A Semmelweis Egyetem kancellárjának
K/9/2016. (II.29.) **határozata**

az Informatikai biztonsági szabályzat jóváhagyásáról

Az SZMSZ 21. § (14) bekezdésében és 22. § (3) bekezdésében kapott felhatalmazás alapján a Semmelweis Egyetem kancellárja az alábbi döntést hozta:

1. § A Semmelweis Egyetem kancellárja jóváhagyja az Informatikai biztonsági szabályzatot.

2. § A szabályzat bevezetésével összefüggő átmeneti rendelkezések:

(1) Az Informatikai Biztonsági Felelőst a szabályzat hatályba lépését követő 30. munkanapig ki kell jelölni.

(2) Az informatikai kockázatok felmérését első alkalommal az Informatikai Biztonsági Felelős kijelölését követő 60 munkanapon belül kell elvégezni. A kockázatkezelési akcióterveket a kockázatfelmérést követő 30 munkanapon belül kell elkészíteni.

(3) Az Informatikai Biztonsági Fórum alakuló ülését az informatikai kockázatkezelési akciótervek elkészítését követő 30 munkanapon belül meg kell tartani.

(4) A szabályzat hatályba lépését követően külső partnerekkel megkötendő szerződésekben érvényesíteni kell a szabályzatban leírt követelményeket. A szabályzat hatályba lépésekor már hatályos, külső partnerekkel kötött szerződések esetén a szerződő felet a szabályzat hatályba lépését követő 30 munkanapon belül tájékoztatni kell a szabályzat rá vonatkozó rendelkezéseiről.

(5) Az informatikai igazgatónak a szabályzatban meghatározott szervezeti környezetet és vezetői irányítási rendszert a szabályzat hatályba lépését követő 90. munkanapig kell kialakítania.

(6) Az informatikai biztonságnak a szabályzatban leírt valamennyi műszaki feltételét legkésőbb 2018. december 31-ig kell kialakítani.

(7) A felhasználók informatikai biztonsági tudatossági képzésének a feltételrendszerét legkésőbb a szabályzat hatályba lépését követő 2016. december 31-ig kell kialakítani.

(8) A felhasználók által használt saját tulajdonú informatikai eszközök nyilvántartásba vételét a szabályzat hatályba lépését követő 90. napig végre kell hajtani.

3. § Jelen határozat és azzal az Informatikai biztonsági szabályzat a Jogi és Igazgatási Főigazgatóság (JIF) alhonlapján való **közzétételt követő napon lép hatályba.**

Budapest, 2016. február 29.

dr. Szász Károly
kancellár

Hatályba lépés: 2016. március 02.

Dokumentum adatlap

I.

Szervezet neve:	Semmelweis Egyetem	
Dokumentum típusa:	Szabályzat	x
Dokumentum címe:	Informatikai Biztonsági Szabályzat	
Iktatószám:	7630-2/KMFI//2016	
Elfogadó:	Kancellár	x
Elfogadások száma:	1	
Elektronikus változatok elnevezése	Informatikai_Biztonsagi_Szabalyzat_2016	

II.

Előkészítő	**ügyintéző**	**vezető**
Medvey András		Boros András
Társelőkészítő	**ügyintéző**	**vezető**

Jóváhagyó rektor □ Dr. Szász Károly
kancellár x kancellár
rektor és kancellár □

……...
aláírás

III.

III/1. A szabályozó dokumentum és az előterjesztés egyeztetése az SZMSZ 17. § (9) és 35. § (1) bekezdésben foglaltakkal mindegyikével megtörtént.

előkészítő vezető: Boros András
műszaki főigazgató

III/2. A szabályozó dokumentumok végrehajtása költségvetési hatással nem jár □
A szabályozó dokumentumok végrehajtása költségvetési hatással jár X

előkészítő vezető: Boros András
műszaki főigazgató

IV.

Választott véleményezők (szakmai egyeztetés)		tett észrevételt	nem tett észrevételt	nem küldött választ
	EFMI	☐	☐	☐
	Szolgáltatási igazgatóság	☐	☐	☐
	Biztonságtechnikai igazgatóság	☐	☐	☐
	Ellenőrzési igazgatóság	☐	☐	☐
	Adatvédelmi felelős	☐	☐	☐
	Kommunikációs és Rendezvényszervezési igazgatóság	☐	☐	☐
	EOK gazdasági igazgatóság	☐	☐	☐
	VSZÉK gazdasági igazgatóság	☐	☐	☐
	Kórélettani Intézet informatikus	☐	☐	☐
	Neurológiai Klinika informatikus	☐	☐	☐
	I. Nőgyógyászati Klinika informatikus	☐	☐	☐
	I. Pathológia informatikus	☐	☐	☐
Kötelező véleményezők SZMSZ 17. § (9) bekezdés és a 35. § (1) bekezdés alapján	kancellár	☐	☐	☐
	rektor	☐	☐	☐
	általános és oktatási rektorhelyettes	☐	☐	☐
	klinikai rektorhelyettes	☐	☐	☐
	tudományos rektorhelyettes	☐	☐	☐
	Általános Orvostudományi Kar dékánja (ÁOK)	☐	☐	☐
	Egészségtudományi Kar dékánja (ETK)	☐	☐	☐
	Egészségügyi Közszolgálati Kar dékánja (EKK)	☐	☐	☐
	Fogorvostudományi Kar dékánja (FOK)	☐	☐	☐
	Gyógyszerésztudományi Kar dékánja (GYTK)	☐	☐	☐
	Doktori Tanács elnöke	☐	☐	☐
	Emberierőforrás-	☐	☐	☐

	gazdálkodási Főigazgató (EGF)			
	Gazdasági Főigazgató (GF)	□	□	□
	Jogi és Igazgatási Főigazgató (JIF)	□	□	□
	Műszaki Főigazgató (MF)	□	□	□
Egyéb kötelező véleményező	Minőségfejlesztési vezető	□	□	□

Tartalomjegyzék

1. AZ INFORMATIKAI BIZTONSÁGI SZABÁLYZAT CÉLJA

A Semmelweis Egyetem (a továbbiakban: Egyetem) érdekében kiemelten fontos a vagyonának részét képező **egyetemi elektronikus adatvagyon**, valamint az ezt kezelő **információs rendszerek** és rendszerelemek biztonsága.

Elvárás az Egyetem és az egyetemi polgárok részéről az elektronikus információs rendszerekben kezelt **adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának**, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a **kockázatokkal arányos védelmének** biztosítása, amelynek keretében cél:

- az Egyetem egységes információbiztonsági szabályainak meghatározása,
- a működési kockázat csökkentése – a biztonsági intézkedések költségével egyensúlyban,
- a biztonságos hardver- és szoftverfeltételek, valamint információs rendszeralkalmazási- és eljárási követelmények egységes keretbe foglalása,
- a rendkívüli eseményekre, katasztrófa elhárításra, valamint a rendkívüli időszaki kötelezettségekre történő felkészülés, illetve bekövetkezésük esetén az Egyetem információs rendszerei működőképességét biztosító szabályrendszer meghatározása.

Az Egyetem 2026-ig terjedő stratégiája a működtetés területén alapvető célként fogalmazta meg a belső szabályozások segítségével a **tiszta jogi és felelősségi viszonyok** kialakítását. A stratégia végrehajtásakor rövidtávú célként jelölték meg a medikai, gazdasági és oktatási IT rendszerek fejlesztését; középtávú célként az intézményi IT infrastruktúra felkészítését az E-health-re; hosszútávú célként az erős, egységes és vállalatszerű menedzsment működtetését, a központi stratégiai beszerzés és készletgazdálkodás megvalósítását, a technológiai háttér javítását és az intézményi infrastruktúra modernizálását.

Az Egyetem birtokában lévő, hatalmas mennyiségű és felbecsülhetetlen értékű **személyes adat, különleges adat és egészségügyi adat biztonságos kezelése** érdekében alkalmazandók az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (Infotv.), valamint az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (Eüak.) előírásai. A nemzeti felsőoktatásról szóló CCIV törvény (Nftv.) 18 §-a határozza meg a felsőoktatási intézmények által kezelhető személyes adatok körét és adatkezelés célját, 19 § (3) bekezdése pedig a közhiteles felsőoktatási információs rendszerhez (FIR) való kapcsolódás kötelezettségét.

Az informatikai biztonság szempontjából kiemelten fontos az Infotv. azon rendelkezése, miszerint az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, **köteles** továbbá **megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az Infotv., valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek**. Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

Alapelvként rögzítette az Infotv. azt, hogy az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lennie a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.

Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) **célja az informatikai biztonsági irányelvek érvényre juttatásának biztosítása,** az ehhez szükséges egyes informatikai biztonsági szerepkörök, feladatok, folyamatok szabályainak meghatározása, az informatikai biztonsággal összefüggő követelmények meghatározása. Az IBSZ magában foglalja az Egyetemre vonatkozó informati-

kai biztonsági feladatok és felelősségi körök meghatározását, valamint a kezelt, feldolgozott, tárolt, továbbított adatok bizalmasságát, sértetlenségét és rendelkezésre állását fenyegető veszélyek felderítésére, megelőzésére, elhárítására vonatkozó előírásokat.

Figyelemmel

- az Egyetem által kezelt adatok bizalmasságára,
- az Egyetem kapcsolódási kötelezettségére más állami nyilvántartásokhoz,
- az Egyetem stratégia céljai között megjelölt fejlődési irányokra, és arra, hogy
- az Egyetem közreműködőként kerülhet olyan helyzetbe, hogy minősített adatot kell átvennie a minősített adat kezelőjétől

az informatikai biztonság elvárt szintjének a meghatározásakor az Egyetem irányadónak tekinti az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (a továbbiakban: Infobizttv.) megfogalmazott alapelveket és megoldásokat anélkül, hogy az Infobizttv. hatálya kiterjedne rá.

Az Infobizttv.-ben rögzített előírásoknak történő megfelelésre az Egyetem fokozatosan, a szervezeti stratégia középtávú megvalósításáig készül fel. Az informatikai biztonságot érintő fejlesztések az éves informatikai feladatterv összeállításakor kerülnek bemutatásra és megtervezésre.

2. AZ IBSZ HATÁLYA

2.1 Személyi hatálya

Jelen szabályzat személyi hatálya kiterjed:

a) az Egyetemnél, az Egyetem által alapított, az Egyetem többségi tulajdonában lévő szervezeteknél foglalkoztatott közalkalmazottakra, munkavállalókra, szerződéses jogviszonyban álló, jogi és természetes személyekre, jogi személységgel nem rendelkező szervezetekre,
b) az Egyetemmel szerződéses kapcsolat keretében információcserét (küldés és/vagy fogadás, tárolás/továbbítás) folytató szervezetekkel történő kommunikációra, függetlenül a szervezet betöltött szerepétől, szervezeti helyétől, elhelyezésétől és az Egyetemhez fűződő kapcsolatától,
c) az Egyetemmel hallgatói vagy más képzési jogviszonyban álló személyekre – a jelen szabályzatban meghatározott eltérésekkel.

2.2 Tárgyi hatálya

Az IBSZ tárgyi hatálya kiterjed:

a) az Egyetem minden információkezeléssel és feldolgozással kapcsolatos folyamatában résztvevő informatikai eszközre, mely az Egyetem területén található, illetve ezen eszközök elhelyezésére szolgáló létesítményekre.
b) az Egyetem tulajdonában vagy használatában lévő informatikai eszközökre és az informatikai eszközök által kezelt, tárolt, továbbított adatokra, információkra.
c) az Egyetem informatikai hálózatára csatlakozó, de nem az Egyetem tulajdonában lévő eszközökre.

3. AZ INFORMATIKAI BIZTONSÁGI RENDSZER MŰKÖDTETÉSE

3.1 A jogszabályoknak és a belső szabályzatoknak való megfelelés

A vonatkozó jogszabályok, belső szabályzatok a 7.1 számú mellékletben találhatóak.

3.2 Informatikai biztonsági kockázatmenedzsment

Annak érdekében, hogy az Egyetemnél az informatikai biztonság érvényesítése során a kockázatarányos védelem elve érvényesüljön, a *Kockázatkezelési szabályzatban* meghatározott kockázatmenedzsment folyamatot az informatikai biztonsági kérdésekkel kapcsolatosan folyamatosan alkalmazni kell.

A kockázatmenedzsment célja, hogy az információk bizalmasságát, sértetlenségét, valamint rendelkezésre állását veszélyeztető kockázati tényezők azonosításával, a kockázatok csökkentésével biztosítsa az informatikai biztonság növelését, szinten tartását.

A teljes körű kockázatfelmérést jelentős változás esetén (technológia, ill. szolgáltatás be- / kivezetése), de legalább kétévente kell végrehajtani az informatikai rendszer minden elemére (technikai eszközök, személyek, eljárások, szabályok).

A felmerült kockázatok kezelésére (csökkentésére) akcióterveket kell készíteni, melyeknek a feltárt kockázatok függvényében az alábbiakat kell tartalmazniuk:

- javaslatokat a technikai eszközök megváltoztatására, vagy fejlesztésére (pl.: új védelmi eszközök alkalmazása, vagy a jelenlegi átkonfigurálása);
- javaslatokat az érvényben lévő szabályozás megváltoztatására;
- javaslatokat a személyi állományra vonatkozóan;
- a kockázatok tudatos felvállalását, ha a védelmi intézkedés közvetlen és közvetett anyagi vonzata nagyobb vagy közel azonos, mint a fenyegetettség által elszenvedhető közvetlen és közvetett anyagi kár.

Az informatikai rendszerek bevezetésére vonatkozó részletes kockázatfelmérést kell végrehajtani a rendszertervezés és rendszerbevezetés időszakában.

Az IT biztonsági kockázatok felmérését a Kancellár által kijelölt személy végzi és koordinálja.

3.3 Megelőző intézkedések rendszere

A megelőző intézkedések célja a nem kívánatos biztonsági események megelőzése.

Az Egyetem a megelőző intézkedéseket az alábbi formában működteti:

- az Egyetem **információtechnológiai védelmi intézkedéseket** (hálózatvédelem, vírusvédelem, jogosultság kezelés, stb.) foganatosít annak érdekében, hogy a nagy gyakorisággal bekövetkező fenyegető tényezők előfordulási gyakoriságát vagy hatását csökkentse;
- az Egyetem **szabályozott folyamatokat** vezet be, munkautasításokat ad ki annak érdekében, hogy garantálja a biztonsági kontrollok működtetését, illetve az esetleges incidensek feltárását (jogosultságkiadás, fejlesztés, stb.);
- az Egyetem rendszeres biztonságtudatossági **oktatásokat** végez a humánkockázatok csökkentésére.

3.4 Az informatikai biztonság irányításának alapjai

Annak érdekében, hogy az informatikai biztonság folyamatosan, minden területen a kívánt biztonsági szinten működjön, az alábbi irányelveket kell érvényesíteni a napi munka során:

- a szabályzat személyi hatálya alá tartozó személyeknek az IBSZ-ben foglalt előírások ismeretében és azokat betartva kell munkájukat végezniük;
- az informatikai biztonsági incidenseket észlelésükkor jelentenie kell az azt észlelőnek az Informatikai Igazgatóság vagy az Informatikai biztonsági felelős felé. A bejelentés módja lehet telefon, email vagy a GLPI rendszerben történő bejegyzés. A telefonos bejelentés történhet az Operatív Irányítóközponton keresztül is. A GLPI-ben való rögzítés (a bejelentő vagy az incidens kezelője által) minden esetben kötelező;
- Az informatikai biztonsági incidenseket az incidens kezelőjének olyan részletezettséggel szükséges dokumentálnia, hogy a dokumentáció az alábbi célnak megfeleljen:
  - minden IT incidenst az erre szolgáló nyilvántartásban rögzíteni kell, hogy elemezni lehessen a szolgáltatásokra vonatkozó incidensek számosságát, időtartamát és hatását;
  - a bekövetkezett incidenseket figyelembe kell venni a kockázatfelmérés során az egyes fenyegetettségek bekövetkezési valószínűségének meghatározásánál;
  - felhasználói incidensekből statisztikailag ki lehessen nyerni az elkövetési magatartást;
- A biztonsági incidensekből levont tapasztalatokat folyamatosan értékelni kell és azokat figyelembe kell venni a védelmi rendszer tervezése, szervezése, működtetése során.

3.5 Helyesbítő intézkedések rendszere

Az Egyetem informatikai biztonsági rendszerében meghatározott szabályoktól való eltérést az Informatikai Igazgató – az IT biztonsági felelős egyetértésével - írásban, indokolással engedélyezhet. Vitás esetben az Informatikai Biztonsági Fórum előzetes állásfoglalásának az ismeretében a Kancellár a döntéshozó. Az engedélyezés során meg kell vizsgálni az eltérési igény okát, és indokolt esetben az Informatikai Biztonsági Felelősnek gondoskodnia kell arról, hogy az a szabályozás részévé váljon, annak érdekében, hogy a rendszerben minél kevesebb kivételes kezelést igénylő eset keletkezzen. Egyéb esetekben az eltérést kivételként kell kezelni és a szükséges intézkedéseket a szabályzat előírásai szerint kell meghozni.

Az incidensek természetét és gyakoriságát az Informatikai Biztonsági Felelősnek kell folyamatosan figyelemmel kísérnie, illetve szükség esetén javaslatot kell tennie a védelmi intézkedések módosítására.

Védelmi intézkedés módosítását kell alkalmazni az alábbi esetekben:

- amennyiben a korábbi védelmi intézkedés szintje nem érte el a kívánt biztonsági szintet, meg kell fontolni egy szigorúbb intézkedés bevezetését;
- amennyiben egy védelmi intézkedés az indokoltnál jobban korlátozza az egyetemi polgárok munkavégzését;
- amennyiben az informatikai rendszer változása miatt a korábbi biztonsági kontrollok érvényüket vesztik;
- amennyiben az adott kontroll elavul és/vagy jobb, újabb technológiák bevezetése válik indokolttá.

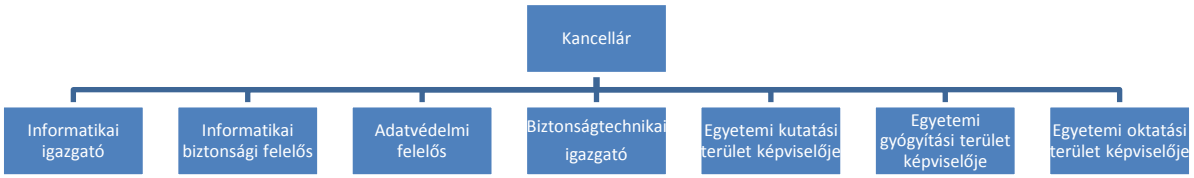
4. AZ INFORMATIKAI BIZTONSÁG SZERVEZETE

4.1 Az Informatikai Biztonsági Fórum

Az informatikai biztonsági tevékenységeket az Egyetem működtetői, oktatási, gyógyítói és kutatási területeiről delegált - és megfelelő feladat- és munkaköri funkciókkal felruházott képviselők révén kell koordinálni. A koordinációs tevékenység elvégzése az Informatikai Biztonsági Fórum (IBF) keretében történik.

Az IBF vezetője a Kancellár.

Az IBF szervezeti felépítése:



Az IBF működése:

Az IBF értékelő, döntés-előkészítő testület, évente legalább egyszer ülésezik. Üléseit – a napirend megjelölésével - a Kancellár hívja össze. Az ülés összehívására és napirendi pontra bármelyik tag javaslatot tehet. Az Informatikai biztonsági felelős javaslatára, az általa megjelölt napirenddel az ülést kötelező összehívni.

Feladata: a stratégiai célok informatikai biztonságot érintő kérdéseinek, valamint az informatikai biztonság növelése érdekében történő fejlesztési és módosítási igényeknek a megvitatása, rendkívüli informatikai biztonsági események kezelése.

Az IBF üléseire indokolt esetben tanácskozási joggal rendelkező külső szakértőt is meghívható.

A rendkívüli biztonsági esemény kezelése történhet elektronikus úton is (email-en történő javaslattétel, véleményezés).

Az IBF által megvitatott javaslatokról a Kancellár dönt.

4.2 Informatikai biztonsági szerepkörök

Az Egyetem informatikai biztonsági rendszerének működtetése a Kancellár feladata, tevékenységét az Informatikai igazgató és az Informatikai biztonsági felelős útján gyakorolja. E szabályzatban meghatározott intézkedési jogköröket a Kancellár által más személyek, szervezeti egységek részére átruházott hatáskörként kell értelmezni. A leadott hatáskör e személyek és szervezeti egységek egyéb felelősségét nem érinti.

4.2.1 Kancellár

Felelőssége:

Az Nftv. 13/A § (2) bekezdésének a) pontja, és az Egyetem Szervezeti és Működési Szabályzatának 33 § (2) bekezdésének a) pontja alapján a Kancellár felel az Egyetem informatikai tevékenységéért,

amelynek keretében felelőssége az informatikai biztonsággal kapcsolatos felsővezetői döntések meghozatala, a szükséges pénzügyi keretek biztosítása.

