Déli Agrárszakképzési Centrum
7100 Szekszárd, Palánk 19. Pf.:228. OM azonosító: 036410
e-mail: centrum@deliaszc.hu ; honlap: www.deliaszc.hu
Telefon: (36)-74/319-876; 74/418-942; 74/446-373

Informatikai szabályzat

Déli ASzC

Kelt: 2020. július 1.

Jóváhagyja:

.....
Simonné Szerdai Zsuzsanna
főigazgató

Hatályba lépteti:

.....
Jeszenka Ildikó
kancellár

TARTALOMJEGYZÉK

1. Bevezetés

AZ INFORMATIKAI BIZTONSÁGI SZABÁLYZAT TÁRGYA

Az Informatikai Biztonsági Szabályzatának (továbbiakban IBSZ) tárgya a Déli Agrárszakképzési Centrum (továbbiakban Déli ASzC) 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.

AZ IBSZ RENDELTETÉSE

Az IBSZ

- a hatályos jogszabályokkal,
- valamint a DÉLI ASZC működési és ügyrendi előírásaival

összhangban teremti meg a DÉLI ASZC információ és informatikai biztonságát.

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

AZ IBSZ MINŐSÍTÉSE

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

A DÉLI ASZC intézményeivel tanulói jogviszonyban levő regisztrált, informatikát használó tanulói a házirendenden keresztül ismerhetik meg az IBSZ-ből származtatott, tanulókra vonatkozó jogokat és kötelességeket.

AZ IBSZ HATÁLYAI

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 DÉLI ASZC informatikai rendszereinek teljes életciklusára (tervezés, fejlesztés, beszerzés, bevezetés, üzemeltetés, kivonás).

<u>Személyi-szervezeti hatályok</u>

Az IBSZ személyi-szervezeti hatálya kiterjed:

- A DÉLI ASZC valamennyi informatikát alkalmazó vagy az informatika környezetében működő szervezeti egységére.
- A DÉLI ASZC valamennyi informatikát alkalmazó vagy az informatika környezetében dolgozó teljes és részmunkaidős alkalmazottjára.
- A DÉLI ASZC-kal szerződéses kapcsolatban álló informatikai vagy informatikához kapcsolódó munkát végző természetes és jogi személyekre. Valamint, más szervezetek

képviseletében a DÉLI ASZC informatikai eszközeit használó munkahelyein vagy ezek környezetében tartózkodó személyekre.
- A DÉLI ASZC intézményeivel tanulói jogviszonyban levő regisztrált, informatikát használó hallgatójára.

Tárgyi hatályok

Az IBSZ tárgyi hatálya kiterjed:
- A DÉLI ASZC tulajdonában lévő, illetve az általa használt valamennyi informatikai berendezésre (számítógépek, nyomtatók, külső háttértárolók, stb.), a számítástechnikai eszközre (aktív hálózati elemek, adathordozók, stb.).
- A DÉLI ASZC területén ideiglenesen használt, a DÉLI ASZC informatikai infrastruktúrájához bármilyen módon kapcsolódó, más szervezetek tulajdonát képező informatikai berendezésekre.
- A teljes számítástechnikai infrastruktúrára (szerverek, kliensek, nyomtatók, rack-szekrények, számítógépes vezetékes illetve vezeték nélküli hálózatok, hálózati aktív eszközök, szünetmentes áramforrások, stb.).
- A szoftverekre (rendszerprogramok, segédprogramok, alkalmazások, adatbázis-kezelők, fejlesztő eszközök, operációs rendszerek, firmware-ek, stb.).
- Az informatikai folyamatban használt összes dokumentációra (tervezési, fejlesztési, üzemeltetési, szervezési, műszaki, informatika biztonsági, fizikai biztonsági dokumentációk stb.).

Területi hatályok

Az IBSZ területi hatálya kiterjed a DÉLI ASZC összes szervezeti egységére, és mindazon területekre, ahol a DÉLI ASZC informatika használatával a tevékenységét kifejti, függetlenül geográfiai elhelyezkedésétől.

Az IBSZ további hatályai

Az IBSZ további hatályai kiterjednek:
- A védelem körébe vont adatok és információk teljes körére, felmerülésüktől, feldolgozási helyüktől és az adatok fizikai megjelenési formájától függetlenül.

AZ ADMINISZTRATÍV BIZTONSÁGI INTÉZKEDÉSEK ÉLETCIKLUSA

Szabályzat, utasítás készítés

A szabályzatokat, 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.

Jóváhagyás és érvényesítés

- Az IBSZ-t a DÉLI ASZC kancellárja, az IBSZ hatáskörébe tartozó operatív utasításokat az IT biztonsági felelős hagyja jóvá.
- Az IBSZ-ben előírt eljárások és szabályok érvényesítése hagyományos vezetési eszközökkel történik, melynek elemei:
  - Irányítás (Tervezés, feladatszabás, előírások, stb.)
  - Ellenőrzés
  - Felelősségre vonás

AZ INFORMATIKAI BIZTONSÁGI RENDSZER MŰKÖDTETÉSE

Megfelelés a jogszabályoknak és a belső szabályzatoknak

A DÉLI ASZC működése követi a rá vonatkozó törvényi előírásokat és jogszabályokat:

- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
- az információs önrendelkezési jogról és az információszabadságról 2011. évi CXII. törvény
- A DÉLI ASZC Szervezeti és Működési Szabályzata

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 IT biztonsági rendszerrel kapcsolatos nem megfelelő működésekről, észrevételekről, javaslatokról a DÉLI ASZC bármely dolgozója köteles tájékoztatni az informatikai vezetőt, illetve az IT biztonsági felelőst.
Az IT biztonsági felelős az igényeket, bejelentéseket megvizsgálja, azokra intézkedési terveket dolgoz ki, amelyeket a DÉLI ASZC kancellárja elé terjeszt jóváhagyásra. Jóváhagyás esetén az IT biztonsági rendszer fejlesztése, módosítása az IT biztonsági felelős felügyelete mellett történik.

VÉDELMI INTÉZKEDÉSEK MEGHATÁROZÁSA

AZ ADATOK ÉS ESZKÖZÖK BIZTONSÁGI BESOROLÁSA ÉS ELLENŐRZÉSE

Számadási kötelezettségek az informatikai eszközökkel kapcsolatban

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

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.

Az adatok osztályozásának irányelvei

A DÉLI ASZC-nál 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:

Osztályozási szintek	Bizalmasság	Sértetlenség	Rendelkezésre állás
1. Nyilvános	Nyilvános	Nem védett	Általános
2. Bizalmas	Belső használatra vagy Bizalmas	Védett	Fontos
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 DÉLI ASZC-nak 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 egy alkalmazottja tölti be, aki az adott belső funkcionális részfolyamatot végzi.
Az adatok osztályozása után meg kell határozni az osztályba sorolási szintnek megfelelően az adatok elvárt rendelkezésre állását is. Ennek alapján a helyi IT biztonsági 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 állású adatokat kezelnek, akkor azok közül a legszigorúbb követelményt kell figyelembe venni.

Adatok nyilvántartása és jelölése

A DÉLI ASZC 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 megjelenési formájától függetlenül az adatok tárolására szolgáló eszközöket jelölni kell a bizalmasság szerint.
Amennyiben egy eszköz többféle minősítésű adatot tárol, akkor a legmagasabb kategóriának megfelelő címkézést kell végrehajtani.
Az adatok jelölési követelményei az 1. számú mellékletben találhatók.

<u>Az adathordozók biztonságos kezelése</u>

Az adathordozók biztonságos kezelésének kialakításával megakadályozható a DÉLI ASZC magasabb szintű adatbiztonsági kategóriákba besorolt adatainak illetéktelen kézbe való kerülése.
A DÉLI ASZC tulajdonában lévő, magasabb szintű adatbiztonsági kategóriákba besorolt adatok tárolására használt adathordozókat egyedi azonosítóval kell ellátni. Az adathordozóra tett címkén, az adattal dolgozó DÉLI ASZC alkalmazottnak fel kell tüntetnie az adott tartalomra vonatkozó bizalmassági kategóriákat. Kezelését ennek megfelelően kell megvalósítani.

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.

Adathordozók másolására vonatkozó szabályok

- „Titkos" adatokat hordozható adathordozóra másolni csak az IT biztonsági felelős és az adatgazda engedélyével szabad.
- Másolás előtt a hordozható adathordozót, a rajta lévő adatok biztonsági osztályba sorolásának megfelelően címkézni kell.
- A másolás után meg kell győződni, hogy a másolt adatok egyeznek-e az eredetivel. Ezt követően az eredeti példánynál leírtak szerint szintén címkézni kell.

Az adathordozók szállításával kapcsolatos szabályok

- „Titkos" adatokat tartalmazó adathordozót a DÉLI ASZC területéről kiszállítani csak az IT biztonsági felelős engedélyével és az adatgazda tudtával szabad.
- Az adathordozó szállítását úgy kell megoldani, hogy az adathordozó felügyelet nélkül soha ne maradhasson.
- Az adathordozó szállítása közben is biztosítani kell az adathordozó gyártója által meghatározott környezeti paramétereket. Általában az adathordozókat magas hőnek, fröccsenő víznek, fizikai behatásnak, mágneses adathordozó esetén elektrosztatikus, és mágneses térnek kitenni is tilos.
- A minősített adatokat tartalmazó adathordozók szállítását dokumentálni kell.

Az adathordozók selejtezésével kapcsolatos szabályok

- Az adathordozók használata során figyelni kell a gyártó által meghatározott selejtezési időpontra, ezen idő után nem biztonságos a használatuk.
- Az elavult, meghibásodott adathordozók selejtezési eljárásáról, a DÉLI ASZC rendszerein az IT biztonsági rendszergazdának kell gondoskodnia. Selejtezésekor az adattárolót adatmegsemmisítési eljárásnak kell alávetni, amely visszavonhatatlanul garantálja az adatok megsemmisítését. Működésképtelen adattárolókat mechanikai úton kell használhatatlanná tenni (pl. átfúrás).
- Az alkalmazandó adatmegsemmisítési eljárás kiválasztása az IT Biztonsági felelős, illetve az IT biztonsági rendszergazdának feladata.
- Függetlenül attól, hogy az adatmegsemmisítést belső vagy külső szakember végzi, a tevékenységet megsemmisítési jegyzőkönyvben kell rögzíteni.
- Az adathordozók újrafelhasználása csak az adatmegsemmisítési eljárás lefolytatását és vírusellenőrzés végrehajtását követően lehetséges.

Szervezeti és személyi biztonság

Informatikai biztonság szervezeti feltételei

A DÉLI ASZC informatikai rendszerében az IT biztonságot az IT biztonság szervezeten keresztül egységesen kezeli. Az IT biztonság szervezet működési feltételeinek megteremtése érdekében a DÉLI ASZC IT biztonsági fórumot működtet és IT biztonsági pozíciókat definiál.
Az IT biztonsággal kapcsolatos stratégiai döntések optimális meghozatalára IT biztonsági fórum működik. Az IT biztonsági fórum szerepét a DÉLI ASZC Informatikai Bizottsága tölti be.
A fórumon résztvevő személyek az alábbiak:

- DÉLI ASZC Kancellár
- DÉLI ASZC Főigazgató
- DÉLI ASZC IT biztonsági felelős
- DÉLI ASZC Intézmények vezetői

Az IT biztonsági fórum évente legalább egy alkalommal ülésezik. Az ülésen született döntéseket, megállapodásokat jegyzőkönyvben dokumentálják, azokat a fórumon résztvevő minden szervezet magára nézve kötelezőnek fogadja el. A fórumot a DÉLI ASZC kancellárja hívja össze.
A kancellár az IT biztonság központi szervezésére és végrehajtására IT biztonsági felelőst, a helyi feladatok koordinációjára és végrehajtására IT biztonsági rendszergazdát nevez ki.

