Információbiztonsági szabályzat

Hatálybalépés napja: 2022.

Dokumentum adatlap

I.

Szervezet neve:	Semmelweis Egyetem
Dokumentum címe:	Információbiztonsági szabályzat
Elfogadó:	Szenátus
Elfogadó határozat száma:	65/2022. (IX.02.) számú szenátusi határozat
Hatálybalépés napja:	2022.

II.

Előkészítő szakmai szervezeti egység	**ügyintéző**	**vezető**
Informatikai Főigazgatóság Információbiztonsági felelős	Csaba László	Czinderi Gábor
Jogi előkészítő	**ügyintéző**	**vezető**
Jogi és Igazgatási Főigazgatóság	Ágh Ágnes	Dr. Kovács Zsolt

Tartalom

1. AZ INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT (IBSZ) HATÁLYA

1.1 Személyi hatálya

Jelen szabályzat személyi hatálya kiterjed:

a) a Semmelweis Egyetemnél (a továbbiakban: Egyetem), foglalkoztatott, munkavállalókra, az Egyetemmel szerződéses jogviszonyban álló jogi és természetes személyekre, jogi személyiséggel nem rendelkező szervezetekre, a velük kötött szerződés szerinti mértékben,
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.

1.2 Tárgyi hatálya

Az IBSZ tárgyi hatálya kiterjed:

a) az Egyetem minden információkezeléssel és feldolgozással kapcsolatos folyamatában résztvevő informatikai eszközre, nyilvántartást strukturáltan megvalósító rendszerre, mely az Egyetem területén található, valamint 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, függetlenül azok földrajzi elhelyezkedésére.

1.3 Vezetői elkötelezettség

Minden egyetemi szervezeti egység vezetője közreműködik az információbiztonság kultúrájának kialakításában és fenntartásában.

2. AZ INFORMÁCIÓBIZTONSÁGI RENDSZER MŰKÖDTETÉSE

2.1 A jogszabályoknak és a belső szabályzatoknak való megfelelés

A vonatkozó jogszabályok, belső szabályzatok a **Hiba! A hivatkozási forrás nem található. Hiba! A hivatkozási forrás nem található.** mellékletben találhatóak.

2.2 Információbiztonsági kockázatmenedzsment

(1) Az informatikai kockázatmenedzsment célja, hogy az információk bizalmasságát, sértetlenségét, valamint rendelkezésre állását veszélyeztető kockázati tényezők azonosításával, a kockázatok csökkentésével biztosítsa az információbiztonság növelését, szinten tartását.
(2) A teljes körű kockázatfelmérést jelentős változás (technológia, vagy szolgáltatás be- és kivezetése) esetén, de legalább kétévente kell végrehajtani az informatikai rendszer minden elemére (technikai eszközök, személyek, eljárások, szabályok).

(3) A felmerült kockázatok kezelésére (csökkentésére) intézkedési javaslatokat kell készíteni, melyeknek a feltárt kockázatok függvényében az alábbiakat kell tartalmazniuk:
   a) javaslatokat a technikai eszközök megváltoztatására, vagy fejlesztésére (pl.: új védelmi eszközök alkalmazása, vagy a jelenlegi átkonfigurálása);
   b) javaslatokat az érvényben lévő szabályozás megváltoztatására;
   c) javaslatokat a személyi állományra vonatkozóan;
   d) 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.

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

(5) Kockázatelemzés, kockázatfelmérés nélkül az Egyetemen nem engedélyezhető új informatikai rendszer bevezetése, függetlenül attól, hogy kész terméket kívánnak az Egyetem bármely egységénél beszerezni vagy új rendszert fejlesztetni.
   a) Kiemelten fontos az információbiztonsági véleményezés a kutatásfejlesztés, valamint a medikai érintettségű rendszerek esetében.
   b) Adatvédelmi érintettség esetén az információbiztonságért felelős vezetőnek (a továbbiakban: IBF) egyeztetnie szükséges az adott kérdéskörben az adatvédelmi tisztviselővel.

(6) Az információbiztonsági kockázatok felmérésének, a kockázatok elemzésének felelőse az IBF.

2.3 Megelőző intézkedések rendszere

Az Egyetem a nem kívánatos biztonsági események megelőzésére az intézkedéseket alkalmazza:

a) informatikai technológiai védelmi intézkedéseket (hálózatvédelem, vírusvédelem, jogosultság kezelés, stb.) foganatosít annak érdekében, hogy a nagy gyakorisággal bekövetkező fenyegető tényezők előfordulási gyakoriságát vagy hatását csökkentse;
b) szabályozott folyamatokat vezet be, eljárásrendekben, munkautasításokban rögzíti a biztonsági kontrollok működtetését, valamint az esetleges incidensek feltárását és kezelését;
c) rendszeres biztonságtudatossági oktatásokat végez a humánkockázatok csökkentésére.

2.4 Az informatikai biztonság irányításának alapjai

a) a szabályzat személyi hatálya alá tartozóknak az IBSZ-ben foglalt előírások ismeretében és azokat betartva kell munkájukat végezniük;
b) a szabályzatokat közzététel útján megismerhetővé kell tenni, az új belépőket oktatásban kell részesíteni, szükség esetén további képzéseket kell szervezni;
c) az információbiztonsági incidens esetén a 2.5 Információbiztonsági incidensek bejelentése, kezelése pontban szabályozottak szerint kell eljárni.

2.5 Információbiztonsági incidensek bejelentése, kezelése

Az informatikai és a személyi információbiztonsági incidenseket észlelésükkor jelentenie kell az azt észlelőnek.

a) Az információbiztonsági incidens bejelenthető közvetlenül az IBF, továbbá adatbiztonsági kérdésben az adatvédelmi tisztviselő felé, e-mail-en, személyesen, vagy telefonon. Aktuális elérhetőségeik az egyetem honlapján „Telefonkönyv” menüpont alatt érhetők el.
b) A bejelentés megtehető az infobiztonsag@semmelweis.hu e-mail címen (kezelője az IBF), vagy a GLPI rendszerben történő bejegyzéssel is. A GLPI rendszerbe való incidensfelvétel történhet telefonos bejelentéssel az Operatív Irányító Központon keresztül.
c) A biztonsági incidenseket az alábbiak szerint szükséges dokumentálni:
   ca) minden incidenst az erre szolgáló nyilvántartásban rögzíteni kell, hogy elemezni lehessen a szolgáltatásokra vonatkozó incidensek számosságát, időtartamát és hatását,
   cb) a bekövetkezett incidenseket figyelembe kell venni a kockázatfelmérés során az egyes fenyegetettségek bekövetkezési valószínűségének meghatározásánál,
   cc) az e-mail-es vagy GLPI-be való bejelentés fogadóhelyén az incidens felvevője, kezelője köteles az IBF-et, továbbá érintettsége esetén az adatvédelmi tisztviselőt haladéktalanul értesíteni.
d) Az incidensekből levont tapasztalatokat folyamatosan értékelni kell, és azokat figyelembe kell venni a védelmi rendszer tervezése, szervezése, működtetése során.
e) Információbiztonsági incidens kezelése során a bizonyítékokat – azok incidens elemzéséhez – össze kell gyűjteni.

2.6 Helyesbítő intézkedések rendszere

(1) Az Egyetem információbiztonsági rendszerében meghatározott szabályoktól való eltérést az informatikai főigazgató – az IBF egyetértésével – kizárólag írásban, indokolással engedélyezhet. Erről az engedélyekről nyilvántartást vezet.
(2) Az incidensek természetét és gyakoriságát az IBF folyamatosan figyelemmel kíséri, szükség esetén javaslatot tesz a védelmi intézkedések módosítására.
(3) Védelmi intézkedés módosítását kell alkalmazni, amennyiben:
   a) a korábbi védelmi intézkedés szintje nem érte el a kívánt biztonsági szintet;
   b) amennyiben egy védelmi intézkedés az indokoltnál jobban korlátozza az egyetemi polgárok munkavégzését;
   c) az informatikai rendszer változása miatt a korábbi biztonsági kontrollok érvényüket vesztik;
   d) az adott kontroll elavul és/vagy jobb, újabb technológiák bevezetése válik indokolttá.

3. AZ INFORMÁCIÓBIZTONSÁG SZERVEZETE

Az informatikai és az információbiztonsági feladatokat ellátó szervezeti egységeket szervezeti szinten el kell különíteni.

3.1 Információbiztonsági szerepkörök

Az Egyetem információbiztonsági rendszerének működtetése a kancellár feladata, tevékenységét az informatikai főigazgató és az IBF útján gyakorolja. E szabályzatban meghatározott intézkedési jogköröket a kancellár által más személyek, szervezeti egységek részére átruházott hatáskörként kell értelmezni.

3.1.1 Kancellár

(1) Felelőssége:
   a) A nemzeti felsőoktatásról szóló CCIV. törvény 94. § (2a) pontja és az Egyetem Szervezeti és Működési Szabályzat (a továbbiakban: SZMSZ) I.1. rész 30. § (2) bekezdésének a) pontja alapján a kancellár felel az Egyetem informatikai tevékenységéért,
   b) amelynek keretében felelőssége az informatikai biztonsággal kapcsolatos felsővezetői döntések meghozatala, a szükséges pénzügyi keretek biztosítása.

(2) Feladatai:
   a) az Információbiztonsági szabályzat kiadása,
   b) az Egyetem informatikai biztonsággal összefüggő beszerzéseinek gazdálkodási szempontú értékelése, megvalósíthatóságuk vizsgálata, pénzügyi erőforrások biztosítása;
   c) döntéshozatal az IBF hatáskörét meghaladó ügyekben.

3.1.2 Informatikai főigazgató

(1) Felelőssége:

Az informatikai biztonsághoz szükséges szervezeti és műszaki környezet létrehozása és folyamatos biztosítása, vezetői irányítási rendszer működtetése.

(2) Az informatikai biztonsággal kapcsolatos feladatai:
   a) az informatikai rendszer funkcionális és biztonsági követelményeknek megfelelő működtetése a rendelkezésére bocsátott költségkeret betartásával;
   b) az informatikai rendszer folyamatos rendelkezésre állásának biztosítása;
   c) az informatikai folyamatok és tevékenységek tervezése és folyamatos fejlesztése;
   d) a rendkívüli helyzetek elhárítása;
   e) az informatikai rendszer biztonsági komponenseinek üzemeltetéséhez szükséges humán és technikai erőforrások biztosítása a rendelkezésére álló erőforrások hatékony felhasználásával;
   f) az informatikai rendszerüzemeltetés és rendszerhasználat rendszeres független felülvizsgálatának biztosítása;
   g) érvényesíti az információbiztonsági követelményeket a hatáskörébe tartozó szolgáltatásokkal kapcsolatban kötött külső szolgáltatói szerződésekben;
   h) 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
   i) az informatikai szervezeti egység vezetők bevonásával gondoskodik a mentési stratégia kialakításáról, a mentési rend elkészítéséről, ellenőrzi a mentési eljárások betartását, gondoskodik a mentések tárgyi és személyi feltételeiről;
   j) rendszeresen – az Egyetem Informatikai Katasztrófa-elhárítási Tervében leírtak szerint – gondoskodik a katasztrófahelyzet kezeléssel kapcsolatos tesztek elvégzéséről;
   k) a programfejlesztési igények, fejlesztési programok kezelése, az elkészült termékek informatikai ellenőrzése az Egyetem belső szabályzatai és jelen IBSZ előírásai szerint.

(3) Az Információbiztonságért felelős vezetővel megosztott feladatai:
   a) az Egyetem információbiztonsági követelményeinek alkalmazása és betartatása;
   b) gondoskodni arról, hogy az információbiztonsági feladatok és követelmények beépüljenek a hatáskörébe tartozó szolgáltatások üzemeltetési folyamataiba,

c) a VPN kapcsolatok létesítésének engedélyezése, az Információbiztonságért felelős vezető előzetes jóváhagyása alapján
d) a fokozottan védett területekre történő belépés és az ott történő munkavégzés engedélyezése, az engedélyek rendszeres felülvizsgálata.

3.1.3 Biztonságtechnikai igazgató

(1) Felelőssége:
a fizikai biztonsággal kapcsolatban teljes utasítási és szabályozási joggal rendelkezik.
(2) Az informatikai biztonsággal kapcsolatos legfontosabb feladatai:
a) gondoskodik az informatikai szervezet fizikai biztonsággal kapcsolatos feladatainak végrehajtásáról és felügyeletéről;
b) személyesen, vagy munkatársán keresztül részt vesz a hatáskörébe tartozó szolgáltatásokat érintő informatikai biztonsággal kapcsolatos incidensek kivizsgálásában, az intézkedési javaslatok kidolgozásában;
c) részvétel biztosítása a rendszeres ellenőrzések során személyesen, vagy munkatársán keresztül.

3.1.4 Információbiztonságért felelős vezető (IBF)

(1) Felelőssége:
A biztonsági szabályok betartatása az üzemeltetési folyamatok során, az információbiztonság elvárt szintjének a biztosítása, folyamatos fejlesztése, intézkedési javaslatok megfogalmazása a biztonsági incidensek megelőzésére, valamint a bekövetkezett incidensek hatásának mérséklésére.
Felelős a beszerzések, informatikai fejlesztések során a biztonsági követelmények érvényre juttatásáért, egy bekövetkezett információbiztonsági esemény kapcsán az okok feltárásáért, a felelősök beazonosításáért.
Az IBF az Egyetem Informatikai Főigazgatóságával együttműködésben látja el feladatait, kancellár általi kinevezés, vagy megbízás alapján.
(2) Feladatai:
a) a munkatervében meghatározottak szerint az Egyetemen folyó tevékenységek információbiztonsági szempontból történő értékelése, a meglévő biztonsági szint megtartása és fokozása;
b) az Egyetem információbiztonsági dokumentációs rendszerének rendszeres karbantartása;
c) az IBSZ betartatásának ellenőrzése és folyamatos felügyelete;
d) az IBSZ-ben nem szabályozott kérdésekben a lehetséges veszélyforrások felderítése és javaslattétel a megelőzésre;
e) az informatikai rendszerekben kialakított biztonsági funkciók és az Egyetem információbiztonsági követelményei összehangolásának ellenőrzése;
f) az informatikai rendszerek biztonságát elősegítő eszközök üzemeltetésének rendszeres ellenőrzése, független felülvizsgálatának megszervezése;
g) információbiztonsági incidens menedzsment feladatok ellátása:
ga) a biztonsági incidensek kezelése;

gb) az incidensek kivizsgálása vagy kivizsgáltatása;
gc) az incidensekre tett lépések megfelelőségének ellenőrzése;

h) az Egyetemmel bármilyen módon adatforgalmi vagy információadási/fogadási kapcsolatban (adathálózat, adathordozók cseréje, stb.) álló külső szervekkel történő szerződéskötés esetén az informatikai biztonság területét érintő részekkel kapcsolatban ellenőrzési, javaslattételi joga és kötelezettsége van;
i) a programfejlesztési munkák, valamint a beszerzések során megkeresésre előzetesen véleményezi, valamint ellenőrzi vagy ellenőrizteti az informatikai biztonság szempontjainak a megvalósulását;
j) biztosítani kell, hogy csak információbiztonsági szempontból megbízható szoftverek készüljenek vagy kerüljenek beszerzésre;
k) az Egyetem informatikai védelmi- és biztonsági rendszere tervezésében való részvétel;
l) az informatikai védelmi- és biztonsági rendszer rendszeres felülvizsgálata, a védelmi eszközökkel való ellátottság rendszeres ellenőrzése;
m) az Egyetem adatkezelési tevékenységének és az informatikai kommunikációs hálózatának információbiztonsági szempontú ellenőrzése;
n) felkérés alapján részvétel a Minőségbiztosítási Osztály minőségügyi belső auditján az információbiztonsági kérdések felmerülésekor;
o) 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;
p) annak ellenőrzése, hogy megtörtént-e minden informatikai konfigurációs-elem (rendszerelem) nyilvántartásba vétele és azonosítása az informatikai vagyontárgyak hatásos védelemének kialakításához;
q) annak ellenőrzése, hogy megtörtént-e a leselejtezésre kerülő eszközök adathordozóin, háttértárain tárolt adatok végleges, visszaállíthatatlan módon való törlése;
r) az informatikai munkafolyamat információbiztonságot érintő bármely részének előzetes bejelentési kötelezettség nélküli ellenőrzése;
s) az információbiztonságot érintő utasítás-tervezetek készítése és véleményezése;
t) gondoskodik az Egyetem informatikai rendszerének felhasználói szintű információbiztonsági oktatásáról, az információbiztonsági tudatosság növeléséről, a szabályzat jelentős változásairól az érintettek figyelmét felhívja ;
u) kapcsolattartás információbiztonsággal kapcsolatos szolgáltató, tanácsadó szervezetekkel, valamint törvényben felhatalmazott ellenőrző szervekkel.

