DEBRECENI EGYETEM

Információbiztonsági Szabályzat

Tartalomjegyzék

I. ÁLTALÁNOS RENDELKEZÉSEK

I.1 A szabályozás célja, Információbiztonsági politika (IBP)

A Debreceni Egyetem (a továbbiakban **Egyetem**) kiemelt figyelmet fordít az informatikai rendszerei sértetlenségének és rendelkezésre állásának, valamint az abban kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítására a zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének megteremtésén keresztül. Mindezekre figyelemmel az Egyetem megalkotja az Információbiztonsági Szabályzatát (a továbbiakban IBSZ) az Információbiztonsági politikát is alapul véve.

I.1.1 Információbiztonsági Politika (IBP)

(1) A biztonság erősítése és fenntartása érdekében az IBSZ 1. számú mellékleteként az Egyetem kiadja Információbiztonsági Politikáját, aminek betartása és ismerete minden érintett számára kötelező, és amelynek karbantartása, folyamatos felülvizsgálata, szükség esetén módosítása az informatikai biztonsági vezető (információbiztonsági felelős) feladata. A jelen szabályzat elválaszthatatlan részét képező IBP-t évente felül kell vizsgálni.

(2) Amennyiben az Egyetem informatikai rendszereiben, vagy a vonatkozó jogszabályokban jelentős változások következnek be, akkor az IBP-t felül kell vizsgálni és módosítani kell. A módosítások, felülvizsgálatok kezdeményezése és a módosítások elvégzése az informatikai biztonsági vezető (információbiztonsági felelős) feladata. A módosításokat az Egyetem illetékes vezetőjeként a Kancellár hagyja jóvá.

(3) Az IBP-t az Egyetem minden munkatársával éves rendszeres Információbiztonsági oktatás keretében ismertetni kell. Az IBP-t az Egyetem honlapján kell folyamatosan elérhetővé tenni.

I.1.2. Az Információbiztonsági Szabályzat (IBSZ) célja

(1) Az Információbiztonsági Szabályzat (IBSZ) célja:
   a) az Egyetem szervezeti egységei, az Egyetem által alapított jogi személyiségű szervezet számára az információbiztonsággal kapcsolatos követelmények és szabályozások dokumentálása,
   b) a szerepkörök, feladatok, folyamatok, felelősségi körök definiálása,
   c) az elvárt és betartandó magatartásformák és gyakorlatok meghatározása a szervezeti elvárásoknak megfelelően, a vonatkozó jogszabályok és szakmai ajánlások figyelembe vételével,
   d) támogassa a biztonság erősítését, az üzletileg káros behatások számának csökkentését, védelmi prevenció kidolgozását, a katasztrófakezelés költséghatékony optimalizálását.

(2) Jelen szabályzat magába foglalja az Egyetem informatikai biztonságra vonatkozó szabályozását is. A szabályzatban meghatározott védelmi elveknek megfelelő működés biztosításának a rendszerek fennállásának teljes ciklusa alatt érvényesülniük kell (megtervezés, üzembe helyezés, működés, megszüntetés-kivonás).

(3) Az Egyetem nagy mennyiségű és heterogén adatot (személyes, gazdasági, gazdálkodási, kutatási, oktatási, egészségügyi) kezel, birtokol, amiknek az eszmei értéke felbecsülhetetlen, értékben nem kifejezhető. Így ezek védelme a bizalmasság, sértetlenség és rendelkezésre állás kritériumok biztosításához kiemelt stratégiai fontosságú, összetett és csak közös akarattal megvalósítható feladat.

(4) Az IBSZ célja olyan szabálykörnyezet létrehozása, ami a „Tűzfaltól a papírkosárig” átfogó, tudatos és követhető elvárásokat fogalmaz meg az informatikai, adat és információ védelem Egyetem szintű, Egyetem érdeke szerinti megvalósítására.

(5) A szabályozás kiterjed, a „home office” munkavégzés szélesebb körben történő alkalmazásával az otthoni, privát hálózatra és az informatikai munkaeszközöknek az Egyetem, mint munkáltató érdekében történő használatára is.

(6) Az információbiztonsági szabályozás kidolgozása során az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (a továbbiakban: Ibtv.) megfogalmazott irányelvek betartása volt az irányadó, valamint az ISO27001 szabvány ajánlásainak figyelembe vétele.

(7) Az Ibtv. 5. § értelmében: Az e törvény hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell:
   a) az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint
   b) az elektronikus információs rendszer és elemeinek sértetlensége és
   c) rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

I.2 A szabályzat hatálya

I.2.1. A szabályzat szervezeti hatálya

Jelen szabályzat szervezeti hatálya kiterjed:

a) az Egyetem összes szervezeti egységére,
b) az Egyetem által alapított jogi személyiségű szervezetekre,

I.2.2. A szabályzat személyi hatálya

Jelen szabályzat személyi hatálya kiterjed:

a) az Egyetem valamennyi polgárára (munkavállaló és hallgató)
b) az Egyetem informatikai rendszereinek valamennyi felhasználójára,
c) az Egyetem által alapított szervezetek munkavállalóira,
d) az Egyetemmel szerződéses vagy egyéb jogviszonyban álló természetes és jogi személyekre.

