SZÍNHÁZ- ÉS FILMMŰVÉSZETI EGYETEM

SZFE 1865

3/2024. (05.06.) számú rektori szabályzat

A Színház-és Filmművészeti Egyetem Információbiztonsági Szabályzata

Hatályos: 2024. május 07. napjától

1. §
A szabályozás célja

(1) A jelen Információbiztonsági Szabályzat (a továbbiakban: 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 és egyetemi szabályzatoknak 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.

(2) A Szabályzat általános célja, hogy az Egyetem 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.

2. §
A szabályzat hatálya

(1) A Szabályzat hatálya kiterjed az Egyetem valamennyi szervezeti egységére, vele jogviszonyban álló személyre, akik feladataik teljesítése során vagy egyéb céllal, jogosultsággal, vagy annak hiányában felhatalmazással, a Szabályzat 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.

(2) A felhasználókkal kötendő valamennyi jogviszony vonatkozásában a jogviszonyra vonatkozó szerződésben rögzített hivatkozás mellett biztosítani kell a Szabályzat rendelkezéseinek érvényesülését. Az Egyetem informatikai rendszereihez és adatállományához olyan személy nem kaphat hozzáférést, aki az Egyetemmel, vagy a fenntartó Alapítvánnyal nincs munkaviszonyban, vagy munkavégzésre irányuló egyéb jogviszonyban.

(3) A Szabályzat személyi hatálya kiterjed az Egyetem által foglalkoztatott valamennyi munkavállalóra, illetve munkavégzés céljából egyéb jogviszonyban álló jogi és természetes személyre, és az Egyetemmel hallgatói jogviszonyban álló személyekre.

(4) A Szabályzat tárgyi hatálya kiterjed:
- a) az Egyetemen üzemelő számítógépes rendszer teljes konfigurációjára, az ahhoz tartozó rendszer- és felhasználói szoftverekre, valamint ezek dokumentációira;
- b) a papír alapon rögzített, tárolt, használt vagy továbbított adatokra;
- c) a számítógépes feldolgozásra szánt, feldolgozás alatt álló, és a feldolgozás után számítógépes adathordozókon tárolt, a feldolgozás eredményeként létrejött adatra;
- d) a számítástechnikai eszközök alkalmazásának teljes folyamatára, tevékenységeire;
- e) a számítástechnikai infrastruktúra elhelyezésére szolgáló helyiségekre.

3. §
A Szabályzat létrehozása, felülvizsgálata és módosítása

(1) A Szabályzat létrehozása, felülvizsgálata és szükség szerinti módosítása az információbiztonsági felelős feladata és felelőssége, együttműködve az Egyetem informatikai szakterületért felelős munkatársaival. A Szabályzat létrehozásában, felülvizsgálatában és módosításában közreműködnek az elektronikus információbiztonsági feladatok ellátásában közreműködő személyek, szervezeti egységek, valamint a rendszer üzemeltetéséért, fejlesztéséért felelős szervezeti egységek vezetői.

(2) 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.

(3) A Szabályzatot az időszakos felülvizsgálaton túl felül kell vizsgálni és szükség esetén módosítani kell:
   a) a Szabályzatban hivatkozott szervezetek vagy munkakörök változása esetén;
   b) súlyos információbiztonsági események bekövetkezése esetén;
   c) az információs vagy informatikai biztonság szabályozását érintő jogszabályváltozások esetén;
   d) 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.

(4) A Szabályzat betartásának ellenőrzése az információbiztonsági felelős feladata, melyben közreműködnek az információbiztonsági feladatok ellátásában közreműködő személyek, szervezeti egységek, valamint a rendszer üzemeltetéséért, fejlesztéséért felelős szervezeti egységek vezetői.

(5) 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 szükséges dokumentálni. A kivételek engedélyezése tekintetében a gazdasági főigazgató jogosult dönteni. Új, bevezetés alatt álló rendszer esetén a szabályzati követelmények teljesülésére vonatkozó kivétel nem alkalmazható.

4. §
Informatikai erőforrásokhoz való hozzáférés igénylése munkaerő felvételénél

(1) Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed az Egyetem teljes személyi állományára, valamint minden olyan az Egyetemmel egyéb jogviszonyban álló 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 áll az Egyetemmel jogviszonyban, 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).

(2) A Humán Erőforrás Iroda az új munkavállaló 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.

(3) A beérkezett igényekre a rendszergazda haladéktalanul köteles visszajelezni, és a szükséges technikai eszközöket kapacitás függvényében biztosítani.

(4) A kapcsolódó részletes szabályozást az informatikai rendszerekhez és eszközökhöz való hozzáférés, kiadás és visszavétel tekintetében az Egyetem hatályos Hozzáférésvédelmi Szabályzata tartalmazza.

5. §
Adatvagyon kezelése, hozzáférése

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

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

(3) 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.

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

6. §
Az informatikai biztonsági oktatás és képzés

(1) Az Egyetem valamennyi munkavállalója – feladatának és jogkörének figyelembevételével – megfelelő képzésben részesül az Egyetem biztonsági szabályairól és eljárásairól. Ezeket az ismereteket évente naprakész ismeretek közlésével fel kell újítani. A képzés magában foglalja:
   a) a biztonsági követelményeket;
   b) a jogi felelősséget;
   c) a szervezet óvintézkedéseit;
   d) az informatikai eszközök helyes használatát, például a bejelentkezési eljárást, a szoftverek használatát;
   e) biztonsági incidensek kezelésének folyamatát;
   f) adatvédelmi ismereteket;
   g) általános biztonság tudatossági ismereteket.

(2) Az általános tájékoztatás keretében az új belépők számára a Humán Erőforrás Iroda levélben küldi ki az oktatási anyagot. Különleges esetekben amennyiben a szabályok jelentősen megváltoznak, vagy jelentős biztonsági incidens esetén, ad-hoc jellegű képzés is tartható.
(3) 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 gazdasági főigazgató dönthet.

(4) Különleges biztonsági képzést a gazdasági főigazgató engedélyével elsődlegesen a következő szerepeket betöltő alkalmazottak kaphatnak:
   a) az informatikai rendszerek tervezésében és fejlesztésében kulcsszerepet betöltő munkavállaló,
   b) informatikai rendszerek üzemeltetésében kulcsszerepet betöltő munkavállaló.

(5) A lefolytatott képzéseken készült aláírt jelenléti íveket és a kapcsolódó tematikát 3 évig meg kell őrizni a Humán Erőforrás Irodán.

(6) Az Egyetem felhasználói által használt, de nem az Egyetem 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.

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

7. §
Az Egyetem által biztosított informatikai eszközök

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

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

(3) Az Egyetem által biztosított eszközökön kizárólag jogtiszta szoftverek és dokumentációk használhatók, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak.

