SZÍNHÁZ- ÉS FILMMŰVÉSZETI EGYETEM

SZFE 1865

REKTORI-KANCELLÁRI KÖZÖS UTASÍTÁS

IKT.SZ.: SZFE/2370/2021

Színház- és Filmművészeti Egyetem
30/2021. (09.15.) számú rektori-kancellári közös utasítása
a Színház- és Filmművészeti Egyetem Informatikai Biztonsági Szabályzatáról

Hatályos: 2021. szeptember 17. napjától

Tartalomjegyzék

1 ÁLTALÁNOS RENDELKEZÉSEK

1.1 A szabályozás célja

- Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ, vagy Szabályzat) célja a Színház- és Filmművészeti Egyetem (továbbiakban: **Egyetem**) által használt elektronikus információs rendszer, alkalmazások és szolgáltatások, valamint az általuk kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának szabványos, szabályozott és egységes biztosítása, illetve a kapcsolódó jogszabályoknak való megfelelés. Az egységesítés érdekében jelen szabályzat keretjelleggel meghatározza mindazokat a normákat és magatartásformákat, amelyek megvalósítják a kockázatokkal arányos, folyamatos és komplex információvédelmet az információs rendszer (a továbbiakban: rendszer) fizikai, adminisztratív és logikai védelmi területén (ahol ez értelmezhető, az informatikai rendszerre szűkítve).
- Az IBSZ általános célja, hogy a szervezet által használt és működtetett információs rendszer biztonságát garantáló eljárásokat és előírásokat átlátható és nyomon követhető formában egységes keretbe foglalva rögzítse az informatikai biztonság magasabb fokú kialakításának további szabályozása érdekében.
- Az IBSZ kiadásának célja továbbá a szervezet által használt információs rendszer alkalmazásának és felhasználásának biztonsági szempontból történő szabályozása.

1.2 A szabályzat hatálya

1.2.1 A szabályzat szervezeti hatálya

A szabályzat hatálya kiterjed az Egyetem valamennyi szervezeti egységére, akik feladataik teljesítése során vagy egyéb céllal, jogosultsággal, vagy annak hiányában felhatalmazással, az IBSZ tárgyi hatálya alá tartozó eszközöket, alkalmazásokat és szolgáltatásokat (továbbiakban együtt informatikai rendszert) használnak, adatokat vagy dokumentumokat, információkat hoznak létre, tárolnak, használnak vagy továbbítanak, valamint azokra, akik ilyen tevékenységekkel kapcsolatosan döntéseket hoznak.

A felhasználókkal kötendő valamennyi jogviszony vonatkozásában a jogviszonyra vonatkozó szerződésben rögzített hivatkozás mellett biztosítani kell az IBSZ rendelkezéseinek érvényesülését. Az Egyetem informatikai rendszereihez és adatállományához olyan személy nem kaphat hozzáférést, aki valamely jogviszony által nem kötődik a szervezethez.

1.2.2 A szabályzat személyi hatálya

A szabályzat hatálya kiterjed az Egyetem által foglalkoztatott valamennyi munkavállalóra, illetve munkavégzés céljából egyéb jogviszonyban álló jogi és természetes személyre, és az Egyetemmel hallgatói jogviszonyban állókra.

1.2.3 A szabályzat tárgyi hatálya

A szabályzat tárgyi hatálya kiterjed:

- az Egyetemen üzemelő számítógépes rendszer teljes konfigurációjára, az ahhoz tartozó rendszer- és felhasználói szoftverekre, valamint ezek dokumentációira;
- a papír alapon rögzített, tárolt, használt vagy továbbított adatokra;
- a számítógépes feldolgozásra szánt, feldolgozás alatt álló, és a feldolgozás után számítógépes adathordozókon tárolt, a feldolgozás eredményeként létrejött adatra;
- a számítástechnikai eszközök alkalmazásának teljes folyamatára, tevékenységeire;
- a számítástechnikai infrastruktúra elhelyezésére szolgáló helyiségekre.

1.2.4 A szabályzat időbeni hatálya

A szabályzat érvényes a hatálybalépés napjától, visszavonásig.

1.3 A szabályzat elkészítése felülvizsgálata és módosítása

A szabályzat elkészítése, felülvizsgálata és szükség szerinti módosítása az Információbiztonsági Felelős feladata és felelőssége, együttműködve az Egyetem informatikai munkatársaival. A szabályzat elkészítésében, felülvizsgálatában és módosításában közreműködnek az elektronikus információbiztonsági feladatok ellátásában közreműködő személyek, szervezeti egységek, munkacsoportok, valamint az elektronikus információs rendszer üzemeltetéséért, fejlesztéséért felelős szervezeti egységek vezetői.

1.3.1 Időszaki felülvizsgálat

A Szabályzatot legalább évenként felül kell vizsgálni és szükség esetén módosítani kell. A vizsgálat alapja az ellenőrzések, rendkívüli események naplói, valamint a kockázatelemzés és -kezelés megállapításai.

1.3.2 Rendkívüli felülvizsgálat

A Szabályzatot az időszakos felülvizsgálaton túl felül kell vizsgálni és szükség esetén módosítani kell:

- a szabályzatban hivatkozott szervezetek vagy munkakörök változása esetén;
- súlyos információ biztonsági események bekövetkezése esetén;
- az információs vagy informatikai biztonság szabályozását érintő jogszabályváltozások esetén;
- az információs vagy informatikai rendszer nagy mértékű változása esetén.

A felülvizsgálatok eredményéről az Információbiztonsági Felelős tájékoztatja a szervezet vezetőjét, amennyiben módosításra van szükség azt megteszi a szabályzatot újonnan ki kell adni.

1.4 A szabályzat betartásának ellenőrzése

A szabályzat betartásának ellenőrzése az Információbiztonsági felelős feladata, melyben közreműködnek az információbiztonsági feladatok ellátásában közreműködő személyek, szervezeti egységek, munkacsoportok, valamint az elektronikus információs rendszer üzemeltetéséért, fejlesztéséért felelős szervezeti egységek vezetői.

1.5 Kivételkezeléssel kapcsolatos feladatok

Kivétel alatt kell érteni minden olyan kontroll nem teljesülését, mely a jelen szabályozásban rögzített követelményeket nem tudja teljesíteni.

A Szabályzattól való kivételeket minden esetben jegyzőkönyvben dokumentálni szükséges. A kivételek engedélyezése tekintetében a Kancellár jogosult dönteni.

- Új, bevezetés alatt álló (elektronikus) információs rendszer esetén a szabályzati követelmények teljesülésére vonatkozó kivétel nem alkalmazható.

2 FOGALOMTÁR

FOGALOM	MAGYARÁZAT
Adathordozó	Adathordozó minden olyan eszköz, mely adatokat, szervezeti és személyes információkat tárol. Mobil adathordozó: olyan informatikai eszköz, amely egyik helyről könnyen elvihető másik helyre, ott azonnal üzembe helyezhető, illetve mobil (azaz mozgás közben is használható)
Adatvagyon	A szervezet adatvagyona minden olyan üzleti, szervezeti, és személy adat melynek adatkezelője a szervezet függetlenül attól, hogy az elektronikusan vagy más módon tárolt.
Biztonsági esemény	Nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.
Elektronikus információs rendszer	Az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese. [EIR]
Informatikai erőforrás	Informatikai erőforrások a rendszerek, tárhelyek, az eszközök melyekkel a felhasználó gazdálkodik, melyeket használ.
Kimeneti információ	képernyő, nyomtatás, fájl, e-mail Külső fél számára és belső használatra készített beszámolók, tájékoztatók, bizonylatok, nyilatkozatok, megrendelők, tranzakciók.
Külső elektronikus információs rendszer	Külső EIR az olyan rendszer melyet nem a szervezet üzemeltet, illetve nem olyan rendszer mely kifejezetten a szervezet által szolgáltatási szerződés keretében igénybe vett rendszer, hanem jogszabályi vagy egyéb kötelezettségből adódóan használandó rendszer esetleg a szervezet döntése alapján használt egyéb, általánosan hozzáférhető rendszer.
Legszűkebb funkcionalitás	Az a funkcionalitás mely biztosítja a munkavégzést / működést, és tilt minden egyéb funkciót.
Napló	A számítógépen végzett műveletek (felhasználói tevékenység), a gép által küldött hibaüzenetek és/vagy a hálózaton bejövő és kimenő adatok rögzítésére, nyomon

	követésére szolgáló adatállomány.
Nyilvános kulcsú infrastruktúra	A nyilvános kulcsú infrastruktúra az a rendszer, melynek feladata a digitális aláíráshoz szükséges nyilvános kulcsok létrehozása, kibocsátása, publikálása, menedzselése és visszavonása. A nyilvános kulcsú technológiák segítségével biztosítjuk a rendszerben a következő tulajdonságok meglétét: hozzáférés, hitelesítés, letagadhatatlanság, integritás és bizalmasság.
Személyes adat	Az érintett-tel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés.

3 EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ – SZEMÉLY – BIZTONSÁG

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed az Egyetem teljes személyi állományára, valamint minden olyan az Egyetem más jogviszonnyal kapcsolódó személyre, aki az Egyetem elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem az Egyetem tagja, a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, a kötelezettségeket érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

3.1 Informatikai erőforrásokhoz való hozzáférés igénylése munkaerő felvételénél

A HR Osztály az új munkatárs munkába állása előtt, legkésőbb a munkába állás napján köteles a Rendszergazdát tájékoztatni. A bejelentést írásos formában (e-mail) kell megtenni. Az új munkatárs hozzáférési jogosultságát és eszközöket az érintett vezető haladéktalanul köteles igényelni a Rendszergazdánál.

A beérkezett igényekre a Rendszergazda haladéktalanul köteles visszajelezni, és a szükséges technikai eszközöket biztosítani [a rendelkezésre álló készletek erejéig].

A kapcsolódó részletes szabályozást az informatikai rendszerekhez és eszközökhöz való hozzáférés, kiadás és visszavétel tekintetében a Hozzáférésvédelmi szabályzat tartalmazza.

3.2 Adatvagyon kezelése, hozzáférése

Az adatok kezelésével, illetve a számítógépes rendszer üzemeltetésével kapcsolatos feladatok ellátására felhatalmazott munkavállalók az adatokhoz csak a feladatuk ellátásához szükséges mértékben férhetnek hozzá.

A szervezeti egység vezetője az adott szervezeti egységnél keletkező valamennyi adathoz korlátozás nélkül hozzáférhet.

Az adatvagyon felhasználása, elérése, módosítása, másolása, törlése kizárólag a felhasználónak személyre szabottan biztosított jogosultságnak megfelelően történhet. Minden felhasználó az adatvagyont köteles úgy kezelni, hogy az teljes mértékben megfeleljen az általa ellátott feladatok jellegének, illetve célkitűzéseknek.

A szervezet adatvagyonát csak a szervezet eszközein, illetve a szervezet által biztosított rendszerekben, adattárhelyeken lehet kezelni (tárolni, módosítani, törölni…stb.) Kivételt jelent ideiglenesen - amennyiben máshogy megoldható – külső adattároló eszközök használata. Külső adattároló eszköz lehet a pen-drive, mobiltelefon, illetve az otthoni számítógép is. Ezen eszközökön a szervezet adatainak titkosított tárolása elvárt az adatok bizalmasságának megőrzése érdekében. Pen-driveon jelszóval védett zip állományok; nem a szervezet tulajdonában lévő eszköz: részleges vagy teljes drive titkosítás (Veracrypt, Bitlocker…stb.) használata elvárt.

3.3 Az informatikai biztonsági oktatás és képzés

Az Egyetem valamennyi alkalmazottja – feladatának és jogkörének figyelembevételével - megfelelő képzésben részesül a szervezet biztonsági szabályairól és eljárásairól. Ezeket az ismereteket évente naprakész ismeretek közlésével fel kell újítani. A képzés magában foglalja:

- a biztonsági követelményeket;
- a jogi felelősséget;
- a szervezet óvintézkedéseit;
- az informatikai eszközök helyes használatát, például a bejelentkezési eljárást, a szoftverek használatát;
- biztonsági incidensek kezelésének folyamatát;
- adatvédelmi ismereteket;
- általános biztonság tudatossági ismereteket.