I.2. 3. A szabályzat tárgyi hatálya

Jelen szabályzat tárgyi hatálya kiterjed:

a) az Egyetem valamennyi informatikai rendszerére,
b) a teljes informatikai infrastruktúra eszközrendszerére,
c) az informatikai rendszerben feldolgozás alatt álló és ott tárolt, illetve a feldolgozás eredményeként létrejött, minden adatra és adathordozóra, függetlenül annak feldolgozási, vagy előállítási módjától és megjelenési formájától,
d) az informatikai rendszerek és folyamatok összes dokumentációjára (tervezési, fejlesztési, üzemeltetési, felhasználási),
e) a számítástechnikai alkalmazások teljes életciklusára,
f) a kezelt, tárolt, továbbított adatra, információra,
g) kommunikációs és telekommunikációs eszközeire,
h) nem Egyetemi tulajdonban lévő, de az Egyetem belső hálózatára - szolgáltatás biztosítása céllal - csatlakoztatott informatikai eszközökre,

i) Iratkezelési szabályzat- és információbiztonság alá tartozó dokumentációkra, iratokra és azok kezelésére és postázási folyamatára.

I.2. 4. A szabályzat területi hatálya

A szabályzat területi hatálya kiterjed a szabályzat tárgyi hatálya alá tartozó informatikai erőforrások üzemelési és használati helyszíneire;

a) az Egyetem valamennyi saját helyszínére és bérelt helyiségeire,
b) a kiszervezett adatfeldolgozási- és üzemeltetési tevékenységeinek helyszíneire,
c) az irodán kívüli használatra kiadott eszközök, illetve saját tulajdonú hivatali munkavégzésre használt eszközök esetében azok használatának helyére.

I.2. 5. A szabályzat időbeni hatálya

Jelen szabályzat a hatálybalépés napjától, további rendelkezésig, visszavonásig vagy hatályon kívül helyezésig irányadó.

I.3 Vonatkozó jogszabályok, belső szabályozások

I.3.1. Vonatkozó jogszabályok, szabványok, ajánlások:

1) 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)
2) 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv)
3) 2013. évi V. törvény a Polgári Törvénykönyvről (Ptk.)
4) 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
5) 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
6) 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
7) 246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
8) ISO/IEC MSZ 27001:2014 Informatika. Biztonságtechnika. Információbiztonsági irányítási rendszerek. Követelmények.
9) az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (a továbbiakban: GDPR).
10) Magyarország Alaptörvénye VI. cikk
11) 1997. évi XLVII törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről
12) 2011. évi CCIV törvény a nemzeti felsőoktatásról
13) 2012. évi I. törvény a munka törvénykönyvéről
14) 2011. évi CXC. törvény a nemzeti köznevelésről
15) 2009. évi CLV. törvény a minősített adat védelméről
16) 2012. évi C. törvény a Büntető Törvénykönyvről (magán titok 223. § és levéltitok 224. §, személyes adattal visszaélés 219. § és közérdekű adattal visszaélés 220. §)
17) 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről
18) Szabványok, ajánlások és egyéb kapcsolódó dokumentumok

I.3.2. Vonatkozó belső szabályozások

1) DE Kancellária ügyrend
2) A DE Belső Adatvédelmi Szabályzata
3) DE Egészségügyi Adatkezelési és Adatbiztonsági Szabályzata
4) A DE Közérdekű adatok megismerésére irányuló kérelmek intézésének és kötelezően közzétett adatok nyilvánosságra hozatalának szabályzata
5) A DE UniPass Kártya szabályzata
6) Belső kontroll szabályzat
7) Beszerzési Szabályzat
8) Közbeszerzési Szabályzat
9) DE Informatikai szolgáltatások
10) Iratkezelési szabályzat
11) Selejtezési Szabályzat
12) Szerződéskötés eljárási rendje

I.4 A szabályzattal kapcsolatos felelősségek és feladatok

Felelősségek

	IBSZ elkészítése, módosítása		IBSZ elfogadása	IBSZ rendszeres felülvizsgálata	IBSZ betartásának ellenőrzése	
DE Szenátusa			J			
Kancellár	T			T	T	
Információ biztonsági felelős (IBF)	V		T	V	J	V
IT üzemeltető szervezetek vezetői	V	K	T	V	K	V
Adatvédelmi tisztviselő	V	K	T	T	T	

R: responsible. „V"égrehajtó
A: accountable, „J"óváhagyó
C: consulted, „K"onzulens
I: informed, „T"ájékoztatandó

Felelősség hozzárendelési mátrix

RACI modell

I.5 A szabályzat elkészítése, felülvizsgálata és módosítása

I.5.1. A Szabályzat elkészítése

(1) Az IBSZ elkészítése, a szakmai egyeztetések lefolytatása, a Kancellári engedélyeztetés és a Szenátusi elfogadásra való előterjesztés kezdeményezése az Egyetemi Információ biztonsági felelős (IBF) feladata és felelőssége. A szabályzat elkészítésnek folyamatába konzulensként be kell vonni az IT üzemeltetést végző szervezeti egységeket (ISZK, SAP, UD Infopark Kft.) és az Egyetem Adatvédelmi Tisztviselőjét.