8. §
Magántulajdonú informatikai eszközök használata a feladatok ellátásához

(1) Az egyetemi működéshez kapcsolódó feladatok ellátásához magántulajdonú eszközök is használhatók, melyek segítségével távolról érhetők el a rendszerek. Ezen eszközök tekintetében a következő elvárásokat kell betartani:
   a) a kapcsolódó eszközt védeni kell illetéktelen hozzáféréstől, azt úgy kell használni, hogy az Egyetem adataihoz jogosultsággal nem rendelkező személy az eszközhöz ne férhessen hozzá;
   b) a kapcsolódás során meg kell győződni arról, hogy a kapcsolat biztonságos és védett, nyilvános wifi hálózat a kapcsolódáshoz nem javasolt;

c) a kapcsolódó eszköz biztonsági funkciói tekintetében elvárás:
   ca) a bejelentkezést megfelelő komplex jelszóval védeni (lásd jelszó követelmények Felhasználói kézikönyv);
   cb) az eszközön automatikusan frissülő vírusírtó használata;
   cc) az eszköz zárolása amennyiben a felhasználó eltávolodik tőle.

(2) Magántulajdonú eszközön egyetemi adat 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.

9. §
Mobil informatikai tevékenység, távmunka

(1) 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. A 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 a felhasználónak gondoskodni kell a rejtjelezett adattárolásról és adatátvitelről. Távmunka (távoli hozzáférés) esetén az Egyetem érintett szervezeti egységeinek gondoskodniuk kell a biztonságos adatkapcsolat létrehozásáról, a kapcsolatot tartó hely és eszköz védelméről.

(2) A mobil eszközök (pl.: laptopok, notebook-ok, otthoni munkaállomások, tabletek, mobil telefonok) használóinak mind a fizikai biztonság, mind a logikai védelem területén a jelen Szabályzatban foglaltakat kell figyelembe venniük. A távmunka során is be kell tartani az Egyetem szabályzataiban foglaltakat:
   a) A mobil eszközök nem hagyhatók felügyelet nélkül, amennyiben nem biztosítható azok előírt védelme.
   b) A kommunikációhoz védett csatornáról kell gondoskodni, nyilvános publikus hálózatok használata nem javasolt.
   c) Vírus- és behatolás védelmi eszközöknek működniük kell a mobil eszközön.
   d) A mobil eszközökön tárolt adatok bizalmasságának védelmére fokozott figyelmet kell fordítani.
   e) A mobil számítástechnikai berendezéseket nyilvános helyeken használóknak ügyelni kell arra, hogy elkerüljék a jogosulatlan személyek általi betekintés kockázatát.
   f) 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.
   g) A hordozható informatikai eszközök jogos birtokosa felelős az eszköz teljes biztonságáért és annak ellenőrzéséért.
   h) A rendszer csak limitált visszacsatolási információt szolgáltathat a felhasználónak a hitelesítési eljárás alatt, így megakadályozza a felhasználót abban, hogy ismereteket szerezzen a hitelesítési folyamatról.
   i) Az interaktív kapcsolatok zárolása: a felhasználó 15 perces 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.

j) Távmunka végzése technológiai szempontból a laptoppal rendelkező munkavállalók számára engedélyezett, ugyanakkor az Egyetem szabályainak megfelelően a távoli munkavégzést vezetővel kell engedélyeztetni.
k) Távmunka esetén is gondoskodni kell a helyszínen a biztonsági követelmények és előírások betartásáról, a megfelelő és rendszeres ellenőrzésről.
l) A távmunkát végző munkavállaló csak a kijelölt csatlakozási pontokon keresztül csatlakozhat az Egyetem hálózatához.
m) A rendszergazda határozza meg a belépési pontokat, azzal, hogy azok jóváhagyásáról a gazdasági főigazgató dönt.

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

(4) Az Egyetemen a munkavállalói és hallgatói e-mail címeket a következő konvenció szerint kell képezni:
vezetéknév.keresztnév@szfe.hu
vezetéknév.keresztnév@hallgato.szfe.hu

(5) Névegyezés esetén szükséges egyéb azonosító integrálása a levelezési címbe, azonos emailcím nem használható akkor sem amennyiben az azonos nevű személyek nem azonos időben tartoznak a szervezethez.

(6) 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.

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

a) A levelek nem képviselhetnek a hatályos magyar jogba ütköző magatartásformát (pl.: tiltott tartalmak – pornográfia, szerzői jogok megsértése. stb.).
b) 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).
c) Tilos a felhasználóknak a szervezeti e-mailcímüket nem feladatuk ellátásához köthetően használni (pl.: regisztráció letöltési weboldalak, online játék oldalak stb.).
d) Levelet küldeni csak a levél tartalmában érintett személy(ek) részére szabad.
e) Tilos a levelek fejlécének megváltoztatása, hamis levelek küldése.
f) 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.
g) Informatikai biztonsági vizsgálat, auditálás, illetve hibakeresés céljából az Egyetem informatikai rendszereinek teljes hálózati forgalma megfigyelhető és rögzíthető. A felhasználó

a Szabályzatismeretéről 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:

ga) kéretlen levelek;

gb) vírusokat tartalmazó levelek;

gc) informatikai támadásokat megvalósító üzenetek;

gd) adathalászatot megkísérlő üzenetek.

10. §
Viselkedési szabályok az interneten

(1) Az Egyetem internet használati jogokkal rendelkező felhasználói a munkájukkal kapcsolatban korlátlanul használhatják az Egyetem által biztosított internet szolgáltatást.

(2) A felhasználók a szervezet nevében csak a gazdasági főigazgató előzetes engedélyével tölthetnek fel internetre adatokat, anyagokat.

(3) Az Egyetem tulajdonát képező adatbázisok tartalmának interneten keresztül történő hozzáférésének lehetővé tétele megfelelő jogosultságigénylés mellett a Campus Igazgatóság feladata. Az engedély megadása ilyen esetben vonatkozhat egyedi esetre vagy egyes rendszerekkel kapcsolatos feladatok elvégzésére az arra felhatalmazott munkavállalók részére.

(4) Az internet magán célú használata tiltott, az alábbi szabályokat kell betartani:
   a) tilos a pornográf, online játék, fogadási oldalak, csevegő oldalak, letöltő oldalak és törvénybe ütköző tartalmakat szolgáltató oldalak látogatása.
   b) Az internetről magán céllal tilos fájlokat letölteni.
   c) 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.

11. §
A felhasználó feladatai a munkahely elhagyásakor

(1) 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.

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

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

(4) A munkavállaló mindig csak a munkával kapcsolatos dokumentumokat 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.

(5) 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.

(6) A munkavégzés során keletkező jegyzeteket, vázlatokat, illetve példányokat a hatályos iratkezelési szabályok figyelembevételével meg kell semmisíteni amennyiben már nincs szükség rájuk.