Az informatikai biztonsággal kapcsolatos szerepkörök

Az IT biztonsági felelős és a lokális IT biztonsági rendszergazdák felelősségi területeikbe az alábbi feladatkörök tartoznak:

- Vírusvédelem
- Határvédelem
- Jogosultság kezelés
- Mentések

Az informatikai biztonsági szervezet működései rendje

Informatikai biztonsági feladatkörök

Az IT biztonsági auditor feladatai

- Megtervezi, végrehajtja és dokumentálja a tervezett és a rendszeres belső informatika biztonsági, adatvédelmi, és fizikai biztonsági ellenőrzéseket az IT biztonsági felelős 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 IT biztonsági felelőst.

IT biztonsági felelős feladatai

- Felelős a kockázatkezelési feladatok rendszeres végrehajtásáért, a feltárt kockázatok csökkentésére vonatkozó akciótervek végrehajtásának ellenőrzéséért.
- Javaslatot tesz a DÉLI ASZC Kancellárjának a felvállalható rendszer biztonsági kockázatokra, felhívja a figyelmét a nem felvállalható kockázatokra.
- Felelős az adatosztályozási folyamat fenntartásáért.
- Kezeli, és rendszeresen felülvizsgálja a DÉLI ASZC életbeléptetett biztonsági alapdokumentumait (stratégia, politikák, szabályzatok, katasztrófaterv, stb.). Kijelöli az alacsonyabb szintű, eljárás- vagy eszköz/technológia - specifikus biztonsági

dokumentumok elkészítéséért felelős szervezeti egységeket vagy informatikai vezetőket.

- Együttműködik a DÉLI ASZC tagintézményi informatikai vezetőivel az informatikai rendszerek védelmére megvalósítandó rendszer biztonsági követelmények kialakításában.
- Együttműködik a DÉLI ASZC tagintézményi informatikai rendszergazdáival az IT biztonság fokozása, a biztonsági incidensek elhárítása érdekében
- Ellenőrzi az informatikai rendszer-fejlesztések, bővítések, beszerzések, ezekre vonatkozó szolgáltatási, rendelkezésre állási és más egyéb (pl. szállítási) szerződések egységes rendszer, hálózat és biztonsági szempontból való megfelelőségét.
- Véleményezi a rendszer szintű és hálózati eszköz hozzáférési jogosultságokra, eszköz/objektum hozzáférésekre vonatkozó alkalmazotti, tanulói, adminisztrátori, belső és külső informatika biztonsági ellenőri kéréseket és technikai megoldásokat a Logikai hozzáférési eljárás fejezetben meghatározott jogosultsági előírások, továbbá az IBSZ más fejezetei, illetve a rendszer specifikus fejlesztői dokumentációk alapján.
- Felügyeli a belső és külső informatika biztonsági ellenőrzések végrehajtását.
- Együttműködik az adatgazdával és a létesítmény biztonsági vagy műszaki felelősével az informatikai biztonsághoz kapcsolódó feladatokban.
- Részt vesz a rendszer biztonsági oktatások tematikájának meghatározásában, szakmai felügyeletében.

Adatgazdák IT biztonsági feladatai

Az adatgazdák a DÉLI ASZC 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 DÉLI ASZC adatnyilvántartásainak kialakításában, naprakészen tartásában.
- Rendkívüli események esetére meghatározza a maximális átállási időt (sebezhetőségi ablakot).

IT biztonsági rendszergazdák

Feladataik az alábbi öt fő terület szerint csoportosíthatók:

Vírusok

- Folyamatosan figyeli a megjelenő vírusokról és sérülékenységekről szóló jelentéseket, szükség esetén javaslatokat tesz az IT biztonsági felelősnek 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 IT biztonsági felelősnek.
- Szükség esetén beavatkozik, illetve végrehajtja a mentesítést.
- Elvégzi a DÉLI ASZC-nál 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 IT biztonsági felelősnek 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.
- IT biztonsági felelős 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, katasztrófa 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 DÉLI ASZC 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 IT biztonsági felelősnek és a helyi informatikai vezetőnek.

Általános rendszergazdák

A DÉLI ASZC rendszergazdái a helyi specialitásokat figyelembe véve végzik a helyi rendszerekkel kapcsolatos vírusvédelmi-, mentési-, jogosultság kezelési feladatok végrehajtását, amelyeket a helyileg kinevezett IT biztonsági rendszergazda felügyel, illetve ő maga végez.

A szükséges kompetenciákat, feladatokat és felelősségeket helyileg kell szabályozni.

A személyekhez kapcsolódó biztonsági előírások

Az IT biztonság szintjének fenntartása, mint kiemelt feladat, a DÉLI ASZC-ban a teljes személyi állomány felelőssége.
Az IT biztonság minimálisan betartandó előírásait a „Felhasználói nyilatkozat" tartalmazza.
A felhasználói nyilatkozat tudomásulvétele és aláírása a DÉLI ASZC-nál az informatikai rendszer használatának a feltétele.

Fegyelmi eljárások, szankcionálások

Az IT biztonsági 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 DÉLI ASZC „Belső használatra" illetve „Bizalmas", vagy annál magasabb minősítésű adata, dokumentuma kerül illetéktelen kezekbe.
- a szabálysértés következtében a DÉLI ASZC „Fontos" vagy annál magasabb minősítésű rendelkezésre állás szerint minősített adata, dokumentuma a rendelkezésre állási követelménynek nem tud eleget tenni.
- a szabálysértő a DÉLI ASZC „Védett", vagy annál magasabb sértetlenség szerint minősített adatát, dokumentumát szándékosan meghamisította.
- a szabálysértés következtében a DÉLI ASZC biztonsági rendszerének védelmi megoldásai illetéktelenek kezébe jutottak.
- a szabálysértés következtében bekövetkezett vagyoni hátrány (vagyoni kár, többletköltség) eléri, vagy meghaladja a 10 000 forintot. 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 IT biztonsággal kapcsolatos fegyelmi eljárás lefolytatását az alábbi személyekből álló bizottság hajtja végre:

- A helyi IT üzemeltetésért felelős informatikai vezető, vagy az általa delegált személy
- Munkaügyi vezető, vagy az általa delegált személy
- A szabálysértő személy közvetlen munkahelyi vezetője vagy tanuló esetében a tanulói képviselet megbízottja
- IT biztonsági felelős, vagy az IT biztonsági rendszergazda

Amennyiben a fegyelmi eljárás a felsorolt személyek valamelyikére irányul, új tagságot kell kijelölni.
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.

Informatikai biztonság tudatosítása

A személyi kockázatok csökkentése érdekében meg kell oldani a DÉLI ASZC informatikai rendszerének üzemeltetőinek, használó alkalmazottainak és tanulóinak a biztonsággal kapcsolatos tudatosítását. Ezzel kapcsolatban minden évben tájékoztatást kell tartani.

Külső személyek általi hozzáférések

A DÉLI ASZC informatikai rendszerein csak 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 DÉLI ASZC tanulói 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 DÉLI ASZC vezetői számára szolgáltatott távoli rendszerhozzáférések és a távoli levelezési rendszer hozzáférés biztosítása.)

Külső személyek hozzáféréseit minden esetben naplózni kell.

A hozzáférés csak a munka elvégzésének idejére adható.

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 IT biztonsági 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 a helyi informatikai vezető, magasabb szinten az IT biztonsági felelős, végső esetben a DÉLI ASZC Kancellárja áll rendelkezésre.

Felhasználói felelősségek

A felhasználó általában felelősséggel tartozik:

- A hivatkozott törvények betartásáért,
- A DÉLI ASZC szabályzataiban megfogalmazott előírások betartásáért,
- A törvényekben, szabályzatokban megfogalmazott előírások bárki által történő megszegésének jelentéséért,
- Az IT biztonságért felelős személyekkel való együttműködésért.

Az IT biztonság személyi vonatkozásai

Az IT biztonság a DÉLI ASZC teljes személyi állományának felelőssége. A személyi kockázatok csökkentése érdekében:

- Biztosítani kell a felhasználók rendszeres IT biztonsági oktatását, tudatosítását, tájékoztatását.
- A felhasználóknak rendelkezniük kell a munkaköri kötelességük ellátásához szükséges számítógépes ismeretekkel. A szükséges kompetenciákat a munkaköri leírás tartalmazza.
- Tájékoztatni kell a felhasználókat az IT biztonsággal kapcsolatos feladataikról, és felelősségeikről.
- Minden felhasználónál tudatosítani kell a biztonsági szabályok megsértésével járó szankciókat, és azokat következetesen be kell tartatni.

FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG

A DÉLI ASZC-nál három biztonsági zónát különböztetünk meg a fizikai és környezeti biztonság szempontjából:

- 3-as számú biztonsági zóna: Azok a helyiségek, ahol nincs informatikai eszköz elhelyezve, vagy azoknak folyamatos, állandó felügyelete biztosított.
- 2-es számú biztonsági zóna: Azok a helyiségek, ahol a felhasználói informatikai eszközök vannak elhelyezve.
- 1-es számú biztonsági zóna: Szerverszobák (Kiszolgálók és hálózati aktíveszközök).

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

Eszközök kivitele

Az eszközök átmeneti kivitele

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

- az informatikai eszközökön tárolt adatokat az IT biztonsági rendszergazdának visszaállíthatatlanul törölnie kell (pl. szoftveres úton bináris felülírással) vagy selejtezéskor használhatatlanná kell tenni az adattárolót (pl. a diszk átfúrásával),
- 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 el szállíttatni.
- a szállítólevél kiállításának feltétele a kiegyenlített számla, vagy a selejtezési jegyzőkönyv.

IT FOLYAMATOK BIZTONSÁGA

Informatikai rendszerek tervezése és jóváhagyása

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

Az IT biztonsági felelősnek 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 DÉLI ASZC szoftveres, hardveres illetve egyéb standardjainak való megfelelés

IT eszközök beszerzésének biztonsága

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

Az üzemeltetés biztonsága

A megbízható és biztonságos üzemeltetés érdekében szabályokat, eljárásokat kell kidolgozni az informatikai rendszerhez kapcsolódó folyamatok - javítások, karbantartások, szoftvertelepítések és beállítások, stb. - végrehajtására.
A szabályokat, eljárásokat össze kell hangolni az érvényben lévő IT biztonsági 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 a kancellár gondoskodik. Az IT biztonsági felelős feladata a dokumentációk évenkénti felülvizsgálata.

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 IT biztonsági, 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 IT biztonsági előírásokat érvényesíteni kell a fejlesztéssel, bővítéssel kapcsolatos szerződésekben, megállapodásokban.
A fejlesztési, bővítési dokumentációk elkészítéséért a fejlesztésért felelős lokális informatikai vezető gondoskodik. A fejlesztési és bővítési dokumentációkat „Bizalmas" minősítésű információnak kell tekinteni.
A fejlesztési, bővítési és egyéb rendszerdokumentációk biztonságos tárolásával kapcsolatos ellenőrzés az IT biztonsági felelős feladata.

Rendszergazdai tevékenységek naplózása

A DÉLI ASZC üzemeltetésű rendszereken végzett rendszergazdai (operátori) tevékenységként értelmezzük a DÉLI ASZC alapfeladatát támogató informatikai rendszer üzemeltetetését, javítását, karbantartását rendszergazdai jogosultsággal végző tevékenységeket.
Ezen tevékenységek megkezdését a lokális informatikai vezető tudtával és szükség esetén koordinálásával/felügyeletével kell az arra kijelölt/megbízott rendszergazdáknak elvégeznie.
Az elvégzett munkát vagy tevékenységet naplózni kell írásos, vagy elektronikus formában (pl.

szerver napló).

