása milyen mértékben befolyásolja az általa érintett folyamatok végrehajtását, illetve a SZIE tevékenységét tekintve mennyire fontos ügyviteli, működési folyamathoz tartozik.

Bekövetkezési valószínűség: Annak az esélye, hogy a veszélyforrás képezte fenyegetettség támadás formájában bekövetkezik.

Bizalmasság: A SZIE ügyfeleire, illetve ügyletmenetére vonatkozó adatok védelme illetéktelen hozzáférés, illetve felhasználás ellen. Az információkhoz, adatokhoz csak az arra jogosítottak és csak az előírt módokon férhetnek hozzá. Ez vonatkozhat programokra, mint szélesebb értelemben vett információkra is. (Például, ha valamely eljárás előírásai egy programmal kerülnek leírásra, és azt szükséges titokban tartani.)

Biztonság: Az informatikával kapcsolatban, az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az adatok rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.

Biztonsági szint: A rendszerek megbízhatóságát és érzékenységét jellemző minőségi (kvalitatív) osztályozás. Ahol a megbízhatóság a rendszer azon jellemzője, amely megadja, hogy az üzemeltetési feltételek zavartalan fennállása esetén milyen mértékben várható el a hibátlan és rendeltetésszerű működés. Az érzékenység pedig meghatározza, hogy az adott rendszer elemei mennyire védettek és ellenállóak a különböző hatásokkal és károkozásokkal szemben.

Cselekvési (akció) terv: Egy meghatározott (káresemény bekövetkezése esetén végrehajtandó eljárásrend, amely tartalmazza a sebezhetőségi ablakot, a helyettesítő és visszaállítási feladatokat, meghatározza a végrehajtásban érintett személyeket, csoportokat vagy szervezeti egységeket, valamint azok felelősségi- és jogkörét.

Dologi kár: A SZIE eszközeiben, fizikai vagyontárgyaiban közvetlenül bekövetkező kár vagy veszteség.

Elektronikus aláírás: Személyek és/vagy digitális adatok hitelesítésére alkalmas módszer. Két részből áll: a személyhez kötött aláírást generáló részből, és az ellenőrzést bárki számára lehetővé tevő részből.

Esemény: A SZIE rendszereiben előálló időleges kiesést vagy zavarokat, és akár - gazdasági, reputációs, személyi vagy dologi - kárt is okozó, illetve törvényi következményekkel járó történés.

Fenyegetettség: A SZIE informatikai infrastruktúráját fenyegető azon veszélyforrások összessége, amelyek bekövetkezése esetén az informatikai rendszer nem tudja teljesíteni a vállalt rendelkezésre állást, akadályozva ezzel a normális üzemmenet folytonosságát, illetve az adatok sértetlensége és bizalmassága sérül.

Fenyegetettség-hatáselemzés: Az egyes informatikai szolgáltatásokkal kapcsolatban a kiesés lehetséges okainak, az egyes okok bekövetkezési valószínűségének felmérése. (A vizsgálatot követően lehetővé válik a kiesés legvalószínűbb okaival szemben a hatékony, célzott védekezés.)

Fenyegető tényező: Azon esemény, amelynek bekövetkezése közvetlenül vagy közvetve a kritikus informatikai szolgáltatások kiesését eredményezi.

Fizikai biztonság: Az erőforrások bizalmassága és sértetlensége, valamint rendelkezésre állása sérelmére bekövetkező szándékos vagy véletlen fizikai támadásokkal, veszélyforrásokkal szembeni védettség.

Fokozott készültségi szint: A napi működés során olyan, előre látható, tervezett esemény következik be, vagy tevékenység kerül végrehajtásra, amelynek magas kockázata miatt - ami adódhat a végrehajtás egyediségéből is - külön tervezés és felkészülés szükséges az esemény elhárításához vagy a tevékenység végrehajtásához, és esély van arra, hogy rossz esetben magas készültségi szintre kerülnek a folyamatok.

Gazdasági kár: Azt fejezi ki, hogy egy adott informatikai szolgáltatás bizonyos ideig tartó kiesése milyen közvetlenül is mérhető, pénzben kifejezhető veszteségeket okoz a SZIE-nek (anyagi károk, kártérítések stb. formájában).

Helyreállítási eljárás: A vészhelyzetként értékelhető incidens bekövetkezése és az azt követő észlelése után végrehajtandó eljárásrend, amely biztosítja, hogy a sérült kritikus ügyviteli folyamat, vagy annak valamely alternatívája a sebezhetőségi ablakon belül a SZIE által vállalt tevékenységi szinten működőképes.

Helyreállítási terv: A helyreállítási eljárásokat tartalmazó dokumentum

Hitelesség: A rendszerben kezelt adat bizonyíthatóan hiteles forrásból származik. (Az entitás olyan tulajdonsága, amely egy vagy több hozzá kapcsolódó tulajdonságot más entitás számára bizonyíthatóvá tesz.)

Információ: Egy adatküldemény tartalma, függetlenül az információ hordozójától.