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

12. §
A vezetők felelőssége

1) A vezetők felelőssége, hogy megkövetelje a munkavállalóktól és az egyéb, munkavégzésre irányuló jogviszonyban állóktól, hogy a biztonsági intézkedéseket a meghatározott szervezeti szabályzatokkal és eljárásokkal összhangban alkalmazzák. A vezetőknek biztosítaniuk kell, hogy a munkavállalók és az egyéb jogviszonyban állók:
   a) 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;
   b) vegyenek részt információbiztonsági oktatásokban;
   c) alkalmazkodjanak a foglalkoztatás feltételeihez, tartsák be az ide vonatkozó biztonsági szabályzatokat, a biztonságot érintő kérdésekben megfelelő, naprakész jártasságuk legyen.

13. §
Személyi biztonság a jogviszony megszűnésekor, megszüntetésekor vagy módosítása esetén

(1) 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 munkavállaló vagy egyéb, munkavégzésre irányuló jogviszonyban álló személy esetében a jogosultságok megvonása az adatfeldolgozó eszközök visszaadása esetenként mérlegelendő.

(2) Kilépő munkavállaló esetén a levelezés automatikusan átirányításra kerülhet az Egyetem egy másik email-címére, melyet a kilépő munkavállaló szervezeti egységének vezetője meghatároz. Az automatikus továbbítás csak az Egyetem egy másik belső email-címére történhet, külsős email-címre nem, és maximális ideje 3 hónap. 3 hónap után a levelezés tartalmát törölni / archiválni kell.

(3) Az eszközök visszaadásához, a jogosultságok visszavonásához kapcsolódó részletes szabályozást az informatikai rendszerekhez és eszközökhöz való hozzáférés, kiadás és visszavétel tekintetében az Egyetem hatályos Hozzáférésvédelmi Szabályzata tartalmazza.

(4) A jogviszony megszűnése, megszüntetésekor az Egyetem szempontjából biztonsági alapkövetelmény, hogy a munkavállalók vagy egyéb, munkavégzésre irányuló jogviszonyban álló személyek szabályozott módon hagyják el a szervezetet.

(5) A jogviszony megszűnése után a felhasználóknak titoktartási nyilatkozatot szükséges aláírniuk az Egyetem adatainak és információinak megfelelő biztonsága érdekében.

(6) Az elektronikus információs rendszerek felhasználói fiókjait, email címeit évente legalább egyszer ellenőrizni szükséges. Az ellenőrzést a Campus Igazgatóság támogatásával a Humán Erőforrás Iroda végzi. Az inaktív, szükségtelen felhasználói fiókokat ezen felülvizsgálatok után meg kell szüntetni.

(7) Azokkal szemben, akik az Egyetem hatályos informatikai biztonsági szabályait és eljárásait vétkesen megszegik fegyelmi eljárást kell kezdeményezni és lefolytatni. A fegyelmi, felelősségi, kártérítési eljárást a Munka Törvénykönyv, vagy a Polgári Törvénykönyvről szóló 2013. évi V. törvény rendelkezései alapján szükséges lefolytatni.

14. §
Külső szervezetre vonatkozó követelmények

(1) Az Egyetem a külső szervezettel kötött megállapodásban, szerződésben megköveteli, hogy:
   a) a külső szervezet határozza meg az Egyetemmel kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat;
   b) a szerződő fél feleljen meg az Egyetem által meghatározott személybiztonsági követelményeknek;
   c) a szerződő fél a szervezetet érintő biztonsági auditokban közreműködjön;
   d) 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.

(2) A rendszergazda folyamatosan, de legalább évente egyszer ellenőrzi a szerződő felek személybiztonsági követelményeknek való megfelelését, és az ezzel kapcsolatos jelentését megküldi a gazdasági főigazgatónak.

15. §
Adathordozók védelme

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

(2) Az adathordozók kezelésének legfontosabb biztonsági követelményei:
   a) Gondoskodni kell az adathordozók ellenőrzéséről és fizikai védelméről.
   b) Meg kell védeni a dokumentumokat, a számítástechnikai adathordozókat, az input/output adatokat és a rendszerdokumentációkat a károsodástól, eltulajdonítástól, jogosulatlan megismeréstől.
   c) 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.
   d) Az adathordozókat úgy kell védeni fizikai és környezeti behatásoktól, hogy biztosítani lehessen az adatok sértetlen és hiteles állapotának megőrzését.
   e) Minden adathordozót biztonságos környezetben, a gyártó előírásainak megfelelően kell tárolni.
   f) Az Egyetem elektronikus információs rendszerében minden felhasználó jogosult adathordozók használatára a kapcsolódó – egyes esetekben adathordozó specifikus (pl.: mobiltelefon, mentési adattároló) – szabályozások alkalmazása mellett.

16. §
Üzletmenet folytonossága

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

17. §
Alapfeladatok ellátását támogató rendszerek

(1) Jelenleg az Egyetem működésének folytonosságát figyelembe véve a következő rendszerek folyamatos működése elvárt és biztosított:
   a) Microsoft Cloud (M365)
   b) Neptun
   c) Poseidon
   d) sERPa
   e) Nexon
   f) Kulissza.

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

18. §
A folyamatos működésre felkészítő képzés

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

a) felhasználóknak: mentések, adatkezelés
b) informatikusoknak: technológiák és üzemeltetés.

19. §
Az elektronikus információs rendszer mentései

(1) 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.

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

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

(3) Az automatikus mentés kiterjed a következő mappákra:

a) Dokumentumok,
b) Képek,
c) Asztal.

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

(5) 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.

(6) 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.

20. §
Mentési eszközök

(1) 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.

(2) 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.

(3) 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.

21. §
A mentett adatok tárolása

(1) 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.

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

(3) 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.

(4) A mentési adathordozók tartalmát legkésőbb 3 év után törölni szükséges.

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

a) munkavállaló távozása után azon fájlokat melyek a felhasználó saját személyes mappáiban kerültek tárolásra, azaz nem közös használatú fájlok,

b) legkésőbb 3 hónappal a munkavállaló távozása után törölni kell.

22. §
Mentési feladatok

(1) A mentési tevékenységgel megbízott felelőst a rendszergazda jelöli ki. A mentésért felelős személy feladata a rendszergazda által meghatározott mentési és helyreállítási elvárásoknak megfelelően:

a) mentési job-ok beállítása (honnan - hova és mit mentsen a szervezet előírásainak megfelelően);

b) mentések elvégzése;

c) mentési média ellenőrzése és rendelkezésre állás biztosítása;

d) mentés folyamatának ellenőrzése;

e) mentés eredményének ellenőrzése évenkénti visszatöltési tesztek segítségével, melyek eredményéről a rendszergazdát és a gazdasági főigazgatót értesíteni szükséges.

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

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

a) a mentés tartalmát;

b) a mentés időpontját;

c) mentés jellegét (teljes mentés, inkrementális kumulatív, inkrementális, differenciált stb.);

d) a mentés eredményét (sikeres / sikertelen, hiba oka).

(4) 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 vezető utasításának megfelelő ideig őrizni. Ha az előírt mentéseket valamely okból nem lehet megvalósítani, már meglévő korábbi mentéseket csak a rendszergazda engedélyével szabad törölni.