Az általános tájékoztatás keretében az új belépők számára a HR osztály levélben küldi ki az oktatási anyagot. Különleges esetekben amennyiben a szabályok jelentősen megváltoznak, vagy jelentős biztonsági incidens esetén, ad-hoc képzés is tartható.

A biztonsági képzés mélysége az Egyetem belüli általános fontossághoz igazodik, egyes esetekben az adott szerep biztonsági követelményeinek megfelelően változik. Amennyiben szükséges, egyes résztémákat kezelő oktatást is biztosítani lehet, melyről a Kancellári Kabinet vezetője dönthet.

Különleges biztonsági képzést a Kancellár engedélyével elsődlegesen a következő szerepeket betöltő alkalmazottak kaphatnak:

- az informatikai rendszerek tervezésében és fejlesztésében kulcsszerepet játszó alkalmazott,
- informatikai rendszerek üzemeltetésében kulcsszerepet játszó alkalmazott;

A lefolytatott képzéseken készült aláírt jelenléti íveket és a kapcsolódó tematikát 3 évig meg kell őrizni a HR osztályon.

A szervezet felhasználói által használt, de nem a szervezet által üzemeltetett alkalmazások esetében a Rendszergazda feladata a rendszerek biztonságos használatával kapcsolatos képzések megszervezése, melyekre a rendszerek bevezetésekor és a rendszerek jelentős változásakor van szükség.

A rendszerek használatával kapcsolatos képzéseket az új belépők szervezeti feletteseiktől kapják meg a betanítás során.

3.4 Az Egyetem által biztosított informatikai eszközök

Az Egyetem által a munkaviszonyhoz vagy egyéb jogviszonyhoz kapcsolódó feladatok ellátásához biztosított eszközök (asztali számítógép, laptop, mobiltelefon, levelezés, tárhelyek) csak a feladatok ellátásához kapcsolódó módon használható, azok privát célból használata nem megengedett.

Az eszközök informatikai biztonsági paramétereinek állítása a felhasználók számára jogosultság mellett sem megengedett (például vírusírtó kikapcsolása).

A következő szoftverhasználati korlátozásokat kell figyelembe venni:

- a szervezet által biztosított eszközökön kizárólag jogtiszta szoftverek és dokumentációk használhatók, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak.

3.5 Magántulajdonú informatikai eszközök használata a feladatok ellátásához

A szervezethez kapcsolódó feladatok ellátásához magántulajdonú eszközök is használhatók, melyek segítségével távolról érhetők el a rendszerek. Ezen eszközök tekintetében a következő elvárásokat kell betartani:

- a kapcsolódó eszközt védeni kell illetéktelen hozzáféréstől, azt úgy kell használni, hogy a szervezet adataihoz jogosultsággal nem rendelkező személy az eszközhöz ne férhessen hozzá;
- a kapcsolódás során meg kell győződni arról, hogy a kapcsolat biztonságos és védett, nyilvános wifi hálózat a kapcsolódáshoz nem javasolt;
- a kapcsolódó eszköz biztonsági funkciói tekintetében elvárás:
- a bejelentkezést megfelelő komplex jelszóval védeni (lásd jelszó követelmények Felhasználói kézikönyv);
- az eszközön automatikusan frissülő vírusírtó használata;
- az eszköz zárolása amennyiben a felhasználó eltávolodik tőle.
- Magántulajdonú eszközön a szervezet adata csak ideiglenes jelleggel tárolható, amennyiben lehetséges az adatok tárolását el kell kerülni. Amennyiben ez nem lehetséges, elvárt az adatok titkosított tárolása vagy jelszóvédelemmel, vagy jelszóvédett titkosított meghajtón történő tárolással.

3.6 Mobil informatikai tevékenység, távmunka

A mobil informatikai eszközön, illetve a távoli hozzáféréssel végzett munka esetén is meg kell teremteni az informatikai biztonságot. A szükséges védelemnek összhangban kell lennie ennek a speciális munkavégzésnek a kockázataival. mobil számítástechnikai eszközök használata során mérlegelni kell egyrészt a nem védett környezetben való munkavégzés kockázatait, másrészt a védekezés szükséges módját és eszközeit. A mobil számítástechnikai eszközökön az felhasználónak gondoskodni kell a rejtjelezett adattárolásról és adatátvitelről. Távmunka (távoli hozzáférés) esetén a szervezet érintett szervezeti egységeinek gondoskodniuk kell a biztonságos adatkapcsolat létrehozásáról, a kapcsolatot tartó hely és eszköz védelméről.

3.6.1 Mobil eszközökkel történő informatikai tevékenység

A mobil eszközök (laptopok, notebook-ok, otthoni munkaállomások, tabletek, mobil telefonok) használóinak mind a fizikai biztonság, mind a logikai védelem területén a jelen IBSZ-ben foglaltakat kell figyelembe venniük. Ezek közül a legfontosabbak:

- A távmunka során is be kell tartani a szervezet szabályzataiban foglaltakat.
- A mobil eszközök nem hagyhatók felügyelet nélkül, amennyiben nem biztosítható azok előírt védelme.
- A kommunikációhoz védett csatornáról kell gondoskodni, nyilvános publikus hálózatok használata, nem javasolt.
- Vírus- és behatolás védelmi eszközöknek működniük kell a mobil eszközön.
- A mobil eszközökön tárolt adatok bizalmasságának védelmére fokozott figyelmet kell fordítani.
- A mobil számítástechnikai berendezéseket nyilvános helyeken használóknak ügyelni kell arra, hogy elkerüljék a jogosulatlan személyek általi betekintés kockázatát.
- Bizalmas üzemeltetési információkat hordozó eszközt nem szabad felügyelet nélkül hagyni, és ha lehetséges, fizikailag el kell zárni vagy különleges zárat kell alkalmazni a berendezés biztosítására.
- A hordozható informatikai eszközök gazdája felelős az eszköz teljes biztonságáért és annak ellenőrzéséért.
- A rendszer csak limitált visszacsatolási információt szolgáltathat a felhasználónak a hitelesítési eljárás alatt, így megakadályozza a felhasználót abban, hogy ismerteket szerezzen a hitelesítési folyamatról.
- Az interaktív kapcsolatok zárolása felhasználó 15 perc inaktivitása után a rendszer megszakítja a kapcsolatot. / Az aktuális képernyőtartalmat olvashatatlanná kell tenni, le kell tiltani minden felhasználói tevékenységet, a hozzáférést / kijelzőket és zárolni kell a munkameneteket.

3.6.2 A távmunka

Távmunka végzése technológiai szempontból a laptoppal rendelkező kollégák számára engedélyezett, ugyanakkor a szervezet szabályainak megfelelően a távoli munkavégzést vezetővel kell engedélyeztetni.

Távmunka esetén is gondoskodni kell a helyszínen a biztonsági követelmények és előírások betartásáról, a megfelelő és rendszeres ellenőrzésről.

A távmunkát végző csak a kijelölt csatlakozási pontokon keresztül csatlakozhat a szervezet hálózatához.

A Rendszergazda határozza meg ezeket a belépési pontokat, azzal hogy azok jóváhagyásáról a Kancellári Kabinet vezetője dönt.

3.7 E-mail használat

A belső hálózaton hozzáférhető levelezőrendszer munkaeszköznek minősül, adattartalmának ellenőrzésére a munkáltató jogosult.

Az Egyetemen a munkavállalói és hallgatói e-mail címeket a következő konvenció szerint kell képezni:

vezetéknév.keresztnév@szfe.hu

vezetéknév.keresztnév@hallgato.szfe.hu

Névegyezés esetén szükséges egyéb azonosító integrálása a levelezési címbe, azonos email cím nem használható akkor sem amennyiben az azonos nevű személyek nem azonos időben tartoznak a szervezethez.

A szervezeti levelezőrendszer magáncélú levelezésre nem használható. A megvalósuló adatkezelés (informatikai rendszerben történő tárolás, törlés stb.) során fokozottan érvényesíteni kell a célhoz kötöttség elvét és a levéltitok védelmét. A nem kívánatos adatkezelés elkerülése érdekében a felhasználó köteles magáncélú leveleit – magáncélú használat tiltása ellenére beérkezett vagy küldött(!) - 48 órán belül törölni/eltávolítani, ennek elmaradása esetén azok adattartalma indokolt esetben (informatikai üzemzavar, hibakeresés stb.) vizsgálható.

A felhasználóknak az elektronikus levelező szolgáltatás használatának folyamán az alábbi szabályokat kell betartaniuk:

- A levelek nem képviselhetnek a hatályos magyar jogba ütköző magatartásformát (pl.: tiltott tartalmak – pornográfia, szerzői jogok megsértése. stb.).
- Tilos kéretlen levelek (spam), lánclevelek, hoax-ok, adathalászati célú levelek (phising) illetve bármilyen „nem hasznos" üzenetek akár belső, akár külső e-mail címek felé küldése, továbbítása. (kiemelten a folyamatos és rendszeres adattovábbítás).
- Tilos a felhasználóknak a szervezeti e-mail címüket nem feladatuk ellátásához köthetően használni (pl.: regisztráció letöltési weboldalak, online játék oldalak stb.).
- Levelet küldeni csak a levél tartalmában érintett személy(ek) részére szabad.
- Tilos a levelek fejlécének megváltoztatása, hamis levelek küldése.
- Ismeretlen feladótól érkező, gyanús, csatolt fájlt tartalmazó, vagy ismeretlen linket ajánló (pl.: idegen nyelvű, láthatóan reklámcélú, olyan dokumentumra hivatkozó, amiről a címzett nem tud) elektronikus üzenetek csatolmányait, illetve a kapott linkeket nem szabad megnyitni, e leveleket törölni kell.

Informatikai biztonsági vizsgálat, auditálás, illetve hibakeresés céljából a szervezet informatikai rendszereinek teljes hálózati forgalma megfigyelhető és rögzíthető. A felhasználó az IBSZ ismeretéről és elfogadásáról szóló nyilatkozatával elfogadja, hogy a rendszer használata egyben a felhasználó beleegyezését is jelenti az adatkezelésbe. Elektronikus levelek esetén a vizsgálat, illetve megfigyelés nem szükségképpen terjed ki a levelek tartalmára, de kivételesen indokolt esetben (pl. hibaelhárítás) a levelek megnyitására az Információbiztonsági felelős utasítása alapján sor kerülhet. Időszakos, illetve rendszeres biztonsági vizsgálat, avagy auditálás során a levelek az alábbi technikai tulajdonságok alapján kerülnek vizsgálatra:

- kéretlen levelek;
- vírusokat tartalmazó levelek;
- informatikai támadásokat megvalósító üzenetek;
- adathalászatot megkísérlő üzenetek.

3.8 Viselkedési szabályok az interneten

Az Egyetem internet használati jogokkal rendelkező felhasználói a munkájukkal kapcsolatban korlátlanul használhatják a szervezet által biztosított internet szolgáltatást.

A felhasználók a szervezet nevében csak a Kancellári Kabinet vezetőjének előzetes engedélyével tölthetnek fel internetre adatokat, anyagokat.

A szervezet tulajdonát képező adatbázisok tartalmának interneten keresztül történő hozzáférésének lehetővé tétele megfelelő jogosultságigénylés mellett az informatikai szakterület feladata. Az engedély megadása ilyen esetben vonatkozhat egyedi esetre vagy egyes rendszerekkel kapcsolatos feladatok elvégzésére az arra felhatalmazott munkatársak részére.

Az internet magán célú használata tiltott, az alábbi szabályokat kell betartani:

- tilos a pornográf, online játék, fogadási oldalak, csevegő oldalak, letöltő oldalak és törvénybe ütköző tartalmakat szolgáltató oldalak látogatása.
- Az internetről magán céllal tilos fájlokat letölteni.
- Informatikai biztonsági megfontolásokból tilos az Egyetemen a csevegő és azonnali üzenetküldő programok használata. Kivétel ez alól a szervezet által esetlegesen biztosított hasonló szolgáltatást nyújtó szoftver Egyetemen belüli használata.