Feladatai:

- az Informatikai Biztonsági Szabályzat kiadása
- az Informatikai Üzemeltetési Szabályzat kiadása
- az Egyetem informatikai biztonsággal összefüggő beszerzéseinek gazdálkodási szempontú értékelése, megvalósíthatóságuk vizsgálata, pénzügyi erőforrások biztosítása;
- döntéshozatal az IBF hatáskörébe tartozó ügyekben.

4.2.2 Informatikai igazgató

Felelőssége: az informatikai biztonsághoz szükséges szervezeti és műszaki környezet létrehozása és folyamatos biztosítása, vezetői irányítási rendszer alkalmazása.

Az informatikai biztonsággal kapcsolatos önálló feladatai:

- az informatikai rendszer funkcionális és biztonsági követelményeknek megfelelő működtetése a rendelkezésére bocsátott költségkeret betartásával;
- az informatikai rendszer folyamatos rendelkezésre állásának biztosítása;
- az informatikai folyamatok és tevékenységek tervezése és folyamatos fejlesztése;
- a rendkívüli helyzetek elhárítása;
- az informatikai rendszer biztonsági komponenseinek üzemeltetéséhez szükséges humán és technikai erőforrások biztosítása a rendelkezésére álló erőforrások hatékony felhasználásával;
- az informatikai rendszerüzemeltetés és rendszerhasználat rendszeres független felülvizsgálatának biztosítása;
- érvényesíti az informatikai biztonsági követelményeket a hatáskörébe tartozó szolgáltatásokkal kapcsolatban kötött külső szolgáltatói szerződésekben;
- gondoskodik a működésfolytonosságot biztosító szabályozás, tervek rendelkezésre állásáról, folyamatos megfelelőségéről, a működésfolytonossági tesztek elvégzéséről és a működésfolytonosság megszakadása esetén értesítendő személyek aktuális elérhetőségeit tartalmazó címlista (vészhelyzeti hozzáférések) rendelkezésre állásáról
- az informatikai szervezeti egység vezetők bevonásával gondoskodik a mentési stratégia kialakításáról, a mentési rend elkészítéséről, ellenőrzi a mentési eljárások betartását, gondoskodik a mentések tárgyi é személyi feltételeiről;
- rendszeresen – az Egyetem Informatikai Katasztrófa-elhárítási Tervében leírtak szerint – gondoskodik a katasztrófahelyzet kezeléssel kapcsolatos tesztek elvégzéséről;
- a programfejlesztési igények, fejlesztési programok kezelése, az elkészült termékek informatikai ellenőrzése az Egyetem belső szabályzatai és jelen IBSZ előírásai szerint;
- gondoskodik az Egyetem informatikai rendszerének felhasználói szintű informatikai biztonsági oktatásáról.

Az Informatikai Biztonsági Felelőssel megosztott feladatai:

- a fokozottan védett területekre történő belépés és az ott történő munkavégzés engedélyezése, az engedélyek rendszeres felülvizsgálata;
- az Egyetem informatikai biztonsági követelményeinek alkalmazása és betartatása;
- gondoskodni arról, hogy az informatikai biztonsági feladatok és követelmények beépüljenek a hatáskörébe tartozó szolgáltatások üzemeltetési folyamataiba,

- a VPN kapcsolatok létesítésének engedélyezése, az Informatikai Biztonsági Felelős előzetes jóváhagyása alapján.

4.2.3 Biztonságtechnikai igazgató

Felelőssége: a fizikai biztonsággal kapcsolatban teljes utasítási és szabályozási joggal rendelkezik.

Az informatikai biztonsággal kapcsolatos legfontosabb feladatai:

- gondoskodik az informatikai biztonsági szervezet fizikai biztonsággal kapcsolatos feladatainak végrehajtásáról és felügyeletéről;
- személyesen, vagy illetékes munkatársán keresztül részt vesz a hatáskörébe tartozó szolgáltatásokat érintő informatikai biztonsággal kapcsolatos incidensek kivizsgálásában, az intézkedési javaslatok kidolgozásában;
- rendszeres ellenőrzésekben történő részvétel biztosítása személyesen, vagy illetékes munkatársán keresztül.

4.2.4 Informatikai Biztonsági Felelős

Felelőssége**:** a biztonsági szabályok betartatása az üzemeltetési folyamatok során, az informatikai biztonság elvárt szintjének a biztosítása, folyamatos fejlesztése, intézkedési javaslatok megfogalmazása a biztonsági incidensek megelőzésére, illetve a bekövetkezett incidensek hatásának mérséklésére. Felelős a beszerzések, informatikai fejlesztések során a biztonsági követelmények érvényre juttatásáért, egy bekövetkezett informatikai biztonsági esemény kapcsán az okok feltárásáért, a felelősök beazonosításáért.

Feladatai**:**

- a munkatervében meghatározott terv szerint az Egyetemen folyó tevékenységek informatikai biztonsági szempontból történő értékelése, a meglévő biztonsági szint megtartása, illetve fokozása;
- az Egyetem informatikai biztonsági dokumentációs rendszerének rendszeres karbantartása;
- a biztonsági szabályok betartatásának felügyelete;
- az IBSZ betartatásának ellenőrzése;
- az IBSZ-ben nem szabályozott kérdésekben a lehetséges veszélyforrások felderítése és javaslattétel a megelőzésre;
- közreműködés az IT biztonsági kockázatok felmérésében, kezelésében, a bevezetett intézkedések hatásosságának visszamérésében;
- az informatikai rendszerben kialakított biztonsági funkciók és az Egyetem informatikai biztonsági követelményei összehangolásának ellenőrzése;
- az informatikai rendszer biztonságát elősegítő eszközök üzemeltetésének rendszeres ellenőrzése, független felülvizsgálatának megszervezése;
- informatikai biztonsági incidens menedzsment feladatok ellátása:
  - a biztonsági incidensek kezelése;
  - az incidensek kivizsgálása vagy kivizsgáltatása;
  - és az incidensek kapcsán felmerült problémák elhárítására tett lépések ellenőrzése;
- az Egyetemmel bármilyen módon adatforgalmi, illetve információadási/fogadási kapcsolatban (adathálózat, adathordozók cseréje, stb.) álló külső szervekkel történő szerződéskötés esetén – az Egyetem érdekeinek lehető legteljesebb védelme érdekében – az informatikai biztonság területét érintő részekkel kapcsolatban ellenőrzési, javaslattételi joga és kötelezettsége van;

- a programfejlesztési munkák, valamint a beszerzések során ellenőrizni, illetve ellenőriztetnie kell, hogy az informatikai biztonság szempontjai maradéktalanul megvalósulnak-e. Gondoskodnia kell arról, hogy csak informatikai biztonsági szempontból megbízható szoftverek készüljenek, illetve kerüljenek beszerzésre;
- az Egyetem informatikai védelmi- és biztonsági rendszere tervezésében való részvétel;
- az informatikai védelmi- és biztonsági rendszer rendszeres felülvizsgálata, a védelmi eszközökkel való ellátottság rendszeres ellenőrzése;
- az Egyetem adatkezelési tevékenységének és az informatikai kommunikációs hálózatának informatikai biztonsági szempontú ellenőrzése;
- az informatikai rendszer változásainak folyamatos nyomon követése és az annak során tapasztaltaknak megfelelően, módosítási javaslatok elkészítése az Egyetem informatikai biztonsági dokumentációs rendszerére vonatkozólag;
- az általa észlelt vagy hozzá beérkezett bejelentések alapján, az adatfeldolgozás- és kezelés biztonságát sértő események, szabálysértések kivizsgálása – az esetleges rossz szándékú hozzáférési kísérletek, illetéktelen adatfelhasználás kiszűrése, a biztonsági területi felelősökkel együttműködve a rendszerek eseménynaplóinak kiértékeltetése, intézkedésekre történő javaslattétel;
- az informatikai rendszerben kialakított, aktuálisan beállított jogosultságok és a jóváhagyott jogosultságok összevetése, ellenőrzése;
- annak ellenőrzése, hogy megtörtént-e minden informatikai konfigurációs-elem (rendszerelemek) nyilvántartásba vétele és azonosítása az informatikai vagyontárgyak hatásos védelemének kialakításához;
- annak ellenőrzése, hogy megtörtént-e a leselejtezésre kerülő eszközök adathordozóin, háttértárain tárolt adatok végleges, visszaállíthatatlan módon való törlése;
- az informatikai munkafolyamat bármely részének előzetes bejelentési kötelezettség nélküli ellenőrzése;
- az információ-, informatikai biztonság tudatosságának növelése – az oktatási anyagok véleményezése és közreműködés az oktatási anyagok elkészítésében;
- az informatikai biztonságot érintő utasítás-tervezetek készítése és véleményezése.

Az Informatikai biztonsági felelős a Kancellár által kijelölt, az Informatikai igazgatótól szervezetileg független személy.

4.2.5 Kari/tömbigazgatóság szintű informatikai vezető

Felelőssége: végrehajtási és ellenőrzési felelősség; az informatikai biztonság megvalósulását eredményező helyi környezet folyamatosságának biztosításában.

Az informatikai biztonsággal kapcsolatos legfontosabb feladatai:

- A helyi informatikai rendszereknek a követelményeknek megfelelő működtetése.
- A helyi informatikai rendszerek folyamatos rendelkezésre állásának és funkcionális működésének biztosítása.
- A helyi informatikai rendszerek biztonsági komponenseinek üzemeltetéséhez szükséges humán és technikai erőforrások biztosítása a rendelkezésére álló erőforrások hatékony felhasználásával.
- Közreműködés az IT biztonsági kockázatok felmérésében, kezelésében, a bevezetett intézkedések hatásosságának visszamérésében.
- Érvényesíti az informatikai biztonsági követelményeket a hatáskörébe tartozó informatikai szolgáltatásokkal kapcsolatban kötött külső szolgáltatói szerződésekben.

- Intézkedik a hatáskörébe tartozó mentési stratégia kialakításáról, ellenőrzéseket végez a mentések elvégzéséről, az ezzel kapcsolatos incidensek kezelésében, gondoskodik a mentések tárgyi-személyi feltételeiről.
- Részt vesz a területén az informatikai biztonsági események kivizsgálásában, és az abból adódó intézkedések végrehajtásában.
- A területéhez tartozó fokozottan védett területekre történő belépés és az ott történő munkavégzés engedélyezése, az engedélyek rendszeres felülvizsgálata a Biztonságtechnikai igazgatóval közösen.

4.2.6 Egyéb informatikai biztonsági szerepkörök

A informatikai biztonsági területeken végzendő feladatok az informatikai igazgatóság infrastruktúra- és alkalmazás-üzemeltetési munkatársai munkaköri leírásában, illetve az egyes rendszerek technológiai leírásában találhatók. Ezek a biztonsági területek az alábbiak:

- vírusvédelem;
- határvédelem (tűzfalak, spamszűrő, aktív hálózati eszközök, VPN);
- mentések;
- jogosultság-kezelés;
- alkalmazás üzemeltetés.

4.2.7 Szervezeti egység vezető

Felelős a Szabályzatban előírtak betartatásáért, hatás- és jogosultsági körének megfelelően az előírásait megszegőkkel szemben a felelősségre vonás kezdeményezéséért, a szervezeti egységet érintő szerződésekben a Szabályzat előírásainak a vállalkozókkal, szolgáltatókkal, szakértőkkel szembeni érvényesítéséért.

Köteles a tudomására jutott, az egyetem információbiztonságát veszélyeztető, működését sértő eseményekről, körülményekről – azok jellegétől függően – az informatika biztonsági felelősi feladatokat ellátó munkatársnak információt nyújtani.

Közreműködik a szakterület információbiztonsági, IT biztonsági kockázatai feltárásában, a kockázatok felmérésében, értékelésében, és kezelésében.

4.2.8 Felhasználó

Felelős az egyetemi feladatai ellátása érdekében az informatikai eszközök rendeltetésszerű használatáért, az Informatikai biztonsági szabályzatban leírtak betartásáért. Az Egyetem informatikai infrastruktúráját kizárólag munkájával összefüggő feladatok végzéséhez használhatja.

Informatikai biztonsági feladatai:

- Köteles a Szabályzat előírásait a szakmai feladatköréhez szükséges mértékben megismerni, a Szabályzatban és a kapcsolódó szabályzatokban, utasításokban foglaltakat maradéktalanul végrehajtani, a munkakörének ellátásához szükséges oktatáson részt venni.
- Köteles minden olyan tudomására jutott információt, eseményt, körülményt a munkahelyi vezetőjének jelezni, amely az egyetem információs rendszerei biztonságos működését veszélyezteti, a funkcionális működési rendjét sérti.
- Köteles azonnal jelenteni az informatikai eszközök és alkalmazások működésében bekövetkezett hibákat, rendellenességeket.
- Felelős a rábízott, az egyetem tulajdonát képező információs eszközök megőrzéséért, rendeltetésszerű használatáért, a kezelési előírások maradéktalan betartásáért.
- az eszközökön lévő információk védelme;

- az alkalmazások felhasználói leírásainak az ismerete és az alkalmazások használatakor azok betartása.

A felhasználó az Egyetem informatikai rendszerében saját tulajdonú eszközt csak előzetes bejelentés és nyilvántartásba vétel esetén használhat. Az informatikai igazgató – az informatikai biztonsági felelős véleményének előzetes beszerzését követően – megtilthatja a felhasználó saját tulajdonú eszközének az Egyetem hálózatára vagy az Egyetem tulajdonában lévő informatikai eszközre történő csatlakoztatását, ha az eszköz nem kezelhető vagy nem vállalható informatikai biztonsági kockázatot rejt.

4.3 Külső ügyfelek és partnerek

4.3.1 Külső személyekkel összefüggő kockázatok azonosítása

Az Egyetem információit és információ-feldolgozó eszközeit fenyegető kockázatokat azonosítani kell. Kiemelt figyelmet kell fordítani a külső ügyfelek/szerződéses munkavállalók tevékenységében rejlő kockázatok azonosítására és kezelésére. A kockázatok kezelésére az Egyetem informatikai rendszereit és/vagy informatikai szolgáltatásait használó vagy az informatikai biztonságra hatást gyakorolni képes külső személyekkel (pl. a szerződések aláíróival) olyan írásbeli megállapodást – „Titokvédelmi megállapodást/záradékot"- kell kötni, amely vagy tartalmazza, vagy utal minden olyan informatikai biztonsági követelményre, amely biztosítja az IBSZ-nek és az Egyetemen bevezetett szabályoknak való megfelelést. A szerződésben meg kell jelölni, hogy az Egyetem területén külső munkát végző tevékenységét ki felügyeli. Az Egyetem informatikai rendszeréhez és információihoz külső fél számára megfelelő hozzáférést biztosítani csak a titokvédelmi megállapodás aláírását követően lehet. A titokvédelmi megállapodást a külső felekkel kötött szerződések mellékleteként kell megőrizni, a jogosultságigényléskor pedig utalni kell arra, hogy a Titoktartási megállapodás rendelkezésre áll.

4.3.2 A biztonság kérdésének kezelése harmadik féllel kötött megállapodásokban

A külső személyekkel, illetve hallgatókkal kapcsolatosan – amennyiben értelmezhetők – a következő feltételeket kell a velük kötött szerződésbe foglalni vagy részükre dokumentáltan rendelkezésre bocsátani:

- az IBSZ-ben meghatározott informatikai biztonsági követelmények kivonatát
- az Egyetem kezelésében lévő adatok másolásának és nyilvánosságra hozatalának korlátozásait;
- hozzáférés-ellenőrzési megállapodást, amely tartalmazza:
  - a megengedett hozzáférési módokat;
  - a hozzáférés és jogosultságkezelés folyamatát;
  - a külső személy képviselőinek egyértelmű megfeleltetését az igénybe vehető informatikai szolgáltatásokkal, azok használatra vonatkozó jogokkal és kiváltságaikkal együtt;
  - a hozzáférési mód ellenőrzési feltételeit;
- a szerződésben rögzített felelősségek auditálásának jogát, vagy az auditok további külső személlyel történő elvégeztetésének jogát;
- a problémamegoldás folyamatát;
- a biztonsági eseményekről és a biztonság megsértéséről szóló jelentési kötelezettségek, értesítések és a kivizsgálásokra vonatkozó intézkedéseket;
- a szerződés teljesítésébe további alvállalkozók bevonásának feltételeit, titoktartásukra vonatkozó megállapodásokat.

Az Egyetem informatikai rendszerében a külső személyek által távolról elért, menedzselt vagy diagnosztizált eszközeihez való kapcsolódást minden hozzáférés igénylésekor egyedileg kell engedélyezni és felügyelni**.**

A külső személyek hozzáférését a hozzáférés indokának megszűnte után azonnal meg kell szüntetni, illetve a szerződés lejártakor automatikusan – ez a Jogosultságkezelő felelős, nem címtár alapú authentikációt használó alkalmazások tekintetében az Alkalmazás adminisztrátor feladata.

A harmadik féllel kötött megállapodások informatikai biztonsági szempontú ellenőrzése a JIF bevonásával, az Informatikai Biztonsági Felelős, valamint az Informatikai Igazgató közös feladata.

4.3.3 Titoktartási megállapodások

Minden alkalmazottnak és az Egyetem informatikai rendszereit és/vagy szolgáltatásait használó külső szervezetnek, személynek (cégnek, egyéni munkavállalónak, stb.) titoktartási nyilatkozatot kell aláírnia, melyben nyilatkozik arról, hogy a munkája során tudomására jutott, a nem publikus egyetemi információkat sem a munkavégzés során, sem annak vége után nem hozza harmadik fél tudomására.

5. RÉSZLETES VÉDELMI INTÉZKEDÉSEK MEGHATÁROZÁSA

5.1 Informatikai vagyontárgyak kezelése

5.1.1 Informatikai vagyonleltár

Valamennyi informatikai vagyontárgyat (információ-feldolgozó eszközt vagy ahhoz kapcsolódó kiegészítő eszközt, perifériát, tároló eszközt) egyértelműen azonosítani kell és valamennyi vagyontárgyról eszközleltárt kell felvenni és folyamatosan karbantartani. A leltár felvételével és karbantartásával kapcsolatos utasításokat az Egyetem leltárkezelési szabályzata, illetve az Informatikai Igazgatóság Szervezeti ügyrendje tartalmazza.

A nyilvántartásban kötelezően kell szerepeltetni a következő konfigurációs-elemeket:

- hardver elemek (kiszolgálók, kliensek, hálózati aktív és passzív eszközök, háttértárolók, nyomtatók, stb.);
- szoftver elemek (operációs rendszer, alkalmazás, fejlesztőeszköz, stb.);
- információs elemek (adatbázisok, adatállományok, stb.);
- szolgáltatási elem (világítás, energia ellátás, légkondicionálás, stb.);
- dokumentációs elem (rendszerdokumentációk, felhasználói kézikönyvek, üzemeltetési utasítások, folytonossági tervek, stb.).

Valamennyi nyilvántartásba vett információ-feldolgozó eszközhöz hozzá kell rendelni azokat a felelősöket, akik az adott eszközök biztonságáért felelnek (un. vagyongazda)

Információk, adatokhoz történő hozzáférések esetében a felelős az Adatgazda, hardverek, szoftverek esetében az Informatikai Igazgató.

Az Egyetem informatikai rendszerében csak az Informatikai Igazgató és az Informatikai Biztonsági Felelős által jóváhagyott, konfigurációs leltárba felvett:

- hardverelemeket lehet használni;
- jogtiszta szoftvert lehet telepíteni és/vagy futtatni.

Amennyiben a felhasználó azt tapasztalja, hogy a konfiguráció megváltozott – és erről előzetesen nem kapott értesítést – köteles arról az Egyetem GLPI alkalmazásán vagy email-en keresztül tájékoztatni a Informatikai igazgatóságot (az Igazgatóság szervezeti e-mail címén).

5.1.2 Vagyontárgyak tulajdonjoga

Valamennyi, az Egyetemen keletkezett, illetve az Egyetem által rendelkezésre bocsátott információ és az információfeldolgozással összefüggő vagyontárgy az Egyetem tulajdona.

5.2 Az emberi erőforrások biztonsága

5.2.1 Személyekkel kapcsolatos biztonsági intézkedések

Az Egyetem dolgozóival meg kell ismertetni a „Felhasználói Informatikai Biztonsági Nyilatkozatot”, amely tartalmazza:

- a felhasználók által alkalmazandó informatikai biztonsági szabályok összefoglalását;
- az informatikai rendszerek használatával kapcsolatosan elvárt és tiltott magatartásokat, továbbá azok megsértésének szankcióit;
- az informatikai rendszer számára nagy kockázattal járó fenyegetések és veszélyforrások közérthető magyarázatát, a biztonságtudatosság fokozása érdekében.

Minden egyetemi dolgozó számára a munkakörükhöz igazodó és kötelező informatikai biztonsági oktatást kell nyújtani. Az oktatáson való részvételt a dolgozó aláírásával igazolja vagy elektronikus formában megoldható tesztet kell kitöltenie az oktatás anyagából.