23. §
Biztonsági események, incidensek kezelése

(1) 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.

(2) 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.

(3) Informatikai biztonsági incidens előfordulása esetén az abban érintett munkavállalóknak 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.

(4) 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.

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

(6) Az eseménykezelési tevékenységekből levont tanulságokat be kell építeni az eseménykezelési, üzemeltetési eljárásokba, elvárásokba, továbbképzésekbe.

24. §
Incidenskezelés folyamata

(1) Az incidensek bejelentésének folyamatát az Egyetem hatályos Incidenskezelési Szabályzata írja elő.

(2) A bejelentés fogadása után, ha a rendszergazda önálló hatáskörben nem tudja kezelni a felmerült problémát értesíti az illetékes személyt.

(3) 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 személy felkeresi a kezdeményező felet, és a helyszínen hárítja el a hibát az információbiztonsági felelős 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 kijelölt személy az eszközt dokumentáltan átveszi, és a be- és kiszállításra vonatkozó előírások fokozott figyelembevétele mellett elszállítja hibaelhárításra.

(4) 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 teljes rálátása és irányítási lehetősége van. Olyan elektronikus információs rendszerek esetén, amelyek személyes adatokhoz férnek hozzá, ezek védelmére fokozott figyelmet kell fordítani.

(5) 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.

(6) Az incidensek priorizálása a rendszergazda feladata, ezen irányú képzés biztosításáért a gazdasági főigazgató felel.

25. §
Incidenskezelés prioritások

(1) 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:

a) határsértés és illegális tevékenység észlelése (behatolás),

b) vírus-vészhelyzet (tömeges fertőzés), vagy központi vírusvédelmi eszköz kiesése,

c) adminisztrátori jogosultságok sérülése,

d) folyamatos működéshez szükséges rendszer, vagy rendszer elemek teljes kiesése,

e) informatikával összefüggésbe hozható bűncselekmények,

f) jogszabályi előírások megsértése.

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:

a) ismétlődő vírusfertőzés, vagy vírusdefiníciós állomány nem frissülése,

b) 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:

a) egyszeri vírusfertőzés, vagy helyi vírusvédelmi eszköz kiesése,

b) 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:

a) vírusvédelmi menedzsment eszközök kiesése,

b) felügyeleti és menedzsment eszközök kiesése,

c) munkaállomás működésével kapcsolatos működési hibák,

d) belső szabály- és eljárássértések,

e) felhasználói hibák.

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

26. §
Incidenskezelés folyamata

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

(2) 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.

(3) 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 a gazdasági főigazgató a rendszergazda véleményének ismeretében hozza meg.

(4) 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.

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

a) szerepkörbe vagy felelősségbe kerülésüket követő 30 munkanapon belül;

b) a képzéseket évente el kell végezni az elektronikus információs rendszer mindenkori állapotának megfelelően, vagy amikor az elektronikus információs rendszer változásai megkívánja.

(6) 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.

27. §
Karbantartás

(1) 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 a campus igazgató a felelős, aki:

a) a karbantartások ütemezését és módját meghatározza;

b) írásban engedélyezi azon tervezett karbantartásokat, melyek szolgáltatáskieséssel járnak, a szolgáltatáskieséssel nem járó karbantartások engedélyezése nem elvárt;

c) kihirdeti a kieső szolgáltatás miatt érintett felhasználók számára a karbantartások várható időpontjait.

(2) A karbantartás során:

a) Az eszközöket csak a rendszergazda jóváhagyását követően lehet leállítani;

b) az elvégzett munkákat jegyzőkönyvezni kell, a jegyzőkönyveket pedig 3 évig meg kell őrizni oly módon, hogy a karbantartások e nyilvántartásból visszakövethetők legyenek;

c) 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.

(3) 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.

(4) Távoli karbantartás végzését vagy szerződéses alapon szerződött partner, vagy az Egyetem informatikusa végzi, egyéb esetben a távoli karbantartást a gazdasági főigazgató 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.

(5) 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 nyilvántartást kell vezetni – a fizikai belépések nyilvántartásának megfelelő folyamat szerint - melynek minimálisan a következőket tartalmaznia:

a) karbantartó neve,

b) cég megnevezése,

c) szerződéses partner megnevezése,

d) belépés dátuma, ideje,

e) távozás dátuma, ideje.

(6) 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.

28. §
Konfigurációkezelés

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

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

(3) 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.

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

29. §
Sérülékenység vizsgálata

(1) 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:
   a) legalább három évente, vagy véletlenszerűen, valamint olyan esetben, amikor új lehetséges sérülékenység merül fel az elektronikus információs rendszerrel vagy alkalmazásaival kapcsolatban, megismétli a sérülékenység tesztet;
   b) 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;
   c) olyan sérülékenységi teszteszközt kell alkalmazni, melynek sérülékenység feltáró képessége könnyen bővíthető az ismertté váló sérülékenységekkel;
   d) a sérülékenységi teszteszközt minden vizsgálat előtt frissíteni is kell ezen új sérülékenységekkel.

(2) Az elektronikus információs rendszerek különleges jogosultsághoz kötött - úgynevezett privilegizált - hozzáférést biztosít a Szervezet az általa kijelölt rendszerelemekhez a sérülékenység teszt végrehajtásához.

(3) Az elvégzett teszt eredménye alapján a szervezet vagy a vizsgálatot végző vállalkozó:
   a) kimutatást készít a feltárt hibákról, valamint a nem megfelelő konfigurációs beállításokról;
   b) felméri a sérülékenység lehetséges hatásait;
   c) elemzi a sérülékenység teszt eredményét;
   d) megosztja a sérülékenység teszt eredményét a rendszergazdával és a gazdasági főigazgatóval, aki dönt a további érintettekről;
   e) a feltárt sérülékenységeket a lehető leghamarabb javítja, vagy azok lehetséges hatását más eszközökkel csökkenti.

(4) 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.

30. §
Rendszer és szolgáltatás beszerzés eljárásrendje

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

(2) Az Egyetem informatikai rendszeréhez csak olyan eszköz és informatikai rendszer csatlakoztatható, mely:

a) megfelel a szervezet által elvárt funkcionális, biztonsági és dokumentációs követelményeknek, és melyet a

b) melyet a rendszergazda adott ki;

c) idegen eszközök esetében olyan eszköz, mely megfelel a szervezet információbiztonsági szabályainak, melyek biztonságáért (illetve a kapcsolódó adatvédelmi szabályok betartásáért) az eszközt csatlakoztató felhasználó felel.

(3) 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 a gazdasági főigazgató dönt arról, hogy ezek megfelelnek-e a szervezet általános védelmi intézkedéseinek.

(4) 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.