3.9 A felhasználó feladatai a munkahely elhagyásakor

A munkavállaló a munkavégzés befejezése után köteles a számítógépet és a hozzá kapcsolódó eszközöket kikapcsolni. A munkaidő lejártát követően az irodát utoljára elhagyó munkavállaló köteles ellenőrizni, hogy minden számítástechnikai eszközt kikapcsoltak-e.

A munkavállaló amennyiben szünetelteti munkavégzését és felügyelet nélkül hagyja számítógépét, úgy azt zárolni köteles.

A munkaidő lejártát követően az irodát utoljára elhagyó munkavállaló köteles ellenőrizni, hogy az iroda minden helyisége, ablakai, ajtói zártak legyenek, és - ahol van – a biztonsági berendezések (pl. riasztó) élesítve legyenek.

3.10 Tiszta asztal tiszta képernyő szabályok a munkavégzés közben

A munkavállaló mindig csak a munkával kapcsolatos dokumentumok tarthatja elérhetően az íróasztalon és a képernyőn. Az érzékeny / személyes adatokat tartalmazó dokumentumokat, IT adathordozókat, mobil eszközöket a munka végeztével, illetve hosszabb távollét esetén munkanap közben is megfelelően el kell zárni.

Számítógép és mobil eszközök képernyő asztalaira egyidejűleg minimális, csak a munkával kapcsolatosan szükséges adatokat, illetve dokumentumokat helyezzük ki. Az eszközök fizikai elhagyása esetén megfelelő eljárással (zárolás, jelszavas képernyővédelem alkalmazásával) gondoskodni kell arról, hogy kívülállók ne tudjanak betekinteni a rendszerbe, ne férjenek hozzá a rendszerhez.

A munkavégzés során keletkező jegyzeteket, vázlatokat, illetve példányokat meg kell semmisíteni amennyiben már nincs szükség rájuk.

Prezentációk során oda kell figyelni, hogy mi kerül kivetítésre. Megbeszélések után a tárgyalókból minden dokumentumot el kell távolítani, a táblák tartalmát le kell törölni.

3.11 A vezetők felelőssége

A szervezeti vezetők felelőssége, hogy megkövetelje az alkalmazottjaitól és az általuk menedzselt alvállalkozóktól, hogy a biztonsági intézkedéseket a meghatározott szervezeti szabályzatokkal és eljárásokkal összhangban alkalmazzák. A vezetőknek biztosítaniuk kell, hogy a munkavállalók és alvállalkozók:

- ismerjék biztonsági felelősségüket, a biztonsági eljárások alkalmazását és az adatfeldolgozó lehetőségek korrekt használatát, mielőtt az érzékeny információkhoz vagy információs rendszerekhez hozzáférnek, hogy ezzel is a minimálisra csökkentsék a lehetséges biztonsági kockázatokat;
- vegyenek részt információbiztonsági oktatásokban;
- alkalmazkodjanak a foglalkoztatás feltételeihez, tartsák be az ide vonatkozó biztonsági szabályzatokat, a biztonságot érintő kérdésekben megfelelő, naprakész jártasságuk legyen.

3.12 Személyi biztonság a jogviszony megszűnésekor, megszüntetésekor vagy kinevezés módosítás esetén

A jogviszony megszűnése, megszüntetése, az éppen használt adatfeldolgozó eszközök és jogosultságok leadásával jár. A felhasználók feladatainak elhatárolása alapvető biztonsági követelmény, éppen ezért a jogosultságok megvonása teljes mértékben indokolt. Az Egyetemen belül másik szervezeti egységhez

átirányított alkalmazott vagy alvállalkozó esetében a jogosultságok megvonása az adatfeldolgozó eszközök visszaadása esetenként mérlegelendő.

Kilépő dolgozó esetén a levelezés automatikusan átirányításra kerülhet a szervezet egy másik email címére, melyet a kilépő dolgozó szervezeti egységének vezetőej meghatároz. Az automatikus továbbítás csak a szervezet egy másik belső email címére történhet, külsős email címre nem, és maximális ideje 3 hónap. 3 hónap után a levelezés tartalmát törölni / archiválni kell.

Az eszközök visszaadásához, a jogosultságok visszavonásához kapcsolódó részletes szabályozást az informatikai rendszerekhez és eszközökhöz való hozzáférés, kiadás és visszavétel tekintetében a Hozzáférésvédelmi szabályzat tartalmazza.

3.13 A jogviszony megszűnésének, megszüntetésnek biztonsági kérdései

A jogviszony megszűnése, megszüntetésekor a szervezet szempontjából biztonsági alapkövetelmény, hogy az alkalmazottak és alvállalkozók szabályozott módon hagyják el a Szervezetet.

A jogviszony megszűnése után a felhasználóknak Titoktartási nyilatkozatot szükséges aláírniuk a szervezet adatainak és információinak megfelelő biztonsága érdekében.

Az eszközök visszaadásához, a jogosultságok visszavonásához kapcsolódó részletes szabályozást az informatikai rendszerekhez és eszközökhöz való hozzáférés, kiadás és visszavétel tekintetében a Hozzáférésvédelmi szabályzat tartalmazza.

Az elektronikus információs rendszerek felhasználói fiókjait, email címeit évente legalább egyszer ellenőrizni szükséges. Az ellenőrzést az informatikai osztály támogatásával a HR osztály végzi. Az inaktív szükségtelen felhasználói fiókokat ezen felülvizsgálatok után meg kell szüntetni.

3.14 Fegyelmi eljárás

Azokkal szemben, akik a szervezet Informatikai Biztonsági Szabályait és eljárásait vétkesen megszegték, fegyelmi eljárást kell kezdeményezni és lefolytatni. A fegyelmi, felelősségi, kártérítési eljárást a Munka Törvénykönyvében foglaltak alapján.

3.15 Külső szervezetre vonatkozó követelmények

Az Egyetem a külső szervezettel kötött megállapodásban, szerződésben megköveteli, hogy:

- a külső szervezet határozza meg az Egyetemmel kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat;
- a szerződő fél feleljen meg az Egyetem által meghatározott személybiztonsági követelményeknek;
- a szerződő fél a szervezett érintő biztonsági auditokban közreműködjön;
- a szerződő fél dokumentálja és tartassa be a személybiztonsági követelményeket, beleértve azt az esetet, amikor a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az Egyetem elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az Egyetemnek.

A Rendszergazda folyamatosan, de legalább évente egyszer ellenőrzi a szerződő felek személybiztonsági követelményeknek való megfelelését, és az ezzel kapcsolatos jelentését megküldi a Kancellári Kabinet vezetőjének.

4 ADATHORDOZÓK VÉDELME

Biztosítani kell az adathordozók fizikai védelmét annak érdekében, hogy a dokumentumok, a számítógépek adathordozói, a bemenet/kimenet adatai és a rendszer dokumentációi a jogosulatlan megszerzésétől, módosítástól, eltávolítástól és rombolástól megfelelően védve legyenek. A papír alapú dokumentumok kezelésére vonatkozó irányelveket és biztonsági követelményeket a szervezet Iratkezelési Szabályzata tartalmazza.

Az adathordozók kezelésének legfontosabb biztonsági követelményei:

- Gondoskodni kell az adathordozók ellenőrzéséről és fizikai védelméről.
- Meg kell védeni a dokumentumokat, a számítástechnikai adathordozókat, az input/output adatokat és a rendszerdokumentációkat a károsodástól, eltulajdonítástól, jogosulatlan megismeréstől.
- Minden adathordozót újra alkalmazás előtt, illetve selejtezés után az adatok megsemmisítését eredményező megfelelő eljárással törölni kell. Ha ez nem valósítható meg, akkor az adathordozót fizikailag kell működésképtelenné tenni olyan módon, hogy a rajta lévő információ ne legyen visszanyerhető.
- Az adathordozókat úgy kell védeni fizikai és környezeti behatásoktól, hogy biztosítani lehessen az adatok sértetlen és hiteles állapotának megőrzését.
- Minden adathordozót biztonságos környezetben, a gyártó előírásainak megfelelően kell tárolni.

4.1 Hozzáférés az adathordozókhoz

Az Egyetem elektronikus információs rendszerében minden felhasználó jogosult adathordozók használatára a kapcsolódó – egyes esetekben adathordozó specifikus (pl.: mobiltelefon, mentési adattároló) – szabályozások alkalmazása mellett.

4.2 Az adathordozók tárolása

Az adathordozókat mindenkinek biztonságos helyen kell tárolni, védve azokat az illetéktelen hozzáféréstől, elvesztéstől. Ez a szabály nem mentesíti a felhasználót a mobil adathordozókon tárolt személyes adatok titkosítása alól, mely szükséges minden esetben.

4.3 Adathordozók szállítása

Az Egyetem tulajdonát képező számítástechnikai eszközöket, adathordozókat, kizárólag a Rendszergazda engedélyével szabad kivinni az Egyetem által tulajdonolt, vagy más jogcímen használt ingatlanokból.

Ez alól kivételt képez a dolgozók számára biztosított laptop, mobiltelefon, adattároló eszköz, mely eszközök szabadon kivihetők, ugyanakkor amennyiben védendő szervezeti adatot vagy személyes adatot tartalmaznak, az adatok titkosítása javasolt.

Az Egyetem területéről kivitt egyéb eszközöket nyilván kell tartani.

Javítás vagy megsemmisítés céljából adattároló eszköz kivitele esetén adathordozó csak úgy vihető ki, ha arról minden adat visszaállíthatatlan módon törlésre került. Amennyiben ez nem lehetséges, az adatot titkosítani szükséges, amennyiben pedig egy esetleges meghibásodás miatt ez sem lenne lehetséges, az eszközt folyamatosan kísérni kell, illetve a helyreállítást / megsemmisítést végző vállalkozóval Titoktartási megállapodást kell kötni.

4.4 Adathordozók törlése

Biztonságos törlés az írható és olvasható adathordozók többszörös felülírásával valósul meg, mely során az adatok törlését Gutmann (35 menetes) vagy a Schneier (7 menetes) törlési eljárásokkal vagy ezekkel egyenértékű, az adatok helyreállíthatatlanságát biztosító szoftverrel kell elvégezni. A szoftver a fájlok törlését követően véletlenszerű algoritmus alapján előállított adatokkal írja felül azok fizikai és logikai helyét az adathordozón.

Asztali számítógépek és laptopok visszavételekor a rajtuk lévő adatokat legkésőbb 30 nap múlva törölni kell, az eszközt pedig újra kiadás előtt újra kell telepíteni.

4.5 Ismeretlen tulajdonos

Az Egyetem megtiltja az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható.

4.6 Az adathordozók selejtezése

Alapvető biztonsági cél, hogy az adathordozókat visszaállíthatatlanul, dokumentáltan selejtezzék. A különféle szabványokban definiált adattörlési és megsemmisítési eljárások a lehető legkisebbre csökkentik az információ kiszivárgásának kockázatát.

- Az adathordozót visszaállíthatatlan módon kell selejtezni, típustól függően fizikai vagy logikai úton.
- Selejtezés során minden adathordozót a legerősebb biztonsági eljárással kell selejtezni.
- Adathordozó selejtezéssel foglalkozó cég igénybevétele esetén kulcsfontosságú biztonsági tényező a megfelelő kvalitású szerződő fél kiválasztása, valamint az informatikai biztonsági feltételek szerződésbe foglalása.
- Azok az adathordozók, amelyeket nem lehet törölhetők, azokat fizikailag meg kell semmisíteni.
- Az adathordozó védelme csak az adatok törlését, valamint a bizalmas adattartalomra utaló valamennyi jelzést eltávolítását követően szüntethető meg.

4.7 Adathordozók megsemmisítése

Az adathordozók típusának és fizikai megvalósulásának megfelelő módszert kell választani a megsemmisítéséhez.

Az adathordozók megsemmisítése a következő módszerekkel engedélyezett:

- Mágnesszalagok: El kell távolítani a tokból, majd mechanikusan be kell zúzni, kémiai úton megsemmisíteni vagy elégetni.
- Lemezek: A lemezt szabálytalan alakú darabokra kell vágni (legalább 8 darabra), a darabokat deformálni kell vagy elégetni.
- Merevlemezek: Fel kell nyitni és el kell égetni, a mágneses felületet el kell távolítani, illetve szét kell szedni és az adathordozót apró darabokra vágni, vagy cél eszközzel feldarabolni.
- Más szilárd anyagú tárolók: össze kell törni, kémiai úton használhatatlanná tenni vagy el kell égetni.