Az informatikai biztonságtudatossági képzést az Informatikai igazgatóság szervezi, tematikáját és előadóját az Informatikai biztonsági felelős biztosítja.

5.2.2 Az informatikai biztonság tudatosítása, oktatás és képzés

Az Egyetem informatikai rendszerei felhasználóinak a munkakörükhöz igazodó informatikai oktatást kell biztosítani, lehetőleg az informatikai rendszer használata előtt, illetve az általuk használt informatikai infrastruktúra változásakor (pl. új hardver vagy szoftver használatba vétele előtt), valamint az IT biztonsági kockázatok jelentős változásakor, új kockázati elem megjelenésekor.

Az oktatás előkészítése során az Informatikai Igazgatóság feladata:

- a szükséges tanfolyamok meghatározása;
- javaslat a képzésben részesítendő munkakörök/szerepkörök meghatározására;
- oktatásra javasoltak meghatározása
- az oktatók személyére vonatkozó javaslattétel (amennyiben a képzés nem külső szervezésű).

5.2.3 Feladatok a közalkalmazotti jogviszony megszűnésekor, illetve változásakor

A közalkalmazotti jogviszony megszüntetésekor, illetve megváltoztatásakor az Informatikai igazgatóság adott területért felelős munkatársai a következő feladatokat hajtják végre:

- jogosultságok megszüntetése vagy módosítása úgy, hogy a régi állapot mentésre vagy dokumentálásra kerül;
- a felhasználó (Egyetem munkájához kapcsolódó) elektronikusan tárolt információit, e-mailjeit és egyéb általa létrehozott hivatalos adatot másolni kell az általa használt informatikai eszközről, illetve bármely egyéb adathordozóról és biztosítani szükséges a kilépő dolgozó által használt szerver tárhely hozzáférését a munkahelyi vezetője által megadott felhasználó számára és biztosítani szükséges az e-mailjeinek megadott címre történő továbbítását.
- az Egyetem a hálózati meghajtókat és levelezőrendszerét a munkavégzés támogatására vezette be, az esetlegesen itt tárolt magáncélú tartalmakról, levelekről a jogviszony megszűnésekor az Egyetem megkeresésre sem készít semmilyen adathordozón másolatot. A felhasználó feladata az ilyen tartalmak, levelek egyetemi levelezőrendszerből történő eltávolítása legkésőbb az utolsó munkában töltött napig.
- A jogviszony megszűnését követő 30 nap múlva a kilépő munkavállaló egyetemi elektronikus levelező címét az informatika megszünteti, törlik, és ezt követően a Semmelweis Egyetem nem vállal felelősséget az egyetemi e-mail címre címzett levelekért.
- A munkahelyi vezető felelőssége, hogy a kilépés napja és az e-mail cím megszüntetése közötti időszakra az átirányítást kérvényezze az általa megadott felhasználó email címére.

A fenti feladatokat az érintett alkalmazott munkahelyi vezetője kezdeményezi a kilépésre vonatkozó űrlapon.

5.2.3.1 Informatikai vagyontárgyak visszaszolgáltatása

Valamennyi alkalmazottnak, szerződéses viszonyban álló munkavállalónak és minden, az Egyetem informatikai rendszereit és/vagy szolgáltatásait használó külső félnek vissza kell szolgáltatnia az Egyetem valamennyi használatra átvett informatikai vagyontárgyát, amikor alkalmazása, szerződése, illetve megállapodása lejár vagy megszűnik. A visszaszolgáltatás azon szervezeti egység részére történik, ahol a vagyontárgy nyilvántartásba van véve.

Az Informatikai Igazgatóságnak, vagy a helyi illetékes informatikai szervezetnek az eszköz leadásakor ellenőriznie kell, hogy a felhasználó az általa átvett és az Elszámoló lapon rögzített hardver-, szoftver specifikációval és üzemképes állapotban adja-e vissza a vagyontárgyat.

5.2.3.2 Hozzáférési jogok megszüntetése

Valamennyi alkalmazottnak, a szerződőknek és harmadik feleknek az információkhoz és információ-feldolgozó eszközökhöz való hozzáférési jogosultságát fel kell függeszteni, meg kell szüntetni, amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár, vagy azt módosulás esetén a változáshoz kell igazítani.

A változtatási kérelem benyújtásának biztosítása az érintett alkalmazott közvetlen vezetőjének a feladata, melyet a változást megelőzően, de lehetőleg legkésőbb a szerződéses/munkaviszony megszűnését megelőző 3. munkanapig kell írásban jeleznie az Informatikai Igazgatóság Felhasználói Támogatás osztálya számára.

A kérelmekben előírt feladatok végrehajtása az Informatikai Igazgatóság feladata

A fentiek alól kivételt képeznek a hallgatói jogviszonyukat befejező hallgatók tanulmányi rendszer jogosultságai, melyek a jogviszony lezárását követően is érvényben maradnak (csak olvasási jog).

5.3 Az informatikai környezet fizikai védelme

5.3.1 Területek védelme, biztosítása

Az Egyetem Vagyonvédelmi és Rendészeti Szabályzata rendelkezik az Egyetem épületeinek, értékeinek és polgárainak védelmének megszervezéséről, a figyelembe veendő szempontrendszerekről és a feladatkörökről.

5.3.1.1 Az informatikai helyiségek kijelölése, határzóna kialakítása

Azokon a területeken, ahol információkat vagy információ-feldolgozó eszközöket tárolnak, biztonsági határzónákkal kell védeni az illetéktelen hozzáféréstől. A fizikai védelem kialakítása során olyan megoldásokat kell bevezetni, amelyek alkalmasak az egyértelmű és egyedi azonosításra, monitorozásra.

Informatikai helyiségek az egyetem mindazon helyiségei, amelyekben az informatikai infrastruktúra központi elemei elhelyezésre kerülnek:

- szerverek;
- telefonközpontok;
- hálózati elosztószekrények, központi hálózati eszközök;
- alkalmazói és irodai szoftverek és informatikai rendszer- vagy eszköz dokumentációk törzspéldányai;
- biztonsági mentések.

Az informatikai helyiségek tételes nyilvántartását az Informatikai Igazgató vezeti.

5.3.1.2 Fizikai belépés ellenőrzése

Az Informatikai Igazgatóság alakítja ki, működteti és felügyeli az informatikai helyiségekbe való belépés rendjét, gondoskodik az új vagy visszavont engedélyekkel kapcsolatos jogosultsági információk elektronikus beléptető rendszer adatbázisában történő szükség szerinti átvezetéséről vagy átvezettetéséről.

Az Informatikai Biztonsági Felelős az Informatikai igazgatóság és a Biztonságtechnikai igazgatóság munkatársával havonta, szúrópróbaszerűen ellenőrzi a beléptető rendszer adatait (ki lépett be, mikor és milyen céllal).

5.3.2 Védett helyszínek

Az Egyetem helyiségei informatikai biztonsági szempontból négy kategóriába sorolhatók:

Kiemelten védett kategória

Kiemelten védett kategóriába sorolt helyiségnek kell tekinteni azokat a helyiségeket, ahol nem nyilvános adatok feldolgozására, tárolására alkalmazott központi informatikai erőforrások találhatók. Ezen helyiségek egyben zárt területnek is minősülnek, ezért az ott meghatározott szabályokat is be kell tartani velük kapcsolatban.

Kiemelten védett kategóriába a következő helyiségeket kell sorolni:

- szerverszoba (szerverek, kommunikációs központ, stb.);
- a mentett, archivált adatokat tartalmazó helyiség.

Fokozottan védett kategória

Fokozottan védett kategóriába sorolt helyiségnek kell tekinteni azokat a helyiségeket, ahol nem nyilvános adatok feldolgozására, tárolására alkalmazott kiegészítő informatikai erőforrások találhatók.

Fokozottan védett kategóriába a következő helyiségeket kell sorolni:

- a gerinchálózatot kiszolgáló aktív hálózati elemek elhelyezésére szolgáló helyiségek;
- Informatikai Igazgatóság, Kari/Tömbigazgatóság Informatikai szervezete által használt raktár;
- informatikai dolgozók napi munkavégzésre használt irodái, helyiségei.
- mentések végzésére szolgáló helyiségek

Általánosan védett kategória

Általánosan védett kategóriába sorolt helyiségnek kell tekinteni azokat a helyiségeket, ahol nem nyilvános adatok feldolgozására alkalmazott informatikai erőforrások találhatók.

Általánosan védett kategóriába a következő helyiségeket kell sorolni:

- felhasználói irodák, tantermek, előadók.

Egyéb kategória

Egyéb kategóriába sorolt helyiségnek kell tekinteni azokat a helyiségeket, ahol informatikai aktív hálózati eszközök találhatóak, de adatok tárolása, feldolgozása nem történik.

Egyéb kategóriába a zárt szekrényben, nyilvános folyosón elhelyezett aktív hálózati elemeket kell sorolni.

5.3.2.1 Kiemelten védett helyiségek védelme

Fizikai védelem, tűzvédelem

A fizikai védelmi és tűzvédelmi szabályokat az Egyetem Tűzvédelmi Szabályzata, valamint Vagyonvédelmi és Rendészeti Szabályzata tartalmazza.

A belépés rendje

A kiemelten védett területeken a munkavállalók és egyéb okból belépők beléptetési rendjére az alábbi szabályok vonatkoznak:

- a kiemelten védett területekhez történő hozzáférés kizárólag erre felhatalmazott személyek számára lehetséges, ezt a beléptető rendszer általi kikényszerítéssel kell megvalósítani;

- a kiemelten védett területekre vonatkozó belépési jogokat rendszeresen felül kell vizsgálni, a szükséges változtatásokat el kell végezni;
- egyéb okból csak indokolt esetben történhet kiemelten védett területre belépés, és tájékoztatni kell az érintettet arról, hogy a kiemelten védett területen csak kísérővel mozoghat, valamint fel kell jegyezni az érkezés és a távozás pontos idejét, a belépés célját és belépést engedélyező nevét.

A fentiek megvalósításáért az Informatikai Igazgatóság infrastruktúrájának az üzemeltetési vezetője a felelős.

A munkavégzés szabályai

A kiemelten védett területen történő munkavégzésre a következő biztonsági szabályok vonatkoznak:

- fokozottan kell érvényesíteni a munkavégzés megszervezésénél az információkhoz való hozzáférés minimalizálását, a szándékos károkozás megakadályozását;
- ha nem tartózkodik senki a kiemelten védett területen, akkor a területet biztonságosan le kell zárni, és rendszeresen ellenőrizni kell ezt az állapotot;
- a kiemelten védett területen külső szervezet alkalmazottja, csak a következők betartásával végezhet munkát:
  - kiemelten védett területre külső személy alkalmazottja csak rendkívüli esetben és csak korlátozott ideig kaphat munkavégzésre engedélyt;
    - munkavégzésre jogosító engedélyt az Informatikai Igazgató, vagy a Kari/Tömbigazgatóság Informatikai szervezet vezetője adhat, mely engedélyeket az Informatikai Biztonsági Felelős ellenőriz;
    - minden kiemelten védett területen történő, külső személy bevonásával végzett, tervezett munkavégzésről a munka megkezdése előtt 1 nappal, rendkívüli munkavégzésről (sürgős hibaelhárítás) a munka megkezdésével egy időben értesíteni kell az Informatikai Igazgatót és az Informatikai Biztonsági Felelőst;
    - kiemelten védett területeken felügyelet nélkül nem végezhet munkát harmadik fél alkalmazottja;
- meg kell győződni róla, hogy a kiemelten védett területre történő belépéskor, a munkát végző személynél csak a munkavégzéshez szükséges elektronikus eszközök találhatók.

Fotó, film, hangfelvétel, vagy egyéb adatrögzítésre, adattovábbításra alkalmas eszköz használata a kiemelten védett területen, külön engedély hiányában tilos. Ezt az engedélyt személyre és időtartamra korlátozva az Informatikai Igazgató adja ki és az Informatikai Biztonsági Felelős ellenőrzi.

5.3.2.2 Fokozottan védett helyszínek védelme

A fokozottan védett helyszínek védelmére vonatkozó szabályokat az Egyetem Tűzvédelmi Szabályzata, valamint Vagyonvédelmi és Rendészeti Szabályzata tartalmazza.

5.3.2.3 Általánosan védett helyiségek védelme

Az általánosan védett helyszínek védelmére vonatkozó szabályokat az Egyetem Tűzvédelmi Szabályzata, valamint Vagyonvédelmi és Rendészeti Szabályzata tartalmazza.

5.3.2.4 Egyéb helyszínek védelme

Az egyéb helyszínek védelmére vonatkozó szabályokat az Egyetem Tűzvédelmi Szabályzata, valamint Vagyonvédelmi és Rendészeti Szabályzata tartalmazza.

5.3.2.5 Az informatikai logisztikai funkciókra elkülönített terület védelme

Annak érdekében, hogy megelőzhető legyen az Egyetem informatikai rendszereihez való jogosulatlan hozzáférés, a logisztikai funkcióra használt területeket (ki-, beszállítási, rakodási területek) lehetőség szerint el kell különíteni az informatikai adatfeldolgozást végző létesítményektől, szerverszobától.

A logisztikai helyiségek védelmét, az oda való be-, és kilépést, szállítást az Egyetem Informatikai Igazgatósága biztosítja.

5.3.2.6 Külső és környezeti veszélyekkel szembeni védelem

Az Egyetem Informatikai Katasztrófa Elhárítási Terve és az azt segítő szoftver megoldások tartalmazzák a természet és az ember által előidézett katasztrófák által okozott károk elleni védelmet.

Az Egyetem Informatikai Katasztrófa Elhárítási Tervének elkészítésért az Informatikai Igazgató felel. A Működés-folytonossági Tervek, eljárások elkészítése, tesztelése és karbantartása az Informatikai igazgató felelőssége, az adott informatikai rendszer adatvagyonáért operatív szinten felelős Adatgazdák bevonásával.

5.3.3 Informatikai eszközök védelme

5.3.3.1 Informatikai eszközök elhelyezése és védelme

Az informatikai eszközöket úgy kell elhelyezni, illetve védeni, hogy kockázati besorolásuknak megfelelő mértékű legyen a környezeti fenyegetésekből és veszélyekből eredő kockázat, valamint a jogosulatlan hozzáférés lehetősége.

5.3.3.2 Kábelezés biztonsága

Az adatátvitelt biztosító, az információszolgáltatásokat támogató elektromos energiaátviteli és távközlési kábelhálózatot védeni kell az illetéktelen hozzáféréstől és a károsodástól:

- a táp és adat kábeleket lehetőleg föld, álpadló alatt, álmennyezet fölé vagy kábeltálcában kell vezetni;
- a rendezőszekrényeket minden esetben kulcsra kell zárni;
- az áramellátásért felelős kábeleket az adatkábelektől szeparáltan kell elhelyezni, megelőzve ezzel az interferenciát;
- kábelek típusát, állapotát (szakadt, rossz) egyértelmű azonosítást lehetővé tevő módon kell jelöléssel ellátni, valamint a szakszerű javításról gondoskodni;
- a kábelezés nyomvonalát és típusát kábelezési rajzokon és nyilvántartásokban kell rögzíteni, úgy, hogy az létesítményeken belüli pontos futásvonal és elhelyezés leolvasható legyen;
- a be- és átkötéseket minden esetben dokumentálnia kell az azt végző rendszergazdának, kivitelező szakembernek.

Fentiekért az ***Informatikai Igazgató*** felel, ideértve a zárható szekrények és helyiségek kulcsainak tárolását, nyilvántartását.

Kiemelt fontosságú rendszerek esetében (melyek a mindenkori legmagasabb adatosztályozási kategóriába eső adatokat teszik központilag elérhetővé) „A biztonsági osztályok követelmény katalógusa" mellett az alábbi pontok irányadók:

- végpontok és elérési pontok (pl. fali ajzat) elzárása szükséges;
- alternatív, redundáns vonalak biztosítása;
- üvegszálas kábel használata a hagyományos UTP helyett;
- patch panelek és elosztószekrények elérésének fokozott korlátozása.

5.3.3.3 Informatikai eszközök karbantartása

Az informatikai eszközök karbantartását folyamatos rendelkezésre állásuk és sértetlenségük biztosítása érdekében a gyártó útmutatása alapján, előírásszerűen el kell végezni. A karbantartás megvalósításáért az Informatikai Igazgató a felelős.

5.3.3.4 Vagyontárgyak – telephelyről való eltávolítás, elszállítás

Informatikai eszközök, szoftverek csak az IT infrastruktúra üzemeltetés osztály vezetőjének, vagy a Kari/Tömbigazgatóság Informatikai szervezet vezetőjének az engedélyével vihetők ki az Egyetem székhelyéről vagy telephelyéről külső szervizbe.

Az adattároló média, az információ és más értékek fokozott fenyegetettségnek vannak kitéve szállítás közben, ezért alábbi kontrollok megfelelő alkalmazásával kell gondoskodni biztonságukról. Ennek érdekében:

- a szállítást csak egyetemi közalkalmazott (informatikus, rendkívüli esetben kézbesítő) vagy az Egyetemmel szerződésben álló szerviz cég munkatársa, vagy megbízott futár végezheti;
- amennyiben a javításra átadott eszköz hibáját nem az adattároló okozza, úgy lehetőség szerint az adattárolót el kell távolítani az eszközből a szerviznek történő átadás előtt;
- a szolgáltató cégekkel kötött szerződésekbe titoktartási kitételeket kell belefoglalni;
- a szállítandó eszközöket megfelelő csomagolással kell ellátni a fizikai károsodások megelőzése érdekében;
- a nem nyilvános adatokat tartalmazó adathordozók szállítása esetén (pl.: mentések) az alábbi kontrollokat is alkalmazni kell:
  - zárható tároló doboz alkalmazása;
  - olyan csomagolás alkalmazása, mely felbontás után nem zárható vissza az eredeti formában, így az esetleges illetéktelen hozzáférés felderíthető;

Amennyiben a vagyontárgyat (például szervizelésre kijelölt nyomtató) külső személy szállítja el, az átadónak meg kell bizonyosodnia arról, hogy a szállítást végző személy valóban az adott külső partnerhez tartozik-e (pl. fényképes igazolvány, megbízólevél, céges bélyegző megléte, stb.). Az átvételről átadás-átvételi nyilatkozat kiállítása szükséges.

5.3.3.5 A mobil informatikai eszközök biztonsága az épületen kívül

Az Egyetem tulajdonában lévő mobil eszközök (hordozható számítógép, okostelefon, táblagép, PDA), melyek munkavégzés céljából kerültek átadásra, a felhasználó személyére való tekintet és az eredeti beszerzés forrására való tekintet nélkül, az Egyetem működési területén kívüli célra (pl. magán- vagy más gazdasági társaságok céljára) csak külön engedély esetében használhatók.

A használatot a szervezeti egység vezetőjének kell jóváhagynia.

Az alábbi irányelvek betartása kötelező:

- az eszköz vagy az egyetemi információkat tartalmazó média nem maradhat felügyelet nélkül nyilvános helyen; gépkocsiban;
- az Egyetem informatikai rendszeréhez kapcsolódni csak az Egyetem eszközével és az Informatikai igazgatóság által biztosított módon (pl. webmail, Novell authentikáció, VPN csatorna) lehet;
- a gyártó előírásait mindig be kell tartani az eszköz védelme érdekében;
- amennyiben az Egyetem informatikai rendszeréhez idegen tulajdonú eszköz csatlakoztatása szükséges, arra csak az Informatikai igazgató és az IT biztonsági felelős engedélyével kerülhet sor, írásbeli engedély alapján, amely tartalmazza a csatlakozási ok megjelölését és időtartamát is.

A VPN kapcsolatok szabályos beállításáért az Informatikai Igazgató felelős.

5.3.3.6 Az informatikai eszközök biztonságos selejtezése, illetve újrafelhasználása

Az informatikai eszközök selejtezésével kapcsolatban a Selejtezési Szabályzat előírásait kell alkalmazni.

Az adatokat tartalmazó informatikai eszközök selejtezésére az alábbi speciális szabályok vonatkoznak:

- az adathordozó, adattároló törlését vagy újrafelhasználásra való előkészítését (és az ehhez kapcsolódó műveleteket) csak az Informatikai Igazgatóság, vagy a Kari/Tömbigazgatóság Informatikai szervezetének munkatársa végezheti el. Minden raktározási és tárolási lépésben az illetéktelen hozzáféréstől védve kell tárolni az eszközöket;
- valamennyi olyan információ-feldolgozó eszközt, amely adattároló eszközt foglal magában, ellenőrizni kell, hogy az azon tárolt adatok és szoftverek a selejtezést megelőzően végleges eltávolításra, illetve biztonságos felülírásra kerüljenek;
- a használatból kivont információ-feldolgozó eszközöket egy hónapig raktározni kell az esetleges visszaállítás érdekében, feliratozva, illetéktelen hozzáféréstől védve;
- adathordozók megsemmisítését vagy újrafelhasználását az Adatgazda kezdeményezheti;
- az eszközökben található adathordozókról az adatokat újrafelhasználás, az eszköz használatból történő végleges kivonása előtt (az 1 hónapos várakozási idő után) visszaállíthatatlan módszerrel törölni kell;
- a bontásra, megsemmisítésre átadott gépek esetében is visszaállíthatatlan módszerrel törölni kell az adatokat.
- Amennyiben a nagymennyiségű adathordozók megsemmisítését külső munkavállaló vagy szervezet végzi, a megsemmisítést kizárólag erre a feladatra megfelelő felkészültséggel rendelkező végezheti. A velük kötött szerződésben kell külön rögzíteni a titoktartási feltételeket, illetve a szerződőnek garanciát kell vállalni az adatok visszaállíthatatlan megsemmisítésére, teljes és időbeli korlátozás nélküli titoktartásra is.