3.1.5 Kari/tömbigazgatóság szintű informatikai vezető

(1) Felelőssége:
Végrehajtási és ellenőrzési felelősség; az informatikai biztonság megvalósulását eredményező helyi környezet folyamatosságának biztosításában.
(2) Az informatikai biztonsággal kapcsolatos legfontosabb feladatai:
a) A helyi informatikai rendszereknek a követelményeknek megfelelő működtetése.

b) A helyi informatikai rendszerek folyamatos rendelkezésre állásának és funkcionális működésének biztosítása.
c) A helyi informatikai rendszerek biztonsági komponenseinek üzemeltetéséhez szükséges humán és technikai erőforrások biztosítása a rendelkezésére álló erőforrások hatékony felhasználásával.
d) Közreműködés az informatikai biztonsági kockázatok felmérésében, kezelésében, a bevezetett intézkedések hatásosságának visszamérésében.
e) Érvényesíti az információbiztonsági követelményeket a hatáskörébe tartozó informatikai szolgáltatásokkal kapcsolatban kötött külső szolgáltatói szerződésekben.
f) Intézkedik a hatáskörébe tartozó mentési stratégia kialakításáról, ellenőrzéseket végez a mentések elvégzéséről, az ezzel kapcsolatos incidensek kezelésében, gondoskodik a mentések tárgyi- személyi feltételeiről.
g) Részt vesz a területén az információbiztonsági események kivizsgálásában, és az abból adódó intézkedések végrehajtásában.
h) A területéhez tartozó fokozottan védett területekre történő belépés és az ott történő munka-végzés engedélyezése, az engedélyek rendszeres felülvizsgálata a Biztonságtechnikai igazgatóval és az IBF-fel közösen.

3.1.6 Egyéb információbiztonsági szerepkörök

Az információbiztonsági területeken végzendő feladatok az Informatikai Főigazgatóság infrastruktúra- és alkalmazás-üzemeltetési munkatársai munkaköri leírásában, valamint az egyes rendszerek technológiai leírásában találhatók. Ezek a biztonsági területek az alábbiak:
a) vírusvédelem;
b) határvédelem (tűzfalak, spamszűrő, aktív hálózati eszközök, VPN);
c) mentések;
d) jogosultság-kezelés;
e) alkalmazás-üzemeltetés.

3.1.7 Szervezeti egység vezető

(1) 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.
(2) Köteles a tudomására jutott, az egyetem információbiztonságát veszélyeztető, működését sértő eseményekről, körülményekről – azok jellegétől függően – az IBF-nek információt nyújtani.
(3) Közreműködik a szakterület információbiztonsági, informatikai biztonsági kockázatai feltárásában, a kockázatok felmérésében, értékelésében, és kezelésében.

3.1.8 Felhasználó

(1) Felelős az egyetemi feladatai ellátása érdekében az informatikai eszközök rendeltetésszerű használatáért, a jelen szabályzatban leírtak betartásáért. Az Egyetem informatikai infrastruktúráját kizárólag munkájával összefüggő feladatok végzéséhez használhatja.

(2) Információbiztonsági feladatai:
   a) 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.
   b) 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.
   c) Köteles azonnal jelenteni az informatikai eszközök és alkalmazások működésében bekövetkezett hibákat, rendellenességeket.
   d) Felelős a rábízott, az egyetem tulajdonát képező információs eszközök megőrzéséért, rendeltetésszerű használatáért, a kezelési előírások maradéktalan betartásáért.
   e) Az általa használt informatikai eszközökön lévő információk védelme.
   f) Az alkalmazások felhasználói leírásainak az ismerete és az alkalmazások használatakor azok betartása.

(3) A felhasználó az Egyetem informatikai rendszerében saját tulajdonú eszközt csak előzetes bejelentés és nyilvántartásba vétel esetén használhat.
   a) A saját tulajdonú eszközön az egyetemi védelmi rendszerekkel legalább egyenértű védelmet kell alkalmazni.
   b) Az informatikai főigazgató – az IBF 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 használata nem kezelhető vagy nem vállalható információbiztonsági kockázatot eredményezne.

3.2 Külső ügyfelek és partnerek

3.2.1 Külső személyekkel összefüggő kockázatok azonosítása

(1) 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.

(2) 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 információbiztonsági 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.

(3) 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.

3.2.2 A biztonság kérdésének kezelése harmadik féllel kötött megállapodásokban

(1) A külső személyekkel vagy hallgatókkal kapcsolatosan – amennyiben értelmezhetők – a következő feltételeket kell a velük kötött szerződésbe foglalni vagy részükre dokumentáltan rendelkezésre bocsátani:
   a) az IBSZ-ben meghatározott információbiztonsági követelmények kivonatát;
   b) az Egyetem kezelésében lévő adatok másolásának és nyilvánosságra hozatalának korlátozásait;
   c) hozzáférés-ellenőrzési megállapodást, amely tartalmazza:
      ca) a megengedett hozzáférési módokat;
      cb) a hozzáférés és jogosultságkezelés folyamatát;
      cc) a külső személy képviselőinek egyértelmű megfeleltetését az igénybe vehető informatikai szolgáltatásokkal, azok használatra vonatkozó jogokkal és kiváltságaikkal együtt;
      cd) a hozzáférési mód ellenőrzési feltételeit;
   d) a szerződésben rögzített felelősségek auditálásának jogát, vagy az auditok további külső személlyel történő elvégeztetésének jogát;
   e) a problémamegoldás folyamatát;
   f) a biztonsági eseményekről és a biztonság megsértéséről szóló tájékoztatási kötelezettségek, értesítések és a kivizsgálásokra vonatkozó intézkedéseket;
   g) a szerződés teljesítésébe további alvállalkozók bevonásának feltételeit, titoktartásukra vonatkozó megállapodásokat.

(2) Az Egyetem informatikai rendszerében a külső személyek által távolról elért, menedzselt vagy diagnosztizált eszközeihez való kapcsolódást minden hozzáférés igénylésekor egyedileg kell engedélyezni és felügyelni. Erről nyilvántartást kell vezetni.

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

(4) A harmadik féllel kötött megállapodások információbiztonsági szempontú ellenőrzése a Jogi és Igazgatási Főigazgatóság bevonásával, az IBF, valamint az informatikai főigazgató közös feladata.

3.2.3 Titoktartási megállapodások

Minden alkalmazott és az Egyetem informatikai rendszereit és/vagy szolgáltatásait használó külső szervezetnek, személy (cégnek, egyéni munkavállalónak, stb.) a munkaköri leírásban, és a munkaszerződésben foglaltak szerint a munkája során tudomására jutott, a nem publikus egyetemi információkat sem a munkavégzés során, sem annak vége után nem hozza harmadik fél tudomására.

4. ADATGAZDAI SZABÁLYOZÁS

4.1 A vezető adatgazdák és a szakterületi adatgazdák kijelölésének az elvei

A vezető adatgazdák és a szakterületi adatgazdák az alábbi elvek szerint kerülnek kijelölésre:

(1) A gazdálkodási, pénzügyi, kontrolling, beszerzési, a tömbigazgatóságokkal kapcsolatos tevékenységek vezető adatgazdája: gazdasági főigazgató.
Szakterületi adatgazdák: a Gazdasági Főigazgatóságon működő igazgatóságok vezetői.

(2) Az egészségügyi tevékenység végzésével kapcsolatos feladatok vezető adatgazdája: Klinikai Központ elnöke.
Szakterületi adatgazdák: a Klinikai Központhoz tartozó szervezeti egységek vezetői – a saját tevékenységi körükben. A medikai rendszerhez (MedSolution), a laborrendszerekhez (GLIMS, Andromeda), a képalkotó diagnosztikai rendszerhez (PACS) és a Fogász rendszerhez külön szakterületi adatgazdákat kell kijelölni. Egy rendszerhez több szakterületi adatgazda is kijelölhető, a vezető adatgazda döntése alapján.

(3) Oktatási tevékenység végzésével kapcsolatos feladatok vezető adatgazdája: oktatási rektorhelyettes.
Szakterületi adatgazdák: az egyetemi karok vezetői, az Egyetemi Doktori Tanács elnöke és az Oktatásigazgatási Hivatal vezetője, a Nemzetközi Hallgatók Képzési Központja vezetője – a karok vezetői esetében az általuk vezetett karok, valamint szervezeti egységek feladatainak a vonatkozásában.

(4) kutatás, tudományos tevékenység végzésével kapcsolatos feladatok vezető adatgazdája: tudományos és innovációs rektorhelyettes.
Szakterületi adatgazda: Innovációs Igazgatóság vezetője vagy a kutatócsoport vezetője, a vezető adatgazda döntése alapján.

(5) Stratégiai, fejlesztési és minőségbiztosítási tevékenységek vezető adatgazdája: stratégiai és fejlesztési rektorhelyettes.
Szakterületi adatgazda: a minőségbiztosítási osztály vezetője az általa ellátandó feladatok vonatkozásában.

(6) Nemzetközi képzési tárgyú tevékenység vezető adatgazdája: nemzetközi képzésért felelős rektorhelyettes.

(7) Jogi, igazgatási, adatvédelmi tárgyú tevékenységek vezető adatgazdája: jogi és igazgatási főigazgató.
Szakterületi adatgazdák: a polgári és gazdasági jogi igazgató, az egészségügyi és oktatási jogi igazgató, perképviseleti igazgató, valamint a Szervezési és Igazgatási Központ vezetője – az általuk vezetett szervezeti egység feladatainak, az Adatvédelmi és Betegjogi Központ vezetője az általa ellátandó feladatok vonatkozásában.

(8) A rektor által irányított további szakterületek vezető adatgazdái feladatkörükben: rektori kabinetvezető.

(9) A kancellár által irányított további szakterületek vezető adatgazdái feladatkörükben:
a) emberierőforrás-gazdálkodási főigazgató
b) műszaki főigazgató
c) ellenőrzési igazgató
d) kancellári kabinetvezető.

4.2 Vezető adatgazda

(1) A vezető adatgazda az általa irányított területen keletkezett és felhasznált adatokért felelősséggel tartozó személy.

(2) Felelős az adatokkal és az adatok felhasználásával kapcsolatos stratégiai szintű döntések meghozataláért és az általa irányított vagy felügyelt területen működő szakterületi adatgazdák tevékenységének az összehangolásáért. A vezető adatgazdai szerepkör a szervezetben betöltött funkcióhoz kapcsolódik.
(3) Az Egyetem egyes működési folyamatai esetében, az általuk használt adatok vonatkozásában a vezető adatgazdák az IBF-fel közösen állapítják meg az adatkezelés stratégiai biztonsági követelményeit.
(4) Az Egyetemen üzemeltetett, adatokat kezelő informatikai rendszerek mindegyikét be kell sorolni egy-egy vezető adatgazda felügyelete alá.
(5) A vezető adatgazda a szabályzat hatályba lépését követően felelős:
   a) az általa felügyelt vagy irányított tevékenységekhez kapcsolódóan keletkezett és jelen szabályzat 3. számú **Hiba! A hivatkozási forrás nem található.**ben **Hiba! A hivatkozási forrás nem található.**felsorolt informatikai rendszerben tárolt és kezelt adatok, információk megbízhatóságát, hitelességét biztosító folyamatok megfelelőségét biztosító szabályzatok meghatározásáért,
   b) a fenti folyamatok kontrollpontjainak a meghatározásáért,
   c) az adatokhoz való hozzáférést szabályozó jogosultsági rendszer alapelveinek a meghatározásáért, az adott alkalmazáshoz kialakított standard jogosultsági rendszer jóváhagyásáért, valamint a szükséges felülvizsgálat megtörténtéért, a módosítások jóváhagyásáért,
   d) az olyan jogosultsági igények elbírálásáért, amelyek nem rendelhetők szakterületi adatgazdákhoz,
   e) a szakterületi adatgazdák és helyetteseik kijelölésének kezdeményezéséért, tevékenységük felügyeletéért,
   f) a szakterületi adatgazdák és az alkalmazásgazdák közreműködésével meghatározza azokat a szakmai igényeket, amelyek alapján az informatikai fejlesztések, beruházások prognosztizálhatók (meghatározza az informatikai stratégia szakmai, felhasználói oldalát).
(6) A jelen szabályzat hatályba lépésekor már meglévő, és a szabályzat (3. számú **Hiba! A hivatkozási forrás nem található.**) mellékletében felsorolt informatikai rendszerek esetében a vezető adatgazdák kijelölése - az általuk az Egyetem szervezetében betöltött pozíciójuk alapján – ezen szabályzat hatálybalépésével megtörténik.
(7) A szabályzat hatályba lépését követően üzembe helyezésre kerülő rendszer esetében a vezető adatgazda kijelölése az érintett rektorhelyettesek előzetes hozzájárulásával a kancellár rendelkezése alapján történik.

4.3 Szakterületi adatgazda

(1) A szakterületi adatgazda – a vezető adatgazda irányítása mellett – felelős a vezető adatgazda általa felügyelt területen keletkezett és kezelt adatokkal kapcsolatos operatív döntések meghozataláért. Egy vezető adatgazdához egyidejűleg több szakterületi adatgazda is tartozhat.
(2) A szakterületi adatgazdákat és helyetteseiket a vezető adatgazda jelöli ki, egyúttal meghatározza azt a tevékenységi kört, amelyek tekintetében a feladatait ellátja, jogait gyakorolja.
(3) A szakterületi adatgazda a vezető adatgazda által kezdeményezett, írásbeli, határozatlan időre szóló kancellári megbízás alapján látja el feladatát. A kijelölt szakterületi

adatgazdákról és a szakterületi adatgazdai kijelölés visszavonásáról az IBF-et és az egyetemi adatvédelmi tisztviselőt haladéktalanul tájékoztatni kell.

(4) A szakterület nagyságától, a kezelendő adatok mennyiségétől, sokféleségétől vagy bonyolultságától függően a vezető adatgazda és a szakterületi adatgazda személye lehet azonos (azaz a vezető adatgazda elláthatja egy személyben a szakterületi adatgazdai feladatokat is).

(5) A szakterületi adatgazda felelős:

a) A vezető adatgazda által meghatározott körben a jelen szabályzat 3. számú mellékletében felsorolt informatikai rendszerekben tárolt és kezelt adatok, információk megbízhatóságát, hitelességét biztosító folyamatok meghatározásáért, napi működtetéséért.
b) A stratégiai szintű vezető adatgazdai döntés alapján az adott informatikai rendszerben tárolt adatok biztonsági osztályba sorolása, valamint az általa felügyelt szakrendszer sajátos szerepköreinek és jogosultsági rendszerének a kialakítása és karbantartása a szakterületi adatgazda feladata.
c) Az adatoknak az azok tárolására rendszeresített informatikai rendszerben való rendelkezésre állásáért.
d) Az általa felügyelt vagy irányított tevékenységek végzésekor az Egyetemen rendelkezésre álló adatok, információk felhasználását (hasznosítását), valamit az adatok külső vagy belső publikálását, átadását biztosító folyamatok meghatározásáért, napi működtetéséért. Részt vesz az adatok hasznosítására vonatkozóan megkötendő megállapodások létrehozatalában és felülvizsgálatában.
e) A fenti folyamatokhoz meghatározott kontrollpontok működéséért.
f) Az Egyetem munkatársaira vagy a külső foglalkoztatottakra vonatkozóan a jogosultsági igénylések jóváhagyásáért vagy elutasításáért.
g) A standard jogosultsági rendszer kidolgozásáért, a szükséges felülvizsgálatok elvégzéséért és – az IBF egyetértése esetén – jóváhagyásra a vezető adatgazda elé történő terjesztésért.
h) Az általa irányított területek munkatársai által jelzett módosítási, fejlesztési igények ellenjegyzéséért.
i) A más szakterületek által jelzett módosítási, fejlesztési igények befogadásáért, támogatásáért vagy elutasításáért.

(6) Legalább kétévente, az IBF-fel egyeztetett időpontban és ütemezés szerint felülvizsgálja az általa felügyelt rendszer felhasználói jogosultságait. A felülvizsgálatot követően intézkedési javaslatot készít a felhasználó szervezeti egységének vezetője felé, majd a szervezeti egység vezetőjének a jóváhagyása után az indokolatlan jogosultságokat haladéktalanul visszavonatja.

(7) Közreműködik az adatok biztonsági besorolásának megfelelő védelmi szabályok meghatározásában.