BIZTONSÁGI INCIDENSEK KEZELÉSE

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

A DÉLI ASZC informatikai rendszerét használója köteles értesíteni az IT biztonsági felelőst vagy a lokális IT biztonsági rendszergazdát az általa észlelt biztonsági incidensekről.
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 (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.

Az incidensek kezeléséért felelős személyek az alábbiak:

- Kisebb incidensek: helyi IT biztonsági rendszergazda
- Vírusvédelmi incidensek: helyi IT biztonsági rendszergazda
- Határvédelmi incidensek: helyi IT biztonsági rendszergazda és IT biztonsági felelős
- Jogosultsági incidensek: IT biztonsági rendszergazda
- Rendelkezésre állási incidensek: Adott rendszer/eszköz rendszergazdája,
- Törvény-, szabály-, és eljárássértések: IT biztonsági felelős

Incidensek priorizáiása

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 kivizsgálását két órán belül meg kell kezdeni, ha az egy magasabb prioritású incidens elhárítása nem akadályozza.

- Egyszeri vírusfertőzés, vagy helyi vírusvédelmi eszköz kiesése.
- 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.

Biztonsági incidensek kezelésének folyamata

Incidens bejelentés bármely DÉLI ASZC informatikai eszközt használó, vagy üzemeltető DÉLI ASZC munkatárstól illetve tanulótól érkezhet munkaidőben.

- 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 az IT biztonsági rendszergazda vagy az általános 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 az IT biztonsági rendszergazda vagy az általános rendszergazda saját hatáskörben nem tudja megoldani a bejelentett incidenst, prioritástól függően azonnal értesíteni kell a helyi informatikai vezetőt vagy az IT biztonsági felelőst. Ebben az esetben a probléma megoldására az adott helyi informatikai vezető és/vagy az IT biztonsági felelős és az IT biztonsági illetve általános 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 IT biztonsági felelős az adott helyi informatikai vezetővel és az IT biztonsági illetve általános 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 IT biztonsági felelős az adott helyi informatikai vezetővel az alábbi döntés előkészítő javaslatokat teszi a DÉLI ASZC Kancellárja részére:
    - A probléma súlyosságát mérlegelve vészhelyzetet kell elrendelni és a vészhelyzeti terveknek megfelelően a normál működésre történő visszaállítást (DRP, vészhelyzeti terv, stb.) végrehajtani.
    - A probléma súlyosságát mérlegelve fejlesztések, vagy beszerzések elindítása.
    - Az incidens okozta kockázatokat csak a DÉLI ASZC informatikai vezetői vállalhatják fel az IT biztonsági felelős javaslata alapján.

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

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.
A hiba okát ismerve intézkedéseket kell tenni a kiváltó ok végleges megszüntetésére, illetve az általa okozott probléma előfordulási gyakoriságának csökkentésére.

ADATVÉDELMI ELJÁRÁSOK MENEDZSMENTJE

A határvédelem megvalósítása

A DÉLI ASZC 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 csak az Internet felé nyújtanak szolgáltatásokat.
A DÉLI ASZC egységes és homogén határvédelmi eszközöket alkalmaz (tűzfal, vírusvédelmi gateway-ek, appliance, stb.) amelyek optimális életciklusa 1 év. Az életcikluson belül az eszköz még megfelelő védelmet nyújt. Az egy éves életciklus leteltével a határvédelmi eszköz fejlesztése (cseréje, upgrade-je, újra licencelése, stb.) szükséges.
Az életcikluson belül a határvédelmi eszközök biztonsági frissítéseit rendszeresen 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 DÉLI ASZC 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.

Vírusvédelem

A vírusvédelem irányelvei:

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

- Megelőzés: a DÉLI ASZC 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 DÉLI ASZC igyekszik rugalmasan, gyorsan, és hatékonyan reagálni.
- Tudatosság: A vírusvédelmi rendszer hatékonyága jelentős mértékben növelhető, ha a vírusvédelemben résztvevő személyek (informatikai dolgozók, felhasználók), felkészültsége, motivációja, illetve tudatos felelősségvállalása biztosított.

A DÉLI ASZC-nál a vírusvédelem központilag irányított folyamat.

A jogosultsági rendszer megvalósítása

Az adatok bizalmasságának és sértetlenségének biztosítása érdekében a DÉLI ASZC-nál egységes jogosultság kezelő és nyilvántartó rendszer működik, amely alapja az Aktív Direktori (AD) rendszer.

Az egységes jogosultság kezelő és nyilvántartó rendszert felépítése és kialakítása olyan, hogy a DÉLI ASZC minden alkalmazottja és tanulója számára biztosítsa a munkájához, illetve tanulásához szükséges és elégséges hozzáféréseket.

A jogosultság kezelő és nyilvántartó rendszer az alábbiakra terjed ki:

- A 3. számú biztonsági zónába történő belépésre jogosultak körének meghatározása.
- A rendszer szintű hozzáférések (hálózati hozzáférések) körének meghatározása.
- Helyi hozzáférések (szerverek, munkaállomások, egyéb eszközök hozzáférései) körének meghatározása.
- Megosztott erőforrásokhoz való hozzáférések (mappák, nyomtatók) objektumonkénti meghatározása.
- A kiadott jogosultságok nyilvántartására.

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

Mentés, archiválás, visszatöltés

Az adatok rendelkezésre állásának biztosítása érdekében a DÉLI ASZC-nál 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.

IT SZOLGÁLTATÁSOK BIZTONSÁGA

Alkalmazás-, és szoftvereszközök használatának szabályozása

A DÉLI ASZC minden intézménye és tanulója számára biztosítja a munkához, illetve a tanulmányokhoz szükséges jogtiszta szoftvert.

A személyhez kötött munkaállomásokra csak azok az alkalmazások, és szoftver eszközök telepíthetők, amelyre az alkalmazottnak a munkájához szüksége van.

A szoftverek telepítése a rendszergazdák feladata.

Az elektronikus adatok és a levelezés biztonságának irányelvei

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

A felhasználók szellemi tevékenység eredményeként előálló és szerzői jogvédelem alá eső elektronikus állományok készítéséhez és tárolásához DÉLI ASZC rendszer illetve erőforrások igénybevételére engedélyt kérhetnek közvetlen munkahelyi vezetőjüktől. A DÉLI ASZC rendszereit és erőforrásait csak az engedélyezett módon és mértékben használhatják. A DÉLI ASZC rendszerein, ily módon elhelyezett adatokért a felhasználót terhel minden jogi felelősség. Eben az esetben, az elhelyezett adatok sértetlenségéért és biztonságáért a DÉLI ASZC semmilyen felelősséget nem vállal. A használatot a DÉLI ASZC kijelölt szakemberei ellenőrizhetik, illetve korlátozhatják.

Az Internet elérés biztonságának irányelvei
A DÉLI ASZC az Internet elérést a DÉLI ASZC ügyviteli és oktatási folyamataihoz, és az azokat támogató folyamatok fenntartásához a Tarr hálózatán keresztül biztosítja.

Fájl kezelés / Címtár kezelés
A DÉLI ASZC informatikai rendszerében kezelt (továbbított, tárolt) elektronikus adatok így a fájlok is a DÉLI ASZC tulajdonát képezik.
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.

A BIZTONSÁGI SZINT MÉRÉSE, MONITOROZÁSA

A BIZTONSÁGI SZINT MÉRÉSÉNEK FELTÉTELEI

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

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

A BIZTONSÁGI SZINT MÉRÉSÉNEK ESZKÖZEI ÉS MÓDSZEREI

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

- Az IT rendszer Internet felöli sérülékenységeinek vizsgálata
- Az IT rendszer Intranet felöli sérülékenységeinek vizsgálata

Technikai szintű auditot a DÉLI ASZC-nál kétévente, a fenyegetettségek felmérésével egy időben kell elvégezni.

Személyi biztonság szintjének mérése
A személyi biztonság szintjének mérését a DÉLI ASZC-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

IT rendszer monitorozása

Az IT rendszer kritikus elemeit, illetve biztonsági eszközeit folyamatosan kell monitorozni. A monitorozás 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.)

A MÉRÉSI ADATOK FELDOLGOZÁSA, VISSZACSATOLÁSA

Az IT biztonság szempontjából kritikus pontokon mérési és ellenőrzési rendszert kell bevezetni. A mérések eredményéről az IT biztonsági felelős évente írásban számol be az Informatikai Bizottságnak. Félévente számol be a DÉLI ASZC Kancellárjának annak érdekében, hogy a központi rendszereket érintő esetlegesen felmerült kockázatok kezelése időben megtörténjen.
A mérési rendszer kontroll pontjait összefoglaló táblázat a 3 számú mellékletben található.

ELLENŐRZÉSI IRÁNYELVEK

Az informatikai 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 informatikai biztonsággal kapcsolatos ellenőrzések területei az alábbiak lehetnek:

- Megfelelőségi vizsgálat. Célja felderíteni, hogy a DÉLI ASZC szervezeti egységei rendelkeznek-e a törvényi előírásokban meghatározott személyi, eljárási, tárgyi

feltételekkel, és azok megfelelően dokumentáltak-e.

- Az informatikai biztonság szintjére vonatkozó vizsgálat. Célja felderíteni, hogy a DÉLI ASZC szervezeti egységeinél az informatikai biztonság szintje megfelel-e a meghatározott védelmi szintnek.
- Az informatikai biztonsági szabályok betartásának ellenőrzése. Célja felderíteni, hogy a DÉLI ASZC informatikai biztonsági szabályait az illetékes személyek ismerik-e, illetve betartják-e. Ez az ellenőrzés az informatikai biztonság egy-egy területére is leszűkíthető.

Az ellenőrzések során elsősorban az alábbiakat kell vizsgálni:

- Az IT biztonsági rendszer működése megfelel-e a törvényi előírásoknak
- Az IT biztonsági szabályok érvényesítve vannak-e a folyamatokban
- Az IT biztonsági rendszer előírt dokumentumai léteznek-e, illetve naprakészek-e
- Az IT személyzet, illetve a felhasználók rendelkeznek-e a megfelelő IT biztonsági 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 informatikai 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 IT biztonsági rendszer, illetve annak egyes elemeit rendszeresen felülvizsgálatra kerülnek. A biztonsági rendszerek felülvizsgálati idejét összefoglaló táblázat a 3. számú mellékletben található.

A SZERVERTEREM KIALAKÍTÁSÁNAK KÖVETELMÉNYEI

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 folyosók, lépcsők 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:
- Álpadló, a berendezések mennyezetről való táplálása
- Falak, nyílászárók vízbehatolás elleni védelme
- Ún. védőtálcák alkalmazása a berendezések elhelyezésére

A szerverterem behatolás védelme

A szerverterem behatolás-védelmének biztosítása érdekében az alábbi szempontokat kell érvényesíteni:

- Biztonsági záras, kulccsal záródó ajtó, mely kifelé kézzel nyitható (a menekülés biztosítása érdekében).

A szerverterem tűzvédelme

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

- Kézi tűzoltó-berendezések elhelyezése a bejárat közvetlen közelében.

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.

A szerverterem klímatizálása

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

- A szerverteremben lehetőség szerint klíma-berendezéseket kell üzemeltetni, a megfelelő üzemi hőmérséklet szabályozására. Amennyiben ez nem lehetséges, a megfelelő szellőztetéssel kell biztosítani a megfelelő hőmérsékletet.