Informatikai katasztrófa: Az informatikai szolgáltatások olyan kiesése, amelynek következtében megszakad a SZIE informatikai rendszerének folyamatos és rendeltetésszerű működése, és ez jelentős hatást gyakorol a normál ügyviteli, ill. működési tevékenységek folyamatosságára és működőképességére.

Informatikai vészhelyzet: Az állapot, amikor az informatikai rendszer utolsó működőképes állapotát az üzemeltetési szabályok előírásszerű betartásával és végrehajtásával, a meghatározott erőforrások felhasználásával, a megállapított helyreállítási időn belül, nem lehet visszaállítani.

IT erőforrások: Az ügyviteli folyamatok működéséhez nélkülözhetetlen elektronikus adatok, informatikai alkalmazások, technológiai eszközök, környezeti infrastruktúra és humán erőforrások összessége.

Katasztrófahelyzet kezelés tervezése: A káreseményeknek az informatikai rendszerek kritikus elemeire vonatkozó hatásait elemzi és tervet ad olyan globális helyettesítő megoldásokra, valamint megelőző és elhárító intézkedésekre, amelyekkel a bekövetkezett káresemény után az informatikai rendszer funkcionalitása eredeti állapotában visszaállítható. (DRP - Disaster Recovery Plan)

Kockázat: Annak veszélye, hogy egy esemény, fenyegetettség bekövetkezése vagy intézkedés hátrányosan befolyásolja a SZIE lehetőségeit céljainak és stratégiájának megvalósítása során.

Kockázattal arányos védelem: A lehetséges védelmi intézkedések olyan hatékony alkalmazása, amikor egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékekkel.

Kockázatelemzés: Az információs folyamatokra és az adatra hatással lévő veszélyek felbecsülése. A kockázatfelmérés és kockázatfelbecsülés általános folyamata.

Kritikus ügyviteli folyamat: A SZIE azon ügyviteli folyamata, amely működőképességének fenntartása elengedhetetlen a SZIE stratégiai céljainak elérése, teljesíthetősége érdekében.

Kritikus kiesési idő: Az az időszak, amely egy adott informatikai szolgáltatás nyújtásának akadályoztatását jelenti és az információbiztonsági felelősnek még nem szükséges semmilyen lépést tennie az alternatív működés elrendelésére.

Kritikus üzemmeneti szint: A kritikus ügyviteli folyamatok működése megszakadt oly módon, hogy a probléma a folyamatot működtetők, illetve az informatikai üzemeltetés hatáskörében közvetlenül, a folyamat működésének — a sebezhetőségi ablakban meghatározott értéknél - hosszabb szüneteltetése nélkül, nem megoldható. A kritikus üzemmeneti szint esetén az elhárítást külön e célra létrehozott szervezet - Krízis Bizottság - szervezi, aki jogosult az intézkedések végrehajtásához szükséges döntéseket meghozni.

Krízisállapot/Krízishelyzet: Az az állapot, amely a folytonosságot biztosító intézkedésekhez kapcsolódó cselekvési tervekben nem definiált, illetve amelyek esetében a kapcsolódó cselekvési terv nem alkalmazható. Krízishelyzetnek tekintendő minden olyan eset, amikor a normál üzemmenet nem folytatható. (A krízishelyzet addig tart, amíg a normál üzemmenet nem indul el, így akkor és csak akkor vonható vissza a BCP (Business Continuity Plan - Üzletmenet Folytonossági terv) eljárásrend hatálya, illetve oszolhat fel a Krízis Bizottság.)

Maximális kiesési idő: Azon időintervallum, amelyen belül a kiesést szenvedett kritikus informatikai szolgáltatást a helyreállítási/visszaállítási eljárás végrehajtásának eredményeként ismételten működővé kell tenni, mert ellenkező esetben a SZIE már nem elviselhető károkat szenvedne.

Megelőző védelem: Azon technikai, szervezeti és adminisztratív intézkedések halmaza, amelyek célja a fenyegető tényezőkből fakadó események/katasztrófaesemények bekövetkezését megelőzni, vagy annak esélyét csökkenteni, valamint a helyettesítő folyamat beindítását lehetővé tenni.

Minimális szolgáltatás: A SZIE ügyviteli folyamatai közül azon előre definiált, belső szabályzatban rögzített tevékenységek, amelyeket az adott szervezeti egységnek akkor is nyújtania kell, ha üzemzavar, krízishelyzet áll elő.

Normál üzemmenet szint: A napi működés során nem történik rendkívüli helyzet, az informatikai rendszerekbe épített belső ellenőrző funkciók hibát nem jeleznek, az ügyfelek és a felhasználók nem tapasztalnak a SZIE szolgáltatásaival kapcsolatos rendellenességet. Normál üzemi állapotnak tekintett az az eset is, ha az ügyfél a saját üzemeltetésében lévő informatikai rendszer meghibásodása miatt nem képes igénybe venni a SZIE szolgáltatásait. A normál üzemmenet esetén az FH és a megyei/fővárosi munkaügyi központok Szervezeti és Működési Szabályzataiban rögzített hatás- és jogkörök érvényesek, külön intézkedésre, beavatkozásra, hatáskör túllépésre nincs szükség.