5 ÜZLETMENET (ÜGYMENET) FOLYTONOSSÁG TERVEZÉS

Az üzletmenet folytonosság biztosítása egyrészt külsős szolgáltatók által biztosítandó feladat (rendszerek biztonságos üzemeltetése által), másrészt a szervezet rendszereinek tekintetében az informatikai részleg feladata. Ennek érdekében a Rendszergazda évenként ellenőrzi, hogy az informatikai tartalékok folyamatosan működőképes állapotban álljanak rendelkezésre, és az ezzel kapcsolatos jelentését megküldi a Kancellári Kabinet vezetőjének.

5.1 Alapfeladatok ellátását támogató rendszerek

Jelenleg az Egyetem működésének folytonosságát figyelembe véve a következő rendszerek folyamatos működése elvárt.

- Microsoft Cloud (M365)
- Neptun
- Poseidon
- Saldo

Ezen rendszerek mindegyikét külsős szolgáltatók támogatják, így a folyamatos üzemeltetésért felelősséggel ők tartoznak.

5.2 A folyamatos működésre felkészítő képzés

Az Egyetem az elektronikus információs rendszerek folyamatos működésére felkészítő képzést tart melynek témái

- felhasználóknak: mentések, adatkezelés
- informatikusoknak: technológiák és üzemeltetés

5.3 Az elektronikus információs rendszer mentései

A mentési és visszaállítási eljárásokat úgy kell kialakítani, hogy az Egyetem által üzemeltetett rendszerek előre nem látható esemény bekövetkezte után szükség esetén helyreállíthatók legyenek, ezáltal ne sérüljenek az információk, adatok, rendszerek rendelkezésre állásának az Egyetem által elvárt kritériumai, illetve fontos annak biztosítása, hogy egy bekövetkezett információbiztonsági esemény / incidens kivizsgálásához megfelelő minőségű eseménynapló információ is rendelkezésre álljon.

Minimálisan a következő mentéseket kell elvégezni:

- a szervereken tárolt adatokról (alkalmazások, adatbázisok fájlok, dokumentumok, naplóinformációk, konfigurációs információk),
- aktív menedzselhető eszközökről (naplóinformációk, konfigurációs információ) automatikus napi mentést kell készíteni;
- a mentésekért felelős vállalkozónak mentési rendben meghatározott módon szerverek teljes adattartalmáról napi (teljes vagy inkrementális), heti (teljes) és havi (teljes) mentéseket kell készítenie;
- a tranzakció alapú rendszerek esetén tranzakció alapú mentést kell készíteni, ami lehetővé teszi a tranzakció helyreállítást.

A munkatársak munkájának folytonosságát a munkavégzéshez biztosított informatikai eszközök (asztali számítógépek és laptopok) rendszeres Microsoft Cloudba való mentése, biztosítja.

Az automatikus mentés kiterjed a következő mappákra:

- Dokumentumok,
- Képek,
- Asztal.

A havi teljes mentéseket archív biztonsági másolatoknak tekintjük. Ezek kezelése esetében a mentési rend definiálja az adathordozó média típusát, valamint tárolási helyét és körülményeit.

Fontos, hogy az archivált rendszer futtatási környezetét, architektúrájának leírását, teljes dokumentációját is archiválni szükséges, amit minden verzióváltás után frissíteni kell, annak biztosítása érdekében, hogy az archivált adat visszaállítható legyen.

A Rendszergazda köteles esetenként, de legalább 30 naponta a mentések elvégzését és megbízhatóságát ellenőrizni, valamint az archív mentések olvashatóságát és helyreállíthatóságát rendszeresen, de legalább évente ellenőriztetni a mentéseket végző vállalkozóval.

5.3.1 Mentési eszközök

Biztosítani kell, hogy a mentett adatok mindig visszaolvashatók legyenek, ezért a mentéseket olyan eszközökkel kell elvégezni, amelyek garantálják a mentett adatok visszaolvashatóságát. Időnként (minimum évenként) próba visszatöltést kell megvalósítani az alkalmazott eszközök és módszerek megbízhatóságának ellenőrzése céljából.

A mentések elvégzéséhez biztosítani kell a megfelelő számú adathordozó egységet. Folyamatosan figyelemmel kell kísérni a mentendő adatmennyiség változását, és ennek megfelelően kezdeményezni új adathordozók beszerzését. Minden médiatípus esetén legalább 10% tartalékot szükséges tartani.

A mentéshez használt mentési médiák használati idejét a gyártó által megadott élettartam figyelembevételével, 10%-os biztonsági tartalékkal javasolt meghatározni. Az élettartamot figyelembe kell venni mind a többszöri felhasználásnál, mind pedig a hosszú távon megőrzendő adatok tárolásánál. Az élettartamok figyelését a mentésért felelős munkatársaknak kell elvégezniük. Amennyiben egy média élettartama meghaladta a használati időt, a mentésért felelős munkatársnak kell kezdeményeznie a média selejtezését, és az új média beszerzését.

5.3.2 A mentett adatok tárolása

A mentéseket mindig biztonságos helyen kell tárolni. Biztosítani kell, hogy a mentett állományok csőtörés, tűz vagy lopás során ne semmisülhessenek meg. Ezért a biztonsági mentéseket – amennyiben azok éppen nem használt adathordozón vannak - tűzbiztos páncélszekrényben kell tárolni.

Az archív adatokat tartalmazó adathordozókat minden esetben a szerverektől elkülönített helyiségben elzárva kell őrizni.

Javasolt, hogy az adathordozók számmal és vonalkóddal is azonosíthatók legyenek. Az adathordozókkal végzett tevékenységeket az azonosító számhoz kötve ajánlatos dokumentálni. Amennyiben nem áll rendelkezésre olyan technika, amellyel a mentési média címkézése a fent említett módon megtehető, kiemelt figyelmet kell fordítani az egyes mentési elemek egyedi azonosítására.

A mentési adathordozók tartalmát legkésőbb 3 év után törölni szükséges.

Az O365 környezetben tárolt, a dolgozói számítógépekről és laptopokról készülő mentési információk tárolása:

- munkavállaló távozása után azon fájlokat melyek a felhasználó saját személyes mappáiban kerültek tárolásra, azaz nem közös használatú fájlok,
- legkésőbb 3 hónappal a munkavállaló távozása után törölni kell.

5.3.3 Mentési feladatok

A mentési tevékenységgel megbízott felelőst vagy alvállalkozót a Rendszergazda jelöli ki. A mentésért felelős személy/alvállalkozó feladata a Rendszergazda által meghatározott mentési és helyreállítási elvárásoknak megfelelően:

- mentési job-ok beállítása (honnan - hova és mit mentsen a szervezet előírásainak megfelelően);
- mentések elvégzése;
- mentési média ellenőrzése és rendelkezésre állás biztosítása;
- mentés folyamatának ellenőrzése;
- mentés eredményének ellenőrzése évenkénti visszatöltési tesztek segítségével, melyek eredményéről a Rendszergazdát és az IBF-et értesíteni szükséges.

A mentéseket lehetőleg úgy kell elvégezni, hogy azzal a felhasználók munkáját ne akadályozzák.

5.3.4 Mentési naplók

A mentések végrehajtásáról naplót kell vezetni, amelynek a következőket kell tartalmaznia:

- a mentés tartalmát;
- a mentés időpontját;
- mentés jellegét (teljes mentés, inkrementális kumulatív, inkrementális, differenciált stb.);
- a mentés eredményét (sikeres / sikertelen, hiba oka).

A biztonsági eseménynaplókat 3 évre visszamenőleg, a napi mentéseket minimum 1 hónapig, heti mentéseket minimum 2 hónapi, havi mentéseket minimum 6 hónapig kell megőrizni. Az egyedi mentéseket pedig a mentést elrendelő Szervezeti vezető utasításának megfelelő ideig őrizni. Ha az előírt mentéseket valamely okból nem lehet megvalósítani, már meglévő korábbi mentéseket csak az IBF engedélyével szabad törölni.

6 BIZTONSÁGI ESEMÉNYEK / INCIDENSEK KEZELÉSE

6.1 Általános elvárások

Az Egyetem minden informatikai eszközén, folyamatosan figyelni kell a rendszerek esetleges hibaüzeneteit. A felhasználóknak figyelemmel kell kísérni a működési zavar tüneteit, a képernyőn megjelenő üzeneteket. A hiba, illetve incidens elhárítására szükség esetén a felhasználó vegye fel a kapcsolatot az illetékes informatikai munkatárssal.

Minden az informatikai rendszereket érintő vagy az informatikai rendszerekkel összefüggésbe hozható biztonságot veszélyeztető eseményt vagy annak gyanúját haladéktalanul jelenteni kell, illetve mindent meg kell tenni a szükséges bizonyítékok összegyűjtésére.

Informatikai biztonsági incidens előfordulása esetén az abban érintett alkalmazottaknak és külső vállalkozónak törekedni kell arra, hogy a biztonsági események, zavarok okozta károk minimálisak legyenek, valamint a biztonsági események folyamatosan nyomon legyenek követve, és a megfelelő következtetéseket az illetékesek levonják. Mérsékelni kell a biztonságot befolyásoló események és működési zavarok következményeit, nyomon kell követni az eseményeket, biztosítani kell a mielőbbi normális üzemre való visszaállást és a tapasztalatokat írásban kell megfogalmazni.

Amennyiben a rendszerhibát vélhetően külső, illetéktelen beavatkozás, vagy vírustámadás okozta, az érintett munkaállomást, számítógépet / alhálózatot le kell választani a hálózatról, szükség esetén ki kell kapcsolni, vagy a teljes alhálózat működését szüneteltetni kell. Ilyen esetekben fokozottan figyelni kell a hordozható adathordozókra is, melyeket az illetékes informatikai munkatársnak vizsgálat céljára át kell adni.

A meghibásodott számítógépben használt adathordozók kizárólag a biztonsági ellenőrzést követően használhatók más számítógépekben.

Az eseménykezelési tevékenységekből levont tanulságokat be kell építi az eseménykezelési, üzemeltetési eljárásokba, elvárásokba, továbbképzésekbe.

6.2 Incidenskezelés folyamata

Az Incidenskezelési szabályzat írja le az incidensek bejelentésének folyamatát.

- A bejelentés fogadása után, ha az informatika önálló hatáskörben nem tudja kezelni a felmerült problémát értesíti az illetékes támogató munkatársat vagy alvállalkozót.
- Amennyiben probléma megoldható / kivizsgálható e-mailben vagy telefonon nyújtott válaszadással is, a leírt lépéseket a felhasználónak pontról-pontra kell végrehajtania.
- Ha távolról ez nem lehetséges, a kivizsgálással és elhárítással megbízott munkatárs/ alvállalkozó felkeresi a kezdeményező felet, és a helyszínen hárítja el a hibát az IBF vagy megbízottja felügyelete mellett, az adott rendszerre vonatkozó adatvédelmi szabályok betartásával. Olyan elektronikus információs rendszerek esetén, amelyek személyes adatokhoz férnek hozzá, ezek védelmére fokozott figyelmet kell fordítani. Ha a feladatot nem lehet elvégezni a helyszínen, a munkatárs/ alvállalkozó az eszközt dokumentáltan átveszi, és a be- és kiszállításra vonatkozó előírások fokozott figyelembevétele mellett elszállítja hibaelhárításra.
- Távoli segítségnyújtás során a probléma elhárítását végző felelős a felhasználó számítógépe felett, a felhasználó engedélyével ideiglenesen átveheti az irányítást, illetve megtekintheti annak tartalmát. Ilyenkor a felhasználó képernyőjére, aktuális folyamataira az adott munkatársnak/ alvállalkozónak teljes rálátása és irányítási lehetősége van. Ebben az esetben a folyamatot az IBF vagy annak megbízottja felügyeli. Olyan elektronikus információs rendszerek esetén, amelyek személyes adatokhoz férnek hozzá, ezek védelmére fokozott figyelmet kell fordítani.