Az Informatikai Igazgató és az Informatikai Biztonsági Felelős köteles megbizonyosodni arról, hogy az adathordozókon tárolt információk megsemmisítése megtörtént-e és megsemmisítésre csak információk megsemmisítése után adhatóak át a külső vállalkozó részére.

5.3.3.7 Visszaállíthatatlan törlés

A visszaállíthatatlan törlés a szoftveres úton történő törlés esetében, ugyanazon adathordozó legalább háromszoros, titkos adatok/kiemelten védett rendszerek esetében kilencszeres felülírását jelenti, adatot nem tartalmazó mintákkal.

Működésképtelen vagy törölhetetlen eszköz esetében, fizikai törlést kell alkalmazni, az erre alkalmas eszközzel (pl. optikai lemez – CD daráló, roncsolás).

5.4 Az informatikai üzemeltetés biztonsága

5.4.1 Dokumentált üzemeltetési eljárások

Az üzemeltetés eljárásrendjét a SZMSZ-ben meghatározott struktúrában kell kialakítani:

- „Informatikai szabályzatok" szintje (IBSZ, IT üzemeltetési és hálózati szabályzat, szervezeti ügyrend): ezen a szinten az általános követelményeket (szerepkörök, felelősségek, szabályozandó területek) kell megfogalmazni. Rögzíteni kell a munkabeosztásra, a géptermi rendre, a rendszerfelügyeletre, a dokumentálásra vonatkozó általános követelményeket;
- „Eljárásrendek" szintje: ezen a szinten kell definiálni a rendszer specifikus üzemeltetési feladatok ellátásához szükséges technikai előírásokat, az üzemeltetési feladatok végrehajtási módját. Az eljárásrendek tartalmazzák legalább:
  - komponensek;
  - rendszer funkciói;
  - rendszer illeszkedési pontjai;
  - rendszerrel kapcsolatos üzemeltetési feladatok felsorolása és dokumentálási követelményei;
  - rendszerrel kapcsolatos feladat- és felelősségi körök;
  - rendszerrel kapcsolatos katasztrófa elhárítási tervek.

Az eljárásokat, vagy azok kivonatát minden informatikai szereplő számára elérhetővé kell tenni, akinek munkaköre kapcsán arra szüksége lehet.

5.4.2 Változáskezelés

Az információ-feldolgozó eszközök és rendszerek változtatásait nyomon kell követni, a változásokat előzetesen meg kell tervezni (tesztelés, végrehajtás lépései, szükség esetén a visszaállítás lépései) és az Informatikai igazgatóval engedélyeztetni.

5.4.3 Fejlesztési, tesztelési és üzemeltetési eszközök

Az Egyetemen üzemeltetett fejlesztési-, tesztelési- és éles környezeteket fizikailag és logikailag egymástól külön kell választani. A felhasználó számára egyértelműen azonosíthatóvá kell tenni a fejlesztési-, tesztelési-, éles üzemeltetési környezetet és annak kimeneteit (pl.: a képernyőn történő megjelenítés, nyomtatott dokumentumok).

A tesztrendszerrel szemben támasztott követelmények:

- a tesztrendszerben lévő jogosultságoknak azonosnak kell lenni az éles rendszerben lévő jogosultságokkal;
- amennyiben a teszteléshez magasabb jogosultság szükséges a tesztelő személyeknek, mint amivel az éles rendszerben rendelkeznek, akkor anonim adatbázis használata szükséges;
- külső partnerek csak anonimizált adatbázist használhatnak teszteléshez

A fejlesztői környezetben az adatok csak anonimizált módon kerülhetnek tárolásra.

A fejlesztő a fejlesztési tevékenység kapcsán semmilyen körülmények között nem férhet hozzá az éles környezethez és az éles adatbázishoz.

A fejlesztés során kockázatelemzéssel kell megbizonyosodni arról, hogy az új rendszer vagy az új verzió, modul biztonsági kockázatait megfelelő, a kockázattal arányos védelmi intézkedéssel oldotta-e

meg a fejlesztő. Továbbá a tesztelés során meg kell vizsgálni a többi rendszerrel való kapcsolatát, új sérülékenység megjelenése esetén a többi rendszerre vonatkozóan is frissíteni kell a kockázatelemzést.

5.4.4 Védelem rosszindulatú és mobil kódok ellen

5.4.4.1 Vírusvédelem

Az Informatikai Igazgatóság vírusvédelmi felelőseinek kell gondoskodnia arról, hogy az informatikai eszközökre telepítve legyenek az ismert sebezhetőségeket kiszűrő, hibákat megszüntető aktuális védelmi programok és javítócsomagok. A javítócsomagoknak a telepítés előtt a változáskezelési tevékenységekre vonatkozó mindenkori hatályos belső szabályok szerinti tesztelési és jóváhagyási eljáráson kell átesniük.

A felhasználók az Egyetem eszközein csak az Egyetem által biztosított és felügyelt szoftvereket használhatják. Az Egyetem által nem ismert és tesztelt szoftvert a felhasználók nem tölthetnek le, a hálózatról nem futtathatnak, és nem telepíthetnek. Ezt csak az Informatikai Igazgatóság, vagy a Kari/Tömbigazgatóság Informatikai szervezet munkatársai végezhetik az informatikai üzemeltetésre vonatkozó belső szabályok alapján.

A felhasználók kötelesek az adathordozón kapott bármilyen állományt a számítógépre telepített vírusvédelmi szoftverrel leellenőrizni. Ahol lehetséges, az ellenőrzést az automatikus beállításokkal kell kikényszeríteni.

A védelmi programok segítségével meg kell valósítani a munkaállomások valósidejű ellenőrzését, a vírusvédelmi adatbázisok rendszeres és automatikus frissítését, a teljes fájlrendszer ellenőrzések heti rendszerességű ütemezését, a felhasználók munkáját nem akadályozó időpontban.

A vírusvédelmi ellenőrzések eredményeit központi napló formájában elérhetővé és visszakereshetővé kell tenni. A naplók rendszeres ellenőrzése a vírusvédelmi felelős feladata. Vírusvédelmi esemény gyanúja esetén a vírusvédelmi felelős értesíteni köteles az Informatikai Igazgatót és az Informatikai Biztonsági Felelőst.

Az Egyetem számítógép-hálózatába levélmellékletként érkezett állományok közül törölni kell azokat, amelyek jellegük alapján biztonsági szempontból kockázatot jelenthetnek (pl.: futtatható állományok). A törlés tényéről a címzettet automatikusan értesíteni kell.

A törlendő állományok körét – az Informatikai Biztonsági Felelős és az Adatgazdák véleményének figyelembe vételével – az Informatikai Igazgatónak kell meghatározni, és arról a Vírusvédelmi felelősnek kell naprakész nyilvántartást vezetni.

5.4.4.2 Mobil kód elleni intézkedések

Ahol a mobil kód használata engedélyezett, a konfigurációnak biztosítania kell:

- a mobil kód eredetének hitelesítését,
- a letöltési út integritásának ellenőrzését,
- képesnek kell lennie korlátozni a mobil kód műveleteihez való hozzáférést, hozzáférés vezérléssel és/vagy verifikációval (igazolással).

5.4.5 Jogosultság kezelés

5.4.5.1 A felhasználói azonosító, jelszó- és jogosultság menedzsment célja és általános szabályai

A jogosultság kezelés célja, hogy az Egyetem informatikai rendszerében a felhasználói hozzáférés életciklusának valamennyi fázisát lefedve (új felhasználók első nyilvántartásba vételétől a nyilvántartásból történő végső törlésig) biztosítsa, hogy minden felhasználó csak azokhoz az informatikai rendszerekben tárolt információkhoz, adatokhoz, programokhoz és szolgáltatásokhoz férjen hozzá, amelyek munkaköre ellátásához feltétlenül szükségesek; valamint meghatározza az

Egyetem informatikai rendszerében az adatokhoz, információhoz történő hozzáférés ellenőrzésének általános követelményeit.

Az Egyetem tulajdonában vagy használatában lévő valamennyi informatikai eszközön tárolt adathoz hozzáférés csak az Egyetem és a felhasználó közötti jogviszony létrejötte után és a megfelelő jogosultság ellenőrzését követően lehetséges, megvédve az informatikai rendszereket és adatokat a jogosulatlan hozzáféréstől

A felhasználókat megillető jogosultságokat az adatgazdák határozzák meg.

Az egyetemi munkavállalói jogviszonya alapján minden informatikai eszközt használó munkavállalót megilletnek az ún. alap felhasználói jogosultságok.

Az Egyetem tulajdonában vagy használatában lévő valamennyi informatikai rendszer esetében az azonosítást hitelesítő mechanizmust kell működtetni.

A hitelesítés általános módszere a felhasználói azonosítóhoz tartozó jelszó ismeretének ellenőrzése, a magas informatikai biztonsági kockázatú rendszerek esetén kiegészítve a birtoklás alapú hitelesítéssel (pl.: intelligens kártya, token és PIN kód - jelszó).

Az Egyetemnél korlátozni kell:

- az olyan kiváltságos hozzáférési jogokat (pl. local admin jogosultság), amelyek lehetővé teszik, hogy a felhasználó a biztonsági és egyéb kritikus rendszerbeállításokat módosíthassa,
- a nyilvános hálózatokon keresztül engedélyezett hozzáféréseket.

A jogosultságkezelő felelős a jogosultságigénylések és törlések alapján naprakész nyilvántartást vezet az Egyetem informatikai rendszerének felhasználói azonosítóiról, a felhasználók aktuális jogosultságairól a rendelkezésre álló adatok alapján.

5.4.5.2 Felhasználók regisztrálása

A felhasználói jogosultságok kiadását, módosítását és visszavonását dokumentált eljárások alapján kell végezni, a kiosztott jogosultságokat nyilván kell tartani.

A felhasználók azonosítása központilag nyilvántartott felhasználói azonosítók használatával történik. Ahol technológiailag nem kivitelezhető ettől eltérni- szakrendszerek esetén- az Informatikai Biztonsági Felelős engedélyével lehetséges.

Az Egyetem a belépő munkatársak számára – az Emberierőforrás-gazdálkodási Főigazgatóság írásbeli tájékoztatása alapján – a jogosultságkezelői felelős, alkalmazások esetében az alkalmazás adminisztrátor hozza létre a felhasználói azonosítót.

A felhasználói azonosítókat a jogosultságkezelő felelős, alkalmazások esetében az alkalmazás adminisztrátor menedzseli és tartja nyilván.

A felhasználói azonosítókat tartalmazó állományokat csak a jogosultságkezelési felelős illetve az alkalmazás adminisztrátor módosíthatja.

A felhasználói azonosítók visszavonásig, lejáratig vagy újrahitelesítésig érvényesek.

A felhasználói azonosítókat inaktív (felfüggesztett) állapotba kell helyezni, ha

- tulajdonosuk munkavégzésre irányuló jogviszonya megszűnt;
- 5 egymást követő sikertelen bejelentkezési kísérlet történt;
- ha 6 hónapig nem történik bejelentkezés.

5.4.5.2.1 Felhasználói jogosultságok alapszabályai

A felhasználói jogosultságok létrehozásakor és felülvizsgálatakor minden esetben az alapszabályoknak megfelelően kell eljárni:

- az alapértelmezett azonosítókat át kell nevezni és jelszavukat meg kell változtatni;
- a felhasználói azonosítókat minden esetben egyedi felhasználókhoz kell rendelni és tulajdonosát egyértelműen azonosítani kell;
- a közös felhasználói azonosítók használatát csak kivételes esetekben, az Informatikai igazgató engedélyezheti;
- az anonim azonosítókat fel kell függeszteni, illetve törölni kell. Amennyiben bizonyos alkalmazások igénylik ezek használatát, akkor jogosultságukat olvasási korlátozással kell ellátni;
- a ritkán használt azonosítókat a használat idején kívül fel kell függeszteni és csak a használat idejére aktiválni, majd használat után újra fel kell függeszteni.

5.4.5.3 Kiemelt felhasználói jogosultságok kezelése

Az olyan jogosultságokat, amelyek – valamely biztonsági kritérium (bizalmasság, sértetlenség, rendelkezésre állás) szempontjából – más biztonsági kontrollokat bírálnak felül vagy hatástalanítanak, korlátozni és monitorozni kell. Ilyen privilégium például a VPN használata, az adminisztrátori jogosultságok birtoklása. A naplózás kialakítása az Informatikai Igazgatóság feladata.

A kiemelt felhasználói jogosultságok miatt keletkezett kockázatokat csökkenteni kell, továbbá figyelemmel kell kísérni ezen jogosultságok használatát a biztonsági incidensek vagy visszaélések megelőzése érdekében. Alapvető biztonsági szabályok a kiemelt felhasználói jogosultságok kiosztásával kapcsolatban:

- a kiemelt felhasználói jogosultságokat esetileg kell kiosztani, és a használat idejére kell korlátozni, majd vissza kell vonni;
- a kiosztott kiemelt felhasználói jogokat folyamatosan nyilván kell tartani, ez az Adatgazdákkal együttműködve a jogosultságkezelő felelős feladata. A nyilvántartás és a gyakorlati megvalósítás közötti eltérések időközönkénti ellenőrzése az Informatikai Igazgató, valamint az Informatikai Biztonsági Felelős feladata;
- a kiemelt felhasználói jogosultságokat nem szabad az általános felhasználói azonosítóhoz rendelni, helyette az érintett felhasználóhoz ideiglenes, a szükséges privilégiumokkal felruházott, kiemelt jogosultágú csoporthoz tartozó egyedi felhasználói azonosítót kell rendelni;
- a kiemelt felhasználók tevékenységét naplózni kell és rekonstruálható eseményrögzítést lehetővé tevő eszközzel rögzíteni kell;
- a tevékenységrögzítésből felvett eseményeket, „naplókat” az Informatikai Igazgatóság kontrollálja és az Informatikai Biztonsági Felelős bevonásával negyedévente, szúrópróbaszerűen ellenőrzi.

5.4.5.3.1 Kiemelt felhasználói jogosultságok alapszabályai

A kiemelt felhasználói jogosultságok létrehozásakor és felülvizsgálatakor minden esetben az alapszabályoknak megfelelően kell eljárni.

Ezen alapszabályok a következők:

- kiemelt felhasználói jogosultságok halmozását minden esetben kerülni kell, egy azonosító lehetőleg ne kötődjön egyszerre több kiemelt jogosultsággal rendelkező csoporthoz; rendszeradminisztrátori azonosítókat csak az Informatikai szervezet munkatársai kaphatnak, ettől eltérni csak az Informatikai igazgató engedélyével lehet;

- rendszeradminisztrátori azonosítókat minden esetben egyedi felhasználókhoz kell rendelni és tulajdonosát egyértelműen azonosítani kell;
- a ritkán használt, magas jogosultságú azonosítókat a használat idején kívül fel kell függeszteni és csak a használat idejére aktiválni, majd használat után újra felfüggeszteni;
- Az adminisztrátori azonosítók jelszavait minimum 90 naponta meg kell változtatni, a jelszó hossza minimum 12 karakterből kell, hogy álljon és vegyesen kis és nagybetűket, számokat és írásjeleket is tartalmazzanak;
- a rendszerazonosítók (system account) jelszavait elzárva lezárt borítékban az Informatikai Igazgatóságnál, vagy a területileg illetékes informatikai vezetőnél páncélszekrényben kell tárolni és minden változtatás esetén, illetve évente kötelezően cserélni kell;
- a rendszerazonosítókat csak alkalmazások használhatják belépésre, felhasználói azonosítóként nem használhatók;
- a beépített, lokális rendszeradminisztrátori azonosítókat át kell nevezni, jelszavukat elzárva, lezárt borítékban az Informatikai Igazgatóságnál, vagy a területileg illetékes informatikai vezetőnél páncélszekrényben kell tárolni.

5.4.5.4 Jogosultságok kiosztására és nyilvántartására vonatkozó szabályozások

A Felhasználók a munkakörükhöz szükséges jogosultságokkal kell rendelkezniük. Állandó jogosultságot kell igényelni az állandó munkakör ellátáshoz szükséges feladatok elvégzéséhez. Ideiglenes jogosultságot kell igényelni az eseti (pl. betegség, szabadság miatti helyettesítés és munkaerő átcsoportosítás) feladatok elvégzéséhez.

Az egyes szervezeti egység vezetők megtekintési jogosultsággal rendelkeznek az általuk irányított valamennyi terület adatállományához, információjához, ide nem értve a felhasználó személyes, magáncélú mappáihoz való hozzáférést.

Az Egyetem informatikai rendszereiben biztosítani kell, hogy – audit végrehajtás idején –az Adatvédelmi Felelősnek és egyéb ellenőrző szerveknek megtekintési jogosultsága legyen a vizsgálat alapján érintett szervezeti egység adatállományához.

A rendszerfejlesztési és informatikai üzemeltetési jogosultságok szétválasztásának meg kell történnie.

Az Informatikai Igazgatóság a jogosultságok kontrollálását és beállítását hajtja végre. Amennyiben az igényelt jogosultságok összeférhetetlenséget mutatnak (pl.: ellenőrző és jóváhagyó szerepkör egy ugyanazon felhasználó számára) a jogosultság nem adható ki. Ebben az esetben, e-mailben értesíteni kell az igénylőt és az Adatgazdát. A szervezeti vezető évente egyszer, február végéig köteles felülvizsgálni az irányítása alá tartozó felhasználói csoportok, felhasználók jogosultságait. A felülvizsgálatot követően intézkedési javaslatot kell tenni és a szükségtelen jogosultságokat vissza kell vonni.

5.4.5.5 Hitelesítés és jelszavak

Annak érdekében, hogy a jelszavakkal történő központi hitelesítés kellően biztonságos legyen, gondoskodni kell a megfelelő erősségű jelszavak használatáról:

- a jelszavak legalább 8 karakterből álljanak,
- vegyesen kis és nagybetűket, számokat és írásjeleket is tartalmazzanak,
- a felhasználói jelszavak legfeljebb 6 hónapig legyenek érvényesek,
- felhasználó esetében 5 próbálkozás után zárolja az azonosítót,
- rendszergazdák jelszavát 3 havonta cserélni kell,

- rendszergazda jelszavak minimum 12 karakterből álljanak,
- rendszergazda esetében 3 próbálkozás után zárolja az azonosítót,
- a technikai azonosítók a rendszergazdai azonosítókkal megegyezőek, viszont lejárati idejük 12 hónap,
- jelszó változtatásakor a megelőző 5 jelszó valamelyikét ne lehessen újból megadni,
- a kezdeti jelszót az első belépés alkalmával kötelezően meg kelljen változtatni.

A jelszavakat tartalmazó fájlokat (illetve ezeknek a jelszavakat tartalmazó részét) visszafejthetetlen (egyirányú) kódolással kell tárolni, ezekhez az állományokhoz hozzáférési jogosultságot csak az Informatikai Igazgatóság, vagy a Kari/Tömbigazgatóság Informatikai szervezet kijelölt dolgozói kaphatnak.

A jelszavakat tartalmazó fájlok sérülését, jogosulatlan hozzáférési kísérleteket az Informatikai Igazgatóság, vagy a Kari/Tömbigazgatóság Informatikai szervezet dolgozóinak azonnal jelentenie kell az Informatikai Biztonsági Felelősnek és az Informatikai Igazgatónak.

Tilos a jelszót:

- más tudomására hozni;
- más számára ismert vagy hozzáférhető helyen tárolni, így különösen a számítógépre (monitorra) ragasztani;

Javasolt a jelszavakat úgy megválasztani, hogy a jelszó ne az adott személyre jellemző és ezért könnyen kitalálható legyen.

A jelszavakkal kapcsolatos fenti szabályok megszegéséből, így különösen a más jelszavának megismerésével elkövetett esetleges visszaélés következményeiért a szabályokat megszegő felhasználó felelős.

Az informatikai rendszerekbe való bejelentkezés során, továbbá a jelszó megváltoztatásakor gondoskodni kell arról, hogy

- a jelszavak olvashatatlanul jelenjenek meg a képernyőn és
- titkosítva legyenek a hálózati adatátvitel során.

Az egyes rendszerekre vonatkozóan az egyes kiemelt felhasználói azonosítókra vonatkozó szabályokat a 5.4.5.2.1 számú fejezet tartalmazza.