(2) A Szenátus elé terjesztés előtt a dokumentumot, részletezve a verzióváltási módosítási okot, minden informatika szolgáltatást végző szervezeti egység és az Egyetem Adatvédelmi tisztviselője részére szakmai iterációra elő kell terjeszteni. A dokumentum szakmai észrevételekkel ellátott végleges verzióját Szenátusi elfogadásra az IBF terjeszti fel a Kancellár engedélye és jóváhagyása mellett.

I.5.2. Időszaki felülvizsgálat

(1) A szabályzatot rendszeres időközönként, évente egyszer felül kell vizsgálni. A szabályzatot soron kívül felül kell vizsgálni minden olyan változás esetén, amelyek a szabályzatban foglaltak alkalmazhatóságát, megfelelőségét vagy hatékonyságát érintik illetve, ha olyan információbiztonsági incidens történik, amit jelen szabályzási és eljárásrendi környezet az eset egyedisége, ismeretlensége miatt nem érint, nem érinthet.

(2) A szabályzat felülvizsgálata, folyamatos karbantartása az Információbiztonsági felelősséget viselő egyetemi IBF-ként megbízott feladata, aki egyben az Informatikai Biztonsági Központ központvezetője.

I.5.3. Rendkívüli felülvizsgálat

(1) Az IBSZ rendszeres időszaki vizsgálaton kívüli felülvizsgálatára, indokolt esetben módosítására van szükség, ha olyan biztonsági incidens következik be, aminek kezelésére, precedens értékére vonatkozó eljárás, utasítás, kezelés, prevenció nincs lefektetve.

I.6 A szabályzat elfogadása és kihirdetése

(1) Az IBSZ-t az Egyetem Szenátusa fogadja el.

(2) A Szabályzat hatályba lépését követő 2 héten belül minden érintettet e-mailben értesíteni kell, és egyben biztosítani kell a szabályzat folyamatos elérhetőségét. A kommunikációk lebonyolítása az IBF feladata.

(3) A szabályzat és kapcsolódó eljárásrendjei az Egyetem honlapján az „Egyetemről – Közérdekű-Szabályzatok”, a Kancellária honlapján a „Szabályzatok”, menüpont alatt tekinthető meg.

I.7 A szabályzat betartásának ellenőrzése

(1) A szabályzat betartásának ellenőrzése a Kancellária Szervezeti és Működési Szabályzatában foglaltaknak megfelelően az Informatikai Biztonsági Központ szervezeti egység feladata, az IBF felelősségével.

(2) A Szabályzat betartásának ellenőrzésével összefüggésben az IBF-nek az Egyetem Kancellárja felé, míg GDPR érintettség esetén az Adatvédelmi Tisztviselő felé is tájékoztatási kötelezettsége is van.

I.8 Kivételkezeléssel kapcsolatos feladatok

(1) Amennyiben az Egyetem informatikai rendszereinek üzemeltetésében olyan indokolt, szabályzatban nem deklarált - biztonsági integritást nem sértő - megoldást kell a szolgáltatási eredményesség érdekében végrehajtani, azt „kivételes kezelést igénylő esetként” kell tekinteni, és a szabályozásban kezelendő céllá kell minősíteni.

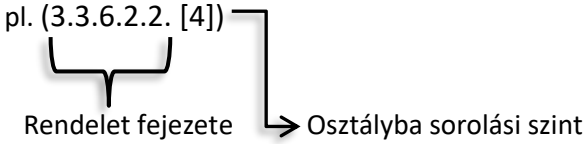
I.9 Szabályzat felépítése

(1) Az IBSZ felépítése, logikai vezetése követi a 41/2015. (VII. 15.) BM rendelet biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményeinek felépítését (így a bevallás kitöltésének segédlete), a fő fejezetcímek, és az alfejezetek vonatkozásában.

I.9.1. Fejezet címek értelmezése

(1) A 41/2015. (VII. 15.) BM rendelet biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó, biztonsági intézkedéseket tartalmazó „Védelmi intézkedés katalógus”-ában felsorolt intézkedések összhangban vannak a rendeletben található fejezetekkel (lenti ábra) és a szervezetnek a védelmi intézkedéseit ennek segítségével kell meghoznia.

(2) Az IBSZ-ben megfogalmazott tényleges védelmi intézkedéseket tartalmazó fejezetek címében megjelennek a Rendelet arra vonatkozó fejezetcímei és a biztonsági követelmények szintjének besorolása is, az átláthatóság és a megfelelőség ellenőrzése érdekében.