A szerver oldali és hálózati incidensek a felhasználók nagy többségét érintik. Ezen feladatok a végfelhasználói prioritással szemben előnyt élveznek, ezért szükség esetén a végfelhasználóhoz kapcsolódó folyamat felfüggesztendő.

Az incidensek priorizálása a Rendszergazda feladata, az informatika munkatársainak ezen irányú képzéséért az Információbiztonsági felelős felel.

6.2.1 Incidenskezelés prioritások

A biztonsági incidenseket a következők szerint kell priorizálni és reagálni:

Az 1. prioritású incidensek kivizsgálását és elhárítását munkaidőben az észlelést követően azonnal, munkaidőn túl 4 órán belül meg kell kezdeni:

- határsértés és illegális tevékenység észlelése (behatolás),
- vírus-vészhelyzet (tömeges fertőzés), vagy központi vírusvédelmi eszköz kiesése,
- adminisztrátori jogosultságok sérülése,
- folyamatos működéshez szükséges rendszer (lásd IBSZ 4.1 alfejezet), vagy rendszer elemek teljes kiesése,
- informatikával összefüggésbe hozható bűncselekmények,
- törvényi szabálysértések.

A 2. prioritású incidens elhárítását munkaidőben az észlelést követően azonnal, munkaidőn kívül 8 órán belül meg kell kezdeni, ha az 1. prioritású incidens elhárítását nem akadályozza:

- ismétlődő vírusfertőzés, vagy vírusdefiníciós állomány nem frissülése,
- felhasználói jogosultságok sérülése.

A 3. prioritású incidensek kivizsgálását munkaidőben az észlelést követően 4 órán belül, munkaidőn kívül bejelentve 72 órán belül meg kell kezdeni. Ilyen például a/az:

- egyszeri vírusfertőzés, vagy helyi vírusvédelmi eszköz kiesése,
- kisebb jogosultsági incidensek (felhasználó elfelejtette a jelszavát, vagy az lejárt stb.).

A 4. prioritású incidensek kivizsgálását kezelését a folyamatban levő magasabb prioritású incidensektől függően kell megkezdeni. Ilyen például a:

- vírusvédelmi menedzsment eszközök kiesése,
- felügyeleti és menedzsment eszközök kiesése,
- munkaállomás működésével kapcsolatos működési hibák,
- belső szabály- és eljárássértések,
- felhasználói hibák.

Az incidensek priorizálása elsősorban a Rendszergazda, helyettesítés esetén az Információbiztonsági felelős feladata.

6.2.2 Incidenskezelés folyamata

Az incidensek elhárítása során ügyelni kell arra, hogy a kivizsgálásához elengedhetetlen információkat megőrizzék, azokat elmentsék vagy feljegyezzék.

Az incidens bekövetkezéséhez és kivizsgálásához, az elhárításhoz kapcsolódó információkat jegyzőkönyvben szükséges rögzíteni oly módon, hogy abból megismerhető legyen a hiba vagy a kihasznált sérülékenység mely az incidenst okozta.

Az incidensek kivizsgálása során feltárt tanulságokat súlyos 1. prioritású incidens esetén azonnal be kell építeni az üzemeltetési / szabályozási folyamatokba, más prioritású incidensek esetén évente szükséges azokat összesíteni, és a kapcsolódó kockázatokat alapul véve dönteni a szükséges változtatásokról. E döntéseket az IBF és a Rendszergazda közösen hozza.

6.2.3 Incidenskezelés dokumentációinak megőrzése / nyilvántartás

Az informatikai biztonsági incidensek vizsgálata során keletkezett, papíralapú és elektronikus, iktatott dokumentumokat az információbiztonsági felelős az informatikai biztonsági incidens vizsgálatának lezárásától számított 10 évig őrzi meg, illetéktelenek számára hozzá nem férhető, zárt helyen.

6.3 Képzés a biztonsági események kezelésére

Az Egyetem biztonsági eseménykezelési képzést biztosít az elektronikus információs rendszer felhasználóinak a számukra kijelölt szerepköröknek és felelősségnek megfelelően:

- szerepkörbe vagy felelősségbe kerülésüket követő 30 munkanapon belül;
- a képzéseket évente el kell végezni az elektronikus információs rendszer mindenkori állapotának megfelelően, vagy amikor az elektronikus információs rendszer változásai megkívánja.

6.4 Biztonsági Eseménykezelési helyzet és képesség mérése

Évente a kockázatelemzési folyamat részeként szükséges felülvizsgálni a bejelentett biztonsági eseményeket, és a tapasztalatokat beépíteni a szabályozásba, a képzésekbe esetleg egyes folyamatok változtatása is szükséges lehet.

7 KARBANTARTÁS

Az informatikai eszközök karbantartását folyamatos rendelkezésre állásuk és sértetlenségük érdekében a gyártó útmutatása alapján, előírás-szerűen el kell végezni. A karbantartási ciklus kialakításáért a Rendszergazda, partnerek szerződtetéséért az IBF a felelős, aki:

- a karbantartások ütemezését és módját meghatározza;
- írásban engedélyezi azon tervezett karbantartásokat, melyek szolgáltatáskieséssel járnak, a szolgáltatáskieséssel nem járó karbantartások engedélyezése nem elvárt;
- kihirdeti a kieső szolgáltatás miatt érintett felhasználók számára a karbantartások várható időpontjait.

A karbantartás során:

- Az eszközöket csak a Rendszergazda jóváhagyását követően lehet leállítani;
- az elvégzett munkákat jegyzőkönyvezni kell, a jegyzőkönyveket pedig 3 évig meg kell őrizni oly módon, hogy a karbantartások e nyilvántartásból visszakövethetők legyenek;
- amennyiben adatot tartalmazó adathordozó kiszállítása válik szükségessé, akkor elsődlegesen az elszállítás előtt minden adatot és információt - mentést követően – törölni kell a berendezésről, amennyiben ez nem lehetséges gondoskodni kell annak titkosításáról. A kiszállítást a Rendszergazda engedélyezi.

A karbantartás után:

- A Rendszergazda ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat.

7.1 Távoli karbantartás

Távoli karbantartás végzését vagy szerződéses alapon szerződött partner, vagy az Egyetem informatikusa végzi, egyéb esetben a távoli karbantartást az IBF engedélyezheti.

A távoli karbantartásról is jegyzőkönyvet kell vezetni, amely a nyilvántartás részét képezi. A jegyzőkönyvet a munkát elvégző szakembernek kell levélben megküldenie.

Távoli karbantartás esetén a karbantartáshoz szükséges kapcsolatot kizárólag a karbantartás idejére szabad felépíteni a karbantartó részére.

7.2 Karbantartók

Abban az esetben, ha saját erőből a karbantartás nem végezhető el, akkor a Rendszergazda kezdeményezi külső fél megbízását. A Rendszergazda által megbízott külső félhez a félhez kéréseket a felhasználók is továbbíthatnak. A karbantartást végző külső felekről belépéskor nyilvántartás kell vezetni – a fizikai belépések nyilvántartásának megfelelő folyamat szerint - melynek minimálisan a következőket tartalmaznia:

- karbantartó neve,
- cég megnevezése,
- szerződött partner megnevezése,
- belépés dátuma, ideje,
- távozás dátuma, ideje.

Külsős vállalkozó munkavégzése esetén folyamatos felügyeletet kell biztosítani a karbantartás során.

A külső féllel kötött szerződésbe kell foglalni, hogy a karbantartást felügyelők jogosultak kérni a karbantartást végző személy személyazonosságának igazolását, illetve, hogy a karbantartást végző személynek kötelessége a felszólításra a szükséges iratokat bemutatni.

8 KONFIGURÁCIÓKEZELÉS

8.1 Legszűkebb funkcionalitás

Az Egyetem biztonságos konfigurálási követelmények szerint, a legszűkebb funkcionalitásra törekedve konfigurálja be a rendszereit.

8.2 Alapértelmezett jelszavak

Alapszabályként az Egyetem minden rendszer esetében gondoskodik a telepítést, üzembe helyezést követően az alapértelmezett jelszó megváltoztatásáról.

8.3 Az elektronikus információs rendszer kapcsolódásai

Az Egyetem belső engedélyhez köti az elektronikus információs rendszerének kapcsolódását más elektronikus információs rendszerekhez (hálózatán belül és azon kívül is). Az engedélyt írásban a Rendszergazda adhatja meg. A rendszerkapcsolatok, az interfészek paraméterei, a kapcsolaton keresztül átvitt elektronikus információk típusa az elektronikus információs rendszerek nyilvántartásában kerül dokumentálásra.

Az Egyetem a külső elektronikus információs rendszerekhez való kapcsolódások konfigurálása során a „minden tiltása, kivételek engedélyezése" elvet követi.

8.4 Sérülékenység vizsgálata

Az Egyetem az elektronikus információs rendszerei és alkalmazásai tekintetében sérülékenység tesztet végez, vagy végeztet, ha azt az elektronikus információs rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik:

- legalább háromévente, vagy véletlenszerűen, valamint olyan esetben, amikor új lehetséges sérülékenység merül fel az elektronikus információs rendszerrel vagy alkalmazásaival kapcsolatban, megismétli a sérülékenység tesztet;
- a sérülékenység tesztet sérülékenységvizsgálati eszközök és technikák alkalmazásával vagy külső szervezet bevonásával azon elektronikus információs rendszerek tekintetében végzi el, amelyek a Szervezet felügyelete, irányítása alatt állnak;
- olyan sérülékenységi teszteszközt kell alkalmazni, melynek sérülékenység feltáró képessége könnyen bővíthető az ismertté váló sérülékenységekkel;
- a sérülékenységi teszteszközt minden vizsgálat előtt frissíteni is kell ezen új sérülékenységekkel.
- Az elektronikus információs rendszerbek különleges jogosultsághoz kötött - úgynevezett privilegizált - hozzáférést biztosít a Szervezet az általa kijelölt rendszerelemekhez a sérülékenység teszt végrehajtásához.

Az elvégzett teszt eredménye alapján a szervezet vagy a vizsgálatot végző vállalkozó:

- kimutatást készít a feltárt hibákról, valamint a nem megfelelő konfigurációs beállításokról;
- felméri a sérülékenység lehetséges hatásait;
- elemzi a sérülékenység teszt eredményét;
- megosztja a sérülékenység teszt eredményét a Rendszergazdával és az IBF-el, aki dönt a további érintettekről;
- a feltárt sérülékenységeket a lehető leghamarabb javítja, vagy azok lehetséges hatását más eszközökkel csökkenti.

Az Egyetem vagy a vizsgálattal megbízott vállalkozó meghatározza, hogy egy támadó milyen információkat képes elérni az elektronikus információs rendszerben, és amennyiben szükséges, ennek minimalizálására javításokat kell végezni.

9 RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS ELJÁRÁSRENDJE

Az Egyetem ezt az eljárásrendet alkalmazza minden olyan esetben, amelyben informatikai szolgáltatást vagy eszközöket szerez be vagy, ha rendszerfejlesztési tevékenységet végez vagy végeztet.

9.1 Informatikai rendszerek és eszközök csatlakozása az Egyetem informatikai rendszeréhez

Az Egyetem informatikai rendszeréhez csak olyan eszköz és informatikai rendszer csatlakoztatható, mely

- megfelel a szervezet által elvárt funkcionális, biztonsági és dokumentációs követelményeknek, és melyet a
- melyet a Rendszergazda adott ki;
- idegen eszközök esetében olyan eszköz, mely megfelel a szervezet információbiztonsági szabályainak, melyek biztonságáért (illetve a kapcsolódó adatvédelmi szabályok betartásáért) az eszközt csatlakoztató felhasználó felel.

9.2 A védelem szempontjainak érvényesítése a beszerzés során

Az Információbiztonsági felelősnek meg kell határoznia, hogy miképpen kell védeni az elektronikus információs rendszert a beszerzett eszköz beillesztéséből adódó kockázatok ellen. Az Egyetem szerződéses követelményként kell meghatároznia a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére a beszerzett rendszerelem / szolgáltatás védelmi intézkedések leírását. Ez alapján az IBF dönt arról, hogy ezek megfelelnek-e a szervezet általános védelmi intézkedéseinek.