(5) 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:

a) funkcionális biztonsági követelményeket;

b) a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint);

c) a biztonsággal kapcsolatos dokumentációs követelményeket;

d) a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;

e) az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat;

f) átadás – átvétel folyamatának leírását, a tesztelési követelményeke

g) dokumentáltsági követelményeket;

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

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

a) rendszerbiztonsági terv;

b) felhasználói kézikönyv;

c) üzemeltetési kézikönyv;

d) üzletmenet-folytonossági / katasztrófaelhárítási terv;

e) fizikai és logikai rendszerterv;

f) mentési rend;

g) az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentáció, amely tartalmazza:

h) a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését;

i) a fejlesztői módosítások átvezetésének módját;

j) az alkalmazást működtető rendszerelemek (operációs rendszer) frissítésének módját;

k) a biztonsági funkciók hatékony alkalmazását és fenntartását;

l) a rendszerelemmel, a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket;

m) a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat;

n) a rendszer működési folyamatainak ismertetését, példákkal illusztrálva;

o) Konfiguráció, hibaelhárítás;

p) Felhasználói konfigurációk lehetősége;

q) Konfigurációs paraméterek;

r) Jellemző hibalehetőségek és azok megoldása;

s) Hibaüzenetek;

t) Hibaelhárítási tevékenységek;

u) üzemeltetési kézikönyv;

v) rendszerismertető, mely a következőket tartalmazza:

w) a rendszer bemutatása, koncepciója és architekturális vázlata;

x) futtatási környezet leírása;

y) kapcsolat más rendszerekkel;

z) interfészek leírása;

aa) jogosultsági rendszer;

bb) rendszeresen, időszakosan elvégzendő üzemeltetési feladatok;

cc) Monitorozás (rendszeres hálózati ill. folyamat monitorozás);

dd) Batch futtatás (rendszeresen elvégzendő, döntési pontokat nem tartalmazó vagy teljeskörűen leírható futtatási feladatok);

ee) Újraindítás és leállítás (jogosultak és engedélyezők köre, engedélyezés folyamata, újraindítás és leállítás feltételei, értesítés módja és értesítési lánc, végrehajtandó lépések, dokumentálás módja);

ff) Outputkezelés (rendszeresen elvégzendő lépések);

gg) Biztonsági mentések (rendszeresen elvégzendő lépések);

hh) Archiválás (rendszeresen elvégzendő lépések);

ii) Rendszerkarbantartás (rendszeresen elvégzendő ellenőrzések);

jj) Programcsere menedzsment szabályozása és gyakorlata (tartalmazhatja a külső céggel kötött szerződés);

kk) Karbantartás (tartalmazhatja a külső céggel kötött szerződés);

ll) Rendszerhiba esetén szükséges teendők;

mm) fejlesztői dokumentáció, forrásprogram.

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

a) a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját;

b) a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit;

c) a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához.

(9) Az infrastrukturális rendszerfejlesztések alkalmával az alábbi dokumentációkat kell elkészíteni:

a) hálózati ábra;

b) fizikai és logikai rendszerterv;

c) rendszerbiztonsági terv;

d) üzemeltetési kézikönyv;

e) az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza:

f) a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,

g) a biztonsági funkciók hatékony alkalmazását és fenntartását,

h) a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket,

i) a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat.

j) A dokumentációk tekintetében eltéréseket az Információbiztonsági Felelős és a Rendszergazda engedélyezhet írásban, a beszerzett eszköz, szoftver, szolgáltatás megismerése után.

(10) 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.

31. §
Külső elektronikus információs rendszerek szolgáltatásai

(1) A szolgáltatási szerződésekben ki kell kötni, hogy a szolgáltatási szerződés alapján igénybe vett elektronikus információs rendszerek szolgáltatásai feleljenek meg az Egyetem elektronikus információbiztonsági követelményeinek.

(2) Az Egyetemnek külső és belső ellenőrzési eszközökkel ellenőriznie kell, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket. Az ellenőrzést ad hoc jelleggel a gazdasági főigazgató rendelheti el.

(3) Az informatikai biztonsággal összefüggő beszerzéseket folyamatba épített időszakos belső ellenőrzési tervnek megfelelően ellenőrizni kell. Az ellenőrzési tervnek ki kell terjednie a következőkre:

a) az ellenőrizendő területek meghatározása;

b) az ellenőrzések, valamint az ellenőrzéseket támogató értékelések gyakorisága;

c) az ellenőrzés eredményének értékelésnek módszertana;

d) Az ellenőrzést a gazdasági főigazgató 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;

e) Az ellenőrzés megállapításaira, illetve az ellenőrzés értékelésére alapozva intézkedési tervet kell kidolgozni és végrehajtani abban az esetben, ha az ellenőrzés az Egyetem 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;

f) Az ellenőrzések eredményét minden esetben meg kell osztani a gazdasági főigazgatóval, aki az eredménytől függően felterjesztheti a rektor felé;

g) A folyamatos ellenőrzéssel kapcsolatos feladatokat a gazdasági főigazgató koordinálja.

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

a) a rendszer leírását, annak funkcióinak összekapcsolását a folyamatokkal;

b) paramétereit, ki- és bemenő adatait, minden olyan további igényt, melyet az Egyetem támaszt az új rendszerrel kapcsolatban specifikációba kell foglalni és azt mind a megrendelő, mind a szállító oldalán el kell fogadni a fejlesztés megkezdése előtt;

c) a specifikáció szerint kell lefolytatni a tesztelést az érintett felhasználók, alkalmazás rendszergazdák és az adatgazdák bevonásával;

d) amennyiben a tesztelések pozitív eredménnyel zárulnak, a szoftver átvehető;

e) a szoftvernek maradéktalanul meg kell felelnie a specifikációnak és a szervezet elektronikus információs rendszeréhez illeszkednie kell, mind funkcionális, mind biztonsági szempontból;

f) 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;

g) oktatások megtartása, rendszer és egyéb dokumentációk (felhasználói leírások, üzemeltetési utasítások stb.) átvétele, eljuttatása az összes érintetthez kötelező.

32. §
Rendszer és információsértetlenség

(1) 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.

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

(3) 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.

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

33. §
Hibajavítás

(1) Az Egyetem azonosítja, belső eljárásrendje alapján jelenti és kijavítja vagy kijavíttatja az elektronikus információs rendszer hibáit.

(2) Telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket az Egyetem feladatellátásának hatékonysága, a szóba jöhető következmények szempontjából.

(3) Az Egyetem a biztonságkritikus szoftvereket a frissítésük kiadását követő 90 napon belül telepíti vagy telepíttetі, beépíti a hibajavítást a konfigurációkezelési folyamatba.