A 4. és 5. szintbe sorolt elektronikus információs rendszernek meg kell felelnie, a rendelet 3.3.6.2.2. fejezetében megfogalmazott elvárásoknak.

		Elektronikus információs rendszerek besorolása				
		[1]	[2]	[3]	[4]	[5]
Törvényi megfelelési kötelem (fejezetcímben feltüntetett besorolás)	[1]	√	√	√	√	√
	[2]		√	√	√	√
	[3]			√	√	√
	[4]				√	√
	[5]					√

Az 1,2 és 3. szintbe sorolt rendszerek nem tartoznak a törvény 3.3.6.2.2. fejezetében foglaltak megfelelési kényszere alá.

HASZNÁLT FOGALMAK

adat:
az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;

adatállomány:
az egy nyilvántartásban kezelt adatok összessége;

adatbiztonság:
az adatok jogosulatlan megszerzése, módosítása, törlése, 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.

adatfeldolgozás:
az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik;

adatfeldolgozó:
az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;

adatgazda:
annak a szervezeti egységnek a vezetője ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik. Felelős az általa kezelt adatokért, továbbá jogosult minősítés vagy osztályba sorolás elvégzésére.

adatkezelés:
az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása,törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése;

adatkezelő:
az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki, vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

adatközlő:
az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatot honlapon közzéteszi;

adatkezelés:
az alkalmazott eljárástól függetlenül az adaton végzett
bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

adatkezelés korlátozása:
a tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölése útján;

adattovábbítás:

az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

adattörlés:

az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

adatmegsemmisítés:

az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;

adminisztratív védelem:

a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;

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.

adatvédelmi incidens:

az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

alapvető szolgáltatásokat nyújtó szolgáltató:

a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI.törvény 2/A. §-a alapján kijelölt szolgáltató;

auditálás:

előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;

azonosítható természetes személy:

az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

álnevesítés:

személyes adat olyan módon történő kezelése, amely – a személyes adattól elkülönítve tárolt - további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely érintettre vonatkozik, valamint műszaki és szervezési intézkedések megtételével biztosítja, hogy azt azonosított vagy azonosítható természetes személyhez ne lehessen kapcsolni;

bejelentés-köteles szolgáltatás:

az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 2. § *j)* pontjában meghatározott szolgáltatás;

biometrikus adat:

egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat;

bizalmasság:

az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

biztonsági esemény:

nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

biztonsági esemény kezelése:

az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása,

következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;

biztonsági követelmények:

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

biztonsági osztály:

az elektronikus információs rendszer védelmének elvárt erőssége;

biztonsági osztályba sorolás:

a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;

biztonsági rendszer:

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

biztonsági szint:

a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

biztonsági szintbe sorolás:

a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

EGT-állam:

az információs önrendelkezési jogról és az információszabadságról szóló törvényben meghatározott állam;

elektronikus információs rendszer:

a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy

c) az *a)* és *b)* pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;

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.

életciklus:

az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;

érintett:

bármely információ alapján azonosított vagy azonosítható természetes személy;

észlelés:

a biztonsági esemény bekövetkezésének felismerése;

európai kiberbiztonsági tanúsítási rendszer*:*

az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 9. pontja szerinti rendszer;

felhasználó:

egy adott elektronikus információs rendszert igénybe vevők köre;

fenyegetés:

olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

fizikai védelem:

a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;

folyamatosság:

az üzleti, egyetemi tevékenységek zavarmentes rendelkezésre állása.

folytonos védelem:

az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;

genetikai adat:

egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered;

globális kibertér:

a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint e rendszereken keresztül adatok ésinformációk formájában megjelenő társadalmi és gazdasági folyamatok együttese;

határvédelmi felelős:

az infrastruktúra üzemeltetés szervezetében kijelölt felelős, aki az informatikai határvédelmi és határbiztonsági rendszerek felelőse. (Pl. tűzfalrendszerek, hálózati hozzáférés-védelem, behatolás érzékelő és megelőző rendszerek, távoli biztonságos elérés, hálózat szegmentációja.)

harmadik személy:

olyan természetes vagy jogi személy, illetve jogi
személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek;

hozzájárulás:
az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez;

információ:
bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;

kiberbiztonság:
a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhezés működtetéséhez;

kibervédelem:
a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését;

kockázat:
a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kárnagyságának a függvénye;

kockázatelemzés:
az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

kockázatkezelés:
az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;

kockázatokkal arányos védelem:
az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;

korai figyelmeztetés:
valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;

közvetett adattovábbítás:
személyes adatnak valamely harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbítása útján valamely más harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítása;

kritikus adat:
a személyes adat vagy valamely jogszabállyal védett adat;

különleges adat:
a személyes adatok különleges kategóriáiba tartozó
minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok,

közérdekű adat:
az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb

közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

közérdekből nyilvános adat:

a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

közös adatkezelő:

az az adatkezelő, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - az adatkezelés céljait és eszközeit egy vagy több másik adatkezelővel közösen határozza meg, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket egy vagy több másik adatkezelővel közösen hozza meg és hajtja végre vagy hajtatja végre az adatfeldolgozóval;

logikai védelem:

az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;

magyar kibertér:

a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne;

megelőzés:

a fenyegetés hatása bekövetkezésének elkerülése;

profilalkotás:

személyes adat bármely olyan - automatizált módon történő - kezelése, amely az érintett személyes jellemzőinek, különösen a munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelésére, elemzésére vagy előrejelzésére irányul;

reagálás:

a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;