4.4 A vezető adatgazda és a szakterületi adatgazda feladatai, felelősségi köre új informatikai rendszerek fejlesztésekor vagy beszerzésekor

(1) A vezető adatgazda az általa irányított területen:

a) jogosult szakmailag dönteni új informatikai alkalmazás fejlesztéséről vagy beszerzéséről, vagy – ha az új fejlesztés vagy beszerzés igénye nem tőle származik – jogosult részt venni a döntés előkészítésében,
b) jogosult jóváhagyni a fejlesztés megkezdését,
c) jogosult jóváhagyni az új fejlesztés tartalmát, különös tekintettel – közbeszerzés esetén – a műszaki leírásra vagy a követelményspecifikációra,
d) kijelöli az informatikai rendszer szakterületi adatgazdáját,
e) meghatározza az új informatikai rendszer jogosultsági rendszerének az alapelveit,
f) amennyiben az új rendszer több szakterületi adatgazdát is érint, összehangolja működésüket,
g) együttműködik az IBF-fel.

(2) A szakterületi adatgazda a vezető adatgazda által meghatározott körben:
a) támogatja a vezető adatgazdát az új alkalmazás fejlesztéséről vagy beszerzéséről meghozandó döntésben,
b) a vezető adatgazdának jóváhagyásra javasolja az új alkalmazás szakmai követelményspecifikációját és a meglévő alkalmazás módosításának a követelményspecifikációját, mely módosításról a vezető adatgazdát tájékoztatni köteles,
c) együttműködik az IBF-fel,
d) az általa irányított területen gondoskodik a fejlesztéshez vagy beszerzéshez kapcsolódó projektben a szükséges létszámú és szakértelemmel rendelkező humán erőforrás rendelkezésre állásáról,
e) gondoskodik:
ea) az alkalmazás által támogatandó szakmai folyamat pontos definíciójáról,
eb) az informatikai rendszer helyes működéséhez szükséges bemenő adatok megfelelőségét elősegítő adatbeviteli ellenőrzési eljárások meghatározásáról,
f) a felelősségi körébe tartozó alkalmazás feldolgozási folyamatainak és kimeneti adatainak a meghatározásáról,
g) végrehajtja a beszerzett (beüzemelt) vagy elkészült alkalmazás bevezetésével, a napi működési folyamatokba illesztésével kapcsolatos teendőket, különös tekintettel:
ga) az alkalmazás használatához kapcsolódó belső szabályozás kialakítására vagy módosítására,
gb) a bevezetésre kerülő vagy módosuló folyamatok gyakorlati alkalmazásának elősegítésére,
gc) az alkalmazásgazda munkájának vezetői támogatására,
gd) a rendszer használatának az ellenőrzését célzó kontrollok kialakítására és működtetésére, a szükség esetén követendő intézkedések foganatosítására,
ge) a munkatársak képzésen történő részvételének biztosítására, ösztönzésére,
gf) megfelelő képzettségű és létszámú erőforrás biztosítására a használatbavétellel jelentkező esetleges többletfeladatok ellátására.

4.5 Alkalmazásgazda

(1) Az alkalmazásgazda az a szakmai kompetenciával rendelkező, felhasználói területi kulcsfelhasználó munkatárs, aki az adott alkalmazás teljes funkcionalitását, felhasználói üzleti logikáját ismeri, valamint a rendszer funkcióit rendszeresen alkalmazza. Támogatja az

érintett rendszert használó szakterületi munkatársakat a rendszer napi használatában, valamint segítséget nyújt a változtatási igények megfogalmazásában.

(2) Az alkalmazásgazdát – a szakterületi adatgazda javaslata alapján – a vezető adatgazda jelöli ki. Egy informatikai alkalmazáshoz több alkalmazásgazda is kijelölhető, ilyen esetben közülük vezető alkalmazásgazdát is ki kell jelölni.

(3) Az alkalmazásgazdának a szakterületi adatgazdákat és felhasználókat támogató feladatai:

a) a hozzárendelt alkalmazás teljes funkcionalitásának, üzleti logikájának az ismerete, amely a rendszer funkcióinak a rendszeres használat szintjén történő alkalmazásán alapul,
b) a szakterületi felhasználók tevékenységének a támogatása az adott alkalmazás használatában,
c) közreműködik a felhasználók által megfogalmazott módosítási, fejlesztési igények pontos definíciójának (követelményspecifikációjának) kialakításában, továbbá – amennyiben egy módosítási, fejlesztési igény több szakterületet érint – gondoskodik az igények, vélemények konszolidálásáról,
d) kapcsolatot tart az alkalmazásfelügyelővel,
e) az alkalmazás használatával kapcsolatos nem informatikai jellegű problémákról a szakterületi adatgazda (vagy szakterületi adatgazdák) tájékoztatása és a megoldási lehetőségek megfogalmazása,
f) a szakterületi adatgazda utasításai alapján közreműködik:
    fa) az adatok azok tárolására rendszeresített alkalmazásban való rendelkezésre állását biztosító folyamatok napi működtetésében,
    fb) a hatáskörébe tartozó informatikai rendszerek kódtárai tartalmának aktualizálásában, érvényességének folyamatos fenntartásában,
    fc) az Egyetemen rendelkezésre álló adatok, információk felhasználását (hasznosítását), valamit az adatok külső vagy belső publikálását, átadását biztosító folyamatok napi működtetésében.

4.6 Alkalmazásfelügyelő

Az alkalmazásfelügyelő az adott alkalmazás informatikai szakértője

a) aki az adott alkalmazás teljes funkcionalitását, üzleti logikáját, az egyetemi tevékenységekben történő alkalmazását ismeri és informatikai szaktudásával támogatni tudja a felhasználókat és az alkalmazásgazdát a felmerült észrevételek, javaslatok, lehetőségek értelmezésében, megfogalmazásában, a rendszer alkalmazásában, működésében;
b) aki az Informatikai Főigazgatóság vagy a kari/tömbigazgatósági informatikai támogató terület munkatársa.

4.7 Adatgazdai rendszerhez kapcsolódó nyilvántartás

(1) A vezető adatgazdákat, a szakterületi adatgazdákat, az alkalmazásgazdákat és az alkalmazásfelügyelőket az Informatikai Főigazgatóság tartja nyilván és teszi közzé honlapján.

(2) A szakterületi adatgazdák és alkalmazásgazdák kijelöléséről, valamint a személyükben beállt változásokról a vezető adatgazda írásban, a kijelöléstől vagy a változástól számított 5 munkanapon belül írásban értesíti az Informatikai Főigazgatóságot.

4.8 Információvédelmi osztályba sorolás

(1) A szakterületi adatgazda az általa felügyelt adatok tekintetében az adatok információvédelmi osztályba sorolásával felelős azért, hogy a felhasználók az adatokat azok biztonsági besorolásának megfelelően kezeljék.
(2) A szakterületi adatgazdának minden adatot, annak megjelenési formájától függetlenül információvédelmi osztályba kell besorolnia. A besorolást a szabályzat **Hiba! A hivatkozási forrás nem található.Hiba! A hivatkozási forrás nem található.** mellékletben felsorolt rendszerek esetében a besorolási ütemterv alapján kell elvégezni.
(3) Az adatok osztályozását kezdeményezni kell:
   a) új informatikai alkalmazás fejlesztése esetén;
   b) új informatikai rendszer bevezetésekor;
   c) informatikai alkalmazás módosítása esetén, amennyiben a módosítás a kezelt adatok körére is kiterjed;
   d) az ügyviteli folyamatokban beállt olyan változás esetén, amely az adott ügyviteli folyamat által kezelt adatok körére is kiterjed;
   e) jogszabályi, törvényi változás során új adatcsoport megjelenése esetén;
   f) egy már meglévő rendszerbe történő új modul integrálása esetén.
(4) A szakterületi adatgazda a besorolásról írásban tájékoztatja a vezető adatgazdát, majd a vezető adatgazdai jóváhagyást követően az IBF-et.

4.8.1 Adatosztályozás és biztonsági szintek

(1) Az Egyetem működésével kapcsolatosan kezelt adatok információvédelmi szempontból lehetnek:
   a) nyilvános adatok;
   b) belső adatok;
   c) bizalmas adatok;
   d) titkos adatok.
(2) Az adatok kezelésére vonatkozó szabályokat a 3. számú **Hiba! A hivatkozási forrás nem található.** tartalmazza.

4.8.2 Az információk jelölése és kezelése

(1) Minden vezető adatgazdának el kell végeznie és háromévente, szükség esetén soron kívül, dokumentált módon felül kell vizsgálnia az adatok besorolását.
(2) A szakterületi adatgazdáknak a hozzájuk tartozó adatkörök nyilvántartásba vételekor vagy módosulásakor az Adatosztályozó lapot (**Hiba! A hivatkozási forrás nem található.Hiba! A hivatkozási forrás nem található.**), vagy annak tartalmával megegyező nyilvántartást kell küldenie az IBF-nek.

5. Részletes védelmi intézkedések meghatározása

5.1 Informatikai vagyontárgyak kezelése

5.1.1 Informatikai vagyonleltár

(1) 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 Leltárkészítési és leltározási szabályzata, valamint az Informatikai Főigazgatóság szervezeti ügyrendje tartalmazza.
(2) A nyilvántartásban kötelezően kell szerepeltetni a következő konfigurációs-elemeket:
   a) hardver elemek (kiszolgálók, kliensek, hálózati aktív és passzív eszközök, háttértárolók, nyomtatók, stb.);
   b) szoftver elemek (operációs rendszer, alkalmazás, fejlesztőeszköz, stb.);
   c) információs elemek (adatbázisok, adatállományok, stb.);
   d) szolgáltatási elem (világítás, energia ellátás, légkondicionálás, stb.);
   e) dokumentációs elem (rendszerdokumentációk, felhasználói kézikönyvek, üzemeltetési utasítások, folytonossági tervek, stb.).
(3) Valamennyi nyilvántartásba vett információ-feldolgozó eszközhöz hozzá kell rendelni azokat a felelősöket, akik az adott eszközök biztonságáért felelnek (ún. vagyongazda).
(4) Információk, adatokhoz történő hozzáférések esetében a felelős a vezető adatgazda, hardverek, szoftverek esetében az informatikai főigazgató.
(5) Az Egyetem informatikai rendszerében csak az informatikai főigazgató és az IBF által jóváhagyott, konfigurációs leltárba felvett:
   a) hardverelemeket lehet használni;
   b) jogtiszta szoftvert lehet telepíteni és/vagy futtatni.

5.1.2 Vagyontárgyak tulajdonjoga

Valamennyi, az Egyetemen működésével kapcsolatban keletkezett vagy 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

(1) Az Egyetem munkatársaival meg kell ismertetni az jelen szabályzat beosztásuk alapján rájuk vonatkozó szabályait:
   a) az alkalmazandó információbiztonsági szabályokat;
   b) az informatikai rendszerek használatával kapcsolatosan elvárt és tiltott magatartásokat, azok megsértésének szankcióit;
   c) az informatikai rendszer számára nagy kockázattal járó fenyegetések és veszélyforrások közérthető magyarázatát, a biztonságtudatosság fokozása érdekében.
(2) Az informatikai biztonságtudatossági képzés tematikáját és előadóját az IBF biztosítja.

5.2.2 Az információbiztonság tudatosítása, oktatás és képzés

(1) Az Egyetem informatikai rendszerei felhasználóinak a munkakörükhöz igazodó informatikai oktatást kell biztosítani, lehetőleg az informatikai rendszer használata előtt vagy az általuk használt informatikai infrastruktúra változásakor (pl. új hardver vagy szoftver

használatba vétele előtt), valamint az információbiztonsági kockázatok jelentős változásakor, új kockázati elem megjelenésekor.

(2) Az oktatás előkészítése során az Informatikai Főigazgatóság feladata
   a) a szükséges tanfolyamok meghatározása;
   b) javaslat a képzésben részesítendő munkakörök/szerepkörök meghatározására;
   c) oktatásra javasoltak meghatározása;
   d) az oktatók személyére vonatkozó javaslattétel (amennyiben a képzés nem külső szervezésű).

5.2.3 Feladatok az egészségügyi szolgálati jogviszony vagy munkaviszony megszűnésekor, valamint változásakor

(1) Az Egyetem a hálózati meghajtókat és levelezőrendszerét a munkavégzés támogatására alkalmazza, az esetlegesen itt tárolt magáncélú tartalmakról, levelekről a jogviszony megszűnésekor megkeresésre sem készít semmilyen adathordozón másolatot. A felhasználó feladata az ilyen tartalmak, levelek egyetemi levelezőrendszerből történő eltávolítása legkésőbb az utolsó munkában töltött napig.

(2) A jogviszony megszűnését követő 30 nap múlva a kilépő munkavállaló egyetemi elektronikus levelező címét az informatika megszünteti, törli, és ezt követően a Semmelweis Egyetem nem vállal felelősséget az egyetemi e-mail címre címzett levelekért.

(3) A foglalkozásra irányuló jogviszony megszüntetésekor vagy megváltoztatásakor az Informatikai Főigazgatóság adott területért felelős munkatársai feladatai:
   a) jogosultságok megszüntetése vagy módosítása, dokumentálása;
   b) a munkahelyi vezető kezdeményezésére a távozó felhasználó (egyetemi munkájához kapcsolódó) elektronikusan tárolt információit, e-mail-jeit és az egyéb, általa létrehozott hivatalos adatokat le kell másolni és biztosítani szükséges a kilépő dolgozó által használt szerver tárhely hozzáférését a munkahelyi vezető által kijelölt felhasználó számára, és az e-mail-ek meghatározott időtartamig történő átirányításával.

5.2.4 Informatikai vagyontárgyak visszaszolgáltatása

(1) 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 vagy megállapodása lejár vagy megszűnik. A visszaszolgáltatás azon szervezeti egység részére történik, ahol a vagyontárgy nyilvántartásba van véve.

(2) Az Informatikai Főigazgatóság, vagy a helyi illetékes informatikai szervezet az eszköz leadásakor ellenőrzi az átvett és az Elszámoló lapon rögzített hardver-, szoftver specifikáció meglétét és üzemképes állapotát.

5.2.5 Hozzáférési jogok megszüntetése

(1) 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 vagy megállapodásuk lejár,

vagy azt módosulás esetén a változáshoz kell igazítani, továbbá ha jogellenes használat történik.

(2) A változtatási kérelem benyújtásának biztosítása az érintett alkalmazott közvetlen vezetőjének a feladata, melyet a változást megelőzően, kell írásban jeleznie az Informatikai Főigazgatóság által meghatározott ügyrend szerint.

(3) A kérelmekben előírt feladatok végrehajtása az Informatikai Főigazgatóság feladata.

5.3 Az informatikai környezet fizikai védelme

5.3.1 Területek védelme, biztosítása

Az Egyetem Vagyonvédelmi és rendészeti szabályzata rendelkezik az Egyetem épületei, értékei és polgárai védelmének megszervezéséről, a figyelembe veendő szempontrendszerekről és a feladatkörökről.

5.3.1.1 Az informatikai helyiségek kijelölése, határzóna kialakítása

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

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

a) szerverek;
b) telefonközpontok;
c) hálózati elosztószekrények, központi hálózati eszközök;
d) alkalmazói és irodai szoftverek és informatikai rendszer- vagy eszköz dokumentációk törzspéldányai;
e) biztonsági mentések.

(3) Az informatikai helyiségek tételes nyilvántartásáról az informatikai főigazgató gondoskodik.

5.3.1.2 Fizikai belépés ellenőrzése

Az Informatikai Főigazgatóság 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.

5.3.2 Védett helyszínek

Az Egyetem helyiségei információbiztonsági szempontból négy kategóriába sorolhatók:

(1) 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, külön meghatározott szabályokkal.

Kiemelten védett kategóriába a következő helyiségeket kell sorolni:

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

(2) 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) a gerinchálózatot kiszolgáló aktív hálózati elemek elhelyezésére szolgáló helyiségek;
b) Informatikai Főigazgatóság, kari/tömbigazgatóság informatikai szervezete által használt raktár;
c) informatikai dolgozók napi munkavégzésre használt irodái, helyiségei.
d) mentések végzésére szolgáló helyiségek

(3) 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.

(4) 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

(1) Fizikai védelem, tűzvédelem

A fizikai védelmi és tűzvédelmi szabályokat az Egyetem Tűzvédelmi szabályzata, valamint Vagyonvédelmi és rendészeti szabályzata tartalmazza.

(2) A belépés rendje

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

a) belépés kizárólag erre felhatalmazott személyek számára lehetséges, ezt a beléptető rendszer általi kikényszerítéssel kell megvalósítani;
b) a kiemelten védett területekre vonatkozó belépési jogokat rendszeresen felül kell vizsgálni, a szükséges változtatásokat el kell végezni;
c) 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 Főigazgatóság Infrastruktúra Üzemeltetési Osztály vezetője a felelős.