Zavarvédelem

A szerverterem zavarálló képességének biztosítására az alábbiakat kell megfontolni:

- Gépészeti eszközök (víz-, gáz-, fűtésvezetékek, stb.) eltávolítása javasolt.

- A szerverteremtől távol kell tartani a kisugárzásra alkalmas eszközöket (mobiltelefonok, GPRS eszközök).

A SZERVERTEREM HOZZÁFÉRÉSI KÖVETELMÉNYEI

A szerverterem nyitásának, és zárásának szabályai
A szervertermet zárva kell tartani., amennyiben a rendszergazda nem tartózkodik benn.

A szerverterembe történő belépés, kilépés rendje
Kerülni kell a szerverteremben indokolatlan belépést.
A szerverterembe csak az arra felhatalmazott személyek léphetnek be.

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.

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 szoftver licencelési lehetőségeket,
- A DÉLI ASZC teljes informatikai rendszerére vonatkozó informatikai fejlesztési és bővítési terveket, a homogén rendszer kialakítására és megtartására irányuló előírásokat és standardokat valamint az IT biztonsági 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 DÉLI ASZC 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 DÉLI ASZC 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 „Beszerzési szabályzat"-ban kell rögzíteni.

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

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

A szolgáltatások minőségének ellenőrzését a lokális informatikai vezető végzi.
Szerződésekre, dokumentumokra vonatkozó előírások

<u>A beszállítói szerződésekre vonatkozó előírások</u>
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 DÉLI ASZC-ról 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.

<u>A szolgáltatói szerződésekre vonatkozó előírások</u>
A szolgáltatói szerződésekben az alábbiak szerint kell érvényesíteni a biztonsági szabályokat:
A szolgáltatónak kollektív titoktartási nyilatkozatot kell tennie a szerződésben, vagy különálló dokumentumban, amelyben a szolgáltató felelősséget vállal arra, hogy az általa szállított megoldásokról, illetve a DÉLI ASZC-ról 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 kel 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 DÉLI ASZC teljes informatikai rendszerére vonatkozó, az egységes üzemvitel kialakítására és megtartására irányuló előírásokat és standardokat valamint az IT biztonsági követelményeket.

A DOKUMENTUMOKKAL KAPCSOLATOS KÖVETELMÉNYEK

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

- 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.

AZ ÜZEMELTETÉSHEZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEK

Az üzemeltetési folyamatok részletes szabályozását az „IT üzemeltetési szabályzat"-ban kell megvalósítani.
Az üzemeltetési szabályzat az alábbi területek részletes szabályozását kell megvalósítani:

- Incidenskezelés:

Tartalmazza az üzemeltetés során bekövetkezett, a normál működéstől eltérő események bejelentésével, kezelésével kapcsolatos eljárásokat, feladatokat, felelősségeket.

- Problémakezelés:

Tartalmazza az ismert üzemeltetési incidensek elhárítására kialakított eljárásokat, feladatokat, és felelősségeket

- Konfigurációkezelés:

Tartalmazza a munkaállomások, szerverek konfigurációival kapcsolatos szabványosítási, dokumentálási, nyilvántartási előírásokat.

- Kapacitáskezelés:

Tartalmazza a munkaállomások, szerverek teljesítmény, és kapacitásnövelési igényeinek mérésével, és kielégítésével kapcsolatos eljárásokat.

- Változáskezelés:

Tartalmazza az IT eszközök változás kezelésével (verzióváltás, frissítések, stb.) kapcsolatos előírásokat, eljárásokat, és felelősségeket.

- Javítások:

Tartalmazza, a meghibásodott IT eszközök javítására vonatkozó eljárásokat, feladatokat, és felelősségeket.

- Karbantartások:

Tartalmazza, az IT eszközök tervszerű megelőző karbantartásával kapcsolatos eljárásokat, feladatokat, és felelősségeket.
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 ügyelni kell arra, 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. tanulói 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 DÉLI ASZC 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.

INFRASTRUKTURÁLIS RENDSZERFEJLESZTÉSSEL KAPCSOLATOS KÖVETELMÉNYEK

SZAKMAI KÖVETELMÉNYEK MEGHATÁROZÁSA

A DÉLI ASZC-ban ki kell dolgozni egy egységes fejlesztési tervet, 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 DÉLI ASZC lokális informatikai vezetői közösen, egymással szorosan együttműködve gondoskodnak.
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 IT biztonsági felelősnek végig kell kísérni. A fejlesztéssel kapcsolatos szerződéseket az IT biztonsági felelősnek véleményezni szükséges.
Infrastrukturális fejlesztéssel kapcsolatos szerződések tartalmi követelményei
Az infrastrukturális rendszerfejlesztésekkel kapcsolatos szerződések tartalmazzák az alábbi követelményeket:

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

Dokumentációval kapcsolatos követelmények
Az infrastrukturális rendszerfejlesztések alkalmával az alábbi dokumentációkat kell elkészíteni:

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

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

ROSSZINDULATÚ PROGRAMOK ELLENI VÉDEKEZÉS ALAPJAI

Vírusvédelmi események

A fertőzés nagyságától függően az alábbi területeket különböztetjük meg:

- Elszigetelt: ha a DÉLI ASZC 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 DÉLI ASZC 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.

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.

A VALÓSIDEJŰ VÉDELEM KIALAKÍTÁSA

A DÉLI ASZC-nál 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 az IT biztonsági rendszergazda számára, és a fertőzés gyanús állományt a rendszer automatikusan karanténba helyezi.
A vírusfertőzésről vagy annak gyanújáról a felhasználó köteles értesíteni a helyi IT biztonsági rendszergazdát.

MANUÁLISAN INDÍTOTT/IDŐZÍTETT TELJES FÁJLRENDSZER ÁTVIZSGÁLÁSA

A védendő kiszolgáló eszközökön a teljes állományrendszer vírusellenőrzését legalább havi egy alkalommal végre kell hajtani. A vírusellenőrzést ütemezve minden szerveren el kell indítani.
A helyi vírusvédelmi eszközökön indított állomány ellenőrzést úgy kell ütemezni, hogy a vírusvédelmi ellenőrzés abban az időszakban kerüljön végrehajtásra, amikor a napi munkát a legkisebb mértékben gátolja, illetve alacsony processzor és memória terhelést okozzon.
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, jog tiszta vírusvédelmi keresőprogramok segítségével is (a vírusvédelmi szoftverek gyártói, valamint a Microsoft rendszeresen ad ki egy konkrét fenyegetettség felismerésére, mentesítésére programot).

A VÍRUSVESZÉLY CSÖKKENTÉSÉNEK HARDVERES ÉS SZOFTVERES LEHETŐSÉGEI

Egyéb hálózati eszközök alkalmazása a vírusvédelemben

A DÉLI ASZC-nál 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.

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.

Szoftverek biztonsági frissítése

A vírusfertőzések kockázatainak csökkentése érdekében a DÉLI ASZC-nál központilag menedzselt Windows SUS 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.

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

Általános előírások

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

A szerverekhez vagy munkaállomásokhoz tilos nem DÉLI ASZC tulajdonú perifériát csatlakoztatni.

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

Levelezés biztonsága

Tilos megnyitni ismeretlen forrásból származó elektronikus levelet. A levél fertőzöttségének elbírálásához az alábbiakat kell figyelembe venni:

- A levél feladója ismert személy-e, illetve várható-e levél a feladótól? (Fertőzött levél ismert személytől, vagy ismerősnek tűnő forrásból is származhat!)
- A levél tárgya: gyanús a levél, ha az nem munkaköri feladatokkal vagy várt információval kapcsolatos.
- A levél címzettje: fertőzött lehet a levél, ha szokatlanul sok a címzettje.
- A levél nyelvezete: fertőzött lehet a levél, ha idegen nyelven, vagy nem a szokásos kommunikációs nyelven íródott.
- A levél csatolmánya: gyanús lehet a levél, ha az alábbi kiterjesztésű csatolt állományt, például ,bat, .com, .exe, .dll, .sys, .bit, .pif, .hlp .txt, vagy beágyazott linket (URL) tartalmaz.
- A fertőzöttnek ítélt elektronikus levelet a mellékletek megnyitása nélkül törölni kell, még a törölt levelek mappájából is.

Internetezés biztonsága

A DÉLI ASZC-nál tilos a fájlletöltő oldalak, Internetes játékoldalak, ún. csevegő oldalak, valamint szexuális szolgáltatásokat kínáló oldalak látogatása.
Tilos az ügyvitellel és az oktatási, kutatási feladatokkal össze nem függő fájlok megnyitása, letöltése az Internetről. A letöltéseket átmeneti mappába (külön létrehozandó) kell elhelyezni.

Adathordozók kezelése

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

Vírusvédelmi incidensek jelentése

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

A VÍRUSVÉDELMI FELELŐSSÉGEK FELADATOK

A DÉLI ASZC-nál a vírusvédelmet egységesen kell kezelni. A vírusvédelmi feladatok végrehajtása kétszintű:

Felső szint: IT biztonsági felelős

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.

Technikai szint: IT biztonsági 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 IT biztonsági 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 mentesítést.
- Rendszeresen, de legalább hetente minden védendő eszközön ellenőrzi vírusvédelem működőképességét, illetve a vírusszignatúrák frissességék.
- szintű eseménynél kivizsgálja a vírus eredetét, és amennyiben lehetséges mentesíti

azt. Amennyiben a fertőzést emberi mulasztás okozta, vagy a jelenséget trójai vagy kémprogram okozta, azt jelenti az IT biztonsági 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.
- Támogatást nyújt a rendszergazdáknak a rendszerek visszaállításánál.
- A visszaállítás után a kivizsgálja a fertőzés okát, lokalizálja annak forrását, majd jelenti az IT biztonsági felelősnek.

A VÍRUSVÉDELMI ESZKÖZÖK ÜZEMELTETÉSE

A vírusvédelmi eszközök üzemeltetéséért a DÉLI ASZC helyi informatikai vezetői a felelősök. Az üzemeltetési feladatokat a következő pontok figyelembe vételével kell végrehajtani:

A vírusvédelmi eszközök javítása

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

A vírusvédelmi eszközök karbantartása

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

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.

ELLENŐRZÉSEK

Általános felülvizsgálat

A vírusvédelmi rendszer általános felülvizsgálatát kétévente független külső szakértőkkel el kell végeztetni; a megrendelés kezdeményezése az IT biztonsági felelős feladata. A felülvizsgálat célja, hogy meghatározza a vírusvédelmi rendszer fejlesztési irányait, annak költségvonzatát.

Éves felülvizsgálat

Az IT biztonsági felelős kötelessége, hogy évente a szabályzat hatálya alá tartozó tárgyi eszközökön auditot végezzen, mely teljes körű:

- a DÉLI ASZC üzemeltetésben lévő összes kiszolgálóra,
- a DÉLI ASZC üzemeltetésben lévő levélforgalmat lebonyolító rendszerekre,
- a határvédelmi eszközökre.

Negyedéves ellenőrzés

Minden három hónapban az IT biztonsági rendszergazdának kötelessége vírus statisztikákat elkészíteni és az IT biztonsági felelős részére eljuttatni.

Az IT biztonsági felelős kötelessége, hogy háromhavonta feldolgozza a központi adatbázisba bejegyzett riasztásokat meghatározva:

- a vírusvédelmi eszközök által felismert és sikeresen elhárított vírustámadásokat,
- a vírusvédelmi eszközök által felismert és sikeresen elhárított, de további emberi beavatkozást kívánó vírustámadásokat,
- a vírusvédelmi eszközök által felismert, de nem mentesített támadásokat,
- a vírusadatbázis frissítésekkel kapcsolatos riasztásokat szerverenként, a vírustámadások eloszlását, telephelyek, vírusfajták szerint.