A speciális felhasználókhoz (pl. kiemelt jogosultságú, közös használatú azonosítók) tartozó jelszavakra a következő- általánostól eltérő- szabályok vonatkoznak:

- a speciális felhasználók jelszavait lezárt borítékban az Informatikai Igazgatóság, vagy a Kari/Tömbigazgatóság Informatikai szervezeti vezetőjének a páncélszekrényében kell őrizni;
- speciális felhasználók jelszavához csak indokolt esetben lehet hozzáférni;
- a boríték felbontásáról minden esetben jegyzőkönyvet kell készíteni, megjelölve a speciális felhasználó igénybe vételének pontos okát és a felbontók személyét (lásd a 7.5 számú mellékletet);
- gondoskodni kell arról, hogy a szükséges műveletek elvégzése után a speciális felhasználó számára új jelszó kerüljön kiadásra és azt haladéktalanul, lezárt borítékban ismét a páncélszekrényébe kell helyezni.

5.4.5.5.1 Jelszó kiválasztás szabályai

A következő szabályok betartása a felhasználók felelősségi körébe tartozik:

- tilos a login nevet használni jelszóként bármilyen formában;
- tilos a saját vezeték vagy keresztnév használata;

- tilos a jelszót valamely funkcióbillentyűhöz hozzárendelni;

A jelszavakkal kapcsolatosan ajánlottak az alábbiak:

- ne legyenek könnyen kitalálhatóak (pl. 11111, 123456, qwerty, stb.)
- ne legyen szótárakban található címszó, mert sok kódfejtő program ezek és más gyakori jelszavak végigpróbálásával igyekszik feltörni a titkosítást;
- ne legyen a felhasználó személyéhez vagy környezetéhez köthető (pl. telefonszám, autórendszám, partner, gyermekek, háziállatok neve, stb.);
- ne legyen 8 karakternél rövidebb a jelszó;
- ajánlott számok, betűk és írásjelek keverékét használni.

5.4.5.6 Igénylés

Az Egyetemmel felhasználói jogosultságot igénylő jogviszonyt létesítő új munkavállaló adatait (aláírt közalkalmazotti kinevezés vagy munkaszerződés alapján) az Enberierőforrás-gazdálkodási Főigazgatóság Ügyfélszolgálatának a munkafelvételi eljárása alapján rögzítik, továbbá kitöltik a felhasználói jogosultság igénylőlapot.

Az adatok rögzítését, valamint a szervezeti egység vezetőjének jóváhagyását követően ezen felhasználói igénylő lapot e-mailben eljuttatják az adott szakterületi adatgazdához, aki a hozzáférés meghatározással továbbítja a Jogosultságkezelő felelősnek. Az Informatikai Igazgatóság végrehajtja a jogosultságok beállítását. A vezető adatgazdák és adatgazdák naprakész listáját az Adatvédelmi felelős tartja karban és teszi közzé alhonlapján.

5.4.5.7 Kiadás és érvényesítés

A Jogosultságkezelő felelős a jogosultságigénylő lap és az előzetes ellenőrzés (összeférhetetlen jogosultságok) végrehajtása után a felhasználóhoz:

- hozzárendel egy felhasználói azonosítót;
- megadja a felhasználó kezdeti jelszavát, aminek
  - meg kell felelnie a jelszavakkal kapcsolatos szabályoknak és
  - egyedinek kell lennie, nem használható rendszeresen ugyanaz a karaktersorozat,
- megadja a felhasználó számára igényelt jogosultságokat;

A Jogosultságkezelő felelős a felhasználói jogosultság igénylőlapon

- rögzíti a felhasználói azonosítót;
- dokumentálja az azonosító létrehozásának és jogosultságok beállításának időpontját.

Sem a Jogosultságkezelő felelős, sem más rendszergazda nem adhatja meg a jogosultságot, amennyiben megítélése szerint az igényelt jogosultságok nyilvánvalóan megsértik az informatikai biztonsági feladatkör-elhatárolási szabályok valamelyikét. A Jogosultságkezelő felelős – a felhasználói jogosultság igénylőlap másolatának továbbításával és az eljárás felfüggesztésének közlésével – tájékoztatja az IT biztonsági felelőst.

Az Adatvédelmi Felelős – szükség esetén az Adatgazdával és a felhasználó vezetőjével konzultálva – felülvizsgálja az egyedi igényt. Amennyiben megítélése szerint az igény egyedi feloldást igényel vagy a munkakör ellátásához szükséges jogosultsági beállítás szükséges, írásban kérvényezi az Informatikai Igazgatótól az engedélyezést, aki feladatként kiosztja Jogosultságkezelő felelősnek a jogosultság beállítását.

A jogosultságok beállítása szerepkörök szerint történik, amennyiben egy adott jogosultság megadásához nem áll rendelkezésre és nem szükséges létrehozni a rendszerben definiált szerepkört, az egyedi jogosultságot az Informatikai Igazgató engedélyével lehet beállítani.

5.4.5.8 Felhasználói azonosító módosítása

A felhasználói azonosító módosítását a felhasználó kezdeményezheti névváltozatáskor (pl. házasságkötés miatt) email vagy a GLPI rendszerben történő bejegyzés útján.

Felhasználói azonosító módosítást kezdeményezhet az Adatgazda és a Jogosultságkezelő felelős is az egyes rendszerek felhasználó azonosító konvencióinak szabványosítása miatt és/vagy új azonosítóképző szabályok bevezetésekor.

A felhasználói azonosító módosításakor a kiadás és érvényesítés szabályait kell értelemszerűen alkalmazni.

A felhasználó számára lehetővé kell tenni, hogy jelszavát bármikor önállóan megváltoztathassa. Elfelejtett jelszó esetén a felhasználó írásbeli kérésére új alap jelszót kell kiadni, melyre a jelszókezelési szabályok mérvadók.

5.4.5.9 Felfüggesztés, visszavonás

A felhasználói jogosultságot igénylő jogviszony megszüntetése esetén a munkahelyi vezető kezdeményezi a területileg illetékes informatikai vezető felé a jogosultság visszavonását, aki intézkedik az Informatikai Igazgatóságnál a jogosultság, illetve a felhasználói azonosító felfüggesztését (ezt a távozó munkatárs kilépő dokumentumán aláírásával igazolja).

A Jogosultságkezelő felelős a bejelentést követően felfüggeszti a felhasználó azonosítóit, visszavonja a rendszerekhez kapcsolódó felhasználói jogosultságokat, valamint gondoskodik az adott felhasználó e-mailjeinek más címre történő továbbításáról.

A visszavonási eljárás dokumentálására a kiadás és érvényesítés dokumentációs szabályait kell alkalmazni.

Az Egyetemről kilépő, felhasználói jogosultsággal rendelkező dolgozó elektronikus postafiókját, személyes könyvtárának, továbbá az általa használt számítógép(ek) merevlemezének tartalmának másolását követően a meghatározott türelmi idő lejárta után, visszafordíthatatlan módon törölni kell.

A jogosultságok felfüggesztésre kerülnek, ha

1. a jogosult:
   - munkaviszonya megszűnik/megszüntetésre kerül;
   - mentesítve lett a munkavégzési kötelezettség teljesítése alól;
   - munkakörének megváltozása nem indokolja a jogosultság fenntartását.
2. külsős jogosult esetén:
   - a megbízás időtartamának lejártával;
   - törvényben és a két fél között köttetett szerződés kizáró okainak bekövetkeztével;
   - felmondással;
   - külön törvényben meghatározott esetben.

5.4.5.10 Felhasználói hozzáférési jogosultságok felülvizsgálata

Rendszeres időközönként (de legalább évente egyszer) az Adatgazdáknak felül kell vizsgálniuk a felhasználói hozzáférési jogosultságokat. Az Adatgazdának a saját nyilvántartását évente felül kell vizsgálnia és változások esetén e-mailben értesíti a Jogosultságkezelő felelőst.

5.4.6 Hálózati szintű hozzáférés ellenőrzés

Az Egyetem számára megbízható hálózati kapcsolatnak számít a belső számítógépes hálózat, minden egyéb hálózat nem bizalmas hálózatnak számít, olyannak, amelyről azt kell feltételezni, hogy potenciális veszélyt jelenthet az informatikai biztonsága számára.

A belső számítógépes hálózatot felhasználási céljuktól függően logikailag szeparált alhálózatokba, VLAN-okba kell rendezni.

A tűzfalak konfigurációja során gondoskodni kell arról, hogy csak az engedélyezett kapcsolati lehetőségek legyenek elérhetők. Az engedélyezett kapcsolati lehetőségek listáját ACL-ek (Access Control List) formájában kell rögzíteni, melyet a Határvédelmi felelős tart nyilván, az Informatikai Biztonsági Felelős pedig 6 havonta ellenőriz.

Kapcsolati listát csak az Informatikai Igazgató engedélyével lehet felvenni, módosítani, törölni.

Az Egyetem és valamennyi partnere között gondoskodni kell a biztonságos, hiteles adatátvitelről, adatcseréről.

A bizalmas és a nem bizalmas hálózatokat csak az Egyetem tűzfalán keresztül lehet összekapcsolni.

Az Egyetemi hálózatban lévő számítógép egyedi külső hálózati kapcsolattal (pl.: modem, ADSL, Webstick) csak indokolt esetben, az adott szakterületi vezető kezdeményezése alapján az Informatikai Igazgató egyedi engedélyével rendelkezhet. Az eszköz telepítését, beüzemelést csak az Informatikai igazgatóság, vagy a területileg illetékes informatikai szervezet végezheti. Az ilyen számítógépeken az Egyetem belső számítógép-hálózatához való kapcsolódáskor nem engedélyezett a külső kapcsolat és a belső hálózat egyidejű használata.

Távoli felhasználók hozzáférésére jogosító engedély, kulcs maximálisan 2 évre adható ki.

Távoli felhasználók hozzáféréseit a tényleges (logikai) hozzáférésekkel meg kell feleltetni.

A távoli hozzáféréssel rendelkező felhasználók jogosultságait félévente felül kell vizsgálnia az Informatikai Biztonsági Felelősnek.

Az Egyetem számítógép-hálózata és külső hálózatok közötti kapcsolat során csak az engedélyezett kommunikációs protokollok továbbíthatók, minden egyéb továbbítása tilos.

Az Egyetem számítógép-hálózatában alkalmazható külső kommunikációs protokollok köréről – a határvédelmi felelős javaslatára az Informatikai Biztonsági Felelős véleményének figyelembe vételével – az Informatikai Igazgató dönt.

Az Egyetem számítógép-hálózata egy tartományos rendszer. Tilos olyan munkaállomást csatlakoztatni a hálózatra, amely

- nem bizalmas hálózati kapcsolattal is rendelkezik;
- nem tagja a megfelelő egyetemi tartománynak és nem rendelkezik jelen szabályzatban előírt védelmi mechanizmusokkal (pl. naprakész vírusvédelmi megoldás).

A Határvédelmi felelős nyilvántartást vezet:

- az engedélyezett protokollokról;
- a hálózati határvédelem informatikai biztonsági architektúra elemeinek beállításairól.

Az Egyetem számítógép-hálózatának vezeték nélküli hálózati szegmensein, valamint a nem bizalmas csatornán keresztüli bizalmas kapcsolat során titkosított adatkapcsolatot kell kialakítani.

A titkosított adatkapcsolat technikai specifikációját a Határvédelmi felelős készíti el, melyet az Informatikai Biztonsági Felelős véleményez és az Informatikai Igazgató hagy jóvá.

5.4.6.1 Behatolás érzékelés

Az Informatikai Biztonsági Felelős legalább kétévente egy alkalommal – független külső technikai szakértők igénybe vételével, az Egyetem informatikai munkatársának az állandó felügyelete mellett – ellenőrzött behatolási kísérletet végeztet.

A behatolási kísérlet idejéről és módjáról – az Informatikai Igazgató és az Informatikai Biztonsági Felelős kivételével – az Egyetem dolgozói és szerződéses partnerei nem szerezhetnek előzetesen tudomást.

A behatolási kísérletről részletes jelentést kell készíteni, amelyet a kísérlet lezárultával az Informatikai Igazgató és az Informatikai Biztonsági Felelős elemeznek és értékelnek.

5.4.6.2 A VPN-nel kapcsolatos biztonsági szabályok – távoli munkavégzés

A VPN kapcsolat létrehozásának célja az Egyetem dolgozói és a külső személyek számára a biztonságos távoli munkavégzés lehetőségének kialakítása.

5.4.6.2.1 VPN felhasználói jogosultságok kiadása, módosítása

A jogosultságok kiadása, a VPN technológián keresztül biztosított hozzáférés szintjének módosítása, a felhasználók hozzáférés menedzsmentje a jelen szabályzatban leírtak szerint történik, a normál hozzáférés biztosító jogosultságokkal megegyező módon.

Az Egyetemnél csak azok a munkavállalók használhatják a VPN-t, akik rendelkeznek az ehhez szükséges jóváhagyással. A jóváhagyás csak a VPN-nel kapcsolatos biztonsági szabályokat oktató tudásanyag elsajátítása után adható meg.

5.4.6.2.2 A VPN használata

Az Egyetem által biztosított VPN rendszert csak munkavégzés céljából, a felhasználó feladatkörében foglalt tevékenységek elvégzése során lehet használni. Az ettől eltérő használat szigorúan tilos.

A VPN kliens munkaállomást a VPN használat ideje alatt a felhasználó más személynek semmilyen formában nem engedheti át.

A távoli felhasználók tevékenysége naplózásra kerül és szükség esetén visszakereshető. Jelen szabályzat be nem tartásából eredő károkért az Egyetem a távoli felhasználót teszi felelőssé. Ilyen esetben az eseményt tartalmazó napló fájl bizonyító erejű.

A VPN rendszer kliens alkalmazását az Informatikai Szervezet rendszergazdája telepíti. A VPN rendszer telepítéséhez és használatához előzetesen szükséges, hogy a távoli felhasználó internet kapcsolattal rendelkezzen.

A VPN kliensprogram beállításait a felhasználó semmilyen módon és semmilyen esetben nem változtathatja meg. A program beállításait csak a Határvédelmi felelős módosíthatja.

A távoli felhasználó az Egyetem informatikai szolgáltatásaiból a levelezést és a fájlszerverekhez való hozzáférést és az Egyetem belső intranet hálózatát veheti igénybe. További IT szolgáltatások (pl. internet elérés) a távoli felhasználó számára nem áll rendelkezésre.

Minden esetben zárolni kell a munkaállomást, ha a felhasználó – akár rövid időre is – magára hagyja azt.

A távoli felhasználóknak nincs lehetőségük a VPN kapcsolattal egyidejűleg más internet kapcsolatot is létrehozni. A VPN kliens gépen személyes tűzfal program működik, melynek feladata, hogy a VPN kapcsolat esetén az Egyetem informatikai rendszereit védje az internet felőli támadásoktól. A tűzfalat kikapcsolni, vagy bármely beállítását megváltoztatni tilos.

5.4.6.3 Elkülönítés a hálózatokban

Az Egyetem informatikai rendszereinek biztonsága érdekében a hálózatot egymástól jól elkülöníthető logikai tartományokba kell osztani. Az egyes tartományok közti adatforgalmat tűzfal alkalmazásával szűrni kell.

Az adott helyen a megfelelő technológia kiválasztása és beüzemelése a Határvédelmi felelős feladata, melyet az Informatikai Igazgató hagy jóvá.

A tűzfalat úgy kell beállítani, hogy csak az előre meghatározott típusú, engedélyezett adatforgalom haladhasson át rajta.

5.4.6.4 Hálózati eszközök konfigurációs szabályai

Minden hálózati eszköz:

- a konfigurációs táblák és ACL-ek minden változásáról naplóbejegyzés készül és megőrzésre kerül;
- az eszközök zárt szekrényben vannak elhelyezve.

Gateway/tűzfal:

A szabályok leírását az Informatikai igazgatóság üzemeltetési utasítása tartalmazza.

5.4.7 Operációs rendszer szintű hozzáférés-ellenőrzés

5.4.7.1 Biztonságos bejelentkezési eljárások

Az operációs rendszerekhez való hozzáférést biztonságos bejelentkezési eljárásokkal kell ellenőrzés alatt tartani. A felhasználói munkaállomásokról csak biztonságos beléptetési folyamat során lehet elérni az Egyetem informatikai erőforrásait.

A biztonságos beléptetési folyamatnak az alábbi követelményeket kell teljesítenie:

- a rendszer a belépés előtt a lehető legkevesebb információt szolgáltassa a technológiáról;
- sikertelen belépés esetén a rendszer nem jelölheti meg, hogy a megadott adatok mely része hibás;
- limitálni kell a sikertelen belépések számát és a belépési folyamat maximális idejét.

A fenti követelmények teljesülését a rendszer paramétereinek beállításával kell megvalósítani. A beállítások megfelelősége az Informatikai Igazgató által megbízott munkatárs feladata és felelőssége.

5.4.7.2 Felhasználó azonosítása és hitelesítése

A felhasználók azonosítására és hitelesítésére vonatkozó eljárásokat a 5.4.5.5 Hitelesítés és jelszavak tartalmazza.

5.4.7.3 Kapcsolati idő túllépése

Az inaktív összeköttetéseket 15 perc időtartamú inaktivitás után bontani vagy zárolni kell.

Ahol ezt az alkalmazás nem automatikusan, alap beállításainál fogva hajtja végre, ott az Alkalmazás adminisztrátornak kell gondoskodnia a megfelelő beállításról.

5.4.8 Mobil számítógép használata és távoli munkavégzés

5.4.8.1 Mobil munkaállomások, egyéb mobil eszközök (Okostelefonok, USB drive, külső HDD, stb.)

A mobil eszközök felhasználói felelősek az általuk használt eszközök biztonságos használatáért:

- a nem nyilvános védelmi osztályba tartozó adatok kiszivárgása, elvesztése, megsérülése miatt bekövetkezett károk esetén;
- a jogosulatlan szoftverhasználatból eredő jogi következmények esetén;
- vírusok és más az Egyetem informatikai rendszerét veszélyeztető szoftverek, okozta károk esetén;
- lopás és az ebből származó károk esetén.

A mobil munkaállomásokon „nem nyilvános" biztonsági osztályba sorolt adatokat csak az Informatikai igazgatóság által biztosított eszközzel titkosított formában szabad tárolni, biztosítva ezzel a mobil munkaállomás illetéktelen kézbe kerülése esetén az adatok biztonságát.

5.4.8.2 Távoli munkavégzés

A távoli munka végzését a Kancellár rendelheti el vagy engedélyezheti. Az elrendelés mérlegelése során ki kell kérnie az Informatikai Biztonsági Felelős véleményét a technikai és informatikai biztonsági kérdések tekintetében.

A távoli munkavégzés technikai feltételeinek meghatározásakor a következő szempontokat kell figyelembe venni:

- távoli munkavégzéssel kapcsolatosan nyilvános hálózatokon kommunikációt csak titkosított formában szabad használni;
- távoli munkavégzés csak abban az esetben végezhető, ha a távoli munkavégzés műszaki feltételei lehetővé teszik az adatok és információk biztonsági osztályba sorolásának megfelelő kezelését és védelmét.

Az engedélyező felelős azért, hogy csak abban az esetben engedélyezze a távoli munkavégzést, amennyiben az nem veszélyezteti az Egyetem informatikai biztonságát, illetőleg a munkavégzés szempontjából az indokolt.

A távoli munkát végző felhasználó azért felelős, hogy a munkavégzés során minden előírást és szabályt betartson, valamint az Egyetem informatikai rendszerének biztonságát ne veszélyeztesse.

5.4.9 Biztonsági mentés

5.4.9.1 Mentési stratégia

Az Egyetem kezelésében, használatában lévő, elektronikus formában tárolt információkról rendszeres időközönként biztonsági mentéseket kell készíteni.

Biztonsági mentéseknek kell készülnie:

- az online elérhető (éles, tartalék, fejlesztői) adatbázisokról és fájlrendszer könyvtárakról;
- az offline elérhető (archivált) adatbázisokról és fájlrendszer könyvtárakról;
- szoftverek telepítőkészletéről.

Az egyes rendszerek üzemeltetőinek minden hatáskörükbe tartozó rendszerre mentési tervet kell készíteniük. A mentési terveknek tartalmaznia kell legalább az alábbiakat:

- mentések követelményei;
  - mentés tárgya, gyakorisága;
  - mentés elkészítésére rendelkezésre álló idő;
  - mentés visszatöltésére rendelkezésre álló idő;
- mentések típusai (teljes, inkrementális, szinkronizált);
- mentések állományai (mentett adattartalom);
- mentések példányszáma;
- mentések időpontjai;
- mentések megtartásának időtartama;
- mentések titkosítása.

Archiválást az Adatgazdák írásbeli kérésére, az általuk készített terv alapján kell végezni.

5.4.9.2 Mentések általános szabályai

Automatikus napi mentések esetén a mentésekért felelős rendszergazdának ellenőrizni kell annak helyességét, hiba esetén automatikus értesítést kell küldenie a Mentési felelős számára, melynek beállítása a felelős feladata.