5.3.2.2 A kiemelten védett helyiségben a munkavégzés szabályai

(1) A kiemelten védett területen történő munkavégzésre a következő biztonsági szabályok vonatkoznak:
   a) fokozottan kell érvényesíteni a munkavégzés megszervezésénél az információkhoz való hozzáférés minimalizálását, a szándékos károkozás megakadályozását;
   b) ha nem tartózkodik senki a kiemelten védett területen, akkor a területet biztonságosan le kell zárni, és rendszeresen ellenőrizni kell ezt az állapotot;
   c) a kiemelten védett területen külső szervezet alkalmazottja, csak felügyelettel és a következők betartásával végezhet munkát:
      ca) kiemelten védett területre külső személy alkalmazottja csak rendkívüli esetben és csak korlátozott ideig kaphat munkavégzésre engedélyt;
      cb) munkavégzésre jogosító engedélyt az informatikai főigazgató, vagy a kari/tömbigazgatóság informatikai szervezet vezetője adhat, az engedélyeket az IBF ellenőrzi;
      cc) 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 főigazgatót és az IBF-et;
   d) meg kell győződni róla, hogy a kiemelten védett területre történő belépéskor, a munkát végző személynél csak a munkavégzéshez szükséges elektronikus eszközök találhatók.

(2) 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 főigazgató adja ki, tartja nyilván és az IBF ellenőrzi.

5.3.2.3 Fokozottan védett helyszínek védelme

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

5.3.2.4 Általánosan védett helyiségek védelme

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

5.3.2.5 Egyéb helyszínek védelme

Az egyéb helyszínek védelmére vonatkozó szabályokat az Egyetem Tűzvédelmi szabályzata, valamint Vagyonvédelmi és rendészeti szabályzata tartalmazza.

5.3.2.6 Az informatikai logisztikai funkciókra elkülönített terület védelme

(1) 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.

(2) A logisztikai helyiségek védelmét, az oda való be-, és kilépést, szállítást az Egyetem Informatikai Főigazgatósága biztosítja.

5.3.2.7 Külső és környezeti veszélyekkel szembeni védelem

(1) 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.
(2) Az Egyetem Informatikai Katasztrófa Elhárítási Tervének elkészítésért az informatikai főigazgató felel.
(3) A Működés-folytonossági Tervek, eljárások elkészítése, tesztelése és karbantartása az informatikai főigazgató 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 és 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

(1) Az adatátvitelt biztosító, az információszolgáltatásokat támogató elektromos energiaátviteli és távközlési kábelhálózatot védeni kell az illetéktelen hozzáféréstől és a károsodástól:
   a) a táp és adat kábeleket lehetőleg föld, álpadló alatt, álmennyezet fölé vagy kábeltálcában kell vezetni;
   b) a rendezőszekrényeket minden esetben kulcsra kell zárni;
   c) az áramellátásért felelős kábeleket az adatkábelektől szeparáltan kell elhelyezni, megelőzve ezzel az interferenciát;
   d) kábelek típusát, állapotát (szakadt, rossz) egyértelmű azonosítást lehetővé tevő módon kell jelöléssel ellátni, valamint a szakszerű javításról gondoskodni;
   e) a kábelezés nyomvonalát és típusát kábelezési rajzokon és nyilvántartásokban kell rögzíteni, úgy, hogy az létesítményeken belüli pontos futásvonal és elhelyezés leolvasható legyen;
   f) a be- és átkötéseket minden esetben dokumentálnia kell az azt végző rendszergazdának, kivitelező szakembernek.
(2) Fentiekért az informatikai főigazgató felel, ideértve a zárható szekrények és helyiségek kulcsainak tárolását, nyilvántartását.
(3) 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:
   a) végpontok és elérési pontok (pl. fali ajzat) elzárása szükséges;
   b) alternatív, redundáns vonalak biztosítása;
   c) üvegszálas kábel használata a hagyományos UTP helyett;
   d) 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, előírás szerűen kell elvégezni. A karbantartás megvalósításáért az informatikai főigazgató a felelős.

5.3.3.4 Vagyontárgyak – telephelyről való eltávolítás, elszállítás

(1) Informatikai eszköz csak az Informatikai Főigazgatóság adott osztályának vezetője, vagy a kari/tömbigazgatóság informatikai szervezet vezetője engedélyével vihető ki az Egyetem székhelyéről vagy telephelyéről külső szervizbe.
(2) 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) a szállítást csak egyetemi alkalmazott (informatikus, rendkívüli esetben kézbesítő) vagy az Egyetemmel szerződésben álló szerviz cég munkatársa, vagy megbízott futár végezheti;
   b) 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;
   c) a szállítandó eszközöket megfelelő csomagolással kell ellátni a fizikai károsodások megelőzése érdekében;
   d) a nem nyilvános adatokat tartalmazó adathordozók szállítása esetén (pl.: mentések) az alábbi kontrollokat is alkalmazni kell:
      da) zárható tároló doboz alkalmazása;
      db) olyan csomagolás alkalmazása, mely felbontás után nem zárható vissza az eredeti formában, így az esetleges illetéktelen hozzáférés felderíthető.
(3) 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

(1) Az Egyetem tulajdonában lévő mobil eszközök (hordozható számítógép, okostelefon, táblagép, stb.), munkavégzés céljából kerültek átadásra, ezért 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 engedéllyel használhatók.
(2) A használatot a szervezeti egység vezetője hagyja jóvá.
(3) Az alábbi irányelvek betartása kötelező:
   a) az eszköz vagy az egyetemi információkat tartalmazó média nem maradhat felügyelet nélkül nyilvános helyen, gépkocsiban;
   b) az Egyetem informatikai rendszeréhez kapcsolódni csak az Egyetem eszközével és az Informatikai Főigazgatóság által biztosított módon (pl. webmail, Novell authentikáció, VPN csatorna) lehet;
   c) a gyártó előírásait mindig be kell tartani az eszköz védelme érdekében;

d) amennyiben az Egyetem informatikai rendszeréhez idegen tulajdonú eszköz csatlakoztatása szükséges, arra csak az informatikai főigazgató és az IBF engedélyével kerülhet sor, írásbeli engedély alapján, amely tartalmazza a csatlakozási ok megjelölését és időtartamát is;
e) mobil eszköz elhagyása, elvesztése vagy másnak tartós használatra való átadásakor, amennyiben az eszközön be van állítva valamilyen egyetemi informatikai szolgáltatás elérése, a felhasználó köteles bejelentést tenni az egyetem Informatikai Főigazgatóságának a szolgáltatás és az eszköz közti kapcsolat mielőbbi törlése érdekében.

(4) A VPN kapcsolatok szabályos beállításáért az informatikai főigazgató felelős.

5.3.3.6 Az informatikai eszközök biztonságos selejtezése és újrafelhasználása

(1) Az informatikai eszközök selejtezésével kapcsolatban a Selejtezési szabályzat előírásait kell alkalmazni.
(2) Az adatokat tartalmazó informatikai eszközök selejtezésére az alábbi speciális szabályok vonatkoznak:
a) Az adathordozó, adattároló törlését vagy újra felhasználásra való előkészítését (és az ehhez kapcsolódó műveleteket) csak az Informatikai Főigazgatóság, vagy a kari/tömbigazgatóság informatikai szervezetének munkatársa végezheti el. Minden raktározási és tárolási lépésben az illetéktelen hozzáféréstől védve kell tárolni az eszközöket.
b) Valamennyi olyan információ-feldolgozó eszközt, amely adattároló eszközt foglal magában, ellenőrizni kell, hogy az azon tárolt adatok és szoftverek a selejtezést megelőzően végleges eltávolításra vagy biztonságos felülírásra kerüljenek.
c) A használatból kivont információ-feldolgozó eszközöket egy hónapig raktározni kell az esetleges visszaállítás érdekében, feliratozva, illetéktelen hozzáféréstől védve.
d) Adathordozók megsemmisítését vagy újra felhasználását az adatgazda kezdeményezheti.
e) Az eszközökben található adathordozókról az adatokat újra felhasználás, az eszköz használatból történő végleges kivonása előtt (az 1 hónapos várakozási idő után) visszaállíthatatlan módszerrel törölni kell.
f) A bontásra, megsemmisítésre átadott gépek esetében is visszaállíthatatlan módszerrel törölni kell az adatokat.
g) 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, valamint a szerződőnek garanciát kell vállalni az adatok visszaállíthatatlan megsemmisítésére, a teljes és időbeli korlátozás nélküli titoktartásra is.

5.3.3.7 Visszaállíthatatlan törlés

(1) 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.
(2) 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

(1)Az üzemeltetés eljárásrendjét a SZMSZ-ben meghatározott struktúrában kell kialakítani:
   a) „Informatikai szabályzatok” szintje (IBSZ, Informatikai 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;
   b) „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:
      ba) komponensek;
      bb) rendszer funkciói;
      bc) rendszer illeszkedési pontjai;
      bd) rendszerrel kapcsolatos üzemeltetési feladatok felsorolása és dokumentálási követelményei;
      be) rendszerrel kapcsolatos feladat- és felelősségi körök;
      bf) rendszerrel kapcsolatos katasztrófa elhárítási tervek.

(2)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 főigazgatóval engedélyeztetni.

5.4.3 Fejlesztési, tesztelési és üzemeltetési eszközök

(1) 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).

(2) A tesztrendszerrel szemben támasztott követelmények:
   a) a tesztrendszerben lévő jogosultságoknak azonosnak kell lenni az éles rendszerben lévő jogosultságokkal;
   b) amennyiben a teszteléshez magasabb jogosultság szükséges a tesztelő személyeknek, mint amivel az éles rendszerben rendelkeznek, akkor anonim adatbázis használata szükséges;
   c) külső partnerek csak anonimizált adatbázist használhatnak teszteléshez.

(3) A fejlesztői környezetben az adatok csak anonimizált módon kerülhetnek tárolásra.

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

(5) 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. 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 kódok ellen

5.4.4.1 Vírusvédelem

(1) Az Informatikai Főigazgatóság vírusvédelmi felelőseinek kell gondoskodniuk 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.
(2) 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 Főigazgatóság, vagy a kari/tömbigazgatóság informatikai szervezet munkatársai végezhetik az informatikai üzemeltetésre vonatkozó belső szabályok alapján.
(3) A felhasználók kötelesek az adathordozón kapott bármilyen állományt a számítógépre telepített vírusvédelmi szoftverrel leellenőrizni. Ahol lehetséges, az ellenőrzést az automatikus beállításokkal kell kikényszeríteni.
(4) A védelmi programok segítségével meg kell valósítani a munkaállomások valós idejű ellenőrzését, a vírusvédelmi adatbázisok rendszeres és automatikus frissítését, a teljes fájlrendszer ellenőrzések heti rendszerességű ütemezését. Az ellenőrzéseket a felhasználók munkáját nem akadályozó időpontban kell elvégzeni.
(5) 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 főigazgatót és az IBF-et.
(6) 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.
(7) A törlendő állományok körét – az IBF és az adatgazdák véleményének figyelembe vételével – az informatikai főigazgatónak kell meghatározni, és arról a Vírusvédelmi felelősnek kell naprakész nyilvántartást vezetni.

5.4.5 Jogosultság kezelés

5.4.5.1 A felhasználói azonosító és jogosultság menedzsment célja és általános szabályai

(1) A jogosultság kezelés célja, hogy az Egyetem informatikai rendszerében a felhasználói hozzáférés teljes életciklusában (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;

(2) Az Egyetem tulajdonában vagy használatában lévő valamennyi informatikai eszközön tárolt adathoz hozzáférés csak az Egyetem és a felhasználó közötti jogviszony létrejötte után és a jogosultság ellenőrzését követően lehetséges, megvédve az informatikai rendszereket és adatokat a jogosulatlan hozzáféréstől.
(3) A felhasználókat megillető jogosultságokat az adatgazdák határozzák meg.
(4) Az egyetemi munkavállalói jogviszonya alapján minden informatikai eszközt használó munkavállalót megilletnek az ún. alap felhasználói jogosultságok.
(5) Az Egyetem tulajdonában vagy használatában lévő valamennyi informatikai rendszer esetében az azonosítást hitelesítő mechanizmust kell működtetni.
(6) A hitelesítés általános módszere a felhasználói azonosítóhoz tartozó jelszó ismeretének ellenőrzése, a magas információbiztonsági kockázatú rendszerek esetén kiegészítve a birtoklás alapú hitelesítéssel (pl.: intelligens kártya, token és PIN kód - jelszó).
(7) Az Egyetemnél korlátozni kell:
   a) az olyan kiváltságos hozzáférési jogokat (pl. local admin jogosultság), amelyek lehetővé teszik, hogy a felhasználó a biztonsági és egyéb kritikus rendszerbeállításokat módosíthassa,
   b) a nyilvános hálózatokon keresztül engedélyezett hozzáféréseket.
(8) 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.
(9) Az információkhoz való jogosulatlan hozzáférés megakadályozása érekében minden esetben zárolni kell a munkaállomást, ha a felhasználó – akár rövid időre is – felügyelet nélkül hagyja azt.

5.4.5.2 Felhasználók regisztrálása

(1) A felhasználói jogosultságok kiadását, módosítását és visszavonását dokumentált eljárások alapján kell végezni, a kiosztott jogosultságokat nyilván kell tartani.
(2) A felhasználók azonosítása központilag nyilvántartott felhasználói azonosítók használatával történik. Ahol technológiailag nem kivitelezhető ettől eltérni- szakrendszerek esetén- az IBF engedélyével lehetséges.
(3) 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.
(4) A felhasználói azonosítókat a jogosultságkezelő felelős, alkalmazások esetében az alkalmazás adminisztrátor menedzseli és tartja nyilván.
(5) A felhasználói azonosítókat tartalmazó állományokat csak a jogosultságkezelési felelős vagy az alkalmazás adminisztrátor módosíthatja.
(6) A felhasználói azonosítók visszavonásig, lejáratig vagy újrahitelesítésig érvényesek.
(7) A felhasználói azonosítókat inaktív (felfüggesztett) állapotba kell helyezni, ha
   a) tulajdonosuk munkavégzésre irányuló jogviszonya megszűnt;
   b) 5 egymást követő sikertelen bejelentkezési kísérlet történt;
   c) ha 6 hónapig nem történik bejelentkezés.

5.4.5.3 Felhasználói jogosultságok alapszabályai

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

a) az alapértelmezett azonosítókat át kell nevezni és jelszavukat meg kell változtatni;
b) a felhasználói azonosítókat minden esetben egyedi felhasználókhoz kell rendelni és tulajdonosát egyértelműen azonosítani kell;
c) a közös felhasználói azonosítók használatát csak kivételes esetekben, az informatikai főigazgató engedélyezheti;
d) az anonim azonosítókat fel kell függeszteni vagy törölni kell, továbbá amennyiben bizonyos alkalmazások igénylik ezek használatát, akkor jogosultságukat olvasási korlátozással kell ellátni;
e) a ritkán használt azonosítókat a használat idején kívül fel kell függeszteni és csak a használat idejére aktiválni, majd használat után újra fel kell függeszteni.

5.4.5.4 Kiemelt felhasználói jogosultságok kezelése

(1) 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 Főigazgatóság feladata.

(2) A biztonsági incidensek vagy visszaélések megelőzése érdekében a kiemelt felhasználói jogosultságok miatt keletkezett kockázatokat csökkenteni kell, továbbá figyelemmel kell kísérni ezek használatát.

A kiemelt felhasználói jogosultságok kiosztásával kapcsolatos alapvető biztonsági szabályok:

a) a kiemelt felhasználói jogosultságokat esetileg kell kiosztani, és a használat idejére kell korlátozni, majd vissza kell vonni;
b) 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 főigazgató, valamint az IBF feladata;
c) 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;
d) a kiemelt felhasználók tevékenységét naplózni kell és rekonstruálható eseményrögzítést lehetővé tevő eszközzel rögzíteni kell;
e) a tevékenységrögzítésből felvett eseményeket, „naplókat” az Informatikai Főigazgatóság kontrollálja és az IBF bevonásával negyedévente, szúrópróbaszerűen ellenőrzi.

5.4.5.5 Kiemelt felhasználói jogosultságok alapszabályai

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

(2) Ezen alapszabályok a következők:
   a) 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 főigazgató engedélyével lehet;
   b) rendszeradminisztrátori azonosítókat minden esetben egyedi felhasználókhoz kell rendelni és tulajdonosát egyértelműen azonosítani kell;
   c) a ritkán használt, magas jogosultságú azonosítókat a használat idején kívül fel kell függeszteni és csak a használat idejére aktiválni, majd használat után újra felfüggeszteni;
   d) 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;
   e) a rendszerazonosítók jelszavait elzárva lezárt borítékban a területileg illetékes informatikai vezetőnél páncélszekrényben kell tárolni és minden változtatás esetén, továbbá évente kötelezően cserélni kell;
   f) a rendszerazonosítókat csak alkalmazások használhatják belépésre, azok felhasználói azonosítóként nem használhatók;
   g) a beépített, lokális rendszeradminisztrátori azonosítókat át kell nevezni, jelszavukat elzárva, lezárt borítékban a területileg illetékes informatikai vezetőnél páncélszekrényben kell tárolni.