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 tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

sérülékenység:

az elektronikus információs rendszer olyan része vagytulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

sérülékenység vizsgálat:

az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;

súlyos biztonsági esemény:

olyan informatikai esemény, amely bekövetkezéseesetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztéskövetkezhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;

számítógépes eseménykezelő központ*:*

az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)];

személyes adat:

az érintettre vonatkozó bármely információ;

szervezet:

az adatkezelést végző, illetve az adatfeldolgozást végző vagy végeztető jogi személy vagy egyéni vállalkozó, valamint az üzemeltető;

teljes körű védelem:

az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;

üzemeltető:

az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

védelmi feladatok:

megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;

zárt célú elektronikus információs rendszer:

a nemzetbiztonsági, honvédelmi, rendészeti, diplomáciai információs feladatok ellátását biztosító, rendeltetése szerint elkülönült elektronikus információs rendszer, amely kizárólagosan a speciális igényekkielégítését, az e célra létrehozott szervezet és technika működését szolgálja;

védelem:

az összes számításba vehető fenyegetést figyelembe vevő védelem. E törvény alkalmazásában egy elektronikus információs rendszernek kell tekinteni adott adatkezelő vagy adatfeldolgozó által, adott cél érdekében az adatok, információk kezelésére használt eszközök - így különösen környezeti infrastruktúra, hardver, hálózat és adathordozók -, eljárások - így különösen szabályozás, szoftver éskapcsolódó folyamatok -, valamint az ezeket kezelő személyek együttesét.

II. AZ INFORMATIKAI BIZTONSÁG SZERVEZETE

II.1 Informatikai biztonsági szerepek és felelősségek

(1) Az informatikai és információbiztonsági feladatokat ellátó szervezeti egységeket szervezeti szinten el kell különíteni. Az Egyetem információbiztonsági feladatainak ellátása során a következő szerepkörök érintettek:

a) Kancellár
b) Informatikai Biztonsági Központ vezető, Információbiztonsági Felelős (IBF)
c) Informatikai Szolgáltató Központ Igazgató
d) Adatgazda
e) Alkalmazásgazda
f) Szervezeti egység vezetője
g) Felhasználó

II.1.1 Kancellár

(1) Az Egyetem információbiztonsági rendszerének működtetése a Kancellár feladata, tevékenységét az az Információbiztonságért felelős vezető és az Informatikai igazgató útján gyakorolja.

II.1.1.1 Felelőssége

a) Az Nftv. 13/A. §, és az Egyetem Szervezeti és Működési Szabályzatának 24. § (3) 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;
c) A Kancellária vezetőjeként felel az informatikai biztonság-, és adatok védelmének megkövetelésééért;
d) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését;
e) biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését

II.1.1.2 Feladatai

a) az Egyetem informatikai biztonsággal összefüggő beszerzéseinek gazdálkodási szempontú értékelése, megvalósíthatóságuk vizsgálata, pénzügyi erőforrások biztosítása;
b) az elektronikus információs rendszer biztonsági osztálya és az Egyetem biztonsági szintje alapján előírt követelményeknek megfelelően az elektronikus információs rendszer biztonságáért felelős személyt (IBF) nevez ki vagy bíz meg;
c) döntéshozatal az IBF hatáskörét meghaladó ügyekben.

II.1.2 Informatikai Biztonsági Központ vezető, Információbiztonsági Felelős (IBF)

(1) Az Informatikai Biztonsági Központ vezetője egyben az Ibtv. törvénynek megfelelően az Egyetem információbiztonsági felelőse (IBF).

II.1.2.1 Hatásköre

(1) Az Egyetem információbiztonságának fenntartása érdekében, illetve információbiztonsági incidens esetében jogosult:

a) az Egyetem olyan helyiségébe ahol információbiztonságot érintő munkavégzés folyik jogosult belépni információbiztonsági ellenőrzés céljából;
b) jogosult az Egyetem tevékenységeihez köthető közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében valamennyi adatot, illetve az elektronikus információs rendszerek biztonságában keletkezett valamennyi dokumentumot bekérheti;
c) minden - információbiztonságot érintő - értekezleten részt venni, észrevételeit és javaslatait megtenni, amelynek számítástechnikai, illetve információbiztonsági vonatkozása van, és ez az értekezlet összehívásakor ismert;
d) jogosult a szolgáltatási szerződések információbiztonsági követelményeinek szakmai meghatározására, véleményezésére és felülvizsgálatára.