A mentéseket tartalmazó adathordozók kezelését egyértelműen és visszakereshető módon nyilvántartatva kell megoldani. A mentéseket tartalmazó médiumokkal kapcsolatban az alábbi adatokat kell vezetni:

- a rendszer (alkalmazás) elnevezése;
- a mentés jellege;
- a mentés példánysorszáma és az összesen készült példányok száma;
- az adatállomány neve;
- a mentés időpontja.

A nyilvántartás a médián elhelyezett egyértelmű azonosító segítségével történik, amelyhez a kapcsolódó információkat elektronikus nyilvántartás rögzíti.

A mentések egyes példányait az alábbi helyszíneken kell tárolni:

- az első példányt abban a helyiségben kell tárolni, ahol a mentés történik, illetve abban a létesítményben, ahol a mentés visszatöltése elvégezhető;
- a második példányt (amennyiben készül) az adott rendszer tartalék központjában; annak hiányában az Egyetem egy erre kijelölt, az első példány tárolási helyétől kellő földrajzi távolságban lévő helyiségében.

A mentések adathordozóit kizárólag az informatikai helyiségeinek valamelyikében, szalagos egység esetén legalább 60 perces tűzállóságot garantáló, zárható szekrényben kell tárolni, egyéb optikai hordozó (DVD) esetén az erre a célra szolgáló gyári tároló egységben (pl.: Jukebox) kell őrizni.

A mentési eljárásokat úgy kell kialakítani, hogy a mentések második példánya minden rendszer esetén kerüljön kialakításra.

A mentési rendszert a fokozottan védett helyszínen (illetéktelen hozzáférés ellen megfelelő védelmet nyújtó szekrényben és/vagy helyiségben) kell elhelyezni, tűzoltó eszközzel ellátott helyiségben, melyben biztosíthatóak az előírt üzemi körülmények (mint például szünetmentes tápellátás, hőmérséklet).

5.4.10 Adathordozók kezelése

5.4.10.1 Az eltávolítható adathordozók kezelése

Adathordozón csak az Informatikai igazgatóság által biztosított eszközzel titkosítva tárolható nem nyilvánosnak minősített adat, információ.

A nagy mennyiségű adat rögzítésére és tárolására képes eszközök és számítógép-perifériák:

- CD (DVD) lemezek írására alkalmas eszközök;
- hordozható merevlemezegységek és más nagykapacitású mobil háttértárolók;
- a számítógéptől függetleníthető memóriák (pl. memory card), vagy ilyen funkciójú egyéb eszközök (pl. pendrive);

Otthoni munkavégzés és bármilyen más célból bármilyen adatot CD-n, elektronikus levélben vagy egyéb más módon (pl.: pendrive) az informatikai infrastruktúrájából kijuttatni csak az ***Adatgazda*** írásos engedélyével szabad. Az adatok kivitelét az Adatgazdának kell engedélyeznie, minden esetben írásos formában.

Az adatkivitelt engedélyező dokumentumot az ***Adatvédelmi Felelős*** szúrópróbaszerűen ellenőrzi.

5.4.11 Figyelemmel követés (naplózás és monitoring)

5.4.11.1 Naplózás általános szabályai

A különböző rendszerek naplóállományainak egységes értelmezhetőségének érdekében olyan naplózási architektúrát kell kialakítani, ami biztosítja, hogy:

- ahol csak technikailag lehetséges, a naplózás szerveroldalon történjen;
- a naplózás a lehető legkevesebb számú naplóállomány használatával történjen;
- automatikus mechanizmus gondoskodjon az egyes eszközök rendszerórájának szinkronizálásáról;
- automatizált megoldások támogassák a különböző naplóállományok összefésülését, feldolgozását és elemzését.

A naplózási architektúra dokumentációjáért az Informatikai Igazgató felelős.

Az egyes rendszerekben a rendszergazdák felelősek a naplózási beállítások naprakész állapotáért.

A naplóállományokhoz írási jogosultsággal csak az automatikus rendszerek férhetnek hozzá, a naplóállományokból a törlés nem engedélyezett, még akkor sem, ha a rendszergazda ezt technikailag meg tudja tenni.

Az egyes naplóállományokhoz, vagy azok részeihez olvasási jogosultsággal rendelkezhet (amennyiben munkaköre, feladata ellátásához arra szüksége van):

- a rendszerek alkalmazás Adminisztrátorai;
- az Informatikai Igazgató;
- az Informatikai Biztonsági Felelős;
- a Kari/Tömbigazgatóság Informatikai szervezeti vezetője.

A naplóállományokhoz való hozzáférési jogosultságokat az Informatikai Igazgató hagyja jóvá, a rendszergazdák dokumentálják, az Informatikai Biztonsági Felelős ellenőrzi.

5.4.11.2 Naplózandó események

Az Egyetem informatikai rendszerében automatikus naplót kell vezetnie az informatikai rendszer biztonsági szempontból lényeges tevékenységéről.

A naplózásnak ki kell terjednie:

- az IBSZ-ben meghatározott eseményekre;
- az arra felhatalmazással rendelkezők által meghatározott, ideiglenesen naplózandó eseményekre.

Ideiglenes naplózást rendelhet el a naplózandó esemény és a naplózás időtartamának és céljának pontos megjelölésével, írásban:

- az Adatgazda;
- a szakterületi vezető.

A naplózandó események köréről az Informatikai Igazgatóság, vagy a Kari/Tömbigazgatósági Informatikai Szervezet arra kijelölt munkatársai vezetnek naprakész nyilvántartást, melyről tájékoztatják az Informatikai Biztonsági Felelőst.

A naplózandó események nyilvántartása alapján a rendszer fejlesztői és a rendszergazdák készítik el az egyes rendszerek naplózási beállításait tartalmazó dokumentációt.

A naplózandó események áttekintése része az IBSZ rendszeres felülvizsgálatának.

Az Informatikai Biztonsági Felelős negyedévente ellenőrzi, hogy az egyes rendszerek naplózási beállításai megfelelnek-e a naplózási események nyilvántartásának.

5.4.11.3 Események meghatározása

Az automatikusan készülő naplókban rögzíteni kell legalább az alábbi eseményeket:

- a rendszerriasztásokat, meghibásodási jelentéseket;
- a rendszer leállítását és újraindítását;
- a rendszerben fellépő hibákat;
- felhasználók felvételét, törlését, felfüggesztését;
- a tranzakciók végrehajtását (fokozottan, illetve kiemelten védett rendszerek esetén);
- a felhasználó bejelentkezést vagy sikertelen bejelentkezési kísérleteket;
- naplózási funkciók indítását és leállítását;
- naplóállomány létrehozását, törlését; (külön jegyzőkönyvben rögzítve);
- a rendszerdátum, -idő megváltoztatását;
- hardverkonfiguráció megváltozását;
- nyilvános hálózaton keresztüli kapcsolat:
  - létrehozása és bontása;
  - ellenoldali fele;
  - forgalom jellege;
  - továbbított vagy fogadott állomány neve, elérési útvonala;
- tűzfal rendszereken átmenő forgalmat.

Az eseményekhez a naplózó funkciónak hozzá kell rendelnie (amennyiben értelmezhető):

- a felhasználó azonosítóját;

- a számítógép azonosítóját (IP cím);
- a dátumát és időpontját;
- a munkaállomás, szerver vagy hálózati eszköz azonosítóját;
- a hozzáféréskor elért állományokat;
- sikertelen hozzáférési kísérletek számát;
- a használt programot.

Gondoskodni kell arról, hogy az összes (belső, külső és ideiglenes) felhasználó és az informatikai rendszereken (üzleti alkalmazások, informatikai környezet, rendszerműveletek, fejlesztés és karbantartás) végzett tevékenység egyedileg beazonosítható legyen, amennyiben ideiglenes naplózást rendel el az Adatgazda.

5.4.11.4 Biztonsági szempontból releváns események jelentési folyamata

Az Informatikai Igazgatóság arra kijelölt felelőseinek naponta ellenőriznie kell a naplóállományok bejegyzései alapján generált riasztásokat.

Incidens esemény bekövetkeztekor vagy ennek alapos gyanúja esetén az információrendszernek automatikusan riasztást kell generálnia és azt el kell küldenie az érintett rendszergazdának. Ilyen esemény bekövetkezése esetén a rendszergazdák feladata az Informatikai Biztonsági Felelős tájékoztatása.

Az informatikai biztonsági szabályok megsértéséről a rendszergazdának haladéktalanul jelentést kell tennie az Informatikai Igazgatónak. Az Informatikai Igazgató – az Informatikai Biztonsági Felelős bevonásával - kivizsgálja a biztonsági eseményt és annak eredményéről értesíti az érintett szervezetek, személyek vezetőit, valamint a Kancellárt, aki dönt a további eljárásról.

5.4.11.5 Eseménynaplók tárolása

Az eseménynaplók bizalmas információkat tartalmaznak az informatikai rendszerekről, valamint a felhasználók tevékenységéről. Bármilyen biztonsági incidens bekövetkezése esetén az eseménynaplók tartalmazzák azokat az információkat, melyek az utólagos vizsgálatok végrehajtásához szükségesek. Az eseménynapló tárolását ezért a következő szempontok figyelembe vételével kell megoldani:

- a naplóadatoknak sértetlenül rendelkezésre kell állniuk az esetleges elévülési időn belül;
- az éles környezetben minimum a teljes mentések közötti időtartamnak megfelelő naplóállományokat kell tárolni;
- biztosítani kell, hogy az adatokban keletkezésük után változtatást már ne lehessen végrehajtani;
- az információk bizalmasságára tekintettel, az adatok nem juthatnak illetéktelenek kezébe.

5.4.11.6 Naplóinformációk védelme

A naplózást végző berendezések beállításait csak az Informatikai Igazgató engedélyével lehet megváltoztatni.

A naplóban rögzített információkat védeni kell az illetéktelen hozzáféréstől. A naplóállományokhoz hozzáférés csak az Informatikai Igazgató jóváhagyása, és az Informatikai Biztonsági Felelős rendszeres (6 havonta történő) ellenőrzése mellett lehetséges.

A naplóban rögzített információkat megváltoztatni, törölni tilos.

5.4.11.7 Rendszergazdai és kezelői naplók

Mind a rendszergazdai, mind a biztonsági eseményeket nyomon kell követni az egyes alkalmazásokban. Gondoskodni kell a naplóállományok rendszeres mentéséről, felülvizsgálatáról, ez az Informatikai Igazgató által kijelölt megbízott informatikai munkatárs feladata.

A rendszergazdai naplókba való betekintéshez, a naplózó rendszer beállításainak megváltoztatásához az Informatikai Igazgató engedélyét kell kérni.

5.4.11.8 Biztonsági szereplők tevékenységeinek felügyelete

A rendszergazdák általi incidens – vagy annak gyanúja – esetén követendő eszkalációs eljárás megegyezik az általános incidens eszkalációs eljárással, kivéve, hogy arról a rendszergazdáknak tilos, viszont az Informatikai Biztonsági Felelősnek és az Informatikai Igazgatónak kötelező jelenteni.

5.4.11.9 Órajelek szinkronizálása

Az Egyetemen belül, illetve adott biztonsági tartományban működő valamennyi érintett információfeldolgozó rendszer órajelét szinkronizálni kell egy közösen megállapított pontos időforráshoz.

5.5 IT szolgáltatások biztonsága

5.5.1 Elektronikus levelezés

Az elektronikus üzenetekben foglalt információkat védeni kell a következő módon:

- védeni kell az üzeneteket a jogosulatlan hozzáféréstől, módosítástól;
- biztosítani kell a pontos címzést és célba juttatást;
- biztosítani kell a szolgáltatás megbízhatóságát és hozzáférhetőségét;
- elektronikus aláírások használatát az arra feljogosítottaknak biztosítani kell;
- külső nyilvános szolgáltatásokat kontroll alatt kell tartani;
- azok a munkavállalók, oktatók használhatják az elektronikus levelezést, akik rendelkeznek az ehhez szükséges jogosultsággal. A jogosultság az elektronikus levelezésre vonatkozó biztonsági szabályok megismerése után adható meg.

5.5.1.1 Logikai védelem – levélszűrés (spam)

Az elektronikus levelezés biztonságának megteremtését kéretlen levél (spam) szűrő rendszer alkalmazásával, valamint vírusvédelmi rendszer használatával kell biztosítani, melyet rendszeresen frissíteni kell.

A levelek kéretlennek (spam) minősítését a kéretlen levélszűrő rendszer alkalmazásával kell elvégezni. A nem gyanús leveleket változatlanul továbbítani kell a címzett számára. A rendszer által spamnek minősülő levelet karanténba kell helyezni, a visszatartott levélről a címzettet tájékoztatni kell. A levelezés szolgáltatásáért felelős rendszergazda a levelet a karanténban megtekintheti, kezelheti (karbantartás, törlés, továbbítás a címzett e-mail címére). A karanténban található kéretlen levelet a rendszernek a beérkezéstől számított egy hónap múlva automatikusan törölnie kell.

5.5.1.2 Az elektronikus levelezés használatának szabályai

Az elektronikus levelezés használata során az alábbi szabályoknak kell megfelelni:

- az Egyetem elektronikus levelező rendszere elsődlegesen belső- és külső kommunikációt szolgálja, a belső folyamatok támogatását szolgálja;
- az elektronikus levelezés használata során az Egyetem fenntartja a jogot arra, hogy indokolt esetben beletekintsen az elektronikus levelekbe, továbbá hogy a felhasználók levelezési forgalmát figyelje, illetve naplózza. A felhasználók tudomásul veszik, hogy az általuk küldött és fogadott elektronikus küldeményeket az Egyetem ilyen módon kezeli, és ennek elfogadásáról írásban nyilatkoznak (Dolgozói nyilatkozat);

- szükség esetén az elektronikus üzenetek bizalmasságának, illetve hitelességének, letagadhatatlanságának védelme érdekében – az adatok biztonsági osztályba sorolásának megfelelően – digitális aláírást és titkosítást kell alkalmazni;
- az Egyetem levelezési rendszeréből a szervezeten kívülre csak olyan információkat lehet kijuttatni, amelyek kijuttatására a felhasználó más csatornán keresztül is jogosult. Nyilvános levelezési fórumokon az Egyetemnél regisztrált levelezési cím feltüntetésével állást foglalni tilos;
- az Egyetemi levelezési cím feltüntetésével, illetve annak használatával – az Egyetem érdekeinek megvalósulását kifejezetten segítő feladatokat kivéve – semmilyen kereskedelmi, hirdetési tevékenységben nem lehet részt venni;
- az elektronikus levél mérete, a hozzá csatolható állománnyal együtt nem haladhatja meg a 20 MB-ot. 20 MB-nál nagyobb levelek a NIIF Intézet erre vonatkozó biztonságos szolgáltatásának segítségével küldhetők ki;
- az elektronikus levelezési rendszerbe beérkező leveleket minden esetben ellenőrizni kell, hogy nem tartalmaznak-e valamilyen, az Egyetem informatikai rendszerét veszélyeztető programot, kódrészletet, scriptet;
- az elektronikus levelezéshez kapcsolódóan tiltottak az alábbiak:
  - a hivatalosan támogatott elektronikus levelező szolgáltatáson (szerveren) kívül más elektronikus levelező szolgáltatást hivatalos levelezésre használni;
  - a hivatalosan támogatott levelező szoftveren kívül más programot használni;
  - az elektronikus leveleket úgy titkosítani, hogy a visszafejtésre használható kulcs nincsen az Egyetem birtokában;
  - az Egyetem hálózatát vagy szervereit nagy terjedelmű vagy nagy mennyiségű levél, illetve kéretlen kereskedelmi üzenetek küldésére használni (ha ilyenre van szükség, akkor azt az Informatikai igazgatóság bevonásával, más technológia alkalmazásával kell teljesíteni);
  - a levelezőrendszert reklám célra, politikai célra, mások munkájának hátráltatására, illetve az internet veszélyeztetésére használni;
  - az Egyetem hálózatát vagy szervereit kéretlen, nagy mennyiségű, illetve kereskedelmi elektronikus levelekre való válaszok begyűjtésére használni;
  - indokolatlanul nagyméretű üzeneteket vagy fájlokat küldeni;
  - láncleveleket vagy hasonló üzeneteket küldeni, illetve”hólabda” levelezést továbbítani (chain letters, olyan üzenet mely tartalmazza azt, hogy a címzettje azt küldje tovább másoknak);
  - a címinformáció hamisítása vagy a fejléc egyéb módon történő módosítása a feladó vagy a címzett személyazonosságának elrejtésére;
  - vírusos levelek szándékos küldése;
  - ügyviteli szempontból titkos, bizalmas, illetve belső információk jogosulatlan nyilvánosságra hozatala.
  - az e-mailben csatolt futtatható állományok megnyitása/letöltése a munkaállomásokra. (leggyakoribb fájl típusok: *.exe, *.bat, *.com, *.scr, *.cpl, *.hta, *.vbs);
  - az e-mailben csatolt tömörített állományok megnyitása/letöltése a munkaállomásokra. A tiltás vonatkozik a jelszóvédett és a nyílt állományokra egyaránt. (leggyakoribb fájl típusok: *.zip, *.rar, *.cab, *.arj, *.lzh, *.gz, *.tar, *.tgz), kivételt ez alól a munkavégzéshez szükséges állományok képeznek;
  - minden ismeretlen (az Egyetemen használt fájl formátumoktól eltérő) kiterjesztésű e-mailhez csatolt állomány megnyitása;
  - ismeretlen feladótól származó levelekben található csatolmány megnyitása;

- kéretlen levelek küldése, továbbítása;
- valótlan információt hordozó levelek tudatos továbbítása;
- az elküldött levél járulékos adatainak (például feladó e-mail címe, küldés időpontja) meghamisítása;
- a munkatársak e-mail címeinek másik félhez történő, jogosulatlan továbbítása;
- az Egyetemi e-mail címről magáncélú regisztrációt végrehajtani. Ennek megfelelően nem engedélyezett az üzleti célú levelezési listákra, fórumokra, hírcsoportokra feliratkozás egyetemi e-mail címmel;
- egyetemi postafiók tartalom automatikus továbbítása külső e-mail címre;
- privát postafiók tartalom automatikus továbbítás az Egyetemi e-mail címre;
- az Egyetem elektronikus levelezési címjegyzékének kiadása harmadik fél számára.

5.5.1.3 Elektronikus levelezési címek képzése

Az elektronikus levelezés során minden, használatra jogosított felhasználó egyedi elektronikus levelezési címet kap. A levelezés során használható címek képzése az alábbiak szerint történik (központi szervezeti egységek):

vezetéknév.keresztnév@semmelweis-univ.hu.

Az egyetem karain alkalmazott email címek domain neve tükrözi a kar angol nyelvű elnevezését:

- med.semmelweis-univ.hu
- pharma.semmelweis-univ.hu
- dent.semmelweis-univ.hu

Amennyiben két vagy több azonos nevű felhasználó kap levelezési címet, a névsorban hátrébb álló felhasználók címe megkülönböztető jelzést kap, a levelezőrendszer által megjelenített nevét pedig a szervezeti egységre utaló kiegészítéssel látjuk el.

5.5.2 Az interneten megtalálható információ használata

A bizalmas (egyetemi hálózat) és a nem bizalmas (pl.: internet) hálózatokat csak az Egyetem tűzfalán keresztül lehet összekapcsolni.

Az Egyetem rendszerében az internet használat az ügyviteli folyamatainak támogatására, illetve azokhoz kötődő információáramlásra szolgál. Az internet használata során az Egyetem fenntartja a jogot arra, hogy a felhasználók internet-forgalmát figyelje, illetve naplózza. A felhasználók tudomásul veszik, hogy az általuk látogatott oldalakra vonatkozó információkat az Egyetem ilyen módon kezeli, és ennek elfogadásáról írásban nyilatkoznak (Dolgozói nyilatkozat).

5.5.2.1 Az internet használata során követendő magatartás

A szerzői jogokra, szabadalmakra és egyéb szellemi tulajdonra vonatkozó szabályok alkalmazása az internetre is vonatkozik. Ebből kifolyólag az alkalmazottak kötelesek:

- az internetről származó anyagok felhasználása előtt beszerezni a forrástól az erre vonatkozó engedélyt;
- hivatkozáskor a forrást azonosítani;
- az Egyetemmel kapcsolatos információk egyetemi honlapon történő közzétételéről a Honlap szabályzatban a Kancellár által kijelölt személy gondoskodik, ettől a felhasználónak eltérni tilos.

Az internet-hozzáféréssel rendelkező alkalmazottak csak közvetlenül az Egyetemen végzett munkájukkal kapcsolatosan tölthetnek le fájlokat. A letöltött fájlok kizárólag engedélyezési feltételeik szerint használhatók.

Az internet hozzáféréssel rendelkező munkatársak nem használhatják az Egyetem internet kapcsolatát szórakoztató szoftverek vagy játékok letöltésére, valamint internetes játékokra. Csak az oktatáshoz, munkavégzéshez szükséges képek és videók letöltése megengedett.