5.4.5.6 Jogosultságok kiosztására és nyilvántartására vonatkozó szabályozások

(1) 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.
(2) 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.
(3) Az Egyetem informatikai rendszereiben biztosítani kell, hogy az adatvédelmi tisztviselőnek és egyéb ellenőrző szerveknek megtekintési jogosultsága legyen a vizsgálat alapján érintett szervezeti egység vizsgálattal érintett adatállományához.
(4) A rendszerfejlesztési és informatikai üzemeltetési jogosultságokat szét kell választani.
(5) Az Informatikai Főigazgatóság végzi a jogosultságok beállítását, visszavonását és ellenőrzését. 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.
(6) A szervezeti vezető rendszeresen, az IBF kezdeményezésére köteles felülvizsgálni az irányítása alá tartozó felhasználói csoportok, felhasználók jogosultságait. A felülvizsgálatot követően intézkedési javaslatot kell tenni és a szükségtelen jogosultságokat vissza kell vonni.

5.4.5.7 Hitelesítés és jelszavak

(1) Annak érdekében, hogy a jelszavakkal történő központi hitelesítés kellően biztonságos legyen, gondoskodni kell a megfelelő erősségű jelszavak használatáról:
   a) a felhasználói jelszavak legalább 8 karakterből álljanak,
   b) vegyesen kis és nagybetűket, számokat és írásjeleket is tartalmazzanak,
   c) a felhasználó jelszavak érvényességi idejét az Informatikai Főigazgatóság a bekövetkezett incidensek hatására és az IBF javaslatára az informatikai főigazgató utasításának megfelelően, kockázatelemzés alapján korlátozhatja.
   d) felhasználó esetében többszöri egymás utáni próbálkozás után zárolja az azonosítót,
   e) rendszergazdák jelszavát rendszeresen cserélni kell,
   f) rendszergazda jelszavak minimum 12 karakterből álljanak,
   g) rendszergazda esetében 3 próbálkozás után zárolja az azonosítót,
   h) a technikai azonosítók a rendszergazdai azonosítókkal megegyezőek, viszont lejárati idejük 12 hónap,
   i) a kezdeti jelszót az első belépés alkalmával kötelezően meg kelljen változtatni.

(2) A jelszavakat tartalmazó fájlokat (valamint ezeknek a jelszavakat tartalmazó részét) visszafejthetetlen (egyirányú) kódolással kell tárolni, ezekhez az állományokhoz hozzáférési jogosultságot csak az Informatikai Főigazgatóság, vagy a kari/tömbigazgatóság Informatikai szervezet kijelölt dolgozói kaphatnak.

(3) A jelszavakat tartalmazó fájlok sérülését, jogosulatlan hozzáférési kísérleteket az Informatikai Főigazgatóság, vagy a kari/tömbigazgatóság informatikai szervezet dolgozóinak azonnal jelentenie kell az IBF-nek és az informatikai főigazgatónak.

(4) Tilos a jelszót:
   a) más tudomására hozni;
   b) más számára ismert vagy hozzáférhető helyen tárolni, így különösen a számítógépre (monitorra) ragasztani.

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

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

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

(8) a jelszavak olvashatatlanul jelenjenek meg a képernyőn és

(9) titkosítva legyenek a hálózati adatátvitel során.

(10) Az egyes rendszerekre vonatkozóan az egyes kiemelt felhasználói azonosítókra vonatkozó szabályokat az 5.4.5.4 számú fejezet tartalmazza.

(11) A speciális felhasználókhoz (pl. kiemelt jogosultságú, közös használatú azonosítók) tartozó jelszavakra a következő – általánostól eltérő- szabályok vonatkoznak:
   a) a speciális felhasználók jelszavait lezárt borítékban – amennyiben az Informatikai Főigazgatóság látja el az adott szervezeti egységnél a felhasználási támogatást, akkor az Informatikai Főigazgatóság, egyébként a kari/tömbigazgatóság – informatikai szervezeti vezetőjének a páncélszekrényében kell őrizni;

b) speciális felhasználók jelszavához csak indokolt esetben lehet hozzáférni;
c) a boríték felbontásáról minden esetben jegyzőkönyvet kell készíteni, megjelölve a speciális felhasználó igénybe vételének pontos okát és a felbontók személyét (lásd a 7. **Hiba! A hivatkozási forrás nem található.**számú mellékletet);
d) 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.

5.4.5.7.1. Jelszó kiválasztás szabályai

(1) A következő szabályok betartása a felhasználók felelősségi körébe tartozik:
a) tilos a login nevet használni jelszóként bármilyen formában;
b) tilos a saját vezeték vagy keresztnév használata;
c) tilos a jelszót valamely funkcióbillentyűhöz hozzárendelni.
(2) A jelszavakkal kapcsolatosan ajánlottak az alábbiak:
a) ne legyenek könnyen kitalálhatóak (pl. 11111, 123456, qwerty, stb.);
b) ne legyen szótárakban található címszó, mert sok kódfejtő program ezek és más gyakori jelszavak végig próbálásával igyekszik feltörni a titkosítást;
c) ne legyen a felhasználó személyéhez vagy környezetéhez köthető (pl. telefonszám, autórendszám, partner, gyermekek, háziállatok neve, stb.);
d) ne legyen 8 karakternél rövidebb a jelszó;
e) ajánlott számok, betűk és írásjelek keverékét használni.

5.4.5.8 Kiadás és érvényesítés

(1) A jogosultságkezelő felelős a jogosultságigénylő lap és az előzetes ellenőrzés (összeférhetetlen jogosultságok) végrehajtása után a felhasználóhoz:
a) hozzárendel egy felhasználói azonosítót;
b) megadja a felhasználó kezdeti jelszavát, aminek
ba) meg kell felelnie a jelszavakkal kapcsolatos szabályoknak és
bb) egyedinek kell lennie, nem használható rendszeresen ugyanaz a karaktersorozat,
c) megadja a felhasználó számára igényelt jogosultságokat.
(2) A jogosultságkezelő felelős a felhasználói jogosultság igénylőlapon.
(3) Rögzíti a felhasználói azonosítót.
(4) Dokumentálja az azonosító létrehozásának és jogosultságok beállításának időpontját.
(5) Sem a jogosultságkezelő felelős, sem más rendszergazda nem adhatja meg a jogosultságot, amennyiben megítélése szerint az igényelt jogosultság nyilvánvalóan megsérti az információbiztonsági feladatkör-elhatárolási szabályok valamelyikét. A Jogosultságkezelő felelős – a felhasználói jogosultság igénylőlap másolatának továbbításával és az eljárás felfüggesztésének közlésével – tájékoztatja az IBF-et.
(6) 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 főigazgató engedélyével lehet beállítani.

5.4.5.9 Felhasználói azonosító és jelszó módosítása

(1) A felhasználói azonosító módosítását a felhasználó kezdeményezheti névváltoztatáskor (pl. házasságkötés miatt) email vagy a GLPI rendszerben történő bejegyzés útján.
(2) Felhasználói azonosító módosítást kezdeményezhet az adatgazda és a jogosultságkezelő felelős is az egyes rendszerek felhasználó azonosító konvencióinak szabványosítása miatt és/vagy új azonosító-képző szabályok bevezetésekor.
(3) A felhasználói azonosító módosításakor a kiadás és érvényesítés szabályait kell értelemszerűen alkalmazni.
(4) 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.

5.4.5.10 Felfüggesztés, visszavonás

(1) Foglalkoztatási jogviszony megszüntetése esetén a távozó munkatársak adatait az Emberierőforrás-gazdálkodási Főigazgatóság megküldi az Informatikai Főigazgatóságnak.
(2) A jogosultságkezelő felelős a bejelentést követően felfüggeszti a felhasználó azonosítóit, visszavonja a rendszerekhez kapcsolódó felhasználói jogosultságokat, valamint gondoskodik az adott felhasználó e-mailjeinek megadott címre történő továbbításáról.
(3) A jogosultságok visszavonását – amely rendszerekben ez megvalósítható – automatizmusok támogatják.
(4) A visszavonási eljárás dokumentálására a kiadás és érvényesítés dokumentációs szabályait kell alkalmazni.
(5) 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.
(6) A jogosultságok felfüggesztésre kerülnek, ha
   a) a jogosult:
      aa) munkaviszonya megszűnik/megszüntetésre kerül;
      ab) mentesítve lett a munkavégzési kötelezettség teljesítése alól;
      ac) munkakörének megváltozása nem indokolja a jogosultság fenntartását.
   b) külsős jogosult esetén:
      ba) a megbízás időtartamának lejártával;
      bb) törvényben és a két fél között köttetett szerződés kizáró okainak bekövetkeztével;
      bc) felmondással;
      bd) külön törvényben meghatározott esetben.

5.4.5.11 Felhasználói hozzáférési jogosultságok felülvizsgálata

Rendszeres időközönként (de legalább évente) a szakterületi adatgazdáknak felül kell vizsgálniuk a felhasználói hozzáférési jogosultságokat.

5.4.6 Hálózati szintű hozzáférés ellenőrzés

(1) Az Egyetem számára megbízható hálózati kapcsolatnak számít a belső számítógépes hálózat, minden egyéb hálózat nem megbízható hálózatnak számít, olyannak, amelyről azt kell feltételezni, hogy potenciális veszélyt jelenthet az informatikai biztonság számára.
(2) A belső számítógépes hálózatot felhasználási céljuktól függően logikailag különválasztott alhálózatokba, VLAN-okba kell rendezni.
(3) 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 IBF pedig 6 havonta ellenőriz.
(4) Kapcsolati listát csak az informatikai főigazgató engedélyével lehet felvenni, módosítani, törölni.
(5) Az Egyetem és valamennyi partnere között gondoskodni kell a biztonságos, hiteles adatátvitelről, adatcseréről.
(6) A megbízható és a nem megbízható hálózatokat csak az Egyetem tűzfalán keresztül lehet összekapcsolni.
(7) Az Egyetemi hálózatban lévő számítógép egyedi külső hálózati kapcsolattal (pl.: modem, ADSL, Webstick) csak indokolt esetben, az adott szakterületi vezető kezdeményezése alapján az informatikai főigazgató egyedi engedélyével rendelkezhet. Az eszköz telepítését, beüzemelést csak az Informatikai Főigazgatóság, 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.
(8) Távoli felhasználók hozzáférésére jogosító engedély, kulcs maximálisan 2 évre adható ki.
(9) Távoli felhasználók hozzáféréseit a tényleges (logikai) hozzáférésekkel meg kell feleltetni.
(10) Az Egyetem számítógép-hálózata és külső hálózatok közötti kapcsolat során csak az engedélyezett kommunikációs protokollok továbbíthatók, minden egyéb továbbítása tilos.
(11) Az Egyetem számítógép-hálózatában alkalmazható külső kommunikációs protokollok köréről – a határvédelmi felelős javaslatára az IBF véleményének figyelembe vételével – az informatikai főigazgató dönt.
(12) Az Egyetem számítógép-hálózata kizárólag az Informatikai Főigazgatóság által meghatározott tartományos rendszer szerint működhet. Tilos olyan munkaállomást csatlakoztatni a hálózatra, amely
   a) nem megbízható hálózati kapcsolattal is rendelkezik;
   b) nem tagja a megfelelő egyetemi tartománynak és nem rendelkezik jelen szabályzatban előírt védelmi mechanizmusokkal (pl. naprakész vírusvédelmi megoldás).
(13) A határvédelmi felelős nyilvántartást vezet:
   a) az engedélyezett protokollokról;
   b) a hálózati határvédelem információbiztonsági architektúra elemeinek beállításairól.
(14) Az Egyetem számítógép-hálózatának vezeték nélküli hálózati szegmensein, valamint a nem megbízható csatornán keresztüli megbízható kapcsolat során titkosított adatkapcsolatot kell kialakítani.
(15) A titkosított adatkapcsolat technikai specifikációját a Határvédelmi felelős készíti el, melyet az IBF véleményez és az informatikai főigazgató hagy jóvá.

5.4.6.1 Behatolás érzékelés

(1) Az IBF legalább kétévente – független külső technikai szakértők igénybe vételével, az Egyetem informatikai munkatársának az állandó felügyelete mellett – ellenőrzött behatolási kísérletet végeztet, melynek költségét meg kell tervezni.
(2) A behatolási kísérlet idejéről és módjáról – az informatikai főigazgató és az IBF kivételével – az Egyetem dolgozói és szerződéses partnerei nem szerezhetnek előzetesen tudomást.
(3) A behatolási kísérletről részletes jelentést kell készíteni, amelyet a kísérlet lezárultával az informatikai főigazgató és az IBF elemeznek és értékelnek.
(4) A fentiektől eltérő behatolási kísérletet, szándékos támadásként, ellenséges szándékú behatolásként kell értékelni és ennek megfelelően eljárni.
(5) Minden egyetemi munkatárs, aki a védelemben hiányosságot fedez fel, köteles annak kihasználása nélkül haladéktalanul tájékoztatni az IBF-et.

5.4.6.2 A távoli eléréssel kapcsolatos biztonsági szabályok

(1) Távoli elérést biztosító megoldás (RDP, VNC, VPN, Proxy szerver, stb.) létesítése kiemelt biztonsági kockázatot jelent, ezért használatuk, üzemeltetésük során kiemelt figyelem szükséges, a távoli elérést biztosító jogok kiadása kontrollált folyamat mentén történik.
(2) 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

(1) A kritikus, különösen érzékeny adatokat tartalmazó rendszerek távoli elérése előzetes engedélyhez kötött. Ebbe a körbe tartoznak a medikai-, gazdálkodási- (SAP), ügyviteli- (Poszeidon), tanulmányi- (Neptun) és a különböző biztonsági rendszerek.
(2) Az engedélyezés rendjét az Informatikai Főigazgatóság honlapján közzétett tájékoztató tartalmazza. Az igénylés Online VPN igénylő rendszeren keresztül lehetséges.

5.4.6.2.2. A VPN használata

(1) Az Egyetem által biztosított VPN rendszer a felhasználó feladatkörében foglalt tevékenységek elvégzésére használható.
(2) A távoli elérés csak működő személyi tűzfal, valamint vírusvédelmi szoftver mellett kezdeményezhető.
(3) A VPN kliens munkaállomást a VPN használat ideje alatt a felhasználó más személynek semmilyen formában nem engedheti át.
(4) A távoli felhasználók tevékenysége naplózásra kerül.
(5) Jelen szabályzat be nem tartásából eredő károkért a távoli felhasználó felel.
(6) A VPN rendszer telepítéséhez és használatához előzetesen szükséges, hogy a távoli felhasználó internet kapcsolattal rendelkezzen.

5.4.6.3 Elkülönítés a hálózatokban

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

(2) Az adott helyen a megfelelő technológia kiválasztása és beüzemelése a Határvédelmi felelős feladata, melyet az informatikai főigazgató hagy jóvá.
(3) 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) a konfigurációs táblák és ACL-ek minden változásáról naplóbejegyzés készül és megőrzésre kerül;
b) az eszközök zárt szekrényben vannak elhelyezve.

Gateway/tűzfal:
A szabályok leírását az Informatikai Főigazgatóság Informatikai üzemeltetési és hálózati szabályzata tartalmazza.

5.4.7 Operációs rendszer szintű hozzáférés-ellenőrzés

5.4.7.1 Biztonságos bejelentkezési eljárások

(1) 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.
(2) A biztonságos beléptetési folyamatnak az alábbi követelményeket kell teljesítenie:
   a) a rendszer a belépés előtt a lehető legkevesebb információt szolgáltassa a technológiáról;
   b) sikertelen belépés esetén a rendszer nem jelölheti meg, hogy a megadott adatok mely része hibás;
   c) limitálni kell a sikertelen belépések számát és a belépési folyamat maximális idejét.
(3) A fenti követelmények teljesülését a rendszer paramétereinek beállításával kell megvalósítani. A beállítások megfelelősége az informatikai főigazgató által megbízott munkatárs feladata és felelőssége.

5.4.7.2 Felhasználó azonosítása és hitelesítése

A felhasználók azonosítására és hitelesítésére vonatkozó eljárásokat az 5.4.5.7 Hitelesítés és jelszavak tartalmazza.