II.1.2.2 Felelőssége

(1) Az IBF felel a szervezetnél előforduló, az elektronikus információs rendszerek védelméhez kapcsolódó feladatok ellátásáért, az információ biztonságával kapcsolatos tevékenységek koordinálásáért a vonatkozó jogszabályok, szabványok, ajánlások előírásainak megfelelően.

II.1.2.3 Feladatai

a) Gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról, és elvégzi ezen tevékenységét tervezését, szervezését, koordinálását és ellenőrzését;
b) Előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot és gondoskodik annak folyamatos aktualizálásáról;
c) Előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását;
d) Véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit;
e) Kapcsolatot tart a hatósággal és az eseménykezelő központtal;
f) Bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet.
g) Végzi a kritikus információbiztonsági projektek szakmai irányítását;
h) Gondoskodik a vezetők és az alkalmazottak informatikai jellegű támadás vagy egyéb informatikai vészhelyzet esetén követendő magatartására vonatkozó oktatásról;
i) Elemzéseket végez és javaslatokat tesz a megfelelő védelmi intézkedésekre és a biztonságos működéssel összefüggő szabályok megváltoztatására;
j) Felügyeli a biztonsági előírások betartását;
k) Irányítja az informatikai rendszer védelmét;
l) Gondoskodik az információvédelemmel összefüggő biztonsági szabályzatok kiadatásáról és karbantartásáról;
m) Részt vesz a belső és külső vizsgálatok előkészítésében és lefolytatásában;
n) Az információvédelemmel összefüggő biztonsági szabályzatok előírásainak durva megsértéséről azonnali jelentési kötelezettsége áll fenn a Kancellárnak, valamint az érintett területek vezetőinek;
o) Az Egyetem munkatársainak megismertetése e szabályzat tartalmával;
p) Az informatikai rendszerek és fejlesztések biztonsági kockázatelemzése, figyelembe véve a GDPR által előírt Adatvédelmi Hatáselemzéshez kapcsolódó kockázatelemzéseket;
q) Az információbiztonság fejlesztésével kapcsolatos intézkedések megtervezése.
r) Az informatikai rendszerek és azok kontrollfolyamatainak ellenőrzése.

s) Az egyetemi szervezeti egységek által nyilvántartott felhasználói adminisztrációk (pl. jogosultsági mátrix) által nyilvántartott jogosultságok érvényesülésének ellenőrzése az Egyetem informatikai rendszereiben előzetes terv alapján, valamint előzetes bejelentési kötelezettség nélkül.
t) A kriptográfiai kulcsok és az Egyetem kiemelt informatikai rendszereiben kiosztott, igényelt jogosultságok nyilvántartásának felügyelete.
u) Az informatikai rendkívüli események és incidensek kivizsgálása.
v) Az IT helyiségekbe való beléptetési eljárás, valamint az IT helyiségekbe belépési jogosultsággal rendelkező személyi kör ellenőrzése, javaslattétel a beléptető rendszer kódjának szükség szerinti cseréjére.
w) Az egyetem információbiztonsági kockázatkezelő rendszerének szabályozása, a kockázatkezeléssel összefüggő feladatok és felelősségek definiálása, a kockázatkezelése tevékenység szabályozása alapján a folyamat irányítása és ellenőrzése.
x) A kockázatok mérséklésére vagy a működés hatékonyságának növelésére vonatkozó ajánlások készítése.
y) Minden olyan feladat, amit a Szervezeti és Működési Szabályzat, külön jogszabály, belső szabályzat, illetve a Kancellár vagy delegáltja a feladatkörébe utal.
z) Információbiztonsági Irányítási Rendszer (ISMS) használatának bevezetése, üzemeltetése. A rendszerből riportok, kimutatások, jelentések készítése.
aa) Informatikai adatvagyon bekérő, nyilvántartó rendszer készítése, bevezetése, üzemeltetése. A rendszerből elemzések, riportok, kimutatások, jelentések készítése.
bb) Felhasználói jogosultságkezelő rendszer készítése, bevezetése, üzemeltetése. A rendszerből elemzések, riportok, kimutatások, jelentések készítése.
cc) A szerződésekben szerepeltetendő általános információbiztonsági rendelkezések kidolgozása az GDPR központ vezetővel és szükség szerinti aktualizálása.

II.1.2.4 Kapcsolattartás a hatóságokkal

(1) Mint egyetemi IBF kapcsolattartói minőségben kommunikál a Nemzeti Kibervédelmi Intézettel, valamint kiber,- hackertámadás bekövetkezésekor, a természetes személyek adatainak érintettség esetén, az Egyetem Adatvédelmi tisztviselőjének közreműködése mellett, a Nemzeti Adatvédelmi és Információszabadság Hatósággal (NAIH).