A JOGOSULTSÁGI RENDSZER ELŐÍRÁSAI

A HOZZÁFÉRÉSI RENDSZER KIALAKÍTÁSA

A hozzáférés követelményrendszere

A DÉLI ASZC-nál a hozzáférési jogosultságok kialakítását szabályozó követelmények a következők:

- 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 DÉLI ASZC 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. Munkájuk végén, vagy az előre meghatározott időtartam lejárta után a jogokat azonnal meg kell vonni.
- A követelményrendszert évente felül kell vizsgálni, és javított formában a rendszergazdák számára át kell adni. A felülvizsgálatot az IT biztonsági felelős végzi.

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.

Felhasználói csoportok létrehozása

A DÉLI ASZC 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 DÉLI ASZC adott intézményéhez tartozó informatikai szervezet nyilvántartja, és a DÉLI ASZC számára közzéteszi az aktuális felhasználói csoport listát

Jogosultságok felhasználói csoporthoz rendelése

A DÉLI ASZC 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

Hozzáférési jogosultságok nyilvántartása

A hozzáférési jogosultságot írásban (elektronikus módon, vagy hagyományosan papíron) és névre szólóan kell meghatározni. Erre a célra szolgál a „Rendszer hozzáférési engedély kérő" amelyet a hozzáférési nyilvántartásban kell nyilvántartani. A „Rendszer hozzáférési engedély kérő"-t a DÉLI ASZC alkalmazottak esetében kell használni.

A hallgatók hozzáférési jogosultságát a tanulói jogviszonyt nyilvántartó szervezeti egységnek kell kötegelt módon (hagyományos módon papír alapú listán vagy elektronikusan) kérnie a lokális informatikai szervezettől, vagy az erre szolgáló elektronikus nyilvántartó rendszerben naprakészen adminisztrálnia. A megfelelő eljárást a helyi informatikai vezető és a nyilvántartást végző szervezeti egység vezetője határozza meg, melyet dokumentumban rögzítenek, és minkét részről gondoskodnak a folyamat működtetéséről és a feladatok végrehajtásáról.

Az informatikai rendszereken belüli hozzáférési jogosultságok nyilvántartása a DÉLI ASZC helyi informatikai szervezeteinek, ezen belül az IT biztonsági rendszergazda feladata.

Külön dokumentumban kell nyilvántartani az egyes rendszerek IT biztonsági felelőseit, általános rendszergazdáit, illetve az egyes szervezeti egységek adatgazdáit!

Felhasználói jogosultságok létrehozása, megszűntetése, megváltoztatása

- Új munkatárs hozzáférési rendszerbe való illesztését, vagy jogosultsággal rendelkező munkatárs jogosultság változási igényét a „Rendszer hozzáférési engedély kérő" űrlap kitöltésével és elküldésével, az adott szervezeti egység vezetője írásban (elektronikusan vagy hagyományos módon) igényeli a helyi informatikai szervezet IT biztonsági rendszergazdájának való megküldésével.
- A DÉLI ASZC informatikai rendszeréhez kizárólag olyan munkatárs kaphat hozzáférést,

akinek a személyi lapja a munkaügyi osztály rendszerébenben rögzítésre kerül.

- Új tanuló hozzáférési rendszerbe való illesztését, vagy jogosultságának felfüggesztési (tanulói jogviszony szüneteltetése) illetve megszüntetési (tanulói jogviszony megszűnése) igényét a nyilvántartást vezető szervezeti egység kötegelt módon kéri a helyi informatikai szervezettől, az előző alfejezetben részletezett módon.
- A jogosultság létrehozása és nyilvántartásba vétele előtt a helyi IT biztonsági rendszergazda ellenőrzi a kitöltött Rendszer hozzáférési engedély kérő űrlapot vagy a kötegelt állományt. Annak jogosultságát aláírásával igazolja vagy elektronikusan archiválja azt.
- A jogosultságot kezelő rendszergazda, vagy az IT biztonsági rendszergazda feladata a kitöltött Rendszer hozzáférési engedély kérő űrlap vagy a kötegelt állomány alapján a felhasználó megfelelő, alkalmazásokra lebontott jogosultsági szintjeinek beállítása, az elektronikus levelező fiók létrehozása, a címtári bejegyzések elvégzése, valamint a felhasználói azonosító aktiválása.
- Minden felhasználó (alkalmazott és tanuló) definiálásánál biztosítani kell az 1 természetes személy = 1 felhasználói azonosító, egy-egy értelmű megfeleltetést, azaz nem lehet közösen használt felhasználói azonosító.
- Alkalmazott esetében a felhasználói hozzáférés zárolása automatikusan történik az alkalmazott kilépésekor. Ennek biztosítására:
    - Azonnali felmondás esetén, illetve ha a kilépő alkalmazott vezetője úgy ítéli meg, a jogosultság azonnal visszavonásra kerül. A kilépő alkalmazott vezetője ebben az esetben telefonon értesíti a helyi IT biztonsági rendszergazdát vagy informatikai vezetőt. A telefonos értesítést írott formában (e-mail vagy papír) is meg kell erősíteni.
    - Határozott idejű felmondás esetén a jogosultság visszavonása a „sétálólap" aláírásával egy időben történik.
- Alkalmazott esetében a helyi informatikai vezető 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, tanuló) jogviszonyában változások következnek be, de a munkáltatói jogviszony (áthelyezés más osztályra, munkakör vagy munkaköri leírás megváltozása) vagy a tanulói kapcsolat valamilyen formája (pl. öreg diák) továbbra is a DÉLI ASZC-hoz köti, a felhasználót a felhasználói és hozzáférési jogosultságokat az új jogviszony szerint kell beállítani.

A JELSZAVAS VÉDELEM FELÉPÍTÉSE, FAJTÁI

A DÉLI ASZC 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, rendszrgazda, 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).

ILLETÉKTELEN HOZZÁFÉRÉS ELLENI VÉDELEM

Jelszómenedzsment

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

A DÉLI ASZC 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 alfanumerikus karaktereket.
- 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, aaaaa, qwert, asdfg, gegegeg, stb.).

- Ne utaljon a felhasználóra, munkakörére, munkahelyére.

A helyes jelszóhasználatról és az alap kritériumokról a felhasználókat - saját érdekükben - tájékoztatni kell.

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 12 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.
- Ha egy alkalmazotti felhasználói azonosító 60 napig inaktív, akkor azt a szervezeti egység vezetőjének tájékoztatása mellett a rendszert üzemeltető rendszergazdának fel kell függeszteni.
- Ha egy tanulói felhasználói azonosító a következő évtől kezdődően (~150 napig) inaktív, akkor azt a tanulói nyilvántartást vezető szervezeti egységnek jeleznie kell a rendszert üzemeltető rendszergazdának, és azt fel kell függeszteni.

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

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 24 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 DÉLI ASZC adott szervezetének vezetője által használt tűzálló páncélszekrényben.

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 DÉLI ASZC helyi informatikai vezetője rendelheti el. A borítékot az informatikai vezető, vagy távollétében helyettese jogosult felbontani. A felbontásnál meg kell határozni a felbontás elrendelésének okát, és a felbontás bekövetkeztéről írásos feljegyzést kell készíteni, és értesíteni kell az IT biztonsági felelőst. Az IT biztonsági felelős illetve IT biztonsági 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: eredeti formában a jelszavakat tárolni nem szabad. Egy utas módon kell titkosítani, és bejelentkezésnél a titkosított jelszavakat kell összehasonlítani.
A felhasználó rendszerek biztonságos jelszó tárolási mechanizmusát, módszerét az IT biztonsági felelős ellenőrzi, illetve hagyja jóvá.
A jelszavak továbbítása a hálózaton titkosítás nélkül tilos.
Alkalmazotti munkaállomásokra vonatkozó előírások
Azokban a helyiségekben, ahol a DÉLI ASZC több munkatársa is tartózkodhatnak, a munkaállomások monitorait lehetőleg úgy kell elhelyezni, hogy a monitorokon esetlegesen kiírásra kerülő bizalmas adatokat illetéktelen személyek vizuálisan leolvasni ne tudják.
Azt a munkaállomást, melyen - nem rendszergazda jogosultságú - bejelentkező névvel felhasználó lépett be, csak abban az esetben szabad felügyelet nélkül hagyni, ha a munkaállomáson jelszóvédelemmel rendelkező képernyő-védőt alkalmaznak, vagy a munkaállomást zárolják.
Azt a munkaállomást, amelyen „rendszergazda" jogosultságú bejelentkező névvel léptek be, személyes felügyelet nélkül hagyni nem szabad. A rendszergazda jogosultsággal belépett munkatárs felelős azért, hogy a kijelentkezéséig a munkaállomás őrzése biztosított legyen.
Felhasználók bejelentkezése
A DÉLI ASZC 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.
Felhasználók logikai hozzáféréssel kapcsolatos kötelességei, felelősségei
A felhasználóknak ismerniük kell a jelszavak, illetve a felhasználó kezelésében lévő berendezések használatára vonatkozó előírásokat.
A DÉLI ASZC informatikai rendszerének használatával kapcsolatos felhasználói feladatok:
A felhasználói jelszavak titkosan kezelendők.
A jelszó elfelejtése esetén a felhasználó az IT biztonsági 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.
A jelszavakat a felhasználó nem írhatja le.
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 IT biztonsági felelősnek.
Felügyelet nélkül hagyott alkalmazotti munkaállomások
Ha a felhasználó szüneteltetni munkaállomáson végzett tevékenységét, ki kell jelentkeznie, vagy zárolnia kell a számítógépet. Amennyiben rendszeresen nem jelentkezik ki, 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.
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 operációs rendszerhez, illetve az alkalmazói rendszerekhez való hozzáférés esetén, ahol lehet, az utolsó sikeresen bejelentkezett felhasználói azonosítónak rejtve kell maradnia (domain policy).

A hozzáférés ellenőrzése

A DÉLI ASZC jogosultsági rendszerét meghatározott időközönként, de legalább évente felül kell vizsgálni, melynek felelőse az IT biztonsági 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 az adott az IT biztonsági felelős vagy IT biztonsági 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 az IT biztonsági felelősnek vagy IT biztonsági 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.

MENTÉS, ARCHIVÁLÁS, ÉS VISSZATÖLTÉS

A dokumentum célja, hogy meghatározza a DÉLI ASZC 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.
Felelősségek
A helyi informatikai vezető elektronikusan tárolt adatok mentésével kapcsolatos feladatai és felelőssége:

- felelős a DÉLI ASZC adott karának vagy intézetének mentési, archiválási rendjének kidolgozásáért.
- felelős a mentési, archiválási rend rendszeres ellenőrzéséért.
- felelős a mentési rendet érintő változások követéséért, illetve a mentési rendről szóló dokumentációk felülvizsgálatáért.
- felelős a mentési feladatokkal megbízott rendszergazda által jelentett incidensek kezelésére vonatkozó intézkedések foganatosításáért, illetve szükség esetén a kezeléshez szükséges erőforrások biztosításáért.
- A mentésért felelős rendszergazda felelőssége:
- felelős a kezelésére bízott informatikai rendszerben tárolt elektronikus adatok mentésének, archiválásának rendszeres, előírásszerű végrehajtásáért.
- felelős a mentések, archiválások végrehajtása során feltárt incidensek a helyi informatikai vezetőnek vagy az IT biztonsági felelősnek való jelentéséért, a helyi informatikai vezetőn és az IT biztonsági felelős irányelvei, illetve ebben a dokumentumban meghatározott követelmények alapján az incidensek kezeléséért.
- felelős a mentések visszatöltéssel történő ellenőrzések végrehajtásáért.
- felelős az archívumban elhelyezett médiák rendszeres ellenőrzéséért, időszakonként történő átcsévéléséért, vagy átmásolásáért.
- felelős a mentéssel, archiválással, illetve visszatöltéssel kapcsolatos dokumentálások elvégzéséért.
- IT biztonsági rendszergazda felelőssége:
- felelős a helyi mentések visszatöltéssel történő ellenőrzéséért.
- felelős a helyi archívumban elhelyezett médiák rendszeres ellenőrzéséért.
- felelős a helyi mentéssel, archiválással, illetve visszatöltéssel kapcsolatos dokumentálások ellenőrzéséért.