34. §
Kártékony kódok elleni védelem

(1) Az Egyetem informatikai rendszereit védeni kell a kártékony kódok ellen. Ennek érdekében a következőket kell betartani:

a) A határvédelmi programoknak a szervereken folyamatosan kell működniük. A programoknak folyamatosan vizsgálniuk kell a bejövő hálózati forgalmat (levelezés, web).

b) A határvédelmi szoftverrendszer elemeinek (programok, szabályrendszerek, vírusdefiníciós adatbázisok) frissítéséről automatizált módszerrel gondoskodni kell. A frissítések hiba nélküli megtörténtét ellenőrizni kell.

c) Hálózati munkaállomások az internethez kizárólag az Egyetem internet kijáratán (központi tűzfalán) keresztül csatlakozhatnak.

d) Vírusvédelem nélkül sem hálózati, sem önálló munkaállomás nem üzemeltethető.

e) 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.

f) A munkaállomásokon valós idejű ellenőrzést (azonnali riasztást) biztosító vírusvédelmet kell használni.

g) A felhasználónak tilos vírusirtót, személyes tűzfalat, vagy egyéb biztonsági szoftvert telepítenie.

h) Külső helyekről származó adattárolókat (Szervezeti okból történő) használat előtt vírusellenőrzésnek kell alávetni és csak akkor lehet használni, ha az adathordozó a vizsgálaton megfelel.

i) 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.

j) Vírusfertőzés gyanúja esetén a szervezet informatikusai a fertőzött gépet lezárhatják, annak használatát a hiba elhárításáig felfüggeszthetik.

(2) 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.

(3) A vírusfigyelmeztetésekkel (vírus hoax) foglalkozó felelősök (rendszergazdák), feladata, hogy figyelemmel kísérjék a legfrissebb vírusok megjelenésével kapcsolatos híreket.

(4) Vírusfigyelmeztetéssel kapcsolatos levelet csak a rendszergazda küldhet.

(5) 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.

(6) A vírusvédelmi rendszerek kiválasztását a rendszergazda javaslata alapján a gazdasági főigazgató hagyja jóvá. A vírusvédelmi rendszer kiválasztásakor figyelembe kell venni a következő szempontokat:

a) Nem megfelelő vírusvédelmi rendszer alkalmazásával az Egyetem vírusvédelme nem lesz kielégítő.

b) A nem megfelelő vírusvédelmi szoftver lassítja a műveleteket és túlzott erőforrás igényt támaszthat. A rendszerek lassulása növeli a sebezhetőséget is.

c) A vírusvédelmi szoftverek vírusdefiníciós állomány állományainak frissítési gyakoriságát.

35. §
Kéretlen üzenetek elleni védelem

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

(2) Új verziók elérhetővé válásakor frissíti a levélszemét elleni védelmi mechanizmusokat, összhangban a konfigurációkezelési szabályzattal és eljárásrenddel.

(3) Az elektronikus információs rendszer automatikusan frissíti a levélszemét elleni védelmi mechanizmusokat azok újabb verzióival.

36. §
Az elektronikus információs rendszer felügyelete

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

(2) 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:

a) Rendszeresen el kell végezni azokat a tevékenységeket, amelyek alapján meg lehet győződni arról, hogy a felügyelt rendszer üzemszerűen működik.
b) Az elektronikus információs rendszer riassza az Egyetem illetékes személyeit, csoportjait, amikor veszélyeztetés vagy lehetséges veszélyeztetés előre meghatározott jeleit észleli.
c) Az Egyetem Campus Igazgatósága folyamatosan figyeli a Nemzeti Kibervédelmi Intézet által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket és folyamatosan figyelemmel kíséri a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézettől 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.
d) Kimeneti információk az Egyetem által külső fél számára és belső használatra készített beszámolók, tájékoztatók, bizonylatok, nyilatkozatok, megrendelők, tranzakciók.

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

a) Gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről.
b) Gondoskodni kell arról, hogy a kimeneti információhoz történő fizikai és logikai hozzáférés csak az arra jogosított személyekre korlátozódjon.
c) Gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat.
d) Biztosítani kell, hogy a megsemmisítési eljárások során a kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.

e) A rendszer kimenő információit (pl.: számla) a vonatkozó jogszabályok, szabályzatok szerint kell megőrizni.

(4) 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.

(5) 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.

37. §
Naplózás és elszámoltathatóság

(1) 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.

(2) A naplóban személyes adatot tárolni nem lehet.

(3) 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.

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

38. §
Biztonsági események naplózása

(1) 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.

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

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

(3) 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.

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

a) dátum;
b) időpont;
c) a felhasználó azonosítója;
d) az erőforrás azonosítója, amelyre a művelet vonatkozik;
e) a művelet eredményessége vagy sikertelensége.

(5) A biztonsági naplóban az egyes eseményekhez kapcsolódóan a következő adatokat is rögzíteni kell:
a) az olyan erőforráson kezdeményezett hozzáférési művelet esetén, amelynél a hozzáférési jogok ellenőrzése kötelező;
b) a hozzáférési kezdeményezés típusa;
c) az olyan erőforrás létrehozása vagy törlése esetén, amelynél az ehhez fűződő jogok ellenőrzése kötelező;
d) a kezdeményezés típusa;

(6) Alapvető naplózási követelmény, hogy:
a) Kerüljön naplózásra a biztonságot érintő összes tevékenység.
b) A naplófájlok tartalmát megadott időintervallum alapján képernyőn és nyomtatón is meg lehessen jeleníteni.
c) A naplóállományokat tilos megsemmisíteni, felülírni, módosítani, azokat archiválni kell.
d) A naplóállományok kódoltak, ellenőrző összeggel ellátottak legyenek.
e) 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.

f) A biztonsági eseménynapló (naplófájl) és a Jegyzőkönyvek adatait védeni kell az illetéktelen hozzáféréstől.
g) A rendszerben a biztonsági eseménynapló fájlok auditálásához szükséges eszközöknek lehetővé kell tenniük egy vagy több felhasználó tevékenységének szelektív vizsgálatát.
h) 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.
i) Az elektronikus információs rendszer automatikusan naplózza a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket, és értesíti ezekről a meghatározott személyeket vagy szerepköröket.

(7) 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:

a) naplózási rendszer, amelyet kiiktattak;
b) üzenetfajták, amelyeket rögzítés után módosítottak;
c) naplófájlok, amelyeket átszerkesztettek vagy töröltek;
d) naplófájlok adathordozói, amelyek kimerültek és ennek következtében vagy nem lehet már velük az eseményekről feljegyzést készíteni, vagy önmagukat írják felül;
e) A biztonsági naplókat archiválni kell, mint a rendszerhasználat bizonyítékait, annak érdekében, hogy ezek az információk (bizonyítékok) későbbi vizsgálatokhoz is felhasználhatók legyenek;
f) A naplóinformációk védelme érdekében a következőket kell betartani;
g) A naplóban rögzített információkat megváltoztatni, törölni tilos;
h) A naplók tartalmának megváltoztatásának megakadályozása érekében lehetőség szerint kriptográfiai mechanizmusokat kell alkalmazni;
i) 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;
j) 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.

(8) Folyamatosan figyelemmel kell kísérni a naplóállományok bejegyzései alapján generált riasztásokat.