II.1.3 Informatikai Szolgáltató Központ Igazgató

(1) Az Egyetem elektronikus információs rendszereinek és az azokat kiszolgáló infrastruktúra biztonságos üzemeltetéséért felelős vezető.

II.1.3.1 Felelőssége

(1) Az informatikai eszközök és rendszerek üzemeltetéséhez szükséges szervezeti és műszaki környezet létrehozása és folyamatos biztosítása.

II.1.3.2 Feladatai

a) az elektronikus információs rendszer funkcionális és biztonsági követelményeknek megfelelő működtetése;
b) az informatikai rendszer folyamatos rendelkezésre állásának biztosítása;
c) az informatikai folyamatok és tevékenységek tervezése és folyamatos fejlesztése;
d) 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) 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;
h) 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;
i) rendszeresen – az Egyetem Informatikai Katasztrófa-elhárítási Tervében leírtak szerint – gondoskodik a katasztrófahelyzet kezeléssel kapcsolatos tesztek elvégzéséről;
j) a programfejlesztési igények, fejlesztési programok kezelése, az elkészült termékek informatikai ellenőrzése az Egyetem belső szabályzatai és jelen IBSZ előírásai szerint;

II.1.3.3 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 vezetővel egyeztetettek alapján;
d) a fokozottan védett területekre (erőforrástermek) történő belépés és az ott történő munkavégzés engedélyezése, az engedélyek rendszeres felülvizsgálata és nyilvántartása;

II.1.4 Adatgazda

(1) Az adatgazda annak az önálló szervezeti egységnek a vezetője, ahol az adat keletkezik, illetve amelyhez jogszabály vagy szervezetszabályozó eszköz az adat kezelését vagy nyilvántartás vezetését elrendeli.

(2) Az Egyetemen üzemeltetett, adatokat kezelő informatikai rendszerek mindegyikét be kell sorolni egy-egy adatgazda felügyelete alá.

II.1.4.1 Felelőssége

(1) Az adatgazda felel:
   a) az adatokkal és az adatok felhasználásával kapcsolatos stratégiai szintű döntések meghozataláért;
   b) általa felügyelt vagy irányított tevékenységekhez kapcsolódóan keletkezett informatikai rendszerben tárolt és kezelt adatok, információk megbízhatóságát, hitelességét biztosító folyamatok megfelelőségét biztosító szabályok betartásáért;
   c) az illetékessége alá tartozó elektronikus információs rendszerek osztályba sorolásáért az IBF-el közösen;

II.1.4.2 Feladata

   a) Az Egyetem egyes működési folyamatai esetében, az általuk használt adatok vonatkozásában az adatgazdák az Információbiztonságért felelős (IBF) vezetővel közösen állapítják meg az adatkezelés biztonsági követelményeit;
   b) Meghatározza az adatokhoz / tevékenységekhez hozzáférőket, a szükséges-elégséges hozzáférési elv alapján, azaz mindenki csak annyi jogot kapjon, amennyi a munkája elvégzéséhez feltétlenül szükséges;
   c) Az alkalmazásgazdák közreműködésével meghatározza azokat a szakmai igényeket, amelyek alapján az informatikai fejlesztések, beruházások prognosztizálhatók (meghatározza az informatikai stratégia szakmai, felhasználói oldalát)

II. 1.5. 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 az adatgazda jelöli ki. Egy informatikai alkalmazáshoz több alkalmazásgazda is kijelölhető.

II.1.5.1 Feladata

   a) az adatgazda utasítása szerint köteles közreműködni az elektronikus információs rendszerek osztályba sorolásában;
   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) az adatgazda utasításai alapján közreműködik:
   - az adatok azok tárolására rendszeresített alkalmazásban való rendelkezésre állását biztosító folyamatok napi működtetésében,
   - a hatáskörébe tartozó informatikai rendszerek kódtárai tartalmának aktualizálásában, érvényességének folyamatos fenntartásában,
   - az Egyetemen rendelkezésre álló adatok, információk felhasználását (hasznosítását), valamit az adatok külső vagy belső publikálását, átadását biztosító folyamatok napi működtetésében.

II.1.5.2 Felelőssége

a) a hozzárendelt alkalmazás teljes funkcionalitásának, üzleti logikájának az ismerete, amely a rendszer funkcióinak a rendszeres használat szintjén történő alkalmazásán alapul,
b) az alkalmazás használatával kapcsolatos nem informatikai jellegű problémákról az adatgazda tájékoztatása és a megoldási lehetőségek megfogalmazása.

II. 1.6. Rendszergazda

(1) A rendszergazda az az üzemeltetésért felelős személy, aki adott rendszer üzemeltetési szakmai kompetenciájával rendelkezik, aki a rendszer beállításait, működés felügyeletét, jogosultság beállításait rendszeresen végzi.

II.1.6.1 Feladata

a) az általa üzemeltetett rendszer nyilvántartását naprakészen tartja;
b) kidolgozza a hatáskörébe tartozó üzemeltetési eljárásokat;
c) biztosítja a rendszerfelügyeletet;
d) üzemelteti a rá bízott elektronikus információs rendszereket.