A 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, adatbáziskezelő, 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.

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 CD-re is kell elvégezni.

Az archiválások rendje

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

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.

Az egyéni archiválások igénylésének rendje

Ha az információk rendelkezésre állási követelményei miatt szükséges, vagy a központi archiválási eljárásban nem szerepel, a felhasználó kérheti adatainak rendkívüli archiválását.
Az archiválási igényeket a helyi informatikai vezetőnek 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.

A MENTÉSEK VISSZATÖLTÉSE

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 (véletlenszerűen).
- 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 IT biztonsági felelős évente egy alkalommal ellenőrzi a visszatöltések dokumentáltságát.

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.

- Mentési médiák kezelése.
- Mentési médiák használatba vétele.
- Az adathordozót használatba vétel előtt külsőleg is fel kell címkézni. A címkén kötelező jelleggel szerepelnie kell a - választott ciklikus mentési rendnek megfelelő - sorozat és napi azonosítónak. A mentési folyamatokban a szalag belső elektronikus azonosítója használható.
- A kazettás médiát a mentés végrehajtása előtt formattálni szükséges.

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.
Mentések, archiválások dokumentálása
A mentések végrehajtását mentési naplóban kell rögzíteni, melynek az alábbi információkat kell tartalmaznia:

- Szervezeti egység megnevezése
- Rendszer megnevezése
- Mentés azonosítója
- Mentés ideje
- Mentés tartalma
- Mentés végrehajtója és aláírása
- Mentés státusza (sikeres, sikertelen)
- A mentési napló ellenőrzését az IT biztonsági felelős végzi.

A hardver eszközökhöz kapcsolódó védelmi intézkedések

HARDVER ESZKÖZÖK FIZIKAI HOZZÁFÉRÉSE

Szerverek fizikai hozzáférése
A DÉLI ASZC szervereit az erre a célra kialakított szerverszobákban kell elhelyezni.
A szerverszoba kialakítási, és hozzáférési követelményeiről jelen szabályzat 3. számú melléklete rendelkezik.
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.

Nyomtatók fizikai hozzáférése

A DÉLI ASZC 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.

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.

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 DÉLI ASZC 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 működő képességét. 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.
- 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, főleg a téli szellőztetésnél kell ügyelni 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.
- 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.

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 (Reset gomb, 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 DÉLI ASZC-nál elfogadott adathordozókat szabad behelyezni.
- Hardver eszközök kezelési rendjével kapcsolatos óvintézkedések
- 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 IT eszközöket az üzembe helyezés során aláírással ellátott zárcímkével lehet ellátni. A felhasználóknak a zárcímkét tilos eltávolítani, vagy megrongálni.
- 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.

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 nyilatkozattal" 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.

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.

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.

Hardver eszközök selejtezése, megsemmisítése, továbbértékesítése

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

A törlési eljárás kiválasztásáról az üzemeltetésért felelős vezető gondoskodik. A törlés folyamatát az IT biztonsági felelős felügyeli.

Minden más tevékenységet a jelen szabályzatban megfogalmazottak, illetve az érvényben levő selejtezési eljárás szerint kell lefolytatni.

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.

A MOBIL ESZKÖZÖK KEZELÉSI RENDJE

Mobil eszközök kezelése

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:

- Helyi biztonsági házirend
- Vírusvédelmi szoftver
- Személyi tűzfal
- Szükség esetén titkosító szoftvert és/vagy hardver megoldás
- A felhasználónak a használatba vétel során ellenőrizni kell:
- A mobil eszköz és tartozékainak meglétét.
- A telepített védelmi eszközök meglétét (vírusvédelmi eszköz, személyi tűzfal)

Az átadás-átvétel tényét dokumentálni kell.

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 informatikai szervezet rendszergazdájától 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, az üzemeltetésért felelős helyi informatikai szervezet kérésére a felhasználó köteles a hordozható eszközt a beavatkozás idejére biztosítani.

Az eszköz tárolása

A DÉLI ASZC-ban hordozható eszközöket használaton kívül zárható szekrényben kell tárolni,

amelyhez a mobil eszköz használójának kizárólagos joga van.
A hordozható személyi számítógépek épületéből való kivitele
A hordozható eszközök az arra jogosultak mobilitását szolgálják, így az épületből való kivitelhez külön engedély nem szükséges.
Mobil eszközök védelmi előírásai
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:

- Erős fizikai behatásnak
- Sugárzó hőnek
- Erős mágneses, vagy elektromágneses térnek
- Fröccsenő víznek
- Poros környezetnek

A hordozható eszközhöz csak a DÉLI ASZC által jóváhagyott, és biztosított perifériák használhatók. A perifériákba csak a DÉLI ASZC által jóváhagyott, és biztosított, szabványos adathordozók használhatók.
A megjelenítő eszköz fokozottan érzékeny a fizikai behatásoknak, ezért annak tisztítását csak erre a célra alkalmas törlőkendőkkel, és tisztítóanyagokkal szabad elvégezni.

Mobil eszközökön tárolt adatok védelme
Titkosítás

A hordozható eszközökön 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.).
Mi a 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 IT biztonsági felelőst, illetve a helyi IT biztonsági rendszergazdát, aki intézkedik a felhasználó jelszavának megváltoztatására.
Az IT biztonsági felelős illetve a helyi IT biztonsági 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.
Távoli hozzáférések, távmunka
Hozzáférések szabályozása
A távoli hozzáféréseket illetve távmunkával kapcsolatos jogosultság kezelését a jelen szabályzatban leírt módon kell végrehajtani.

Eszközök hálózatra csatlakoztatása

Távoli hozzáférés a DÉLI ASZC Internet kapcsolatain az Internet kapcsolaton keresztül üzemeltetett biztonságos virtuális magánhálózat kialakításával (VPN), vagy modemes betárcsázással valósulhat meg.

Modemes adatkapcsolatot adminisztrációs célokra van fenntartva. Betárcsázáskor biztosítani kell azokat az eljárásokat, amelyek a kapcsolat biztonságát garantálják:

Csak visszahívásos módszer alkalmazása engedélyezett

Korlátozni kell az elérhető erőforrásokat

A modemes kapcsolat hívószámát titkosan kell kezelni.

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

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.

Mobil eszközök vezeték nélküli hozzáférése

A belső ügyviteli hálózatra kapcsolódó vezeték nélküli hozzáféréséhez a DÉLI ASZC IEEE 802.1 lg szabványnak megfelelő (WiFi) vezeték nélküli hozzáférést biztosít kizárólag alkalmazottai számára, DÉLI ASZC tulajdonban levő mobil eszközökhöz. Vezeték nélküli kapcsolódás esetén gondoskodni kell az illetéktelen használat, megelőzéséről az alábbi előírások egyidejű betartásával:

- hozzáférési kulcs használatával,
- legalább 128 bites WEP (vagy ennél erősebb illetve hatékonyabb) titkosítással,
- MAC address szűréssel,
- a broadcast tiltása (amennyiben a hozzáférési ponton ez konfigurálható).
- A kiadott hozzáférési kulcsra a jelen szabályzatban foglalt felhasználói jelszavakra vonatkozó előírások és biztonsági intézkedések vonatkoznak.

Ellenőrzések

A mobil eszközök használata szabályainak betartását a helyi IT biztonsági felelős rendszeresen ellenőrzi.

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

A SZOFTVEREKHEZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEK

Szoftverek erőforráskönyvtárainak védelme

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

Szoftverek nem használt funkcióinak tiltása

A DÉLI ASZC-nál 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.

Szoftverek biztonsági frissítése

A helyi IT biztonsági rendszergazdának vagy az általános rendszergazdának rendszeresen

figyelni kell a megjelenő sérülékenységekről szóló jelentéseket.
Ki kell dolgozni a DÉLI ASZC-ban 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.

A „dobozos" szoftverek tárolása

A „dobozos" szoftvereket a helyi informatikai rendszer üzemeltetéséért felelős szervezeti egység, központi helyén kell tárolni. A rendszertelepítésekhez lehetőleg az eredeti példányról készült másolatot kell használni.
Egy időben maximálisan egy másolt példány létezhet.

Szoftverek nyilvántartása

A DÉLI ASZC-nál használt szoftverekre és szoftver licencekre nyilvántartást - a tárgyi eszköz nyilvántartástól 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 szoftvernyilvántartásnak összhangban kell lennie az ügyviteli rendszerek (tárgyi eszköz) nyilvántartásával.

A KOMMUNIKÁCIÓHOZ TARTOZÓ VÉDELMI INTÉZKEDÉSEK

A szervezet elektronikus hivatalos kommunikációja

A Déli ASzC szervezetének elektronikus hivatalos kommunikációja a továbbiakban elsősorban kormányzati e-mail címek igénybe vétele útján folyhat.

Kormányzati e-mail címnek kell tekinteni:

a) a gov.hu végződésű e-mail címeket,
b) a Kormány, illetve a Kormány tagja által irányított vagy felügyelt szerv által biztosított hivatalos elektronikus levelezési címeket,
c) a Kormány tagja vagy kormánybiztos tulajdonosi joggyakorlása alá tartozó gazdasági társaság által biztosított hivatalos elektronikus levelezési címeket,
d) a Kormány, illetve a Kormány tagja által irányított vagy felügyelt szerv vagy a Kormány tagja vagy kormánybiztos tulajdonosi joggyakorlása alatt álló gazdasági társaság tulajdonosi joggyakorlása alá tartozó gazdasági társaság által biztosított hivatalos

elektronikus levelezési címeket, valamint

e) a Kormány irányítása vagy felügyelete alá nem tartozó, Alaptörvényben meghatározott szerv hivatalos elektronikus levelezési címeit.

Kizárólag kormányzati e-mail címre küldhetők ki a továbbiakban az alábbi iratok:

- törvényjavaslatot tartalmazó irat,
- Kormány részére készült előterjesztés, jelentés,
- Kormány döntését igénylő előterjesztés,
- politikai felsővezetői (miniszterelnök, miniszter, államtitkár) döntést igénylő előterjesztés, különösen miniszteri rendelettervezet,
- politikai felsővezető részére készülő előterjesztés, jelentés,
- politikai vezető (kormánymegbízott) részére készülő előterjesztés, jelentés,
- biztosi jogviszonyban álló (kormánybiztos, miniszterelnöki biztos, miniszteri biztos) részére készülő előterjesztés, jelentés,
- szakmai felsővezető (közigazgatási államtitkár, helyettes államtitkár , központi hivatal vezetője és vezetőjének helyettese, kormányhivatal főigazgatója) részére készülő előterjesztés, jelentés
- szakmai vezető (kormányhivatal igazgatója, járási hivatal, illetve fővárosi kerületi hivatal vezetője és vezetőjének helyettese, főosztályvezető, osztályvezető) részére készülő előterjesztés, jelentés,
- minden olyan irat, amely a Kormánynak, a Kormány tagjának, politikai felsővezetőnek vagy vezetőnek, szakmai vezetőnek vagy felsővezetőnek, biztosi jogviszonyban állónak a döntését tartalmazza, mely nem kerül nyilvánosan közzétételre,
- a fentiekről készült tervezet, másolat vagy kivonat, a fentiekkel kapcsolatos munkaanyag

Ezen irattípusok nem kormányzati e-mail címre történő kiküldése tilos, kivéve, ha azt a Déli ASzC szervezetében erre kijelölt vezető kifejezetten, írásban (ez alatt az elektronikus jóváhagyást is érteni kell) engedélyezi. Az erre kijelölt vezető felelősségi körébe tartozik annak mérlegelése, hogy a fenti irattípusok közé tartozó irat nem kormányzati e-mail címre történő továbbítása nem eredményezi-e a dokumentum illetéktelen kezekbe kerülését. (Javaslom, hogy a nem-kormányzati e-mail címmel rendelkező címzett részére rendszeresen megküldendő anyag tekintetében elegendő legyen egyszer kérni az engedélyt, erre az engedélykérés során szükséges legyen utalni.)