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

(10) 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) A naplók tárolását a következő szempontok figyelembevételével kell megoldani:

a) A naplóadatoknak sértetlenül rendelkezésre kell állniuk az esetleges elévülési időn belül.
b) Biztosítani kell, hogy az adatokban keletkezésük után változtatást már ne lehessen végrehajtani.

c) Az információk bizalmasságára tekintettel, az adatok nem juthatnak illetéktelenek kezébe.
d) Az általános alkalmazás naplókat minimálisan 1 évig meg kell őrizni, kivéve, ha kapcsolódó jogszabály vagy belső szabályozó ennél többet kíván meg.
e) 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:
f) folyamatirányítási rendszerek esetén 3 év;
g) szerver operációs rendszerek esetén 3 év;
h) végponti operációs rendszerek esetén 1 év;
i) biztonsági alkalmazások esetén 2 év;
j) vagyonvédelmi rendszerek esetén 3 év;
k) ügyviteli rendszerek esetén 2 év;
l) IPS-es, IDS-ek esetén 2 év;
m) hálózati eszközök esetén 2 év;
n) minden egyéb rendszer esetén 2 év.

(12) 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.

(13) Gondoskodni kell a naplóállományok rendszeres mentéseinek felülvizsgálatáról is.

(14) 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.

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

(16) Külső fél részére hatósági, ellenőrzési, hibakeresési okokból a naplófájlokról – szükség esetén anonimizált – másolat adható ki, a gazdasági főigazgató engedélyével.

(17) A naplózandó események és a naplóban rögzítendő adatok körének áttekintése része az gazdasági főigazgató rendszeres felülvizsgálatának.

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

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

(20) A naplózási beállítások ellenőrzésének eredményét írásba kell foglalni:
a) az elvégzett ellenőrzés időpontja;
b) az ellenőrzést elvégző munkatárs neve;
c) az elvégzett ellenőrzés mely rendszerekre terjedt ki;

d) az ellenőrzés megállapításai;
e) javaslat a felmerült problémák kezelésére.
f) Abban az esetben, ha a rendszerben a tényleges naplózás beállítása eltér az adott rendszer nyilvántartott naplózási beállításától ezt haladéktalanul jelenteni kell az információbiztonsági felelősnek.
g) A naplózást és a naplók folyamatos figyelemmel kísérésének megvalósulását rendszeresen ellenőrizni kell. A naplózás ellenőrzését írásba kell foglalni, amelynek tartalmaznia kell a következő adatokat:
h) az elvégzett ellenőrzés időpontja;
i) az ellenőrzést elvégző munkatárs neve;
j) az elvégzett ellenőrzés mely rendszerekre terjedt ki;
k) az elvégzett ellenőrzés tárgya;
l) az ellenőrzés megállapításai;
m) javaslat a felmerült problémák kezelésére.

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

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

(23) 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.

(24) 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.

(25) 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.

(26) 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.

39. §
Rendszer és kommunikációvédelem

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

a) a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól;

b) csak az Egyetem biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez;

c) az Egyetem korlátozza az elektronikus információs rendszer külső hálózati kapcsolatainak a számát a működéshez szükséges minimumra;

d) az elektronikus információs rendszer a felügyelt kapcsolódási pontjain tilt, és csak kivételként engedélyez hálózati forgalmat;

e) véd a túlterheléses (úgynevezett szolgáltatás megtagadás) jellegű támadásokkal szemben, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján, a meghatározott biztonsági intézkedések bevezetésével.

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

(3) 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.

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

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

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

(7) 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.

(8) 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.

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

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

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

(12) 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.

(13) Az elektronikus információs rendszertől elvárt, hogy az:

a) elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az elektronikus információs rendszer irányítási funkcionalitásától;

b) meggátolja a megosztott rendszererőforrások útján történő jogosulatlan vagy véletlen információáramlást;

c) elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára, ahol erre a feldolgozás jellegéből adódóan szükség van;

d) biztosítja, hogy az alrendszerei védjék a keletkezett maradvány információkat, azok bizalmasságát és sértetlenségét.

40. §
Az Egyetem által biztosított számítógép eszközökre vonatkozó szabályok

(1) Az Egyetem számítógépeinek beszerzése pályázati eljárás keretében valósult meg. Az Egyetem Internet vonalát a Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ) biztosítja. A rendszer alapvető célja az Egyetem ismeretnyújtási tevékenységének, kutatási projektjének biztosítása. A Szabályzat ismeretének hiánya nem mentesíti a felhasználót a megsértése esetén alkalmazható szankciók, valamint a polgári és büntetőjogi következmények alól. A hálózat valamennyi felhasználója felelős a számítógéprendszer biztonságáért, köteles ismerni és betartani a biztonsági előírásokat és a hálózati etika alapszabályait. A rendszergazda szakmai felelősséget vállal a leírtak betartásáért és betartatásáért. A felhasználók kötelesek betartani a számítástechnikai eszközök használatát szabályozó rektori vagy rendszergazdai utasítást, az Internet használata esetén pedig az Internet etikai szabályzatát is. Az Internet elérése router-en keresztül történik. E hálózat segítségével valósul meg a weblapok elérése, e-mailek küldése, fogadása (webes levelezőrendszer segítségével), vagy egyéb Internet szolgáltatások futtatása. Egyes szolgáltatások biztonsági okból tiltva lehetnek.

(2) A számítógép használata során a következő szolgáltatások igényelhetők:

a) Internet elérés,
b) Elektronikus levelezés,
c) Szövegszerkesztés,
d) Táblázatkezelő használata,

e) Prezentáció készítés,
f) Előzetes engedély alapján pendrive-ra másolás.

(3) A felhasználók a rendelkezésükre álló lemezterület mértékéig közösen használhatják a számítógépek adat partícióját állományaik tárolására, továbbá használhatják a számítógépeken elhelyezett nyilvános programokat és más állományokat. Webmail rendszeren keresztül levelezhetnek, használhatják a World Wide Webet és más internetes szolgáltatásokat.

(4) A számítógépekre tilos magánjellegű programokat, játékprogramokat telepíteni. A számítógépben vagy programban kárt okozó felhasználó anyagi és büntetőjogi felelősséggel tartozik. A számítógépek elsősorban az Internet elérését hivatottak szolgálni. Magánjellegű levelezésre (e-mail) külön postafiókot az Egyetem nem biztosít. A számítógépek rendeltetésszerű használatát, az elhelyezett eszközök állapotát, a rendszergazda ellenőrzi. Minden felhasználó felelős a rendszer biztonságáért és az eszközök rendeltetésszerű használatáért. A felhasználónak jelentenie kell, ha tudomást szerez nem megfelelő használati cselekményekről.

(5) Az eszközökön csak jogtiszta szoftverek futtathatók. Adathordozó (pendrive) használata csak a rendszergazda vagy a projektvezető engedélyével lehetséges. A műveletet vírusellenőrzésnek kell megelőznie. Amennyiben vírusfertőzés gyanúja merül fel, a rendszergazdát értesíteni kell, aki elvégzi a vizsgálatot. A vírus eltávolításáig a gépet használni tilos. A számítógépekre programokat, operációs rendszert csak a rendszergazda telepíthet.