5.4.7.3 Kapcsolati idő túllépése

(1) Az inaktív összeköttetéseket 15 perc időtartamú inaktivitás után bontani vagy zárolni kell.
(2) 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.)

(1) A mobil eszközök felhasználói felelősek az általuk használt eszközök biztonságos használatáért:

a) a védett biztonsági osztályba tartozó adatok kiszivárgása, elvesztése, megsérülése miatt bekövetkezett károk esetén;
b) a jogosulatlan szoftverhasználatból eredő jogi következmények esetén;
c) vírusok és más, az Egyetem informatikai rendszerét veszélyeztető szoftverek okozta károk esetén;
d) lopás és az ebből származó károk esetén.

(2) A mobil munkaállomásokon védett biztonsági osztályba sorolt adatokat csak az Informatikai Főigazgatóság 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

(1) A távoli munka végzését a munkáltatói jogkör gyakorlója rendelheti el vagy engedélyezheti. Az elrendelés mérlegelése során ki kell kérnie az IBF véleményét a technikai és információbiztonsági kérdések tekintetében.

(2) A távoli munkavégzés technikai feltételeinek meghatározásakor a következő szempontokat kell figyelembe venni:
a) távoli munkavégzéssel kapcsolatosan nyilvános hálózatokon kommunikációt csak titkosított formában szabad használni;
b) 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.

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

(4) A felhasználó köteles a távoli munkavégzésre előírt szabályokat teljes körűen betartani.

5.4.9 Biztonsági mentés

5.4.9.1 Mentési stratégia

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

(2) Biztonsági mentéseknek kell készülnie:
a) az online elérhető (éles, tartalék, fejlesztői) adatbázisokról és fájlrendszer könyvtárakról;
b) az offline elérhető (archivált) adatbázisokról és fájlrendszer könyvtárakról;
c) szoftverek telepítőkészletéről.

(3) Az egyes rendszerek üzemeltetőinek minden hatáskörükbe tartozó rendszerre mentési tervet kell készíteniük. A mentési terveknek tartalmaznia kell legalább az alábbiakat:
a) mentések követelményei;
aa) mentés tárgya, gyakorisága;
ab) mentés elkészítésére rendelkezésre álló idő;
ac) mentés visszatöltésére rendelkezésre álló idő;
b) mentések típusai (teljes, inkrementális, szinkronizált);
c) mentések állományai (mentett adattartalom);

d) mentések példányszáma;
e) mentések időpontjai;
f) mentések megtartásának időtartama;
g) mentések titkosítása.

(4) Az adatgazdák által meghatározott archiválást írásbeli kérésükre, az általuk készített terv alapján kell végezni.

5.4.9.2 Mentések általános szabályai

(1) Automatikus napi mentések esetén a mentésekért felelős rendszergazdának ellenőrizni kell annak helyességét, hiba esetén automatikus értesítést kell küldenie a mentési felelős számára.

(2) A mentéseket tartalmazó adathordozók kezelését egyértelműen és visszakereshető módon kell nyilvántartani. A nyilvántartás adatai:
a) a rendszer (alkalmazás) elnevezése;
b) a mentés jellege;
c) a mentés példánysorszáma és az összesen készült példányok száma;
d) az adatállomány neve;
e) a mentés időpontja.

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

(4) 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.

(5) A mentési eljárásokat úgy kell kialakítani, hogy a mentések minden rendszer esetén 2 példányban készüljenek.

(6) A mentések egyes példányait az alábbi helyszíneken kell tárolni:
a) az első példányt abban a helyiségben kell tárolni, ahol a mentés történik vagy abban a létesítményben, ahol a mentés visszatöltése elvégezhető;
b) a második példányt az adott rendszer tartalék központjában; annak hiányában az Egyetem egy erre kijelölt, az első példány tárolási helyétől kellő földrajzi távolságban lévő helyiségében.

(7) 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

(1)A nagy mennyiségű adat rögzítésére és tárolására képes eszközök és számítógép-perifériák:
a) CD (DVD) lemezek írására alkalmas eszközök;
b) hordozható merevlemezegységek és más nagykapacitású mobil háttértárolók;

c) a számítógéptől függetleníthető memóriák (pl. memory card), vagy ilyen funkciójú egyéb eszközök (pl. pendrive).

(2) Távoli 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 lehet.

(3) A külső/belső ellenőrzésekhez az adatszolgáltatást a külső/belső ellenőrző szerv által meghatározottak szerint kell a kijelölt kapcsolattartóknak biztosítaniuk.

5.4.11 Figyelemmel követés (naplózás és monitoring)

5.4.11.1 Naplózás általános szabályai

(1) A különböző rendszerek naplóállományainak egységes értelmezhetőségének érdekében olyan naplózási architektúrát kell kialakítani, ami biztosítja, hogy:
   a) ahol a technikailag lehetséges, a naplózás szerveroldalon történjen;
   b) a naplózás a lehető legkevesebb számú naplóállomány használatával történjen;
   c) automatikus mechanizmus gondoskodjon az egyes eszközök rendszerórájának szinkronizálásáról;
   d) automatizált megoldások támogassák a különböző naplóállományok összefésülését, feldolgozását és elemzését.

(2) A naplózási architektúra dokumentációjáért az informatikai főigazgató felelős.

(3) Az egyes rendszerekben a rendszergazdák felelősek a naplózási beállítások naprakészségéért.

(4) 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 tudná tenni.

(5) Az egyes naplóállományokhoz, vagy azok részeihez olvasási jogosultsággal rendelkezhet (amennyiben munkaköre, feladata ellátásához arra szüksége van):
   a) a rendszerek alkalmazás Adminisztrátorai;
   b) az informatikai főigazgató;
   c) az IBF;
   d) a kari/tömbigazgatóság informatikai szervezeti vezetője.

(6) A naplóállományokhoz való hozzáférési jogosultságokat az informatikai főigazgató hagyja jóvá, a rendszergazdák dokumentálják, az IBF ellenőrzi.

5.4.11.2 Naplózandó események

(1) Az Egyetem informatikai rendszerében automatikus naplót kell vezetni az informatikai rendszer biztonsági szempontjából lényeges tevékenységekről.

(2) A naplózásnak ki kell terjednie:
   a) az IBSZ-ben meghatározott eseményekre;
   b) az arra felhatalmazással rendelkezők által meghatározott, ideiglenesen naplózandó eseményekre.

(3) Ideiglenes naplózást rendelhet el a naplózandó esemény és a naplózás időtartamának és céljának pontos megjelölésével, írásban:
   a) az adatgazda;

b) a szakterületi vezető.

(4) A naplózandó események köréről az Informatikai Főigazgatóság, valamint a kari/tömbigazgatósági informatikai szervezet arra kijelölt munkatársai vezetnek naprakész nyilvántartást, melyről tájékoztatják az IBF-et.

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

(6) Az IBF legalább félévente ellenőrzi, hogy az egyes rendszerek naplózási beállításai megfelelnek-e a naplózási események nyilvántartásának.

5.4.11.3 Események meghatározása

(1) 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.

(2) Az automatikusan készülő naplókban legalább az alábbi eseményeket kell rögzíteni:

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

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

a) a felhasználó azonosítóját;
b) a számítógép azonosítóját (IP cím);
c) a dátumát és időpontját;
d) a munkaállomás, szerver vagy hálózati eszköz azonosítóját;
e) a hozzáféréskor elért állományokat;
f) sikertelen hozzáférési kísérletek számát;
g) a használt programot.

5.4.11.4 Biztonsági szempontból releváns események jelentési folyamata

(1) Az Informatikai Főigazgatóság arra kijelölt felelőseinek naponta ellenőriznie kell a naplóállományok bejegyzései alapján generált riasztásokat.

(2) Incidens 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 IBF tájékoztatása.
(3) Az információbiztonsági szabályok megsértéséről a rendszergazdának haladéktalanul jelentést kell tennie az informatikai főigazgatónak és értesíteni kell az IBF-et, aki az informatikai főigazgató és az érintettek 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

(1)Az eseménynaplók megbízható 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.
(2)Az eseménynapló tárolási szabályai:
a) a naplóadatoknak sértetlenül rendelkezésre kell állniuk az elévülési időn belül;
b) az éles környezetben minimum a teljes mentések közötti időtartamnak megfelelő napló-állományokat kell tárolni;
c) biztosítani kell, hogy az adatokban keletkezésük után változtatást már ne lehessen végre-hajtani;
d) az információk bizalmasságára tekintettel, az adatok nem juthatnak illetéktelenek kezébe.

5.4.11.6 Naplóinformációk védelme

(1) A naplózást végző berendezések beállításait csak az informatikai főigazgató engedélyével lehet megváltoztatni.
(2) A naplóban rögzített információkat védeni kell az illetéktelen hozzáféréstől. A naplóállományokhoz hozzáférés csak az informatikai főigazgató jóváhagyása mellett lehetséges.
(3) Az IBF rendszeresen (6 havonta) ellenőrzi a naplózás megtörténtét és nyilvántartását.
(4) A naplóban rögzített információkat megváltoztatni, törölni tilos.

5.4.11.7 Rendszergazdai és kezelői naplók

(1) Mind a rendszergazdai, mind a biztonsági eseményeket nyomon kell követni az egyes alkalmazásokban. Gondoskodni kell a naplóállományok rendszeres mentéséről, felülvizsgálatáról, ez az informatikai főigazgató által kijelölt informatikai munkatárs feladata.
(2) A rendszergazdai naplókba való betekintéshez, a naplózó rendszer beállításainak megváltoztatásához az informatikai főigazgató 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 azt a rendszergazdáknak tilos, viszont az IBF-nek és az informatikai főigazgatónak kötelező jelenteni.

5.4.11.9 Órajelek szinkronizálása

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

5.5 Informatikai szolgáltatások biztonsága

5.5.1 Elektronikus levelezés

Az elektronikus üzenetekben foglalt információkat védeni kell a következő módon:
a) védeni kell az üzeneteket a jogosulatlan hozzáféréstől, módosítástól;
b) biztosítani kell a pontos címzést és célba juttatást;
c) biztosítani kell a szolgáltatás megbízhatóságát és hozzáférhetőségét;
d) elektronikus aláírások használatát az arra feljogosítottaknak biztosítani kell;
e) külső nyilvános szolgáltatásokat kontroll alatt kell tartani;
f) 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)

(1) Az elektronikus levelezés biztonságának megteremtését kéretlen levél (spam) szűrő rendszer alkalmazásával, valamint vírusvédelmi rendszer használatával kell biztosítani, melyet rendszeresen frissíteni kell.
(2) 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

(1) Az elektronikus levelezés során minden, használatra jogosított egyetemi polgár egyedi elektronikus levelezési címet kap.
(2) Hivatalos levelezésre az egyetemi email cím használandó. Ebbe beleértendő az egyetemi polgárok által (megfelelő folyamat igénybevételével) történő VPN kérelem benyújtása is.
(3) Az elektronikus levelezés használata során az alábbi szabályoknak kell megfelelni:
   a) az Egyetem elektronikus levelező rendszere elsődlegesen belső- és külső kommunikációt, a belső folyamatok támogatását szolgálja;
   b) az elektronikus levelezés használata során az Egyetem fenntartja a jogot arra, hogy - indokolt esetben - az Egyetem képviseletében eljáró személyek betekintsenek az elektronikus levelekbe, továbbá hogy a felhasználók levelezési forgalmát figyelje és naplózza. A felhasználók tudomásul veszik, és a használattal kifejezetten hozzájárulnak ahhoz, hogy az általuk küldött és fogadott elektronikus küldeményeket – azok aktív vagy tárolt változatai esetében egyaránt – az Egyetem ilyen módon kezeli;

c) szükség esetén az elektronikus üzenetek bizalmasságának, hitelességének és letagadhatatlanságának védelme érdekében – az adatok biztonsági osztályba sorolásának megfelelően – digitális aláírást és titkosítást kell alkalmazni;
d) az Egyetem levelezési rendszeréből a szervezeten kívülre csak olyan információkat szabad kijuttatni, amelyek kijuttatására a felhasználó más csatornán keresztül is jogosult. Nyilvános levelezési fórumokon az Egyetemnél regisztrált levelezési cím feltüntetésével állást foglalni tilos;
e) az Egyetemi levelezési cím feltüntetésével vagy annak használatával – az Egyetem érdekeinek megvalósulását kifejezetten segítő feladatokat kivéve – semmilyen kereskedelmi, hirdetési tevékenységben nem lehet részt venni;
f) az elektronikus levelezési rendszerbe beérkező leveleket minden esetben ellenőrizni kell, hogy nem tartalmaznak-e valamilyen, az Egyetem informatikai rendszerét veszélyeztető programot, kódrészletet, scriptet;
g) az elektronikus levelezéshez kapcsolódóan tilos:
   ga) a hivatalosan támogatott elektronikus levelező szolgáltatáson (szerveren) kívül más elektronikus levelező szolgáltatást hivatalos levelezésre használni;
   gb) a hivatalosan támogatott levelező szoftveren kívül más programot használni;
   gc) az elektronikus leveleket úgy titkosítani, hogy a visszafejtésre használható kulcs nincs vagy nem kerülhet az Egyetem birtokába;
   gd) az Egyetem hálózatát vagy szervereit nagy terjedelmű vagy nagy mennyiségű levél, továbbá kéretlen kereskedelmi üzenetek küldésére használni (ha ilyenre van szükség, akkor azt az Informatikai Főigazgatóság bevonásával, más technológia alkalmazásával kell teljesíteni);
   ge) a levelezőrendszert pártpolitikai célra, mások munkájának hátráltatására, továbbá az internet veszélyeztetésére használni;
   gf) az Egyetem hálózatát vagy szervereit kéretlen, nagy mennyiségű, továbbá kereskedelmi elektronikus levelekre való válaszok begyűjtésére használni;
   gg) feliratkozni nem szakmai jellegű, továbbá nem az ügyviteli vagy oktatási munkát segítő hírlevél küldő szolgáltatásra
   gh) indokolatlanul nagyméretű üzeneteket vagy fájlokat küldeni;
   gi) láncleveleket vagy hasonló üzeneteket küldeni, valamint ”hólabda” levelezést továbbítani (chain letters, olyan üzenet mely tartalmazza azt, hogy a címzettje azt küldje tovább ismerősöknek);
   gj) vírusos levelek szándékos küldése;
   gk) ügyviteli szempontból titkos, bizalmas vagy belső információk jogosulatlan nyilvánosságra hozatala.
   gl) válaszolni olyan levelekre, amelyek arra szólítanak fel, hogy az Egyetem biztonsági rendszeréről, vagy a felhasználó saját hozzáférési adatairól (felhasználónév, jelszó) adjon tájékoztatást
   gm) az e-mailben csatolt futtatható állományok megnyitása/letöltése a munkaállomásokra.
   gn) ismeretlen feladótól származó levelekben található csatolmány megnyitása;
   go) valótlan információt hordozó levelek tudatos továbbítása;

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

5.5.2 Az interneten megtalálható információ használata

(1) A megbízható (egyetemi hálózat) és a nem megbízható (pl.: internet) hálózatokat csak az Egyetem tűzfalán keresztül lehet összekapcsolni.
(2) Az Egyetem rendszerében az internet használat az ügyviteli folyamatok támogatására, valamint azokhoz kötődő információáramlásra szolgál.
(3) Az internet használata során az Egyetem fenntartja a jogot arra, hogy a felhasználók internet-forgalmát figyelje és naplózza.

5.5.2.1 Az internet használata során követendő magatartás

(1) A szerzői jogokra, szabadalmakra és egyéb szellemi tulajdonra vonatkozó szabályok alkalmazása az internetre is vonatkozik. Ebből kifolyólag az alkalmazottak kötelesek:
a) az internetről származó anyagok felhasználása előtt beszerezni a forrástól az erre vonatkozó engedélyt;
b) hivatkozáskor a forrást azonosítani;
c) az Egyetemmel kapcsolatos információk egyetemi honlapon történő közzétételéről a Honlap szabályzatban a kancellár által kijelölt személy gondoskodik, ettől a felhasználónak eltérni tilos.
(2) Az internet-hozzáféréssel rendelkező alkalmazottak csak közvetlenül az Egyetemen végzett munkájukkal kapcsolatosan tölthetnek le fájlokat. A letöltött fájlok kizárólag engedélyezési feltételeik szerint használhatók.
(3) Az internet hozzáféréssel rendelkező munkatársak nem használhatják az Egyetem internet kapcsolatát szórakoztató szoftverek vagy játékok letöltésére, valamint internetes játékokra. Csak a munkakörhöz, feladatellátáshoz kapcsolódó 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 főigazgatót, aki intézkedik a megfelelő technikai támogatásról.