5.5.2.2 Speciális szakmai helyek

Az Egyetem munkatársai részére – a források megbízhatóságára vonatkozó szabályok betartásával – biztosítja a munkavégzésükhöz szükséges szakmai anyagokat tartalmazó weblapok elérésének lehetőségét. A térítés ellenében látogatható weboldalak elérésére vonatkozó igényeket az igénylő munkatárs vezetőjének kell jóváhagynia. A jóváhagyott igényről feljegyzés formájában értesíteni kell az Informatikai Igazgatót, aki intézkedik a megfelelő technikai támogatásról.

5.5.2.3 Tiltott tevékenységek az internet hálózaton

- minden olyan tevékenység, ami a hatályos jogszabályokba ütközik, különös tekintettel az alábbiakra: mások személyiségi jogainak megsértése; tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték); a szerzői jogok megsértése; szoftver szándékos és tudatos illegális terjesztése;
- profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése;
- 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, trójai programok, hacker eszközök, férgek);
- hálózati forgalom lehallgatása, megfigyelése, kivéve, ha ez az adott munkakörhöz kapcsolódik;
- az internetről a legálisan hozzáférhető programok letöltése, kivéve, ha arra vezetői engedély vonatkozik;
- a szolgáltatások blokkolását, lassítását célzó támadás, az azonosítási, illetve biztonsági intézkedések megsértésére irányuló kísérlet, valamint az egyéb azonosítóhoz, számítógéphez vagy hálózathoz történő illetéktelen hozzáférési kísérlet;
- a felhasználói azonosítóval csak annak tulajdonosa jelentkezhet be. Az adatokhoz történő hozzáférés érdekében választott jelszó titkosságának megőrzése a felhasználó felelőssége. Egy adott azonosítóról folytatott tevékenységért mindig annak tulajdonosa felel, az azonosító kölcsönadása nem megengedett, így felelősségre vonás esetén ez az indok nem elfogadható;
- minden felhasználó kizárólagosan a munkájához kötődő, a munkavégzését segítő oldalak látogatására jogosult, ezért tilos továbbá:
  - sértő, társadalomra veszélyes, jó erkölcsbe ütköző szöveg, kép, ábra vagy egyéb formájú információ publikálása, letöltése;
  - az interneten elérhető szolgáltatást, bármilyen törvényt, szabályozást, szabványt, nemzetközi egyezményt vagy díjszabást sértő módon használni;
  - a felhasználónak az internetes forgalmát titkosítani úgy, hogy a visszafejtő kulcs nincsen az Egyetem birtokában;
  - bármelyik számítógép-hálózat biztonságát rombolni, illetve gyengíteni, más felhasználó jogosultságát jogosulatlanul használni;
  - bármilyen internetes végpontra, illetve hálózati eszközre jogosulatlanul csatlakozni, vagy ezzel próbálkozni;

- bármely végpont működését megzavarni vagy azt az Egyetem hálózatáról vagy annak igénybevételével szándékos túlterhelni (DOS támadás);
- egyetemi tulajdonú eszközöket internetes számítógép erőforrás megosztásokhoz (például: gyógyszerkutatás, SETI számításokhoz, RSA törésekhez) használni;
- a hálózatot a szerzői jogvédelem alá eső anyagok átvitelére használni (még közvetetten is), ha az átvitel során mások szerzői joga sérül;
- tilos kikapcsolni a munkaállomásra telepített biztonsági szoftvereket, eszközöket;

- nem látogathatóak olyan oldalak, melyek megtekintése vagy használata a hivatalos egyetemi tevékenységgel össze nem egyeztethető:
  - az Egyetem érdekeit sértik;
  - rasszista tartalmúak;
  - erotikus oldalak;
  - warez oldalak;
  - terrorizmust támogató oldalak;
  - chat oldalak;
  - fegyverekre vonatkozó információkat tartalmaznak;
  - kábítószerekre vonatkozó információkat tartalmaznak;
  - phishing (adathalász) oldalak;
  - internetes fogadási oldalak, szerencsejáték oldalak;
  - játék oldalak;
- tilos továbbá:
  - az internet segítségével futtatható állományok letöltése a munkaállomásokra. (leggyakoribb fájl típusok: *.exe, *.bat, *.com, *.scr, *.cpl, *.hta, *.vbs);
  - bármely alkalmazás letöltése, legyen az licenc köteles, shareware (próbaverziójú), vagy freeware (ingyenesen használható alkalmazás), ez alól csak az Informatikai igazgatóság által fenntartott kompatibilitási listán szereplő szoftverek kivételek;
  - az internet segítségével tömörített állományok letöltése a munkaállomásokra. Tiltás vonatkozik a jelszóvédett és a nyílt állományokra egyaránt (leggyakoribb fájl típusok: *.zip, *.rar, *.cab, *.arj, *.lzh, *.gz, *.tar, *.tgz), kivétel ez alól a munkavégzéshez szükséges állományok képeznek;
  - média állományok letöltése, kivétel a szorosan munka tevékenységhez kötődő fájlok;
  - az internet segítségével egyetemi tevékenységi-, vagy érdekkörbe tartozó állományok, információk kijuttatása, külső kiszolgálókra való feltöltése, illetve bármilyen módon történő megosztása;
  - böngészés közben tilos bármilyen böngésző bővítés letöltése direkt módon és felugró ablakon keresztül egyaránt. Leggyakrabban felmerülő kiegészítések:
    - JAVA futtató környezet letöltése/frissítése;
    - ActiveX futtató környezet letöltése/frissítése;
    - különböző médialejátszók letöltése/frissítése (például: Windows Media Player, BSPlayer, QuickTime, FlashPlayer, ShockWave Player);
    - MS XML frissítések letöltése/frissítése;
    - eszköztárak (Toolbar-ok) letöltése/frissítése;
    - chat alkalmazások és kiegészítéseik letöltése/frissítése;

- automatizált letöltő alkalmazások, kliensek használata (csak az Informatika számára megengedett a rendszerek frissítéséhez);
- minden olyan alkalmazás letöltése/telepítése/használata, amely alkalmas interneten keresztül történő erőforrás megosztásra;

- Az informatikai üzemeltető személyzet által kialakított megoldásokon kívül tilos irodai munkaállomásokon külső frissítő szerverről való frissítés (például: operációs rendszer-, vírusvédelmi rendszer-, alkalmazás-frissítések).

5.5.2.4 Tiltott internetes oldalak engedélyeztetése

A tiltott oldal nem látogatható vagy nem jelenik meg helyesen. Az Egyetem lehetőséget nyújt arra, hogy amennyiben egy weblap a munkához szükséges, annak elérését külön engedélyezzék.

Az engedélyezést kérni email-en vagy a GLPI alkalmazáson keresztül a prioritás és az elérni kívánt pontos cím megjelölésével lehet.

5.5.2.5 Fájlkezelés / címtárkezelés

- a fájlok kezelése során törekedni kell, hogy a tároló rendszerben az adott fájlnak minél kevesebb példánya tárolódjon;
- nyilvános mappában tilos elhelyezni „fokozott”, vagy ennél magasabb minősítésű dokumentumot;
- a felhasználóknak tilos megosztani az egyéni mappájukat, illetve a saját helyi tárolójuk bármely mappáját;
- az olyan fájlok megosztása, amelyek nem az egyetemi folyamatokkal vannak összefüggésben, az egyetemi közös tárterületeken nem lehetséges;
- a szervezeti és az egyéni mappákban magánjellegű fájlok tárolása nem megengedett.

5.5.3 Webszolgáltatás

Az egyetemi honlap tartalmának (www.semmelweis.hu) módosításának és karbantartásának felelőse a Kommunikációs és Rendezvényszervezési igazgatóság, a honlap szerkesztésével kapcsolatos feladatokat külön szabályzat rendezi.

Az Informatikai Igazgatóság felel a portál elérhetőségéért, az informatikai szolgáltatások rendelkezésre állásáért. A portál speciális információinak naprakészen tartása az adott terület tartalomfelelősének a feladata.

5.6 Működés-folytonosság és katasztrófa-elhárítás menedzsment

Az Működés-folytonossági Terv tartalmazza a működés--működés-folytonosság fenntartó eljárás leírását, a hozzá kapcsolódó dokumentumokat, a szakrendszerekhez tartozó informatikai eszközök helyreállítási terveit.

6. BIZTONSÁGI SZINT MÉRÉSE, MONITOROZÁSA

6.1 Biztonsági szint mérésének feltétele

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

6.1.1 A mérés függetlenségének biztosítása:

A méréseket a felhasználóktól, az informatikai üzemeltetési és a fejlesztési területtől független személy végezze.

A méréseket a mérésben érintettek előzetes értesítése nélkül kell végrehajtani, hogy ne tudjanak felkészülni, illetve ne tudják befolyásolni a mérés eredményét.

6.1.2 A mérés hitelességének biztosítása

Az IT rendszer elemeinek időszinkronizálása szükséges a naplófájlok megbízható kiértékeléséhez.

A biztonsági szint mérésével megbízott személy rendelkezzen a naplófájlok eléréséhez szükséges jogosultságokkal.

Biztosítani kell a naplófájlok sértetlenségét. A naplófájlokhoz csak olyan személyeknek legyen hozzáférése, akiknek a munkájához a hozzáférés feltétlenül szükséges.

A fenti feltételrendszer kialakításáért az Informatikai Igazgató a felelős.

6.2 A biztonsági szint mérésének eszközei és módszerei

6.2.1 A technikai szintű auditok

A biztonság szintje mérésének egyik leghatásosabb módszere a technikai audit jellegű felmérés:

- az IT rendszer internet felőli sérülékenységeinek vizsgálata;
- az IT rendszer intranet felőli sérülékenységeinek vizsgálata.

Technikai szintű auditot az Egyetemnél kétévente, vagy egy új rendszer bevezetésekor a fenyegetettségek felmérésével egy időben kell elvégezni, a végrehajtásért az Informatikai Biztonsági Felelős és az Informatikai Igazgató együttesen felelős.

6.2.2 Működés-folytonossági és katasztrófa-elhárítási tesztek

A működés-folytonosság biztosítása érdekében visszaállítási- és a katasztrófa-elhárítási terveket évente, elemenként tesztelni kell. A tesztelés eredményét a tervezésbe, illetve a szóban forgó eljárásokba (mentés, karbantartás, stb.) vissza kell csatolni.

A működés-folytonossági eljárásrendet a ténylegesen bekövetkező incidensek esetén lehet ’élesben’ alkalmazni, az itt fellelt hiányosságokat, a megszerzett tapasztalatokat a tervekbe vissza kell csatolni (a tanulságok összegyűjtése az incidens-jelentések részévé teendő).

A tesztelés megtervezését, koordinálását az Informatikai Igazgató végzi, a tesztek végrehajtásáért az informatikai szolgáltatások rendszergazdái felelősek.

6.2.3 Az informatikai rendszer monitorozása

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

- határvédelmi incidensek, és hálózati illegális tevékenység. Felügyeletet ellátó személy: Határvédelmi rendszergazda;
- vírusvédelmi incidensek, vírusvédelmi rendszerek állapota (vírus DB és motor verziója eszközönként). Felügyeletet ellátó személy: Vírusvédelmi rendszergazda;
- jogosultság kezelési incidensek. Felügyeletet ellátó személy: Jogosultságkezelésért felelős rendszergazda;
- mentési feladatok sikeres/sikertelen végrehajtása. Felügyeletet ellátó személy: Mentésért felelős rendszergazda;
- külső felhasználók tevékenységei, távoli elérések naplózása. Felügyeletet ellátó személy: Informatikai Biztonsági Felelős;
- rendszergazdák tevékenységei. Felügyeletet ellátó személy: Informatikai Biztonsági Felelős
- biztonsági riasztórendszerek naplózása (UPS, tűzvédelem, stb.). Felügyeletet ellátó személy: Informatikai Biztonsági Felelős.

6.3 A mérési adatok feldolgozása, visszacsatolása

Az informatikai biztonság szempontjából kritikus pontokon mérési és ellenőrzési rendszert kell bevezetni. A mérések eredményéről az Informatikai Biztonsági Felelősnek évente írásban be kell számolnia az Informatikai Igazgatónak, annak érdekében, hogy a központi rendszereket érintő esetlegesen felmerült kockázatok kezelése időben megtörténjen.

A minimálisan szükséges kontroll pontok az alábbiak:

Mérendő terület	Mérendő mennyiség	Beszámolóban szerepel
IT tevékenység	Szerverszobába való belépések naplózása	Nem
	Rendszergazdai hozzáférések (logikai) naplózása	Nem
Illegális IT tevékenység	Észlelt behatolási kísérletek száma	Igen
	Nem egyetemi dolgozó által végzett tevékenység teljes körű naplózása	Nem
Vírusvédelem	Beérkezett vírusok száma / Hatástalanított vírusok száma (statisztikai információ)	Igen
	Nem internetről beérkezett vírustámadások száma, ezek módja	Igen
Mentési rendszer	A teszt-visszatöltések eredményei	Igen
Rendelkezésre állás	Rendszerek kieséseinek száma, ezek oka, időtartama, javítási költsége	Igen
Kapacitásinformációk	Kritikus rendszerekre vonatkozó teljesítményadatok jelentős változása	kivonat

Mérendő terület	Mérendő mennyiség	Beszámolóban szerepel
	Tárolási kapacitásokra vonatkozó információk	Igen
Ellenőrzések eredményei	Feltárt hiányosságok, és azok megszüntetésére vonatkozó intézkedések	Igen
Oktatás helyzete	IT biztonsági oktatásban részt vett személyek száma, a beszámoltatás eredményei	Igen
IT biztonsággal kapcsolatos fegyelemsértések	IT biztonságot megsértő személyekre vonatkozó fegyelmi statisztikák	Igen
Az IT biztonsági rendszer összesített értékelése	Az IT rendszer szintjére vonatkozó megállapítások, javaslatok	Igen
Javaslatok	Javaslatok kidolgozása a hiányosságok megszüntetésére, a biztonsági szint emelésére	Igen

6.4 Ellenőrzési irányelvek

Az informatikai biztonság szinten tartása és növelése érdekében megfelelő kontrollokat kell kialakítani. A kontrollok kialakításánál elsődlegesen azt kell figyelembe venni, hogy azok által az informatikai biztonság szintje mérhető legyen.

Az Informatikai Biztonsági Felelős az Informatikai Igazgatóval együttműködve határozza az ellenőrzések területeit, és minden területhez külön-külön meg kell fogalmazni az ellenőrzési célkitűzéseket, illetve azt, hogy ki végzi el az ellenőrzéseket. A célkitűzések az alábbiak lehetnek:

- törvényeknek, belső szabályozásoknak történő megfelelés;
- nem kívánatos felhasználói tendenciák visszaszorítása;
- nem kívánatos üzemeltetési tendenciák visszaszorítása;
- a felhasználók informatikai biztonsági tudatosság szintjének emelése.

Az ellenőrzési célkitűzések ismeretében meg kell jelölni az ellenőrzés eszközeit (dokumentumok, naplók, szoftverek, adatok, amelyek a biztonsági rendszerről hiteles képet tudnak adni), azok tartalmi követelményeit. Az ellenőrzés eredményét minden esetben ki kell értékelni, és a megfelelő következtetéseket le kell vonni, illetve vissza kell csatolni a biztonsági folyamatra. Szükség esetén felelősségre vonást kell kezdeményezni. Az ellenőrzéseket dokumentumok, dokumentációk, személyes beszámoltatás és helyszíni szemlék alapján lehet végrehajtani.

Az informatikai biztonsággal kapcsolatos ellenőrzések területei az alábbiak lehetnek:

- **megfelelőségi vizsgálat**. Célja felderíteni, hogy az Egyetem rendelkezik-e a törvényi előírásokban meghatározott személyi, eljárási, tárgyi feltételekkel, és azok megfelelően dokumentáltak-e;
- **az informatikai biztonság szintjére vonatkozó vizsgálat**. Célja felderíteni, hogy az informatikai biztonság szintje megfelel-e a meghatározott védelmi szintnek;
- **az informatikai biztonsági szabályok betartásának ellenőrzése**. Célja felderíteni, hogy az informatikai biztonsági szabályokat ismerik-e, illetve betartják-e. Ez az ellenőrzés az informatikai biztonság egy-egy területére is leszűkíthető.

Az ellenőrzések során elsősorban az alábbiakat kell vizsgálni:

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

6.5 Biztonsági rendszerek felülvizsgálata

Az Informatikai biztonsági rendszert, illetve annak egyes elemeit rendszeresen felül kell vizsgálni. A szükséges felülvizsgálatok az alábbiak:

A felülvizsgálat tárgya	A felülvizsgálat gyakorisága
Kockázatfelmérés	legalább 2 évente
Informatikai Biztonsági Szabályzat	legalább 1 évente
Informatikai biztonsági folyamatok	legalább 2 évente
Határvédelem	legalább 2 évente
Vírusvédelem	legalább 1 évente
Mentés, archiválási rend	legalább 2 évente
Informatikai biztonsági oktatás	legalább 2 évente

7. MELLÉKLETEK

7.1 Kapcsolódó jogszabályok listája

7.1.1 Kapcsolódó külső szabályozások

- 2011. évi CCIV. törvény a felsőoktatásról
- 1997. évi CLIV. törvény az egészségügyről
- 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Avtv.)
- Az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK Irányelve a személyes adatok kezelése vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról.
- 331/A/2001. számú adatvédelmi biztosi állásfoglalás: a munkáltató csak az érintett hozzájárulásával tekinthet be a munkavállaló munkahelyi e-mail címén történő levelezésébe.
- 570/A/2001. számú adatvédelmi biztosi állásfoglalás: a munkáltató csak akkor ismerheti meg a munkavállaló internet-használatával kapcsolatos adatait, ha előzetesen felhívta a figyelmét az ezzel kapcsolatos korlátozásra és az ellenőrzés lehetőségére.
- 2001. évi XXXV. törvény az elektronikus aláírásról
- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.
- 2015. évi CXLIII. törvény (kbt.) a közbeszerzésekről.
- 171/2010. (V.13.) Kormányrendelet a kormányzati informatika koordinációjáról és a kapcsolódó eljárási rendről
- 2012. évi I. törvény a munka törvénykönyvéről
- 2012. évi C. törvény a Büntető Törvénykönyvről
- 2013. évi V. törvény a Polgári Törvénykönyvről

7.1.2 Kapcsolódó belső szabályozások

- Informatikai igazgatóság szervezeti ügyrendje;
- IT üzemeltetési és hálózati szabályzat;
- Távközlési szabályzat;
- Neptun szabályzat;
- Kockázatkezelési szabályzat;
- Kritikus alkalmazások üzemeltetési utasításai;
- Adatvédelmi szabályzat;
- Vagyonvédelmi és Rendészeti szabályzat;
- Tűzvédelmi szabályzat;
- Vagyonvédelmi szabályzat;
- Adatgazdai szabályzat;
- Honlap szabályzat.

7.1.3 Kapcsolódó szabványok és ajánlások

- MSZ-ISO/IEC 27001:2006;
- MSZ ISO/IEC 17799:2006;
- Magyar Informatikai Biztonsági Ajánlások (Közigazgatási Informatikai Bizottság 25. számú Ajánlása);
- a MABISZ biztonságtechnikai ajánlása B/I. pontja szerinti teljes mechanikai, fizikai védelem;
- a MABISZ biztonságtechnikai ajánlása C/I/2. pontja szerinti részleges elektronikai jelzőrendszer;
- a MABISZ biztonságtechnikai ajánlása C/II. pontja szerinti beléptető rendszer.

7.2 Felhasználói Informatikai Biztonsági Nyilatkozat (dolgozói nyilatkozat)

7.2.1 A nyilatkozat célja

A nyilatkozat célja a felhasználókban tudatosítani, hogy munkájuk során a lehető legnagyobb gondossággal járjanak el az IT rendszerekben tárolt információk használatakor annak érdekében, hogy az adatok bizalmassága, sértetlensége és rendelkezésre állása a felhasználó szándékos, vagy gondatlan magatartásából ne sérüljön, illetve a felelősségük számon kérhető legyen.

7.2.2 Felelősségi nyilatkozat

Név:....., munkavállaló (születési hely, idő:……..., Lakcíme: ……, Anyja neve: ….……), a Semmelweis Egyetem (továbbiakban: Egyetem) munkavállalója kijelentem, hogy a munkaköröm ellátásához szükséges informatikai biztonsági oktatáson részt vettem, a vonatkozó szabályzatokat megismertem, és a feladataim ellátásához szükséges informatikai biztonsági ismeretekkel rendelkezem.

Tudomásul veszem, hogy az Egyetem informatikai rendszerében kezelt szoftverek, fájlok, egyetemi levelek az Egyetem tulajdonát képezik, így azokat az Egyetem kijelölt szakemberei ellenőrizhetik (lásd Informatikai Biztonsági Szabályzat, továbbiakban: IBSZ).

Tudomásul veszem, hogy a munkavégzéshez az Egyetem által biztosított munkaeszközöket használhatom és az általam használt informatikai eszközökön kizárólag az egyetemi munkakörömmel összefüggő adatokat tárolhatok.

7.2.3 Kötelezettségeim

Az Egyetem információs rendszereinek használata során birtokomba kerülő üzleti titkokat és személyes adatokat (Személyes adatok védelméről szóló 2011. évi CXII. törvény) megőrzöm és a vonatkozó belső szabályzatokat betartom.