Amennyiben a fenti irattípusok közé tartozó irat nem-kormányzati e-mail címre történő továbbítására engedély nélkül kerül sor, akkor annak minden esetben munkajogi következményekkel kell járnia az intézkedésben részt vevő kollegák irányában.

Amennyiben a fentiek szerinti irat nem kormányzati e-mail címre történő megküldése szükséges, akkor az irat továbbítása helyett elsősorban az irat tartalmának kivonatolása útján kell az abban foglaltakat a címzettel közölni. Ennek során lehetőleg kerülni szükséges az utalást arra, hogy a kérdéses tartalom végső soron honnan származik és azt milyen dokumentum tartalmazza, ehelyett elsősorban általános körülírással szükséges utalni a dokumentumban foglaltak keletkeztetőjére.

A fent felsorolt irat nem kormányzati e-mail címre történő továbbítását a kijelölt személy engedélyezi.

Az elektronikus levelezés biztonsága

Az elektronikus levelezés biztonsági követelményei

Az elektronikus levelezés a DÉLI ASZC informatikai rendszerében az egyik fő fenyegetettség forrása. Az elektronikus levelezés biztonsága érdekében az alábbi előírásokat kell betartani:
Szigorúan tilos a közízlést, a DÉLI ASZC jó hírnevét veszélyeztető, erkölcstelen, vagy politikai tartalmú e-mail elküldése.
Tilos a levelező rendszert „Titkos" minősítésű fájlok, dokumentumok kijuttatására használni.
Tilos a beérkező leveleket a DÉLI ASZC-on kívüli postaládára irányítani.
Tilos olyan levelek továbbítása a DÉLI ASZC 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 DÉLI ASZC 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 DÉLI ASZC alkalmazottjának küldhető. Ezzel kapcsolatos automatikus üzenet küldése a DÉLI ASZC-on kívülre tilos.
Tilos kétes forrásból származó levelet megnyitni. A forrást nem megbízhatónak kell tekinteni, ha

- A feladó nem ismert
- A levél címzettje közt sok, nem ismert személy szerepel
- A levél nyelvezete nem a várt
- A levél tárgya nem illeszkedik a DÉLI ASZC ügyviteli vagy oktatási folyamataihoz

Az elektronikus levelezés korlátozásai

Az elektronikus levelezés biztonsága érdekében az alábbi korlátozások vannak érvényben:
A szerver postafiók mérete általában: 200 Mb. Szükség esetén ettől eltérő kapacitást a helyi informatikai vezető engedélyezhet.
A fogadható és küldhető levelek maximális megengedett mérete általában: 20 Mb. Szükség esetén ettől eltérő kapacitást a helyi informatikai vezető engedélyezhet.
Elektronikus levelezésben nem fogadhatók és küldhetők csatolmányként az alábbi kiterjesztésű állományok:

- Futtatható állományok; bat; com; exe;
- Adatbázis állományok; dbf; dat;
- Média állományok: wmv; avi; mpeg; mp3; vaw; mid, pps;
- Egyéb állományok: dll; sys; inf; hlp; bin, pif, vbs;

Elektronikus levelezés magáncélú használata

Mivel minden levelezést a DÉLI ASZC tulajdonát képező infrastruktúra és erőforrások biztosítanak, ezért a magán célú levelek is a DÉLI ASZC tulajdonát képezik. Így a DÉLI ASZC fenntart minden jogot a levelek kezelésével kapcsolatban.
A fentieken túl kerülni kell az Interneten található ingyenes levelezési portálok belülről történő használatát. Az Interneten található ingyenes levelezési portálokat hivatalos ügyekben használni tilos.

Elektronikus levelezés jogosultsága

A DÉLI ASZC valamennyi alkalmazottja és hallgatója hozzáférést kap az elektronikus levelezési rendszerhez.

Elektronikus levelezés ellenőrzése

A DÉLI ASZC fenntartja a jogot - ide értve a magánjellegű levelezést is - a levelezés méretének, gyakoriságának, és ha szükséges tartalmának ellenőrzésére, korlátozására a levelező szerver és az Internet csatlakozás kapacitásának hatékonyabb kihasználása, valamint a DÉLI ASZC informatikai rendszerének biztonsága érdekében.

AZ INTERNET BIZTONSÁGA

Az Internet hozzáférés biztonsági előírásai

Az Internet hozzáférés a DÉLI ASZC 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 Internetről letöltött segéd állományokat (pl., cookie) rendszeresen törölni kell.
Az Internetezés közben el kell utasítani azokat a felbukkanó párbeszéd ablakokat, amelyek segédprogramok telepítésére, vagy egyes funkciók kikapcsolására ösztönöznek.
Tilos az Internetes webhelyek eléréshez szükséges jelszavakat úgy megválasztani, hogy abból a DÉLI ASZC-nál használt jelszóra következtetni lehessen.

Korlátozások az Internet használatában

Tiltott Internetes alkalmazások

A DÉLI ASZC-nál csak a rendszeresített Internetes alkalmazások használhatók
A DÉLI ASZC-nál a felhasználóknak szigorúan tilos olyan internetes alkalmazások használata:

- Melyekkel a DÉLI ASZC, vagy más személyek információinak, alkalmazásainak, bizalmasságának, sértetlenségének, rendelkezésre állásának megsértésére irányul.
- Melyekkel a DÉLI ASZC erőforrásainak illegális megosztására irányul.
- Melyek licenc szerződéseivel a DÉLI ASZC nem rendelkezik.

Tiltott Webhelyek

Szigorúan tilos a DÉLI ASZC érdekeit sértő, erkölcstelen, politikai izgató oldalak látogatása.
Szigorúan tilos ún. chat (társalgó) oldalak látogatása.

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, erkölcstelen, politikai célú állomány letöltése.
A DÉLI ASZC fenntartja a jogot állománytípustól (pl.: mpg, wmv stb.), valamint mérettől függő letöltés korlátozására.
Az Internet tanulói hozzáférése vezetékes illetve vezeték nélküli módon
A DÉLI ASZC a tanulmányi és ehhez kapcsolódó adminisztrációs feladatok ellátásához Internet hozzáférést biztosít a tanulói számára. Az Internet hozzáférés az alábbi három módon biztosított:

- Tanulói géptermekben, a DÉLI ASZC tulajdonában levő hardver eszközök használatával,
- Kollégiumi fizikai port csatlakozás biztosításával, amelyen keresztül a tanulói eszközök csatlakoztathatók,
- A DÉLI ASZC területén felszerelt vezeték nélküli hozzáférési pontok segítségével (WiFi), amelyen keresztül tanulói mobil eszközök csatlakoztathatóak.

A tanulói géptermekben való géphasználat illetve Internet hozzáférés a tanulói nyilvántartásba vételt és a tanulói account (felhasználói név és jelszó) kiadását követően minden további nélkül használható.
A tanulói mobil eszközök csatlakoztatására és az Internet eléréséhez a DÉLI ASZC IEEE 802.1 lg szabványnak megfelelő (WiFi) elérést biztosít, hozzáférési kulcs használatával, 128 bites WEP titkosítással, és MAC address szűréssel.
A csatlakozási kérelem benyújtásának és elbírálásának folyamata:

- A kollégiumi fizikai port és WiFi csatlakozást a hallgatónak elektronikus úton a helyi általános rendszergazdától kell kérnie.
- A kérelmet a hallgató saját, DÉLI ASZC-nál üzemeltetett e-mail címéről kérheti. A hallgatónak a kérelemhez az egyértelmű azonosítás érdekében a következőket kell megadnia:
    - Név,
    - Tanuló- vagy csoportkör száma,
    - A tanulmányi rendszerben vezetett tanulói kódját,
    - A használni kívánt eszköz ún. „MAC address" számát (WiFi és vezetékes kapcsolódás esetén is)
    - Opcionálisan telefonszám,
    - Amennyiben kollégiumi fizikai port hozzáférést igényel a pontos hely meghatározása (kollégiumi épület, emelet, szoba, végpont száma).

A kérelmeket a helyi általános rendszergazda bírálja el a fizikai lehetőségek, a rendszer kapacitása és terhelése valamint a DÉLI ASZC informatikai rendszerének biztonsága és védelme figyelembevételével.
Amennyiben a kérés technikailag teljesíthető, a rendszergazda teendői a következők:

- Archiválja a kérést,
- Sablon alapján válasz e-mailt generál, amelyben röviden tájékoztatja a felhasználót:
- A pozitív elbírálás tényéről,
- Megadja a WiFi hozzáféréshez szükséges technikai információkat (SSID, egyedi hozzáférési kód, a titkosítás típusa és fajtája),
- Tájékoztatja, hogy mikortól érhető el a WiFi vagy fizikai végponton keresztül igényelt szolgáltatás,
- A levél mellékletében elküldi a „Tanulói felhasználói nyilatkozatot" amely tájékoztatja a felhasználót annak jogairól és kötelességeiről.
- A levélben röviden tájékoztatja a felhasználót, hogy az igényelt szolgáltatás igénybevételének feltétel a mellékelt „Tanulói felhasználói nyilatkozat" elfogadása. Amennyiben 1 napon belül a felhasználó nem él ezzel kapcsolatban kifogással, úgy a „Tanulói felhasználói nyilatkozat"-ban foglaltakat a felhasználó elfogadta és magára nézve kötelezőnek ismeri el. A „Tanulói felhasználói nyilatkozat" tartalmazza a DÉLI ASZC IBSZ-éből származtatott használati feltételeket, valamint a felhasználó jogait és kötelességeit.
- Archiválja a válasz e-mailt.
- Intézkedik, hogy a szolgáltatás feltételei a megadott időpontra teljesüljenek (a switchen engedélyezi az adott végponthoz tartozó portot vagy elvégzi a végpont kicsatolását, beállítja a MAC address szűrést, stb.)

Amennyiben a

- tanulói jogviszony megszűnik,
- vagy a hallgató nem fogadja el a használat feltételeit,
- kapacitás illetve teljesítmény problémák lépnek fel,
- illetve olyan incidens történik, amely a DÉLI ASZC informatikai rendszerének a

védelmében vagy más jogszabálysértés következtében arra kényszeríti a helyi informatikai szervezetet, hogy visszavonja az adott szolgáltatást,

- az általános rendszergazda intézkedik a szolgáltatás megszüntetéséről (leveszi az engedélyezett MAC address-t az engedélyezési listáról, tiltja, vagy bontja a kapcsolatot az adott fizikai végponttal, törli a hozzáférési listáról a kiadott kulcsot, stb.) a tanuló tájékoztatása mellett.