5.5.2.3 Tiltott tevékenységek az internet hálózaton

a) 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;
b) profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése;
c) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, módosítása, megrongálása, megsemmisítésére irányuló tevékenység;
d) a hálózat biztonságos működését zavaró vagy veszélyeztető információk, programok terjesztése (pl. vírusok, trójai programok, hacker eszközök, férgek);
e) hálózati forgalom lehallgatása, megfigyelése, kivéve, ha ez az adott munkakörhöz kapcsolódik;
f) a szolgáltatások blokkolását, lassítását célzó támadás, az azonosítási, továbbá biztonsági intézkedések megsértésére irányuló kísérlet, valamint az egyéb azonosítóhoz, számítógéphez vagy hálózathoz történő illetéktelen hozzáférési kísérlet;
g) 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;
h) minden felhasználó kizárólagosan a munkájához kötődő, a munkavégzését segítő oldalak látogatására jogosult, ezért tilos továbbá:
    ha) sértő, társadalomra veszélyes, jó erkölcsbe ütköző szöveg, kép, ábra vagy egyéb formájú információ publikálása, letöltése;
    hb) az interneten elérhető szolgáltatást, bármilyen törvényt, szabályozást, szabványt, nemzetközi egyezményt vagy díjszabást sértő módon használni;
    hc) a felhasználónak az internetes forgalmát titkosítani úgy, hogy a visszafejtő kulcs nincsen az Egyetem birtokában;
    hd) bármelyik számítógép-hálózat biztonságát rombolni vagy gyengíteni, más felhasználó jogosultságát jogosulatlanul használni;
    he) bármilyen internetes végpontra vagy hálózati eszközre jogosulatlanul csatlakozni, vagy ezzel próbálkozni;
    hf) bármely végpont működését megzavarni vagy azt az Egyetem hálózatáról vagy annak igénybevételével szándékos túlterhelni (DOS támadás);
    hg) egyetemi tulajdonú eszközöket internetes számítógép erőforrás megosztásokhoz (például: gyógyszerkutatás, SETI számításokhoz, RSA törésekhez) használni;
    hh) a hálózatot a szerzői jogvédelem alá eső anyagok átvitelére használni (még közvetetten is), ha az átvitel során mások szerzői joga sérül;
    hi) tilos kikapcsolni a munkaállomásra telepített biztonsági szoftvereket, eszközöket;
i) nem látogathatóak olyan oldalak, melyek megtekintése vagy használata a hivatalos egyetemi tevékenységgel össze nem egyeztethető:
    ia) az Egyetem érdekeit sértik;
    ib) rasszista tartalmúak;

ic) erotikus oldalak;
id) warez oldalak;
ie) terrorizmust támogató oldalak;
if) illegális használatú fegyverekre vonatkozó információkat tartalmaznak;
ig) illegális kábítószerekre vonatkozó információkat tartalmaznak;
ih) phishing (adathalász) oldalak;
ii) internetes fogadási oldalak, szerencsejáték oldalak;

j) 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 Fájlkezelés / címtárkezelés

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

5.5.3 Webszolgáltatás

(1) Az egyetemi honlap tartalmának (www.semmelweis.hu) módosításának és karbantartásának felelőse a Marketing és Kommunikációs Főigazgatóság, a honlap szerkesztésével kapcsolatos feladatokat külön szabályzat rendezi.
(2) Az Informatikai Főigazgatóság 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

A Működés-folytonossági Terv tartalmazza a 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 informatikai rendszer biztonsági szintjének hiteles méréséhez az alábbi feltételek biztosítása szükséges:

6.1.1 A mérés függetlenségének biztosítása

(1) A méréseket a felhasználóktól, az informatikai üzemeltetési és a fejlesztési területtől független személy végezze.
(2) A méréseket a mérésben érintettek előzetes értesítése nélkül kell végrehajtani, hogy ne tudjanak felkészülni, továbbá ne tudják befolyásolni a mérés eredményét.

6.1.2 A mérés hitelességének biztosítása

(1) Az informatikai rendszer elemeinek időszinkronizálása szükséges a naplófájlok megbízható kiértékeléséhez.
(2) A biztonsági szint mérésével megbízott személy rendelkezzen a naplófájlok eléréséhez szükséges jogosultságokkal.
(3) Biztosítani kell a naplófájlok sértetlenségét. A naplófájlokhoz csak olyan személyek férhessenek hozzá, akiknek a munkájához a hozzáférés feltétlenül szükséges.
(4) A fenti feltételrendszer kialakításáért az informatikai főigazgató a felelős.

6.2 A biztonsági szint mérésének eszközei és módszerei

6.2.1 A technikai szintű auditok

(1)A biztonság szintje mérésének egyik leghatásosabb módszere a technikai audit jellegű felmérés:
a) az informatikai rendszer internet felőli sérülékenységeinek vizsgálata,
b) az informatikai rendszer intranet felőli sérülékenységeinek vizsgálata.
(2)Technikai szintű auditot az Egyetemnél kétévente, vagy egy új rendszer bevezetésekor a fenyegetettségek felmérésével egy időben kell elvégezni, a végrehajtásért az IBF és az informatikai főigazgató együttesen felelős.

6.2.2 Működés-folytonossági és katasztrófa-elhárítási tesztek

(1) A működés-folytonosság biztosítása érdekében a visszaállítási- és a katasztrófa-elhárítási terveket az IBF által készített ütemterv szerint, elemenként tesztelni kell. A tesztelés eredményét a tervezésbe, valamint a szóban forgó eljárásokba (mentés, karbantartás, stb.) vissza kell csatolni.
(2) A tesztelés megtervezését, koordinálását az informatikai főigazgató végzi, a tesztek végrehajtásáért az informatikai szolgáltatások rendszergazdái felelősek.

6.2.3 Az informatikai rendszer monitorozása

Az informatikai rendszer kritikus elemeit, valamint biztonsági eszközeit folyamatosan monitorozni kell. A monitorozásnak minimálisan az alábbi témákra kell kiterjednie:
a) Határvédelmi incidensek, és hálózati illegális tevékenység. Felügyeletet ellátó személy: határvédelmi rendszergazda.
b) Vírusvédelmi incidensek, vírusvédelmi rendszerek állapota (vírus DB és motor verziója eszközönként). Felügyeletet ellátó személy: vírusvédelmi rendszergazda.
c) Jogosultság kezelési incidensek. Felügyeletet ellátó személy: jogosultságkezelésért felelős rendszergazda.

d) Mentési feladatok sikeres/sikertelen végrehajtása. Felügyeletet ellátó személy: mentésért felelős rendszergazda.
e) Külső felhasználók tevékenységei, távoli elérések naplózása. Felügyeletet ellátó személy: IBF.
f) Rendszergazdák tevékenységei. Felügyeletet ellátó személy: IBF.
g) Biztonsági riasztórendszerek naplózása (UPS, tűzvédelem, stb.). Felügyeletet ellátó személy: IBF.

6.3 A mérési adatok rögzítése, feldolgozása, visszacsatolása

(1) Az informatikai biztonság szempontjából kritikus pontokon mérési és ellenőrzési rendszert kell bevezetni. A mérések eredményéről az IBF évente írásban beszámol az informatikai főigazgatónak, annak érdekében, hogy a központi rendszereket érintő esetlegesen felmerült kockázatok kezelése időben megtörténjen.
(2) A minimálisan szükséges kontrollpontok az alábbiak:

Mérendő terület	**Mérendő mennyiség**	**Beszámolóban szerepel**
Informatikai tevékenység	Szerverszobába való belépések naplózása	Nem
	Rendszergazdai hozzáférések (logikai) naplózása	Nem
Illegális informatikai 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
	Tárolási kapacitásokra vonatkozó információk	Igen
Ellenőrzések eredményei	Feltárt hiányosságok, és azok megszüntetésére vonatkozó intézkedések	Igen
Oktatás helyzete	Információbiztonsági oktatásban részt vett személyek száma, a beszámoltatás eredményei	Igen

Mérendő terület	Mérendő mennyiség	Beszámolóban szerepel
Informatikai biztonsággal kapcsolatos fegyelemsértések	informatikai biztonságot megsértő személyekre vonatkozó statisztikák	Igen
Az informatikai biztonsági rendszer összesített értékelése	Az informatikai rendszer szintjére vonatkozó megállapítások, javaslatok	Igen
Javaslatok	Javaslatok kidolgozása a hiányosságok megszüntetésére, a biztonsági szint emelésére	Igen

6.4 Ellenőrzési irányelvek

(1) 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 szintjéről elegendő információ álljon rendelkezésre, mérhető legyen.

(2) Az IBF az informatikai főigazgatóval együttműködve határozza az ellenőrzések területeit, és minden területhez külön-külön meg kell fogalmazni az ellenőrzési célkitűzéseket, továbbá azt, hogy ki végzi el az ellenőrzéseket. A célkitűzések az alábbiak lehetnek:
   a) jogszabályoknak, belső szabályozásoknak történő megfelelés;
   b) nem kívánatos felhasználói tendenciák visszaszorítása;
   c) nem kívánatos üzemeltetési tendenciák visszaszorítása;
   d) a felhasználók információbiztonsági tudatosság szintjének emelése.

(3) 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, valamint vissza kell csatolni a biztonsági folyamatra. Szükség esetén felelősségre vonást kell kezdeményezni. Az ellenőrzéseket dokumentumok, dokumentációk, személyes beszámoltatás és helyszíni szemlék alapján lehet végrehajtani.

(4) Az informatikai biztonsággal kapcsolatos ellenőrzések területei az alábbiak lehetnek:
   a) megfelelőségi vizsgálat:
      Célja felderíteni, hogy az Egyetem rendelkezik-e a törvényi előírásokban meghatározott személyi, eljárási, tárgyi feltételekkel, és azok megfelelően dokumentáltak-e.
   b) az informatikai biztonság szintjére vonatkozó vizsgálat:
      Célja felderíteni, hogy az informatikai biztonság szintje megfelel-e a meghatározott védelmi szintnek.
   c) az információbiztonsági szabályok betartásának ellenőrzése:
      Célja felderíteni, hogy az információbiztonsági szabályokat ismerik-e és betartják-e. Ez az ellenőrzés az informatikai biztonság egy-egy területére is leszűkíthető.

(5) Az ellenőrzések során elsősorban az alábbiakat kell vizsgálni:

a) az informatikai biztonsági rendszer működése megfelel-e a jogszabályi előírásoknak;
b) az informatikai biztonsági szabályok érvényesítve vannak-e a folyamatokban;
c) az informatikai biztonsági rendszer előírt dokumentumai léteznek-e és naprakészek-e;
d) az informatikai személyzet, valamint a felhasználók rendelkeznek-e a megfelelő informatikai biztonsági ismeretekkel;
e) az adatokra és rendszerekre vonatkozó kezelési szabályok betartását;
f) a naplózási rendszer megfelelő alkalmazását;
g) a biztonsági események kezelésének, a szükséges mértékű felelősségre vonás gyakorlatát;
h) a mentési rendszer megfelelő alkalmazását;
i) az informatikai rendszert fejlesztők, üzemeltetők, és felhasználók informatikai biztonsággal kapcsolatos ismereteit;
j) a hozzáférési jogosultságok nyilvántartásának naprakészségét, a kiadott jogosultságok szükségességét;
k) a dokumentációk pontosságát - naprakészségét, változás követését, megfelelő kezelését / nyilvántartását;
l) az alkalmazott szoftverek jogtisztaságát;
m) a szerződések megfelelőségét;
n) a fizikai biztonsági előírások betartását.

6.5 Biztonsági rendszerek felülvizsgálata

Az információbiztonsági rendszert, valamint annak egyes elemeit rendszeresen felül kell vizsgálni. A szükséges felülvizsgálatok az alábbiak:

A felülvizsgálat tárgya	**A felülvizsgálat gyakorisága**
Kockázatfelmérés - átfogó felülvizsgálat	legalább 2 évente
Információbiztonsági szabályzat	változást követő 90 napon belül
Információbiztonsági folyamatok	legalább 2 évente
Határvédelem	legalább 2 évente
Vírusvédelem	legalább 1 évente
Mentés, archiválási rend	legalább 2 évente
Információbiztonsági oktatás	legalább 2 évente

7. RENDSZEREK BESZERZÉSE, FEJLESZTÉSE ÉS KARBANTARTÁSA

(1) Az informatikai rendszerek és szolgáltatások beszerzését a rendszerek teljes életciklusában információbiztonsági szempontból felügyelni szükséges.
A rendszerek életciklusának szakaszai a következők:
a) követelmény meghatározás,
b) fejlesztés vagy beszerzés,
c) megvalósítás vagy értékelés,
d) üzemeltetés és fenntartás,
e) kivezetés (archiválás, megsemmisítés).

(2) Új rendszerek megvalósítása során a biztonsági követelményeket előzetesen meg kell határozni.
a) Az IBF-fel mindig előzetesen véleményeztetni kell a megvalósítandó technológiát és a meghatározott biztonsági követelményeket annak biztosítására, hogy a megfelelő védelmi intézkedések kerüljenek megvalósításra.
b) Amennyiben a rendszer már rendelkezik a szolgáltatója, gyártója általi információbiztonsági tanúsítással, audittal, ennek dokumentumait is szükséges átadni az IBF részére.
c) Az IBF az információbiztonsági véleményezést írásos formában rögzíti és az érintettek részére elérhetővé teszi.
d) Többszereplős projektek esetén is (pl. állami és nemzetközi pályázatok, egyetemek közötti együttműködés) az egyetemi IBF bevonása szükséges.
e) Amennyiben az adott projektben az információbiztonság képviselete biztosított, erről is szükséges az IBF-et tájékoztatni.

(3) A már bevezetett rendszerek módosítása, továbbfejlesztése során a biztonsági követelmények nem változtathatók olyan irányba, hogy a rendszer biztonsági szintje csökkenjen.

(4) A szállítóknak az Egyetem vagyonelemeihez való hozzáférésének módját, valamint az információbiztonsági követelményeket a szállítókkal kötött szerződésekben rögzíteni kell.

8. MELLÉKLETEK:

1. számú melléklet – Fogalomtár

2. számú melléklet: Kapcsolódó jogszabályok, szabályozások listája

3. számú melléklet: A vezető adatgazdák és a hozzájuk rendelt informatikai rendszerek

4. sz. melléklet: Titokvédelmi megállapodás – formanyomtatványtárból érhető el –

5. számú melléklet: Kiemelten védett területre történő belépés nyilvántartása – formanyomtatványtárból érhető el –

6. számú melléklet: Hálózati végpontok nyilvántartása – formanyomtatványtárból érhető el –

7. számú melléklet: Speciális jelszavakhoz való hozzáférések jegyzőkönyve – formanyomtatványtárból érhető el –

8. számú melléklet: Adatosztályozási és biztonsági szintek

9. számú melléklet: Adatosztályozó lap – formanyomtatványtárból érhető el –

10. számú melléklet – Ellenőrzési nyomvonal

1. számú melléklet: 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.
Adathordozó:	az adat tárolására és terjesztésére alkalmas eszköz.
Adatkezelés:	az adatok tárolásával, továbbításával, megsemmisítésével, nyilvántartásával és feldolgozásával kapcsolatos tevékenységek összessége.
Adatgazda:	annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, továbbá ahol az adat keletkezik.
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 az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 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 és 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 információbiztonsági 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.
Határvédelmi felelős:	az Infrastruktúra Üzemeltetési Osztály keretében kijelölt felelős, amely az informatikai határvédelmi és határbiztonsági rendszerek felelőse (pl. tűzfalrendszerek, hálózati hozzáférés-védelem, behatolásérzékelő és -megelőző rendszerek, távoli biztonságos elérés, hálózat szegmentációja.).

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.
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.
Informatikai biztonság:	az Egyetem informatikai rendszerének olyan kielégítő állapota, amely az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, valamint az informatikai rendszerelemek rendelkezésre állása és funkcionalitása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.
Információbiztonsági dokumentációs rendszer:	többszintű, egymásra épülő rendszer, amely magába foglalja a biztonságpolitikai elvektől a szabályzatokon keresztül a munkautasítások szintjéig az információbiztonsági 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.
Információs vagyon:	adatok, információk, szellemi, erkölcsi javak összessége.
Információbiztonságért felelős vezető:	kinevezés útján látja el az információbiztonsági felelősi feladatokat. Szakterületén ellenőríz, tanácsot ad, véleményez. Egyik legfontosabb feladata, hogy a szervezeten elül kialakítsa és ellenőrizze azokat az információbiztonsági szabályokat, amelyek az informatikai rendszerekkel kapcsolatba lépőkre vonatkoznak.
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, valamint 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.
Rendelkezésre állás:	az informatikai rendszer tényleges állapota, amely megvalósul, ha a rendszer szolgáltatásai állandóan vagy 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, valamint 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, továbbá 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.
Védelmi intézkedés:	a fenyegetettség bekövetkezési valószínűsége, valamint 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- és 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, valamint – lehetőség szerint – megsemmisítésük.
Visszaállítási eljárás:	olyan eljárásrend, amelynek részeként elvégzett tevékenységek, feladatok biztosítják, hogy a helyreállítási eljárással beindított informatikai szolgáltatás alternatívájáról az ügyviteli folyamat visszaáll a normál üzemmenetre.
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.