9.3 Erőforrás igény felmérés

Az Egyetem az elektronikus információs rendszerre és annak szolgáltatásaira vonatkozó biztonsági követelmények teljesítése érdekében a beruházás, vagy költségvetési tervezés részeként a rendszerek teljes életciklusában meg kell határoznia, dokumentálnia és biztosítania kell az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges követelményeket és erőforrásokat.

9.4 Szerződéses követelmények meghatározása a beszerzés során

Az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben követelményként meg kell határozni minimum a következőket:

- funkcionális biztonsági követelményeket;
- a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint);
- a biztonsággal kapcsolatos dokumentációs követelményeket;
- a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;
- az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat;
- átadás – átvétel folyamatának leírását, a tesztelési követelményeket;
- dokumentáltsági követelményeket;

A fenti követelményeket a szerződési sablonok használatával kell rögzíteni. E követelmények kiegészülnek a további szabályozási pontok alapján.

9.5 A rendszerre vonatkozó dokumentáció

Az alkalmazás fejlesztés során a fejlesztőtől – függetlenül attól, hogy külső, vagy belső fejlesztő – a következő dokumentumokat kell minimálisan megkövetelni:

- rendszerbiztonsági terv;
- felhasználói kézikönyv;
- üzemeltetési kézikönyv;

- üzletmenet-folytonossági / katasztrófaelhárítási terv;
- fizikai és logikai rendszerterv;
- mentési rend;
- az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentáció, amely tartalmazza:
- a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,
- a fejlesztői módosítások átvezetésének módját;
- az alkalmazást működtető rendszerelemek (operációs rendszer) frissítésének módját,
- a biztonsági funkciók hatékony alkalmazását és fenntartását,
- a rendszerelemmel, a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket;
- a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat;
- a rendszer működési folyamatainak ismertetését, példákkal illusztrálva;
- Konfiguráció, hibaelhárítás:
- Felhasználói konfigurációk lehetősége;
- Konfigurációs paraméterek;
- Jellemző hibalehetőségek és azok megoldása:
- Hibaüzenetek;
- Hibaelhárítási tevékenységek.
- üzemeltetési kézikönyv;
- rendszerismertető, mely a következőket tartalmazza:
- a rendszer bemutatása, koncepciója és architekturális vázlata;
- futtatási környezet leírása;
- kapcsolat más rendszerekkel;
- interfészek leírása;
- jogosultsági rendszer;
- rendszeresen, időszakosan elvégzendő üzemeltetési feladatok:
- Monitorozás (rendszeres hálózati ill. folyamat monitorozás);
- Batch futtatás (rendszeresen elvégzendő, döntési pontokat nem tartalmazó vagy teljeskörűen leírható futtatási feladatok);
- Újraindítás és leállítás (jogosultak és engedélyezők köre, engedélyezés folyamata, újraindítás és leállítás feltételei, értesítés módja és értesítési lánc, végrehajtandó lépések, dokumentálás módja);
- Outputkezelés (rendszeresen elvégzendő lépések);
- Biztonsági mentések (rendszeresen elvégzendő lépések);
- Archiválás (rendszeresen elvégzendő lépések);
- Rendszerkarbantartás (rendszeresen elvégzendő ellenőrzések);
- Programcsere menedzsment szabályozása és gyakorlata (tartalmazhatja a külső céggel kötött szerződés);
- Karbantartás (tartalmazhatja a külső céggel kötött szerződés);
- Rendszerhiba esetén szükséges teendők.
- fejlesztői dokumentáció, forrásprogram.

Meg kell követelni az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amelynek tartalmaznia kell:

- a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját;
- a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit;

- a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához.

Az infrastrukturális rendszerfejlesztések alkalmával az alábbi dokumentációkat kell elkészíteni:

- hálózati ábra;
- fizikai és logikai rendszerterv;
- rendszerbiztonsági terv;
- üzemeltetési kézikönyv;
- az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza:
- a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,
- a biztonsági funkciók hatékony alkalmazását és fenntartását,
- a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket,
- a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat.
- A dokumentációk tekintetében eltéréseket az Információbiztonsági Felelős és a Rendszergazda engedélyezhet írásban, a beszerzett eszköz, szoftver, szolgáltatás megismerése után.

9.6 Funkciók - protokollok – szolgáltatások

- A szerződésekben kötelezni kell a szállítókat arra, hogy már a fejlesztési életciklus korai szakaszában meghatározzák a használatra tervezett funkciókat, protokollokat és szolgáltatásokat, mely így lehetővé teszi a rendszerelem integrációjának biztosítását.

9.7 Külső elektronikus információs rendszerek szolgáltatásai

- A szolgáltatási szerződésekben ki kell kötni, hogy a szolgáltatási szerződés alapján igénybe vett elektronikus információs rendszerek szolgáltatásai feleljenek meg a szervezet elektronikus információbiztonsági követelményeinek.
- Az Egyetemnek külső és belső ellenőrzési eszközökkel ellenőriznie kell, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket. Az ellenőrzést az IBF végzi szúrópróbaszerűen.

9.7.1 Folyamatos ellenőrzés

- Az informatikai biztonsággal összefüggő beszerzéseket folyamatba épített időszakos belső ellenőrzési tervnek megfelelően ellenőrizni kell. Az ellenőrzési tervnek ki kell terjednie a következőkre:
- az ellenőrizendő területek meghatározása;
- az ellenőrzések, valamint az ellenőrzéseket támogató értékelések gyakorisága;
- az ellenőrzés eredményének értékelésnek módszertana.
- Az ellenőrzést az IBF által az ellenőrzésre kijelölt szervezet, vagy munkacsoport az ellenőrzési tervben foglaltak szerint hajtja végre. Az ellenőrzés során tett megállapításokból értékelni kell az ellenőrzött terület követelményeknek való megfelelőségét.
- Az ellenőrzés megállapításaira, illetve az ellenőrzés értékelésére alapozva intézkedési tervet kell kidolgozni és végrehajtani abban az esetben, ha az ellenőrzés a szervezet által nem tolerálható kockázatot tár fel. Ha az ellenőrzés során személyes felelősség kerül megállapításra, haladéktalanul intézkedni kell a felelősség megfelelő tisztázásáról és a szabályszegés megfelelő szankcionálásáról.
- Az ellenőrzések eredményét minden esetben meg kell osztani az IBF-el, aki az eredménytől függően eszkalálhatja azt a Kancellár felé.
- A folyamatos ellenőrzéssel kapcsolatos feladatokat az IBF koordinálja.

9.8 Elfogadási kritériumok

Az új informatikai rendszerekre, a bővítésekre és az új változatokra vonatkozó elfogadási, átvételi kritériumait rögzíteni kell a következők szerint:

- a rendszer leírását, annak funkcióinak összekapcsolását a folyamatokkal;
- paramétereit, ki- és bemenő adatait, minden olyan további igényt, melyet a szervezet támaszt az új rendszerrel kapcsolatban specifikációba kell foglalni és azt mind a megrendelő, mind a szállító oldalán el kell fogadni a fejlesztés megkezdése előtt;
- a specifikáció szerint kell lefolytatni a tesztelést az érintett felhasználók, alkalmazás rendszergazdák és az adatgazdák bevonásával;
- amennyiben a tesztelések pozitív eredménnyel zárulnak, a szoftver átvehető;
- a szoftvernek maradéktalanul meg kell felelnie a specifikációnak és a szervezet elektronikus információs rendszeréhez illeszkednie kell, mind funkcionális, mind biztonsági szempontból;
- az átadás-átvételi eljárást a szervezet belső szabályait és a jogszabályi előírásokat betartva kell lefolytatni, az eljárás részeként jóváhagyó tesztelést kell végezni, arról és magáról az átadásról is Jegyzőkönyvet kell készíteni;
- oktatások megtartása, rendszer és egyéb dokumentációk (felhasználói leírások, üzemeltetési utasítások stb.) átvétele, eljuttatása az összes érintetthez kötelező.

10 RENDSZER ÉS INFORMÁCIÓSÉRTETLENSÉG

Az egyes alkalmazásokhoz és hálózati mappákhoz (könyvtárakhoz) való hozzáférés (jogosultságok) dokumentált engedélyeztetése útján gondoskodni kell arról, hogy jogosulatlan felhasználó azokat ne módosíthassa, és ne törölhesse.

A mentések és archívumok tárolása és őrzése során biztosítani kell az adatok sérthetetlenségét.

Számítógépes adatvesztés vagy adatsérülés esetén az adatfeldolgozást az adatokat tartalmazó rendszernél azonnal fel kell függeszteni és a kijelölt informatikust azonnal értesíteni kell. Az értesítés történhet e-mail, telefon vagy személyes bejelentés útján. A felmerült probléma tisztázása után a kijelölt informatikus útmutatása szerint lehet csak folytatni a további munkát.

A rendszer sérülésének gyanúja esetén azonnal meg kell kezdeni a körülmények, az okozott kár és a felelősség kivizsgálását. Ez alól kivételt képez, ha az integritássérülésnek következményeképpen várható kár mértéke alacsony és az integritás helyreállítása az adott rendszer eszközeivel megfelelően naplózott módon megoldható.

10.1 Hibajavítás

A szervezet azonosítja, belső eljárásrendje alapján jelenti és kijavítja vagy kijavíttatja az elektronikus információs rendszer hibáit.

Telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket a Szervezet feladatellátásának hatékonysága, a szóba jöhető következmények szempontjából.

A szervezet a biztonságkritikus szoftvereket a frissítésük kiadását követő 90 napon belül telepíti vagy telepítteti, beépíti a hibajavítást a konfigurációkezelési folyamatba.

10.2 Kártékony kódok elleni védelem

A szervezet informatikai rendszereit védeni kell a kártékony kódok ellen. Ennek érdekében a következőket kell betartani:

- A határvédelmi programoknak a szervereken folyamatosan kell működniük. A programoknak folyamatosan vizsgálniuk kell a bejövő hálózati forgalmat (levelezés, web).
- A határvédelmi szoftverrendszer elemeinek (programok, szabályrendszerek, vírusdefiníciós adatbázisok) frissítéséről automatizált módszerrel gondoskodni kell. A frissítések hiba nélküli megtörténtét ellenőrizni kell.
- Hálózati munkaállomások az internethez kizárólag a szervezet internet kijáratán (központi tűzfalán) keresztül csatlakozhatnak.
- Vírusvédelem nélkül sem hálózati, sem önálló munkaállomás nem üzemeltethető.
- A vírusvédelemnek a klienseken, rezidens módon kell futniuk, azaz a rendszer indulásakor automatikusan indul a program, illetve folyamatosan vírusellenőrzést kell végrehajtani a klienseken, amely vizsgálatok eredményét ellenőrizni kell.
- A munkaállomásokon valós idejű ellenőrzést (azonnali riasztást) biztosító vírusvédelmet kell használni.
- A felhasználónak tilos vírusirtót, személyes tűzfalat, vagy egyéb biztonsági szoftvert telepítenie.
- Külső helyekről származó adattárolókat (Szervezeti okból történő) használat előtt vírusellenőrzésnek kell alávetni és csak akkor lehet használni, ha az adathordozó a vizsgálaton megfelel.
- Vírusfertőzés gyanúja vagy nem üzemszerű működés esetén a felhasználóknak haladéktalanul értesítenie kell az kijelölt informatikust, hogy a szakértők megvizsgálják az eseményt, és hiba esetén gondoskodjanak annak elhárításáról.
- Vírusfertőzés gyanúja esetén a szervezet informatikusai a fertőzött gépet lezárhatják, annak használatát a hiba elhárításáig felfüggeszthetik.

- Az a felhasználó, aki az adatait és adathordozóit a vírus ellenőrzés vagy vírusvédelmi intézkedés (vírusirtás) alól bármilyen indokkal kivonja, az abból eredő károkért teljes felelősséggel tartozik.
- A vírusfigyelmeztetésekkel (vírus hoax) foglalkozó felelősök (rendszergazdák), feladata, hogy figyelemmel kísérjék a legfrissebb vírusok megjelenésével kapcsolatos híreket.
- Vírusfigyelmeztetéssel kapcsolatos levelet csak a Rendszergazda küldhet.