(6) Tilos a rendszergazda tudomása nélkül:
a) a rendszer fájljainak átvitele bármely más gépre,
b) a rendszer területére (partíciójára) fájlok felmásolása bármely más gépről vagy adathordozóról, - a rendszer fájljainak megváltoztatása, jogosulatlan elérése,
c) tulajdonosuk tudomása nélkül, illetve a rendszergazda engedélye nélkül tilos valamely felhasználó fájljainak elolvasása, másolása, módosítása. A számítógépek partíciójának tartalmát a rendszergazda bármikor, előzetes bejelentés nélkül is törölheti. A számítógépek beállított háttereit és egyéb beállítást megváltoztatni tilos.

(7) A számítógépes rendszer védelme érdekében (jogosulatlan használat, illetve károkozás ellen), a rendszergazda fenntartja magának azt a jogot, hogy indokolt esetben bárkit a számítógép és a hálózat használatából kizárjon. A rendszergazda joga, hogy a számítógépes rendszereket és a hálózatot bármikor ellenőrizze, leállítsa vagy átkonfigurálja, illetve fenntart magának bármely egyéb intézkedési jogot, amely szükséges lehet a könyvtár számítógépes erőforrásainak megvédéséhez, és a további működés biztosításához. A rendszergazda ezen cselekményeit a felhasználókkal egyeztetni köteles. A rendszergazda vagy az általa felkért karbantartók a karbantartás céljára vagy a hálózat működésének ellenőrzésére bármikor bármelyik gépet igénybe vehetik, sürgős esetben akár az ott folyó munkát megzavarva is. A felhasználó joga és kötelessége, hogy az ellenőrzést megelőzően a munkát megfelelően elmenthesse, az eszközt a vizsgálatra haladéktalanul előkészítse. A rendszergazda az egész hálózat felett jogosultságokkal rendelkezik. Indokolt esetben más is kaphat kiemelt jogokat, ha a feladata ezt szükségessé teszi. Ha a rendszergazda a hálózati vagy a helyi meghajtók ellenőrzése során vírusos állományt talál, joga van azt fertőtleníteni, ha pedig a vírusirtó szoftver nem képes a fertőtlenítésre, akkor letörölni azt. A hálózat zavartalan működése és a támogatások megtartása közös érdekünk.

(8) A hálózat használata során tiltottak az alábbi tevékenységek:

a) a géptermekbe étel, ital bevitele, fogyasztása
b) a gépasztalokon táskák, ruhanemű tárolása,
c) a rendszerek szoftver konfigurációinak megváltoztatása (pl. a C: meghajtó tartalma, tapéta, háttér, képernyővédő, egyéni menüpontok stb. megváltoztatása).
d) a számítógépek bootolását módosítani, bármilyen szoftver beállítást -, pI. a gép BIOS beállítását megváltoztatni,
e) szeméremsértő, obszcén, trágár vagy egyéb megbotránkoztató információk előállítása, feldolgozása, tárolása, továbbítása és interneten való megnyitása,
f) a nem rendszergazda által alkalmazott külső hardverek engedély nélküli csatlakoztatása,
g) a számítógépek eredeti helyének megváltoztatása, a csatlakozások megbontása, a berendezések szétszerelése, alkatrészeinek cseréje,
h) a gépteremből bármit elvinni,
i) a szellemi alkotások lemásolása,
j) a számítógépekre szoftvert telepíteni, felmásolni, Internetre kiajánlani,
k) az internetről nem jogtiszta programokat, alkalmazásokat letölteni,
l) fájlmegosztó, fájlcserélő programok használata,
m) crack kódokat, programindító kulcsokat (akár e-mailben is) kérni, küldeni vagy felajánlani (a fenti tilalmak nem csak a programokra, hanem minden szerzői joggal védett termékre kiterjednek, így pl. a zenei anyagokra, rajzokra is),
n) a számítógépek és a hálózat nem rendeltetésszerű használata és a szándékos károkozás,
o) más számítógépre történő betörés, más jelszavának feltörése vagy ezek kísérlete, valamint olyan erőforrás használata, amelyre az adott felhasználónak nincs jogosultsága,
p) a rendszer erőforrásait külön engedély nélkül tilos kereskedelmi vagy egyéb nem iskolai célra használni,
q) az operációs rendszer könyvtárában bármilyen módosítást végezni,
r) mások leveleinek elolvasása, hamis feladójú levél küldése,
s) mások személyiségi jogainak megsértése,
t) másokra nézve sértő, mások vallási, etnikai, politikai vagy más jellegű érzékenységét sértő, másokat zaklató tevékenység, (pl. pornográf anyagok használata, közzététele, kéretlen levelek),
u) a szerzői jogok megsértése,
v) tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték),
w) profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése,
x) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, módosítása, megrongálása, megsemmisítésére irányuló tevékenység, a hálózat biztonságos működését zavaró vagy veszélyeztető információk, programok terjesztése, (pl. vírusok),
y) a hálózati erőforrások magáncélra való túlzott mértékű használata (pl. túlterheléses támadások, levélbombák, letöltések).

(9) A Szabályzat megsértésének megalapozott gyanúja esetén a rendszergazda letilthatja a használatot. A Szabályzat szándékos és durva megsértésének következménye a hálózati szolgáltatásokból való ideiglenes vagy végleges kizárás. A Szabályzat megsértése visszakereshető és a bekövetkezett károkért az elkövető személyesen felelősségre vonható. A rendszergazda a felsorolt tiltó rendelkezések

megszegői ellen - a vétség fokától függően - eljárhat, és az elkövetés tényéről a vezetést értesítheti. A megszegőket a rendszergazda az általa meghatározott időtartamra eltilthatja a géphasználattól.

(10) A termekben nyílt lángot használni vagy bármilyen tűzveszélyes tevékenységet folytatni tilos. A termekben tilos a dohányzás.

(11) Tilos a gépek elektromos berendezésének védőburkolatát eltávolítani, ezeken bármilyen átalakítási, szerelési munkát végezni.

(12) A felhasználó adataiban hardver- vagy szoftverhiba miatt keletkezett kárért az Egyetem felelősséget nem vállal.

41. §
Záró rendelkezések

(1) Jelen Szabályzat annak aláírását követő napon lép hatályba.

(2) A jelen Szabályzat hatálybalépésével a 30/2021. (09.16.) számú rektori-kancellári közös utasítással elfogadott Informatikai Biztonsági Szabályzata hatályát veszti.

(3) Jelen Szabályzatot a Campus Igazgatóság gondozza.

(4) A Jelen Szabályzat megtalálható és elérhető a www.szfe.hu oldalon.

Budapest, 2024. május 06.

…….
Dr. Sepsi Enikő s.k.
rektor

Mellékletek:
1. számú melléklet: Fogalom magyarázat

1. számú melléklet
Fogalom magyarázat

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.