2. számú melléklet: Kapcsolódó jogszabályok, szabályozások listája

Kapcsolódó külső szabályozások

a) 1997. évi CLIV. törvény az egészségügyről
b) 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről
c) 2001. évi XXXV. törvény az elektronikus aláírásról
d) 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)
e) 2011. évi CCIV. törvény a felsőoktatásról
f) 2012. évi C. törvény a Büntető Törvénykönyvről
g) 2013. évi V. törvény a Polgári Törvénykönyvről
h) 2015. évi CXLIII. törvény a közbeszerzésekről
i) 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
j) Az Európai Parlament és az Európai Tanács (EU) 2016/679 Rendelete. Általános Adatvédelmi Rendelet. (GDPR)

Kapcsolódó belső szabályozások

a) Informatikai üzemeltetési és hálózati szabályzat;
b) Távközlési szabályzat;
c) Neptun szabályzat;
d) Adatvédelmi és közzétételi szabályzat
e) Vagyonvédelmi és rendészeti szabályzat;
f) Tűzvédelmi szabályzat;
g) Informatikai Főigazgatóság szervezeti ügyrendje;
h) Kritikus alkalmazások üzemeltetési utasításai.

Kapcsolódó szabványok és ajánlások

a) MSZ-ISO/IEC 27001:2014;
b) MSZ ISO/IEC 17799:2006;
c) a MABISZ biztonságtechnikai ajánlása B/I. pontja szerinti teljes mechanikai, fizikai védelem;
d) a MABISZ biztonságtechnikai ajánlása C/I/2. pontja szerinti részleges elektronikai jelzőrendszer;
e) a MABISZ biztonságtechnikai ajánlása C/II. pontja szerinti beléptető rendszer.

3. számú melléklet: A vezető adatgazdák és a hozzájuk rendelt informatikai rendszerek

RENDSZER	VEZETŐ ADATGAZDA
Integrált medikai rendszer és alrendszerei (MedSolution, e-MedSolution, GLIMS, Andromeda, MedBakter, AGFA PACS rendszer, CorDB, BedMap, SmartDB)	Klinikai Központ elnöke
KVIK vezetői információs rendszer	orvos-főigazgató
SAP rendszer gazdálkodási modulok (FI, CO, KVM, AM, SD, MM)	gazdasági főigazgató
SAP rendszer HR modul	emberierőforrás gazdálkodási főigazgató
Elektronikus tárhely	emberierőforrás gazdálkodási főigazgató
AVIR vezetői információs rendszer	kontrolling igazgató
Iratkezelő rendszer	Szervezési és Igazgatási Központ igazgató
Egyetemi levelezőrendszer	informatikai főigazgató
Egységes felsőoktatási tanulmányi rendszer	oktatási rektor-helyettes
On-line szakirodalmi források, közcélú adatbázisok elérése	Központi Könyvár igazgató
Központi fájl szerverek	informatikai főigazgató
Egyetemi központi honlaprendszer	marketing és kommunikációs főigazgató
Pályázati nyilvántartó rendszer	Innovációs Központ igazgató
GLPI igénybejelentő rendszer, informatikai bejelentések kezelése	informatikai főigazgató
GLPI igénybejelentő rendszer, üzemeltetési bejelentések	szolgáltatási igazgató
Egyetemi beléptető rendszer	biztonságtechnikai igazgató
Egységes egyetemi zártláncú megfigyelőrendszer	biztonságtechnikai igazgató
Külföldi hallgatók jelentkezését támogató informatikai rendszer (SEMAPHOR)	nemzetközi képzésekért felelős rektorhelyettes

8. számú melléklet: Adatosztályozási és biztonsági szintek

	Nem védett	***Védett adatok***	
Feladat	**Nyilvános adatok**	**Bizalmas és védett adatok**	**Titkos illetve fokozottan védett adatok**
Jelölés	Nincs követelmény.	A bizalmas és/vagy védett adatokat tartalmazó adathordozókat „Belső használatra” vagy „Bizalmas” jelöléssel kell ellátni.	A titkos vagy fokozottan védett adatokat tartalmazó adathordozókat „Titkos” jelöléssel kell ellátni.
Tárolás	Központi tároló helyen, nyilvános eléréssel.	Az adathordozókat zárható helyen szekrényben, vagy zárható asztalfiókban kell tárolni. Az informatikai rendszerben biztosítani kell az adatokhoz való hozzáférés vezérlését.	A titkos vagy fokozottan védett adatokat tartalmazó adathordozókat páncélszekrényben kell tárolni. Az informatikai rendszerben biztosítani kell az adatokhoz való hozzáférés hitelesítésen alapuló vezérlését (pl.: digitális kulcsok használata, PKI megoldás).
Hozzáférés	Nyilvános.	Az adatokhoz való hozzáférés csak az arra jogosult személyek számára biztosított.	Az adatokhoz való hozzáférés csak az arra jogosult személyek számára biztosított.
Adatátvitel	Nincs speciális követelmény.	Szervezeten belüli továbbítása hozzáférési jogosultság függvényében engedélyezett. Szervezeten kívülre való továbbítása csak a vezető adatgazda engedélyével lehetséges az elfogadott titkosítási módszer alkalmazásával.	Titkos vagy fokozottan védett adatokat csak titkosított csatornán, hitelesített felhasználónak szabad küldeni, vagy csak helyi hozzáférés lehetséges.
Adatmegosztás	Nincs speciális követelmény.	Adatmegosztás csak a vezető adatgazda engedélyével lehetséges	Titkos vagy fokozottan védett adatok megosztása tilos!
Megsemmisítés, törlés	Nincs speciális követelmény.	Megsemmisítés a vezető adatgazda engedélyével. Megsemmisítés előtt az adathordozón levő adatokat	Megsemmisítés a vezető adatgazda külön engedélyével.

	Nem védett	*Védett adatok*	
Feladat	**Nyilvános adatok**	**Bizalmas és védett adatok**	**Titkos illetve fokozottan védett adatok**
		visszaállíthatatlanul törölni kell.	Megsemmisítés előtt az adathordozón levő adatokat visszaállíthatatlanul törölni kell.
Felülvizs-gálat	Nincs speciális követelmény.	Minimálisan háromévente.	Minimálisan évente.

10. számú melléklet: Ellenőrzési nyomvonal

Ssz.	**Folyamat lépései**	**Jogszabályi / belső szabályozási alap**	**Előkészítés lépései**	**Felelősségi szintek**					**Folyamat eredménye (dokumentum)**
				feladatgazda	**ellenőrző**	**ellenőrzés módja**	**jóváhagyás**	**jóváhagyás módja**	
1.	Információbiztonsági szabályzat eseti és rendszeres felülvizsgálata	SZMSZ I.1. rész (3.§, 19.§, 30. §,31. §) IBSZ (3.1.4 pont)	A jogszabályi környezet változásának a követése, a szabályzat gyakorlati alkalmazásának a figyelemmel kísérése, értékelése	IBF	kancellár	Előterjesztés egyeztetése	kancellár	Határozat írásba foglalása	Aktualizált szabályzat
2.	Információbiztonsági incidensek kezelése	IBSZ (2.5. pont)	Az informatikai és a személyi információbiztonsági biztonsági incidenseket észlelésükkor jelentenie kell az azt észlelőnek, melyet kivizsgálni szükséges	IBF	kancellár	Jelentés áttekintése	kancellár	Jelentés elfogadása	Jelentés
3.	A VPN kapcsolatok létesítésének engedélyezése, az IBF előzetes jóváhagyása alapján	IBSZ (3.1.2. pont)	A kritikus, különösen érzékeny adatokat tartalmazó rendszerek távoli elérése előzetes engedélyhez kötött.	munkahelyi vezető	informatikai főigazgató	Elektronikus dokumentációs és jóváhagyási rendszer működésének ellenőrzése	IBF	Elektronikus dokumentálás	Engedély

Ssz.	Folyamat lépései	Jogszabályi / belső szabályozási alap	Előkészítés lépései	Felelősségi szintek					Folyamat eredménye (dokumentum)
				feladatgazda	**ellenőrző**	**ellenőrzés módja**	**jóváhagyás**	**jóváhagyás módja**	
4.	A fokozottan védett területekre történő belépés, az ott történő munkavégzés engedélyezése, az engedélyek rendszeres felülvizsgálata	IBSZ (3.1.2. pont)	Vezető adatgazda kérelmezi a fokozottan védett területekre meghatározott személyek belépési jogosultságát.	vezető adatgazda	IBF	Engedélyek áttekintése	informatikai főigazgató	Írásos jóváhagyás	Engedély
5.	Egyetemi információbiztonsági oktatás, az információbiztonsági tudatosság növelése	IBSZ (3.1.4. pont)	Új belépők szervezett oktatása, munkavállalók aktuális információbiztonsági tájékoztatása, kampányok szervezése.	IBF	kancellár	Beszámoló áttekintése	kancellár	Beszámoló elfogadása	Beszámoló
6.	Felhasználó jogosultság felülvizsgálata	IBSZ (4.3. pont)	A rendelkezésre álló jogosultságok felhasználóként áttekintése	szakterületi adatgazda	vezető adatgazda	Jogosultsági dokumentumok átvizsgálása	IBF	Írásos jóváhagyás	Jegyzőkönyv
7.	Információvédelmi osztályba sorolás	IBSZ (4.8. pont)	Ütemterv alapján vagy változás esetén szükséges megtenni	szakterületi adatgazda	vezető adatgazda	Jelentés	IBF	Írásos jóváhagyás	Írásos dokumentum
8.	Informatikai vagyonleltár	IBSZ (5.1. pont)	Eszközazonosítás, eszközleltár felvétele	vagyongazda	IBF	Informatikai leltár nyilvántartás	informatikai főigazgató	Írásos jóváhagyás	Aktualizált vagyonleltár

Ssz.	Folyamat lépései	Jogszabályi / belső szabályozási alap	Előkészítés lépései	Felelősségi szintek					Folyamat eredménye (dokumentum)
				feladatgazda	**ellenőrző**	**ellenőrzés módja**	**jóváhagyás**	**jóváhagyás módja**	
9.	Elektronikus információs rendszerek naplózása	IBSZ (5.4.11. pont)	A naplóállományokhoz való hozzáférési jogosultságokat az informatikai főigazgató hagyja jóvá, a rendszergazdák dokumentálják, az IBF ellenőrzi	alkalmazás-gazda	IBF	Napló állományokhoz kapcsolódó kimutatások	informatikai főigazgató	Írásos jóvá-hagyás	Engedély
10.	Rendszergazdai naplókba betekintés	IBSZ (5.4.11.7. pont)	A rendszergazdai naplókba való betekintéshez, a naplózó rendszer beállításainak megváltoztatásához az informatikai főigazgató engedélyét kell kérni.	rendszergazda	IBF	Napló állományokhoz kapcsolódó kimutatások	informatikai főigazgató	Írásos jóvá-hagyás	Engedély
11.	Informatikai beszerzések kezdeményezése, döntéselőkészítés	IBSZ (4.4. pont)	Informatikai beszerzés kezdeményezése, döntéselőkészítés	szakterületi adatgazda	vezető adat-gazda, IBF	Beszerzési dokumentumok véleményezése	informatikai főigazgató	Aláírás	BML javaslat
12.	Informatikai beszerzések, információbiztonsági szakmai felügyelete	IBSZ (7. pont)	Dokumentumok áttekintése	adatgazda	IBF	Beszerzési dokumentumok véleményezése	informatikai főigazgató	Vélemény írásba foglalása	BML

Ssz.	Folyamat lépései	Jogszabályi / belső szabályozási alap	Előkészítés lépései	Felelősségi szintek					Folyamat eredménye (dokumentum)
				feladatgazda	ellenőrző	ellenőrzés módja	jóváhagyás	jóváhagyás módja	
13.	Működés-folytonossági és katasztrófa-elhárítási tesztek	IBSZ (6.2.2. pont)	A tesztelés megtervezését, koordinálását az Informatikai főigazgató végzi, a tesztek végrehajtásáért az informatikai szolgáltatások rendszergazdái felelősek.	infrastruktúra és alkalmazás üzemeltetők	informatikai főigazgató IBF	módosítási javaslat elkészítése	kancellár	aláírás	IBSZ módosítási javaslatok
14.	A mérési adatok rögzítése, feldolgozása, visszacsatolása	IBSZ (6.3. pont)	A mérések eredményéről az IBF évente írásban be kell számolnia az Informatikai főigazgatónak	IBF	Informatikai főigazgató	Beszámoló	informatikai főigazgató	Beszámoló elfogadása	Beszámoló
15.	Üzemeltetési eljárások ellenőrzése	IBSZ (3.1.2. pont)	utolsó ellenőrzés óta történt szervezeti-, infrastrukturális- és funkcionális változások listája	alkalmazás üzemeltető rendszergazdák	IBF	jelentés elfogadása	informatikai főigazgató	aláírás	éves ellenőrzési jegyzőkönyv
16.	Szakterületi adatgazdák kijelölése	IBSZ (4.2. pont)	Kritikus rendszer vezető adatgazdája kijelöli az adott rendszer szakterületi adatgazdáját	vezető adatgazda	informatikai főigazgató	Az adatgazdai nyilvántartás ellenőrzése	informatikai főigazgató	Az ellenőrzés tényének írásba foglalása	Jegyzőkönyv
17.	Alkalmazásgazdák kijelölése	IBSZ (4.2. pont)	A kritikus rendszer adatgazdája javaslatot tesz az alkalmazásgazda	vezető adatgazda	informatikai főigazgató	Az adatgazdai nyilvántartás ellenőrzése	informatikai főigazgató	Az ellenőrzés tényének	Jegyzőkönyv

Ssz.	Folyamat lépései	Jogszabályi / belső szabályozási alap	Előkészítés lépései	Felelősségi szintek					Folyamat eredménye (dokumentum)
				feladatgazda	**ellenőrző**	**ellenőrzés módja**	**jóváhagyás**	**jóváhagyás módja**	
			személyére a vezető adatgazdánál					írásba foglalása	
18.	Alkalmazásfelügyelők kijelölése	IBSZ (4.6. pont)	Informatikai főigazgató kijelöli a kritikus rendszer alkalmazás-felügyelőjét	informatikai főigazgató	műszaki főigaz-gató	Munkáltatói jogkörben ellenőrzi az informatikai főigazgató feladatellátását	műszaki főigazgató	Az ellenőrzés tényének írásba foglalása	Jegyzőkönyv
19.	Információvédelmi osztályba sorolás	IBSZ (4.3. pont)	Szakterületi adatgazda besorolja az adott rendszer által kezelt adatokat	vezető adatgazda	IBF	Osztályba sorolásról készült adatlapok ellenőrzése	IBF	Az ellenőrzés tényének írásba foglalása	Jegyzőkönyv
20.	Vírusvédelmi incidensek, vírusvédelmi rendszerek felülvizsgálata	IBSZ (6.3. pont)	Statisztikai adatok, jelentések összegyűjtése. Alkalmazott védelmi intézkedések áttekintése	vírusvédelmi rendszergazda	IBF	Nyilvántartás áttekintése	informatikai főigazgató	Az ellenőrzés tényének írásba foglalása	Jegyzőkönyv
21.	Belső használatú programok fejlesztésének, módosításának információbiztonsági felügyelete	IBSZ (7. pont)	Fejlesztési igények összegyűjtése.	szolgáltatás-fejlesztési osztályvezető	IBF	Rendelkezésre álló releváns dokumentumok áttekintése	informatikai főigazgató	Az ellenőrzés tényének írásba foglalása	Információ-biztonsági vélemény, javaslat

Ssz.	Folyamat lépései	Jogszabályi / belső szabályozási alap	Előkészítés lépései	Felelősségi szintek					Folyamat eredménye (dokumentum)
				feladatgazda	ellenőrző	ellenőrzés módja	jóváhagyás	jóváhagyás módja	
22.	Határvédelem felülvizsgálata	IBSZ (7. pont)	Statisztikai adatok, jelentések összegyűjtése. Alkalmazott védelmi intézkedések áttekintése	infrastruktúra üzemeltetési osztályvezető	IBF	Rendelkezésre álló releváns dokumentumok áttekintése	informatikai főigazgató	Az ellenőrzés tényének írásba foglalása	Információ-biztonsági vélemény, javaslat