10.2.1 Vírustámadás elleni védekezés

A kijelölt informatikus feladata, hogy a felhasználói munkaállomásokra, illetve a mobil gépekre telepített vírusvédelmi rendszerek karbantartásáról gondoskodjon, a felhasználóknak támogatást nyújtson, továbbá a vírusdefiníciós állományok és a keresőmotorok szükséges frissítéseiről gondoskodjon.

10.2.2 Vírusvédelmi szoftverek használata

A vírusvédelmi rendszerek kiválasztását a Rendszergazda javaslata alapján az IBF hagyja jóvá. A vírusvédelmi rendszer kiválasztásakor figyelembe kell venni a következő szempontokat:

- Nem megfelelő vírusvédelmi rendszer alkalmazásával a szervezet vírusvédelme nem lesz kielégítő.
- A nem megfelelő vírusvédelmi szoftver lassítja a műveleteket és túlzott erőforrás igényt támaszthat. A rendszerek lassulása növeli a sebezhetőséget is.
- A vírusvédelmi szoftverek vírusdefiníciós állomány állományainak frissítési gyakoriságát.

10.3 Kéretlen üzenetek elleni védelem

Az Egyetem kéretlen üzenetek - úgynevezett levélszemét - elleni védelmet valósít meg az elektronikus információs rendszer belépési és kilépési pontjain, a levélszemét észlelése és kiszűrése érdekében.

- Új verziók elérhetővé válásakor frissíti a levélszemét elleni védelmi mechanizmusokat, összhangban a konfigurációkezelési szabályzattal és eljárásrenddel.
- Az elektronikus információs rendszer automatikusan frissíti a levélszemét elleni védelmi mechanizmusokat azok újabb verzióival.

10.4 Az elektronikus információs rendszer felügyelete

Az Egyetem rendszereinek napi üzemeltetéséhez tartozik azok működésének felügyelete, a mentések elvégzése, illetve hiba esetén az eszközök javítását végzők bevonása.

Az Egyetem rendszereinek felügyelete az alkalmazások, az adatbázisok, a kiszolgálók és az alapszoftverek, az informatikai hálózat és a munkaállomások működésének folyamatos figyelemmel kísérését kívánja meg. Ennek érdekében:

- Rendszeresen el kell végezni azokat a tevékenységeket, amelyek alapján meg lehet győződni arról, hogy a felügyelt rendszer üzemszerűen működik.
- Az elektronikus információs rendszer riassza a Szervezet illetékes személyeit, csoportjait, amikor veszélyeztetés vagy lehetséges veszélyeztetés előre meghatározott jeleit észleli.

10.5 Biztonsági riasztások és tájékoztatások

Az Egyetem folyamatosan figyeli a Kormányzati Eseménykezelő Központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket és folyamatosan figyelemmel kíséri a Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező értesítéseket. Szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki, a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez. Az Információbiztonsági felelős kiemelt feladata,

hogy a jogszabályban meghatározott események bejelentési kötelezettségének eleget tegyen és kapcsolatot tartson az érintett, külön jogszabályban meghatározott szervekkel.

10.6 A kimeneti információ kezelése és megőrzése

Kimeneti információk az Egyetem által külső fél számára és belső használatra készített beszámolók, tájékoztatók, bizonylatok, nyilatkozatok, megrendelők, tranzakciók.

A kimeneti információk kezelésével és szétosztásával kapcsolatban a következők az előírások:

- Gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről.
- Gondoskodni kell arról, hogy a kimeneti információhoz történő fizikai és logikai hozzáférés csak az arra jogosított személyekre korlátozódjon.
- Gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat.
- Biztosítani kell, hogy a megsemmisítési eljárások során a kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.
- A rendszer kimenő információit (pl.: számla) a vonatkozó jogszabályok, szabályzatok szerint kell megőrizni.

10.7 Használatból történő kivonás

Szoftver használatból történő kivonására akkor kerül sor, ha az adott feladat végrehajtása szükségtelenné válik, vagy a végrehajtásra új eljárás került kifejlesztésre, vagy új program került beszerzésre.

A selejtezendő szoftver által kezelt adatokat át kell alakítani új eljárás szerinti formátumra vagy olvasható módon meg kell őrizni archívált tartalomként, de meghatározott ideig, általában egy hónapig a két eljárást párhuzamosan kell használni, hogy a folyamatos működés ne szenvedjen fennakadást. Ezt az időszakot követően a szoftvert selejtezni kell, ami azt jelenti, hogy az adott szoftvert a gépekből törölni kell, és az adathordozókat, ha már biztosan nem kellenek- meg kell semmisíteni, egyéb esetben az élesben használt szoftverektől elkülönítve kell tárolni azokat.

11 NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

Az Egyetemnek az általa üzemeltetett elektronikus információs rendszereiben automatikus naplót kell vezetnie az informatikai rendszer biztonsági szempontból lényeges tevékenységeiről. Olyan naplózási architektúrát kell kialakítani, amely azt biztosítja, hogy ahol technikailag lehetséges, a naplózás szerveroldalon és a lehető legkevesebb számú naplóállomány használatával történjen.

A naplóban személyes adatot tárolni nem lehet.

A naplózási követelményeknek való megfelelést a rendszereknek oly módon kell teljesíteni, hogy az új beszerzésű rendszerek tekintetében (vásárlás és használat esetén is!) a rendszernek képesnek kell lennie ezen elvárások teljesítésére. Azon rendszerek tekintetében, melyek a szabályozás első kiadásakor használatban vannak, a lehető leginkább meg kell felelniük ezen elvárásoknak. Az eltéréseket a használt rendszerek tekintetében dokumentálni szükséges. Megfelelő naplózási információk teljesülése nélkül biztonsági és adatvédelmi incidensek felderítése problémát okozhat.

A naplózási elvárások tekintetében a személyi számítógépeket nem tekintjük önálló rendszereknek ezért azok naplózásától eltekintünk.

11.1 Biztonsági események naplózása

A kivételes és a biztonságot fenyegető eseményeket eseménynaplóba kell bejegyezni, és azt a hozzáférés nyomon követhetősége érdekében meg kell őrizni. Az elszámoltathatóság és auditálhatóság biztosítása érdekében a regisztrálási és a naplózási rendszert (biztonsági napló) úgy kell kialakítani, hogy abból utólag megállapíthatók legyenek az informatikai rendszerben bekövetkezett fontosabb események, különös tekintettel azokra, amelyek a rendszer biztonságát érintik. Ezáltal ellenőrizni lehet a hozzáférések jogosultságát, meg lehet állapítani a felelősséget, valamint az illetéktelen hozzáférés megtörténtét vagy kísérletét.

11.1.1 Naplózandó események

A naplózási rendszernek alkalmasnak kell lennie mindegyik felhasználó által végzett művelet szelektív regisztrálására. A következő eseményeket (sikeres/sikertelen) feltétlenül naplózni kell:

- rendszerindítások, -leállítások;
- rendszeróra állítások;
- be- és kijelentkezési kísérletek (sikeres és sikertelen);
- az azonosítási és a hitelesítési mechanizmus használata;
- hozzáférési jog érvényesítése azonosítóval ellátott erőforráshoz;
- azonosítóval ellátott erőforrás létrehozása vagy törlése;
- felhatalmazott személy műveletei, amelyek a rendszer biztonságát érintik.
- Privilegizált funkciók használata;
- rendszerhibák és korrekciós intézkedések;
- programindítások és -leállások, leállítások;
- az adatállományok és kimeneti adatok kezelésének visszaigazolása.

Az elektronikus információs rendszernek lehetővé kell továbbá tennie, hogy a jogosult személyek vagy szerepkörök (csak privilegizált fiókkal) kiválasszák, mely naplózható események legyenek naplózva az egyes komponensekre, illetve alrendszerekre.

11.1.2 A napló adattartalma

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

- dátum;
- időpont;
- a felhasználó azonosítója;
- az erőforrás azonosítója, amelyre a művelet vonatkozik;
- a művelet eredményessége vagy sikertelensége.

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

- az olyan erőforráson kezdeményezett hozzáférési művelet esetén, amelynél a hozzáférési jogok ellenőrzése kötelező:
    - a hozzáférési kezdeményezés típusa;
- az olyan erőforrás létrehozása vagy törlése esetén, amelynél az ehhez fűződő jogok ellenőrzése kötelező:
    - a kezdeményezés típusa;

11.1.3 Alapvető naplózási követelmények

- Kerüljön naplózásra a biztonságot érintő összes tevékenység.
- A naplófájlok tartalmát megadott időintervallum alapján képernyőn és nyomtatón is meg lehessen jeleníteni.
- A naplóállományokat tilos megsemmisíteni, felülírni, módosítani, azokat archiválni kell.
- A naplóállományok kódoltak, ellenőrző összeggel ellátottak legyenek.
- A biztonsági naplók adatait rendszeresen, de legalább havonta egy alkalommal ellenőrizni és archiválni kell. A biztonsági napló értékelése során meg kell határozni, hogy mely eseményeket kell Jegyzőkönyvezni, melyek azok az események, amelyek szankciókat vonnak maguk után, és mik ezek a szankciók.
- A biztonsági eseménynapló (naplófájl) és a Jegyzőkönyvek adatait védeni kell az illetéktelen hozzáféréstől.
- A rendszerben a biztonsági eseménynapló fájlok auditálásához szükséges eszközöknek lehetővé kell tenniük egy vagy több felhasználó tevékenységének szelektív vizsgálatát.

A biztonsági naplót a létrehozástól folyamatosan karban kell tartani, valamint védeni kell az illetéktelen módosítástól és törléstől, ezért ember számára olvasható formában is el kell tárolni.

11.2 Automatikus naplózás

Az elektronikus információs rendszer automatikusan naplózza a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket, és értesíti ezekről a meghatározott személyeket vagy szerepköröket.

11.3 Naplózási információk védelme

Különös figyelmet kell fordítani a naplózó eszközök biztonságára, mert ha meghamisítják, hamis biztonságérzetet kelthetnek. Óvintézkedéseket kell alkalmazni azért, hogy a szervezet meg legyen védve az olyan illetéktelen változtatásoktól és üzemeltetési problémáktól, mint:

- naplózási rendszer, amelyet kiiktattak;
- üzenetfajták, amelyeket rögzítés után módosítottak;
- naplófájlok, amelyeket átszerkesztettek vagy töröltek;
- naplófájlok adathordozói, amelyek kimerültek és ennek következtében vagy nem lehet már velük az eseményekről feljegyzést készíteni, vagy önmagukat írják felül.

A biztonsági naplókat archiválni kell, mint a rendszerhasználat bizonyítékait, annak érdekében, hogy ezek az információk (bizonyítékok) későbbi vizsgálatokhoz is felhasználhatók legyenek.

A naplóinformációk védelme érdekében a következőket kell betartani:

- A naplóban rögzített információkat megváltoztatni, törölni tilos.
- A naplók tartalmának megváltoztatásának megakadályozása érekében lehetőség szerint kriptográfiai mechanizmusokat kell alkalmazni.
- A napló mentéseket, archív állományokat elkülönítetten, elzárva vagy hozzáférhetetlenül kell tartani. Ezen archív vagy másodlagos naplóállományokhoz csak az IBF férhet hozzá, azokba betekinteni csak engedélyével és részvételével lehet.

Az elektronikus információs rendszerekben naplófunkciók kezelésére csak a szervezet által meghatározott, privilegizált felhasználók lehetnek jogosultak. A biztonsági naplóinformációkhoz hozzáféréssel csak az IBF engedélyével jogosult felhasználók rendelkezhetnek.

11.4 Naplóinformációk figyelése, reagálás a napló információkra

Folyamatosan figyelemmel kell kísérni a naplóállományok bejegyzései alapján generált riasztásokat.

11.5 Rendszer órajel szinkronizáció

Az Egyetemen belül működő valamennyi érintett információ-feldolgozó rendszer órajelét szinkronizálni kell egy közösen megállapított pontos időforráshoz.