Rendelkezésre állás: Az a tényleges állapot, amikor az informatikai rendszer eredeti rendeltetésének megfelelő szolgáltatásokat - amely szolgáltatások különbözők lehetnek - nyújtani tudja (funkcionalitás) meghatározott helyen és időben (elérhetőség), és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva. Ebben az összefüggésben jelentősége van az információ vagy adatok rendelkezésre állásának, elérhetőségének is.

Rendszer-monitorozó eszközök: Az egész informatikai, ill. információs rendszerről, vagy valamilyen csoportosító szempont szerint a rendszer egyes részeiről gyűjtenek folyamatos információkat.

Reputációs (társadalmi, image) kár: A SZIE megbízhatóságába, hitelességébe, illetve a SZIE által nyújtott szolgáltatásokba vetett hit szempontjából mérhető hatások.

Sebezhetőségi ablak: Azon időtartam, amely alatt a helyettesítő megoldás fenntartható az ügyviteli tevékenységek és a törvény által előírt jogi kötelezettségek komolyabb sérülése nélkül. Az adott informatikai szolgáltatás megszakadását követő időtartam, amelyet normális működési rendjének és tevékenységének megszakadása nélkül képes a SZIE elviselni.

Sértetlenség (integritás): Az adatok eredeti állapotának, tartalmának, teljességének és hitelességének biztosítása. Az információkat, adatokat, alkalmazásokat csak az arra jogosultak változtathatják meg, és azok véletlenül sem módosulhatnak. (A sértetlenséget általában az információkra, adatokra, illetve alkalmazásokra is értelmezik, mivel az adatok sértetlenségét csak rendeltetésszerű feldolgozás és átvitel esetén lehet biztosítani.)

Személyi kár: A SZIE alkalmazottainak testi épségét, egészségét érintő hatás, következmény.

Tesztelés: A kialakított üzemmenet folytonossági cselekvési tervek gyakorlati értékelése; a megfogalmazott felkészülési, helyettesítési és helyreállítási tevékenységek szükségességének és megfelelőségének vizsgálata, a szabályozás bármilyen hiányosságának feltárása, az üzemmenet folytonossági tevékenységek alapját adó (informatikai) helyreállítási eljárások vizsgálata, illetve a külső partnerekkel kötött egyezmények betartásának és használhatóságának vizsgálata.

Teszt-környezet: Az informatikai rendszer azon elkülönített része, amelyben az éles üzembe állítás előtti tesztelések az éles környezethez hasonló körülmények között történnek.

Törvényi következmények: Az esetleges jogi következmények, amelyek egy adott informatikai szolgáltatás kieséséből következhetnek.

Türelmi idő: Az az időszak, amely egy adott informatikai szolgáltatás nyújtásának akadályoztatását jelenti és az információbiztonsági felelősnek még nem szükséges semmilyen lépést tennie az alternatív működés elrendelésére.

Ügyviteli folyamat: Olyan tevékenységek összessége, amelyek szükségesek, hogy a SZIE kifejtse szervezeti működését és megvalósítsa oktatási, kutatási, stb. feladatait. (Egy SZIE-es szolgáltatás nyújtásához szükséges tevékenységek, feladatok összessége.)

Üzemmenet folytonosság: A SZIE zavartalan működését, az ügyviteli folyamatokat támogató - elsősorban informatikai, de emellett telekommunikációs, emberi és infrastrukturális - erőforrások egy hosszabb időn át folyamatosan, megszakítás nélkül üzemelnek, illetve a megkívánt mértékben és funkcionalitási szinten rendelkezésre állnak.

Vészhelyzeti esemény: Azon esemény, amelynek bekövetkezése krízishelyzetet teremt. A vészhelyzeti eseménynek több, egymástól független, vagy egymással összefüggő oka lehet. Az okok azon releváns fenyegető tényezők, amelyek az adott esemény kiváltásához vezetnek különböző valószínűségekkel. A normál ügyvitelre történő visszaállás várható határideje meghaladja az üzemzavarnál leírtakat, illetve a probléma nem csupán a SZIE tevékenységeinek egyes elemeit, részlegeit érinti, hanem a SZIE ügyviteli tevékenységének jelentős körénél problémát okoz.

Vészhelyzet kezelés tervezése: A káreseményeknek az informatikai rendszerek kritikus elemeire vonatkozó hatásait elemzi és tervet ad olyan globális helyettesítő megoldásokra, valamint megelőző és elhárító intézkedésekre, amelyekkel a bekövetkezett káresemény után az informatikai rendszer funkcionalitása eredeti állapotában visszaállítható (DRP - Disaster Recovery Plan).

Visszaállítási eljárás: Az az eljárásrend, amelynek részeként elvégzett tevékenységek, feladatok biztosítják, hogy a helyreállítási eljárással beindított kritikus informatikai szolgáltatás alternatívájáról az ügyviteli folyamat visszaáll a normál üzemmenetre.