A kiadott hozzáférési kulcsra a jelen szabályzatban foglalt felhasználói jelszavakra vonatkozó előírások és biztonsági intézkedések vonatkoznak.

Az Internet hozzáférések ellenőrzése

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

ZÁRÓ RENDELKEZÉS

A jelen szabályzat 2020. május 05-én lép hatályba. A tárgyra vonatkozó minden szabályozás hatályát veszti.

Kelt: Szekszárd, 2020. május 05.

Jóváhagyja és hatályba lépteti:

Jeszenka Ildikó
Déli ASzC kancellár

Simonné Szerdai Zsuzsanna
Déli ASzC főigazgató

1. számú melléklet: Az adatok minősítésének és kezelésének rendje

Az adatok osztályozása

Hatásvizsgálat

Az osztályozás alapját a bizalmasság, a sértetlenség, és a rendelkezésre állás sérüléséből, vagy elvesztéséből keletkező, a DÉLI ASZC számára kimutatható lehetséges hátrány nagysága képezi.
A bizalmasság, sértetlenség, és rendelkezésre állás sérüléséből, vagy elvesztéséből vagyoni, erkölcsi, és jogi hátrány származhat. A hátrány mértéke az alábbi besorolás szerint határozható meg:

A hátrány mértéke			
	Elhanyagolható	Jelentős	Súlyos
Vagyoni hátrány			
Vagyoni kár, vagy többletköltség,	A kár nagysága meghaladja a 10 000 forintot	A kár nagysága meghaladja az 500 000 forintot	A kár nagysága meghaladja az 1 000 000 forintot
Erkölcsi hátrány			
Bizalomvesztés a hallgatók körében	A DÉLI ASZC megítélése lényegesen nem változik.	Bizalomvesztés a DÉLI ASZC 1-2 alkalmazottjával szemben	Bizalomvesztés a DÉLI ASZC egy szervezetével szemben.
Bizalomvesztés a dolgozók körében (Munkahelyi hangulat)	A DÉLI ASZC alkalmazottai körében legfeljebb kisebb, átmeneti elégedetlenség (csalódottság) áll fenn.	Bizalomvesztés a DÉLI ASZC egy szervezetének vezetőjével szemben.	Bizalomvesztés a DÉLI ASZC felső vezetésével szemben.
Jogi hátrány			
A törvényesség megsértése	A DÉLI ASZC-al szemben nem indul jogi eljárás	A DÉLI ASZC-al vagy a DÉLI ASZC egy alkalmazottjával szemben jogszabálysértés elkövetése miatt indul eljárás	A DÉLI ASZC-el, vagy a DÉLI ASZC egy alkalmazott] ával szemben vétség vagy bűncselekmény elkövetése miatt indul eljárás.

AZ ADATOK KEZELÉSÉNEK KÖVETELMÉNYEI

A KÖVETELMÉNY RENDSZER

A következő táblázat az adatok kezelésével kapcsolatos követelményeket foglalja össze

Az adatok kezelésének követelményei bizalmasság és sértetlenség szerint:

	„Nyilvános" illetve „Nem védett"	„Belső használatra" vagy „Bizalmas" illetve „Védett"	„Titkos" illetve „Fokozottan védett"
Tárolás	Központi tároló helyen kell tárolni	Személyes, vagy korlátozott hozzáférésű mappában kell tárolni	Titkosított mappában vagy egyedi számítógépen, és titkosított mappában kell tárolni.
Adatátvitel	Nincs követelmény.	A DÉLI ASZC-on 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.	Csak az adatgazda engedélyével törölhető. Az adathordozón (pl. lemezeken) lévő adatokat törölni kell új adatokkal történő felülírás révén. A hibás mágneses/optikai 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: Informatikai biztonsági zónák

1. ZÓNÁK MEGHATÁROZÁSA

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	Az irodákba történő belépés kulccsal történik.	Az irodákba történő belépés kulccsal történik	A zónába történő belépés egyedi azonosítással, (mágneskártya, kód, stb.) és 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.

Zóna követelmények	1. számú biztonsági zóna	2. számú biztonsági zóna	3. számú biztonsági zóna
Áramellátás szabályozása			Az áramellátás szabályozása, és redundanciája szükséges
Biztonsági követelmények	Kézi tűzoltó készülékek kihelyezése szükséges a folyosón.	Kézi tűzoltó készülékek kihelyezése szükséges.	Tűzvédelmi füstérzékelő és a közelben kézi riasztó szükséges. A helységben vagy annak bejáratánál kézi tűzoltó készülék kihelyezése szükséges.
Tűzvédelem	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.
Behatolás-védelem			Felügyeleti (riasztó) eszközökkel kell ellátni.
Biztonsági események naplózása			A felügyeleti eszközök jelentéseit naplózni kell.
Dokumentálási követelmények	A belépések naplózása	A kulcs felvételnél kell dokumentálni.	

3. számú melléklet: Kontroll és felülvizsgálat

1. 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 IT tevékenység	Észlelt behatolási kísérletek száma	X
	Nem DÉLI ASZC 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	IT biztonsági oktatásban részt vett személyek száma, a beszámoltatás eredményei	X
IT biztonsággal kapcsolatos fegyelemsértések	IT biztonságot megsértő személyekre vonatkozó fegyelmi statisztikák	X
Az IT biztonsági rendszer összesített értékelése	Az IT rendszer technikai és biztonsági szintjére vonatkozó megállapítások, javaslatok	X
Javaslatok	Javaslatok kidolgozása a hiányosságok megszüntetésére, a biztonsági és rendelkezésre állási szint emelésére	X

2. 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: Mentési médiák rotálása, selejtezése

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

2. Mentési médiák selejtezése, megsemmisítése

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

Média	Max. élettartam
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.

5. számú melléklet: A biztonsági események kezelése

1. Biztonsági incidensek bejelentése

A DÉLI ASZC alkalmazottainak és tanulóinak az általuk észlelt, a DÉLI ASZC informatikai rendszerében keletkező biztonsági incidenseket be kell jelenteniük a helyi IT biztonsági rendszergazdáknak.

A bejelentésre az alábbi információs csatornák állnak rendelkezésre:

DÉLI ASZC Intézmény	Telefon	e-mail

6. 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 DÉLI ASZC tevékenységét tekintve mennyire fontos ügyviteli, működési folyamathoz tartozik.
Bekövetkezési valószínűség: Annak az esélye, hogy a veszélyforrás képezte fenyegetettség támadás formájában bekövetkezik.
Bizalmasság: A DÉLI ASZC 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 ellenáílóak 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 DÉLI ASZC 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 DÉLI ASZC rendszereiben előálló időleges kiesést vagy zavarokat, és akár -

gazdasági, reputációs, személyi vagy dologi - kárt is okozó, illetve törvényi következményekkel járó történés.

Fenyegetettség: A DÉLI ASZC 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 DÉLI ASZC-nak (anyagi károk, kártérítések stb. formájában).

Helyreállítási eljárás: A katasztrófa esemény 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 DÉLI ASZC 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 DÉLI ASZC informatikai rendszerének folyamatos és rendeltetésszerű működése, és ez jelentős hatást gyakorol a normál ügyviteli iíl. működési tevékenységek folyamatosságára és működőképességére.

Informatikai katasztrófahelyzet: 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.

Katasztrófaesemény: Azon esemény, amelynek bekövetkezése krízishelyzetet teremt. A katasztrófaeseménynek több, egymástól független, vagy egymással összefüggő oka lehet. Az okok azon releváns fenyegetési 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 DÉLI ASZC

tevékenységeinek egyes elemeit, részlegeit érinti, hanem a DÉLI ASZC ügyviteli tevékenységének jelentős körénél problémát okoz.

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 Plán)

Kockázat: Annak veszélye, hogy egy esemény, fenyegetettség bekövetkezése vagy intézkedés hátrányosan befolyásolja a DÉLI ASZC 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 DÉLI ASZC azon ügyviteli folyamata, amely működőképességének fenntartása elengedhetetlen a DÉLI ASZC stratégiai céljainak elérése, teljesíthetősége érdekében.

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 Plán - **Üzletmenet** Folytonossági terv) eljárásrend hatálya, illetve oszolhat fel a Krízis Bizottság.)

Krízis Bizottság: Krízisállapot fennállása esetén a legfőbb döntéshozó fórum. A Krízis **Bizottságok** tevékenységüket alkalomszerűen végzik. A Krízis Bizottságok kialakításának célja, hogy a folytonosságot biztosító intézkedésekhez kapcsolódó cselekvési tervekben nem definiált krízishelyzetek bekövetkezése esetén az előre meghatározott felelősségi körökben, gyorsan és hatékonyan lehessen kezelni a problémákat, hogy a meghatározott szolgáltatási szint minél hamarabb visszaállítható legyen, és a folytonosságot biztosító cselekvési tervekben definiált időtartamon belül az Üzemszerű működés visszaállításra kerüljön.

Magas készültségi szint: A kritikus ügyviteli folyamatok napi működése során olyan, az üzemmenet folytonosságot mérsékelten, illetve részben veszélyeztető problémák merülnek fel, amelyek kezelése a folyamat működtetését végző munkatárs hatáskörében nem megoldható és ezért helyettesítő eljárás indítása szükséges. Magas készültségi szintnek akkor minősül egy állapot, ha a hiba elhárításának várható határideje nem lépi túl a 12 órás időtartamot.

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 DÉLI ASZC 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 csökkentem, valamint a helyettesítő folyamat beindítását lehetővé tenni.

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

Minősített krízishelyzet: Az az állapot, amelyben a DÉLI ASZC ügyviteli szempontból meghatározó területei, vagy a DÉLI ASZC egésze működésképtelen és a működésképtelenség megszüntetése, illetve kiváltása nem szokványos ügyvitellel olyan szintű ráfordítással, vagy működési kockázattal járna együtt, amelyet a DÉLI ASZC nem vállalhat fel, így inkább a szolgáltatás - átmeneti - szüneteltetését hirdeti meg.

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 DÉLI ASZC 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 DÉLI ASZC 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 DÉLI ASZC megbízhatóságába, hitelességébe, illetve a DÉLI ASZC 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 DÉLI ASZC 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 DÉLI ASZC 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 IT biztonsági felelősnek még nem szükséges semmilyen lépést tennie az alternatív működés elrendelésére.
Ügyviteli folyamat: Olyan tevékenységek összessége, amelyek szükségesek, hogy a DÉLI ASZC kifejtse szervezeti működését és megvalósítsa oktatási, kutatási, stb. feladatait. (Egy DÉLI ASZC-os szolgáltatás nyújtásához szükséges tevékenységek, feladatok összessége.)
Üzemmenet folytonosság: A DÉLI ASZC 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.
Üzemmenet folytonosság tervezés: A káresemények, krízishelyzetek által előidézett működési kiesések megelőzését, minimalizálását, illetve a helyreállítási időben alkalmazható, helyettesítő részfolyamat életbe léptetését és visszavonását célzó tervezési lépések összessége. (BCP - Business Continuity Plán)
Üzemmeneti szint: A folyamatok működési zavartalanságának mérésére szolgáló mutató, amelynek kapcsán az egyes üzemmeneti szintekhez egyértelműen hozzárendelésre kerülnek a döntési felelősségek és jogkörök.
Végrehajtó Team: A Végrehajtó Team feladata a vonatkozó cselekvési (akció) tervben meghatározott feladatok végrehajtása.
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

MEGISMERÉSI NYILATKOZAT

Jelen szabályzat tartalmát a mai napon megismertem, az abban foglaltakat munkaköröm ellátása során kötelező érvényűnek tartom.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....