11.6 A naplóbejegyzések megőrzése

Az Egyetem a naplóbejegyzéseket meghatározott - a jogszabályi és az Egyetemen belüli információ megőrzési követelményeknek megfelelő - időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

11.6.1 Naplózás mentése

A naplók tárolását a következő szempontok figyelembevételével kell megoldani:

- A naplóadatoknak sértetlenül rendelkezésre kell állniuk az esetleges elévülési időn belül.
- Biztosítani kell, hogy az adatokban keletkezésük után változtatást már ne lehessen végrehajtani.
- Az információk bizalmasságára tekintettel, az adatok nem juthatnak illetéktelenek kezébe.

Az általános alkalmazás naplókat minimálisan 1 évig meg kell őrizni, kivéve, ha kapcsolódó jogszabály vagy belső szabályozó ennél többet kíván meg.

A biztonsági (security) naplóbejegyzéseket a biztonsági események utólagos kivizsgálásának biztosítása érdekében – amennyiben a jogszabályi követelmények másképp nem rendelkeznek – legalább a következő időtartamig meg kell őrizni:

- folyamatirányítási rendszerek esetén 3 év;
- szerver operációs rendszerek esetén 3 év;
- végponti operációs rendszerek esetén 1 év;
- biztonsági alkalmazások esetén 2 év;
- vagyonvédelmi rendszerek esetén 3 év;
- ügyviteli rendszerek esetén 2 év;
- IPS-es, IDS-ek esetén 2 év;
- hálózati eszközök esetén 2 év;
- minden egyéb rendszer esetén 2 év.

11.6.2 Naplóállomány külön mentése

Abban az esetben, ha a naplóállomány külön, az egyes adatbázisoktól elkülönítve kerül mentésre, az Üzemeltetési dokumentációkban vagy külön nyilvántartásban kell vezetni, hogy az egyes naplómentések, mely adattárolókon helyezkednek el.

11.6.3 Naplóállományok rendszeres mentéseinek felülvizsgálata

Gondoskodni kell a naplóállományok rendszeres mentéseinek felülvizsgálatáról is.

11.6.4 Biztonsági naplók archiválása

A biztonsági naplókat archiválni kell, mint a rendszerhasználat bizonyítékait, hogy ezek az információk (bizonyítékok) későbbi vizsgálatokhoz is felhasználhatóak legyenek. A biztonsági napló adatait

rendszeresen, de legalább havonta egy alkalommal kell archiválni. Az archiválási információkat az Üzemeltetési dokumentációkban vagy külön nyilvántartásban kell vezetni.

11.7 Hozzáférés a naplóállományokhoz

11.7.1 Naplóállományok írása

A naplóállományokhoz írási jogosultsággal az automatikus rendszerek férhetnek hozzá a naplóállományokból.

11.7.2 Naplóinformációk kiadása külső szervezetek számára

Külső fél részére hatósági, ellenőrzési, hibakeresési okokból a naplófájlokról – szükség esetén anonimizált – másolat adható ki, az IBF és a kancellár engedélyével.

11.8 Naplózás ellenőrzése

11.8.1 Naplózandó események, naplóban rögzítendő adatok körének felülvizsgálata

A naplózandó események és a naplóban rögzítendő adatok körének áttekintése része az IBSZ rendszeres felülvizsgálatának.

11.8.2 Kiegészítő információk

Szükség esetén az elektronikus információs rendszer a naplóbejegyzésekben további, az Egyetem által meghatározott kiegészítő, részletesebb információkat is rögzít.

11.8.3 Naplózási beállítások felülvizsgálata

Az elektronikus információs rendszerek esetén évente ellenőrizni kell, hogy az egyes rendszerek tényleges naplózási beállításai megfelelnek-e a nyilvántartott naplózási beállításoknak.

A naplózási beállítások ellenőrzésének eredményét írásba kell foglalni:

- az elvégzett ellenőrzés időpontja;
- az ellenőrzést elvégző munkatárs neve;
- az elvégzett ellenőrzés mely rendszerekre terjedt ki;
- az ellenőrzés megállapításai;
- javaslat a felmerült problémák kezelésére.

Abban az esetben, ha a rendszerben a tényleges naplózás beállítása eltér az adott rendszer nyilvántartott naplózási beállításától ezt haladéktalanul jelenteni kell az Információbiztonsági felelősnek.

11.8.4 A naplózás vizsgálata

A naplózást és a naplók folyamatos figyelemmel kísérésének megvalósulását rendszeresen ellenőrizni kell. A naplózás ellenőrzését írásba kell foglalni, amelynek tartalmaznia kell a következő adatokat:

- az elvégzett ellenőrzés időpontja;
- az ellenőrzést elvégző munkatárs neve;
- az elvégzett ellenőrzés mely rendszerekre terjedt ki;
- az elvégzett ellenőrzés tárgya;
- az ellenőrzés megállapításai;
- javaslat a felmerült problémák kezelésére.

Naplózási hiba bekövetkeztekor, vagy ennek alapos gyanúja esetén automatikusan információbiztonsági eseménykezelési eljárást kell indítani a szervezet informatikai biztonsági eseménykezelési eljárásrendjében foglaltak szerint.

Abban az esetben, ha megállapítást nyer, hogy a naplók figyelése, illetve a naplók riasztásaira alapuló reagálások nem megfelelőek, haladéktalanul jelenteni kell az Információbiztonsági felelősnek.

11.8.5 Naplózási hiba kezelése

Az elektronikus információs rendszernek naplózási hiba esetén riasztást kell küldenie a felügyeletre kijelölt személyeknek vagy szerepköröknek és a rendszer kialakításától és a hibák ismétlődésétől, jellegétől függően elvégzi a rendszer leállítását vagy az automatikus hibajavítást. Az elektronikus információs rendszer naplózás nélkül nem hajthat végre olyan műveleteket, amelyek naplózása elő van írva.

11.8.6 Napló tárkapacitás figyelése

Az Egyetem a naplózásra elegendő méretű tárkapacitást biztosít, folyamatosan figyelemmel kíséri, hogy a naplóállományok számára rendelkezésre áll-e a szükséges tárkapacitás. Abban az esetben, ha a teljes kapacitás 10%-a alá csökken a rendelkezésre álló tárkapacitás, haladéktalanul gondoskodni kell a megfelelő tárkapacitás rendelkezésre állásáról.

11.9 Időbélyegek

Az Egyetem elektronikus információs rendszereinek belső rendszerórákat kell használniuk a naplóbejegyzések időbélyegeinek előállításához. Az időbélyegeket a naplóbejegyzésekben a koordinált világidőhöz (UTC), vagy a Greenwichi középidőhöz (GMT) rendelhető módon kell rögzíteni.

11.9.1 Szinkronizálás

Az elektronikus információs rendszer meghatározott gyakorisággal összehasonlítja a belső rendszerórákat egy hiteles külső időforrással, és ha időeltérés van, szinkronizálja a belső rendszerórákat a hiteles külső időforrással.

12 RENDSZER ÉS KOMMUNIKÁCIÓVÉDELEM

12.1 A határok védelme

Az elektronikus információs rendszer felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt:

- a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól;
- csak az Egyetem biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez;
- az Egyetem korlátozza az elektronikus információs rendszer külső hálózati kapcsolatainak a számát a működéshez szükséges minimumra;
- az elektronikus információs rendszer a felügyelt kapcsolódási pontjain tilt, és csak kivételként engedélyez hálózati forgalmat;
- véd a túlterheléses (úgynevezett szolgáltatás megtagadás) jellegű támadásokkal szemben, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján, a meghatározott biztonsági intézkedések bevezetésével.

12.2 A hálózati szintű hozzáférések menedzsmentje

Az Egyetem informatikai rendszerének elemeit adminisztrációs célból az internet felől elérni csak titkosított kapcsolaton keresztül (VPN), legalább kétfaktoros authentikáció után megengedett.

VPN hozzáférést technikai funkciók ellátásához (például beléptető rendszer), illetve az informatikai dolgozók munkájának ellátásához a Rendszergazda biztosít, felhasználók számára VPN hozzáférést szervezeti igénylés alapján a Rendszergazda ad.

Minden adminisztrációs tevékenységnek egyértelműen személyhez köthetőnek kell lennie, ezért minden felhasználónév konkrét felhasználóhoz kötött.

12.2.1 Kötelező elérési útvonal

Külső hálózatról az informatikai rendszerek csak az erre a célra dedikált védelmi rendszeren (tűzfal, zónák VPN koncentrátor stb.) keresztül lehetnek elérhetőek.

12.2.2 Hálózati részek elválasztása

Az internet és az Egyetem rendszerei között határvédelmi eszköz biztosítja az elválasztást.

12.3 Együttműködésen alapuló számítástechnikai eszközök

Az elektronikus információs rendszereket úgy kell kialakítani, hogy gátolják meg az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha az érintett szervezet engedélyezte azt, és közvetlen kijelzést nyújtsanak a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

12.4 Kriptográfiai eszközök

12.4.1 Digitális aláírás

A digitális aláírások ahhoz szolgáltatnak eszközt, hogy megvédhessük az elektronikus okmányok (dokumentumok) hitelességét (authenticity) és sértetlenségét (integrity). A digitális aláírások akármilyen okmányformára alkalmazhatók, hiszen ezek mind elektronikusan lesznek feldolgozva. Különös gondot kell fordítani a magánkulcs titokban tartására, ezt a védelmet a nyilvánoskulcs-tanúsítványok alkalmazásával kell ellátni.

12.4.2 Nyilvános kulcsú infrastruktúra tanúsítványok

Az Egyetem nyilvános kulcsú tanúsítványokat csak úgy állít ki, amennyiben készül belső hitelesítési rend, és a kiadási folyamat ennek megfelel.

Piaci szolgáltatótól nyilvános kulcsú tanúsítványokat csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatóktól lehet beszerezni.

12.4.3 Kriptográfiai védelem

Az elektronikus információs rendszer csak szabványos, a Nemzeti Média- és Hírközlési Hatóság által biztonságosnak minősített kriptográfiai műveleteket valósíthat meg.

12.4.4 Kriptográfiai vagy egyéb védelem

Az elektronikus információs rendszer amennyiben adatátvitelt valósít meg, kriptográfiai mechanizmusokat kell, hogy alkalmazzon az adatátvitel során az információk megváltozásának észlelésére, ha az átvitel nincsen más alternatív fizikai intézkedésekkel védve.

12.5 Folyamatok és maradványinformációk védelme

Az elektronikus információs rendszertől elvárt, hogy az:

- elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az elektronikus információs rendszer irányítási funkcionalitásától;
- meggátolja a megosztott rendszererőforrások útján történő jogosulatlan vagy véletlen információáramlást;
- elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára, ahol erre a feldolgozás jellegéből adódóan szükség van;
- biztosítja, hogy az alrendszerei védjék a keletkezett maradvány információkat, azok bizalmasságát és sértetlenségét.

13 AZ IBSZ-HEZ TARTOZÓ, ILLETVE AZT KIEGÉSZÍTŐ DOKUMENTUMOK JEGYZÉKE

13.1 Szabályzatok

- A biztonsági események és incidensek kezelésének szabályait az Incidenskezelési szabályzat tartalmazza.
- Az eszközök visszaadásához, a jogosultságok visszavonásához kapcsolódó részletes szabályozást az informatikai rendszerekhez és eszközökhöz való hozzáférés, kiadás és visszavétel tekintetében a Hozzáférésvédelmi szabályzat tartalmazza.

14 ZÁRÓ RENDELKEZÉSEK

1. Jelen Szabályzat annak aláírását követő napon lép hatályba.
2. Jelen Szabályzat hatálybalépésével a 2009. december 1. napjától hatályos az Adatvédelmi és Informatikai Szabályzata hatályát veszti.
3. Jelen Szabályzatot a Kancellári Kabinet gondozza.
4. A Jelen Szabályzat megtalálható és elérhető a www.szfe.hu oldalon.

Budapest, 2021. szeptember 16.

Novák Emil
mb. általános rektorhelyettes

PH

dr. Szarka Gábor
kancellár