Amennyiben munkakörömhöz szerzői jogi oltalom alá eső szoftver(ek) fejlesztése tartozik és a szoftvert valóban a munkaviszonyból folyó kötelességem teljesítése során, vagy az Egyetem rendelkezése alapján hoztam létre, úgy az Egyetem jogosult a szerzői jogi oltalom alá eső szoftver(ek) minden gazdasági jogosultságának gyakorlására. Az Egyetem e jogai a munkaviszony megszűnése után is, - a szerzői jogi védelem időtartamára – fennmaradnak. (Szerzői jogról szóló 1999. évi LXXVI. Törvény)

Kijelentem, hogy az IBSZ-ben leírtakat megértettem és azokat magamra nézve kötelezőnek elismerem. Tudomásul veszem, hogy amennyiben a jelen „Felhasználói Nyilatkozatban” leírtakat megszegem, úgy munkajogi-, kártérítési- és büntetőjogi felelősségem áll fenn.

Budapest , 20…..... . ..... hó ……. nap

.....

Munkavállaló

7.3 Külső partnerekkel kötendő titokvédelmi megállapodás

Alulírott

Név:

Anyja neve:

Szül. hely és idő:

Személyi azonosító okmány száma:

Lakcím:

kijelentem, hogy a Semmelweis Egyetem (SE) Informatikai Biztonsági Szabályzatának külső partnerekre vonatkozó részeit megismertem, azokat magamra nézve kötelezőnek ismerem el.

A SE-n végzett munkám teljesítése során megismert, az SE tevékenységéhez kapcsolódó minden olyan adat, tény, információ, stb. (a továbbiakban: adat) amelynek a nyilvánosságra hozatala, illetéktelenek által történő megszerzése vagy felhasználása az SE vagy az SE által gondozott betegek jogszerű személyes-, pénzügyi-, gazdasági- vagy biztonsági érdekét sértené vagy veszélyeztetné – és amelyet jogszabály egyébként más titokfajtának nem minősít - az SE üzleti titkát képezik. A tudomásomra jutó titkot a vonatkozó jogszabályokra és az SE-vel kötött szerződésben vagy megállapodásban rögzítettekre figyelemmel kezelem. Titoktartási kötelezettségem körében a tudomásomra jutott adatokat illetéktelen részére hozzáférhetővé nem teszem, nem közlöm, át nem adom, nyilvánosságra nem hozom, fel nem használom.

Tudomásul veszem, hogy a titoktartási kötelezettségem időkorlátozás nélkül áll fenn, függetlenül attól, hogy milyen munkakörben és kinek a megbízottja, illetve munkavállalója vagyok.

Tudomásul veszem továbbá, hogy a titoktartási szabályok megsértéséért – az egyéb jogi következményeken túl –felek egymással szemben kártérítési felelősséggel is tartoznak.

7.4 Kiemelten védett területre történő belépés nyilvántartása

Belépés dátuma és pontos ideje		Belépő neve	Kísérő neve	Belépés célja	Távozás dátuma és ideje		Belépő aláírása	Kísérő aláírása

7.5 Hálózati végpontok nyilvántartása

Nr.	Ajtó	Felhasználónév	Eszköznév	Csatlakozó	Rack	Switch	Port	Megjegyzés

7.6 Speciális jelszavakhoz való hozzáférések jegyzőkönyve

Az Informatikai Igazgatóság alulírott munkatársa a speciális jelszavakat tartalmazó borítékot felbontottam.

Felbontás dátuma és pontos ideje		**Felbontást végző személy(ek) neve**	**Felbontás oka**	**Felbontást végző személy(ek) aláírása**

7.7 Fogalomtár

Adat: az információ megjelenési formája, azaz a tények, elképzelések nem értelmezett, de értelmezhető közlési formája.

Adatbiztonság: az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.

Adatbiztonság megsértése: az a cselekmény vagy mulasztás, amely ellentétben áll az adat védelmére vonatkozó biztonsági szabályokkal és amelynek következményei az adatot veszélyeztetik.

Adatgazda: az a személy, aki élve az Egyetem által biztosított jogosultságával, adatot minősít, illetve osztályba sorol és felelős az általa minősített adatok, továbbá az adatok feldolgozásához kapcsolódó rendszerek jogosultságainak kezeléséért.

Adatvédelem: az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségére vonatkozik.

Adminisztratív védelem: szervezési és szabályozási úton megvalósított védelem.

Backup rendszer: az informatikai biztonság megvalósítása során az adatok rendelkezésre állását lehetővé tevő rendszer és program másolatokat őrző rendszer. Rendszerint minimális tartalékkal rendelkező informatikai rendszert is értenek alatta.

Bizalmasság: (szervezeti állapot) - az Egyetem olyan állapota, amely biztosítja, hogy az adatokhoz csak azok a meghatalmazottak férhessenek hozzá, akiknek a szervezet ehhez jogot adott. (adat tulajdonság). Az Infotv. szerint a bizalmasság az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

Biztonság: olyan szervezeti állapot, melyben az adott szervezetnek a lehető legkisebb veszélyekkel kell számolnia, szolgáltatásait a vállalt / előírt feltételekkel és korlátozások nélkül képes nyújtani, a feladatait, funkcióinak ellátását illetően érdemi hatást gyakorló veszteség nem éri, a lehetséges fenyegetettségek bekövetkezési valószínűségéből és a lehetséges kárértékekből származtatott kockázat a szervezet számára elfogadhatóan alacsony és a kockázatkezelési eljárások eredményeként kialakuló maradvány kockázat a szervezet számára az elviselhető tartományban marad. A védeni kívánt informatikai rendszer olyan, az Egyetem számára kielégítő mértékű állapota, amely zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet valósít meg. A biztonság az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.

Biztonsági követelmények: a kockázatelemzés eredményeként megállapított, elfogadhatatlanul magas kockázattal rendelkező fenyegető tényezők ellen irányuló biztonsági szükségletek együttese.

Biztonsági esemény: az informatikai rendszer biztonságában beállt olyan kedvezőtlen változás, amelynek hatására az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása megsérült vagy megsérülhet.

Biztonsági osztályba sorolás: az adatnak az adatkezelés során a kezelés módjára, körülményeire, a védelem eszközeire vonatkozó védelmi szintet meghatározó besorolása, osztályozása.

Biztonsági rendszer: a biztonsági rendszer az informatikai biztonsági rendszerek összessége (logikai védelmet valósít meg, pl.: tűzfal, vírusvédelmi rendszer, jogosultág-nyilvántartó rendszer, stb.).

Egyenszilárdság: a biztonság az intézmény tevékenységét teljesen átfogja, és annak minden pontján azonos erősségű.

Elektronikus aláírás (digitális aláírás): az informatikai rendszerben kezelt adathoz rendelt, kódolással előállított olyan jelsorozat, amely az adat hitelességének és sértetlenségének bizonyítására használható.

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.

Elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

Elszámoltathatóság: az elszámoltathatóság azon követelmény, amely meghatározza minden, az információval vagy az informatikai rendszerrel kapcsolatos tevékenység egyértelmű azonosíthatóságát, utólagos visszakövethetőségét és az adott tevékenységet végrehajtó személyt.

Érintett: bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy.

Felhasználó: az a személy, szervezet vagy csoport, aki (amely) egy vagy több informatikai rendszert igénybe vesz feladatai megoldásához.

Felhasználói hitelesítés: a felhasználó hitelességének ellenőrzése (a belépéskor minden felhasználó ellenőrzése) és különböző azonosító eszközök (pl.: jelszó, chip-kártya, biometrikus azonosítás, stb.) alkalmazása.

Folyamatosság: az üzleti, egyetemi tevékenységek zavarmentes rendelkezésre állása.

Folytonos védelem: olyan védelmi megoldás, amely az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul.

Hálózat: számítógépek (vagy általánosabban informatikai rendszerek) összekapcsolása és az összekapcsolt rendszerek legkülönbözőbb komponensei közötti adatcserét megvalósító logikai és fizikai eszközök összessége.

Hitelesség: egy adat hiteles, ha minden kétséget kizáróan megállapítható annak előállítója és az a tény, hogy az az előállítás óta változatlan maradt. A hitelesség tehát az adat (és az adathordozó) tulajdonsága, amellyel igazolhatjuk, hogy az adat bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.

Hozzáférés: olyan eljárás, amely valamely informatikai rendszer használója számára – jogosultságának függvényében – meghatározott célra, helyen és időben elérhetővé teszi az informatikai rendszer erőforrásait, elérhetővé tesz a rendszerben adatokként tárolt információkat.

Illegális szoftver: az a szerzői jog védelme alatt álló szoftvertermék, amelynek a legalitás igazolásához szükséges dokumentumok (licenc, számla, szállítólevél, ajándékozási szerződés, stb.) nem mindegyike áll rendelkezésre, valamint a szoftver használata nem felel meg a licenc szerződés előírásainak.

Illetéktelen személy: olyan személy, aki az adat megismerésére nem jogosult.

Informatikai biztonság: az Egyetem informatikai rendszerének olyan kielégítő állapota, amely az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, illetve az informatikai rendszerelemek rendelkezésre állása és funkcionalitása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

Informatikai biztonsági dokumentációs rendszer: többszintű, egymásra épülő rendszer, amely magába foglalja a biztonságpolitikai elvektől a szabályzatokon keresztül a munkautasítások szintjéig az informatikai biztonsági irányelveket, teendőket, szereplőket, azok feladatait, jogait, kötelességeit és felelősségeit.

Informatikai rendszer: információs-, ügyviteli-, egyetemi folyamat vagy szolgáltatás működését támogató elektronikus adatfeldolgozó eszközök és eljárások, valamint az ezeket kiszolgáló emberi erőforrások és a kapcsolódó folyamatok összessége. A hardver-, szoftver-, kommunikációs eszközök és ezek kezelő / kiszolgáló szervezeteinek olyan együttese, amelyet az intézmény üzletpolitikájával összhangban céljai megvalósítására használ.

Információ-feldolgozó eszköz: minden olyan számítástechnikai, telekommunikációs és egyéb kategóriájú elektronikai eszköz, mely képes a betáplált (input) adatokat manipulálni és a folyamat végén eredményeket, kimenő adatokat (output) produkálni – az azt használó személy számára értelmezhető formában.

Incidens: minden olyan informatikai vonatkozású esemény, ami nem része a normál működésnek és a felhasználókat akadályozza feladataik ellátásában. A szolgáltatási hiba típusú incidensek a szolgáltatási szintek csökkenésével járnak (vagy ezzel fenyegetnek), míg a szolgáltatási igény típusú incidensek általában valamilyen eszköz vagy információ biztosítását, módosítások végrehajtását igénylik. Egy incidensnek lezárásáig többféle állapota lehet.

Információs vagyon: adatok, információk, szellemi, erkölcsi javak összessége.

Információvédelem: az informatikai rendszerek által kezelt adatok által hordozott információk bizalmasságának, hitelességének és sértetlenségének védelme.

Jogosultság: a lehetőség megadása az informatikai rendszerben végzendő tevékenységek végrehajtására.

Katasztrófa: az informatikai rendszer folyamatos és rendeltetésszerű működésének megszakadása.

Katasztrófahelyzet elhárítás tervezés: az informatikai rendszer rendelkezésre állásának megszűnése, nagy mértékű csökkenése utáni visszaállításra vonatkozó tervezés (DRP – Disaster Recovery Planning).

Kockázat: az informatikai fenyegetettség mértéke, amely valamely fenyegető tényezőből ered és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázat két részből, a kárnagyságból és a bekövetkezés gyakoriságából tevődik össze. Az Infotv. szerint a kockázat a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye

Kockázatelemzés: olyan elemző és értékelő jellegű szakértői vizsgálat, amely az informatikai rendszerekben kezelt adatok és alkalmazások értékelése, gyenge pontjainak és fenyegetettségeinek elemzése útján meghatározza a potenciális kárértékeket és azok bekövetkezési valószínűségét és gyakoriságát. Az Infotv. szerint a kockázatelemzés az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

Kockázatkezelés: védelmi intézkedések kidolgozása, elemzése és meghozatala, amelyet követően a maradványkockázatok elviselhető szintűre változnak. A kockázatkezelés az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;

Kockázatarányos védelem: az a védelem, mely a kockázatokat a releváns fenyegetettségek bekövetkezési valószínűsége és a fenyegetettség bekövetkezésekor keletkező kár függvényeként kezeli, és ahol a védelemre fordított erőforrások értéke arányos a védendő értékek nagyságával, illetve kockázatcsökkentő képességével. Az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;

Kontrollok-óvintézkedések: mindazok a fizikai-, adminisztratív-, technikai-, technológiai módok, eljárások, amelyeket védelmi célból tettek meg és a kockázatot csökkentik.

Kriptográfia: mindazoknak a matematikai eljárásoknak, algoritmusoknak és biztonsági rendszabályoknak a kutatása és alkalmazása, amelyek elsődleges célja az információnak illetéktelenek előli elrejtése.

Különleges személyes adat:

a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,

b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

Külső személy: az Egyetemmel szerződéses kapcsolatban álló személy vagy szervezet, aki vagy amely az Egyetem informatikai rendszerével kapcsolatba kerülhet.

Külső fél: Lásd „Külső személy”.

Legális szoftver: az a szerzői jog védelme alatt álló szoftvertermék, amelynek legalitásának igazolásához minden szükséges dokumentum (licenc, számla, szállítólevél, ajándékozási szerződés, stb.) rendelkezésre áll, valamint a használata a szoftver licenc szerződés előírásainak megfelelő módon történik.

Letagadhatatlanság: a letagadhatatlanság azon követelmény, amely meghatározza az üzleti életben, hogy a felhasználók egy későbbi időpontban ne tudják valamilyen okból önkényesen megtagadni az előzőekben általuk végrehajtott tranzakciót.

Maradványkockázat: az a tudatosan felvállalt kockázat, amely alapvetően – kis mértékben – annak ellenére is fennmarad, hogy a fenyegető tényezők ellen intézkedések eredményesen végrehajtásra kerültek.

Megbízható működés: az informatikai rendszerek, és az általuk kezelt adatok által hordozott információk rendelkezésre állásának és funkcionalitásának védelme.

Mentés: informatikai folyamat, amelynek során az informatikai rendszerben digitálisan tárolt vagy használatban lévő fontos adathalmazokról egy speciális eszközzel egy speciális adathordozóra (mentési médium) másolatokat készítenek.

Mentési médium: adathordozó (a legtöbbször mágneses elven működő szalagos egység), amelyen a mentések által duplikált adattartalmat tárolják.

Mobil eszköz: a hordozható eszközök kategóriájába különböző eszközök tartoznak: hordozható számítógépek (laptop), táblagépek, tenyérszámítógépek (PDA), mobiltelefonok, adathordozók (USB-pendrive, stb.).

Mobil kód: olyan szoftver vagy kód, mely általában egy távoli számítógépről, hálózaton keresztül letöltve, határozott telepítési vagy indítási procedúra nélkül fut vagy futtatható a kliens gépen. Ilyenek például a scriptek (JavaScript, VBScript), Flash animációk, Java kisalkalmazások, MS Office dokumentumok makrói, ActiveX vezérlők.

MS (rövidítés): Microsoft.

Rejtjelezés: nyílt üzenet kódolása kriptográfiai eljárással, eszközzel vagy módszerrel. A rejtjelezés eredménye a rejtjeles üzenet.

Rendelkezésre állás: az informatikai rendszer tényleges állapota, amely megvalósul, ha a rendszer szolgáltatásai állandóan, illetve egy meghatározott időben hozzáférhetők és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva. Az Infotv. szerint a rendelkezésre állás annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

Sértetlenség: az adat olyan tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes, ép, módosulatlan. Informatikai rendszer tulajdonság, amely adott, ha a rendszerben kezelt adatokat, illetve az adatkezelést megvalósító összes többi rendszer komponenst csak az arra jogosultak és csak dokumentáltan változtatják meg, emellett minden egyéb (véletlen vagy szándékos) módosulás kizárt — vagyis az adatok és feldolgozási folyamataik pontosak és teljesek. Az Infotv. szerint a sértetlenség az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

Személyes adat: az érintettel 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.

Teljes körű védelem: teljes körűnek nevezik az informatikai rendszer védelmét, ha az informatikai rendszer összes elemére kiterjed.

Üzleti titok: a működéshez, az üzletmenethez és a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ vagy adat, amelynek titokban maradásához a jogosultnak méltányolható érdeke fűződik, és amelynek titokban tartása érdekében a jogosult a szükséges intézkedéseket megtette.

Üzletmenet folytonosság tervezés: az egyetemi folyamatok rendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetőek legyenek (BCP – Business Continuity Planning).

Védelmi intézkedés: a fenyegetettség bekövetkezési valószínűsége, illetve a bekövetkezéskor jelentkező kár csökkentésére szervezési- vagy technikai eszközökkel tett intézkedés.

Védelmi rendszer: a védelmi rendszer az informatikai rendszer megfelelő szintű biztonságának garantálása érdekében alkalmazott fizikai-, logikai- és adminisztratív védelmi intézkedések összessége.

Vírus: olyan rosszindulatú programtörzs, amely illegálisan készült egy felhasználói program részeként. A felhasználói program alkalmazása során átterjedhet, "megfertőzhet" más, az informatikai rendszerben lévő rendszer-, illetve felhasználói programot, sokszorozva önmagát (ami lehet mutáns is) és a logikai bomba hatás révén egy beépített feltételhez kötötten (pl.: konkrét időpont, szabad lemezterületi helyek száma, stb.) trójai faló hatást indít el.

Vírusvédelmi rendszer: a vírusvédelmi rendszer és a hozzá kapcsolódó védelmi mechanizmusok feladata az informatikai rendszerhez kapcsolódó vírusok felkutatása, működésük, aktív vagy passzív károkozásuk megakadályozása, illetve – lehetőség szerint – megsemmisítésük.

VPN: Virtual Private Network. A virtuális magánhálózat a magánhálózat kiterjesztése, amely megosztott vagy nyilvános hálózatokon (például interneten) keresztüli kapcsolatokat tartalmaz. Virtuális magánhálózattal úgy lehet adatokat küldeni két számítógép között, mintha a két gép közvetlen kapcsolatban lenne egymással. A VPN kapcsolatok segítségével a szervezetek földrajzilag különálló irodákkal vagy más szervezetekkel is létesíthetnek kapcsolatot úgy, hogy a kommunikáció biztonságos maradjon.

Zárt védelem: Zártnak nevezik az informatikai rendszer védelmét, ha az összes releváns fenyegetést figyelembe veszi.

1.1 Ellenőrzési nyomvonalak

Az informatikai biztonság kialakításának és fenntartásának folyamata

Az ellenőrzésekkel kapcsolatosan ld. még a 6.3 és 6.4 fejezeteket.

	folyamat lépései	előkészítés lépései	felelősségi szintek					folyamat eredményeként keletkezett dokumentum
			feladatgazda	ellenőrző	ellenőrzés módja	jóváhagyó	jóváhagyás módja	
	Kockázatértékelés elvégzése, aktualizálása							
	Adatosztályozás elvégzése, aktualizálása							
1.	**hozzáférések** dokumentációjának ellenőrzése	hozzáférések lekérdezése, dokumentumok áttekintése	Alkalmazás üzemeltető rendszergazdák	Informatikai biztonsági felelős	jelentés elfogadása	Informatikai igazgató	aláírás	éves ellenőrzési jegyzőkönyv
2	**területvédelem**: géptermi naplók ellenőrzése	belépések, rendkívüli események regiszterének áttekintése	Infrastruktúra üzemeltetők	Informatikai biztonsági felelős	jelentés elfogadása	Informatikai igazgató	aláírás	éves ellenőrzési jegyzőkönyv
3	**üzemeltetési eljárások** ellenőrzése	utolsó ellenőrzés óta történt szervezeti-, infrastrukturális- és funkcionális változások listája	Alkalmazás üzemeltető rendszergazdák	Informatikai biztonsági felelős	jelentés elfogadása	Informatikai igazgató	aláírás	éves ellenőrzési jegyzőkönyv
5	**katasztrófa elhárítási tesztek**	tesztek tervezése és végrehajtása	Infrastruktúra és alkalmazás üze-	Informatikai igazgató	módosítási javaslat elkészíté-	Kancellár	aláírás	IBSZ módosítási javaslatok

	folyamat lépései	előkészítés lépései	felelősségi szintek					folyamat eredményeként keletkezett dokumentum
			feladatgazda	**ellenőrző**	**ellenőrzés módja**	**jóváhagyó**	**jóváhagyás módja**	
			meltetők		se			
6	**informatikai biztonsági incidensek** elemzése	incidensek regiszterének áttekintése	Infrastruktúra és alkalmazás üzemeltetők	Informatikai igazgató	módosítási javaslat elkészítése	Kancellár	aláírás	IBSZ módosítási javaslatok

n.é.: nem értelmezhető
Ellenőrzési módok: beszámoltatás, jóváhagyás, egyeztetési