II.1.6.2 Felelőssége

a) az általa üzemeltetett elektronikus információs rendszerek jelen IBSZ-ben foglaltak szerinti biztonságos üzemeltetése.

II. 1.7. Szervezeti egység vezetője

(1) Feladata, hogy az általa irányított szervezeti egység munkatársai megismerjék és betartsák a rájuk vonatkozó információbiztonsági előírásokat.

(2) Felelős a 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.

(3) Köteles a tudomására jutott, az egyetem információbiztonságát veszélyeztető, működését sértő eseményekről, körülményekről – azok jellegétől függően – az Információbiztonságért felelős vezetői feladatokat ellátó munkatársnak információt nyújtani.

II. 1.8. Felhasználó

(1) Adott elektronikus informatikai rendszereket munkavégzése során igénybe vevő munkavállaló.

II.1.8.1 Feladata

a) Kötelessége az információk védelmét, azok keletkezésének, feldolgozásának, szétosztásának, tárolásának és selejtezésének teljes folyamata, életciklusa során biztosítani;
b) Valamennyi felhasználó köteles azonnal értesíteni felettesét vagy az Informatikai Biztonsági Központot, információbiztonságot érintő esemény észlelése/bekövetkezése esetén.

II.1.8.2 Felelőssége

a) az Információbiztonsági Szabályzat megismerése és az abban foglalt szabályok betartása;
b) a birtokában lévő, vagy tudomására jutott információk bizalmasságának megfelelő kezeléséért;
c) az elektronikus információs rendszerben végzett műveletekért;
d) az Egyetem elektronikus információs rendszereinek szakszerű kezeléséért;
e) a személyi használatra átvett eszközök megfelelő fizikai védelméért.

III. A SZERVEZET BIZTONSÁGI SZINTJE

III.1 Biztonsági szintbe és osztályba sorolás, informatikai biztonsági kockázatelemzés

(1) A biztonsági szintbe és osztályba sorolás alapvető követelményeit fogalmazza meg a 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.

III.1.1. Biztonsági szintbe és osztályba sorolás

(1) Az Egyetem annak érdekében, hogy az információbiztonsági törvény hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszerek biztonságáért felelős személy irányításával, jogszabályban meghatározott szempontok, kockázatelemzés alapján megvizsgálja (alvállalkozó igénybevétele esetén megvizsgáltatja) elektronikus információs rendszereit. Meghatározza, hogy azok melyik biztonsági osztályba sorolandók.

(2) Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A kezelt adatok és a funkciók figyelembe vételével a lehetséges kármértéket kell megállapítani, míg a kár bekövetkezésének valószínűsége a körülmények mérlegelésével becsülhető. A biztonsági osztályba soroláskor figyelembe veendő káreseményeket a 41/2015. (VII. 15.) BM rendelet 1. számú melléklet 2. pontja rendeli az egyes biztonsági osztályokhoz.

(3) Azokban az esetekben, amikor az Egyetem külső szolgáltatót, illetve jogszabály alapján kijelölt szolgáltatót vesz igénybe, a biztonsági osztályba sorolás a szolgáltató feladata, amelyről az Egyetem, tájékoztatást kell, hogy kérjen. A kockázatelemzés és kockázatkezelés során az Egyetemnek figyelembe kell vennie a külső szolgáltató által meghatározott biztonsági osztály értékét.

(4) A biztonsági osztályba sorolás alkalmával - az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján - 1-től 5- ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt (a 41/2015 [VII.15.] BM rendelet iránymutatása alapján). Az elektronikus információs rendszer biztonsági osztálya alapján kell megvalósítani az előírt védelmi intézkedéseket az adott elektronikus információs rendszerre vonatkozóan.

(5) Az Egyetem illetékes vezetőjeként a Kancellár hagyja jóvá a biztonsági besorolást, de a törvényben meghatározott feltételeknek megfelelő, az elektronikus információs rendszerre irányadó biztonsági osztálynál magasabb, kivételes esetben a hatóság előzetes engedélyével, kockázatokra kiterjedő indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthat az elektronikus információs rendszerre vonatkozóan.

(6) Azokat a kontrollokat, amelyek nem valósulnak meg, kockázatelemzés útján prioritásukat tekintve intézkedési tervben (Cselekvési tervben) kell kezelni.

(7) A biztonsági osztályba és biztonsági szintbe sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni. A soron kívüli biztonsági osztályba és szintbe sorolást az elektronikus információs rendszer biztonságát érintő jogszabályban meghatározott változás vagy új elektronikus információs rendszer bevezetése esetén, ill. a szervezet státuszában, szervezetében, ill. az általa kezelt vagy feldolgozott adatok vonatkozásában bekövetkezett változás

esetén szükséges elvégezni. Az elektronikus információs rendszerek biztonságáért felelős személy vagy általa megbízott személy feladata, hogy a rendszerek biztonsági osztályba sorolását elvégezze, az Egyetem és szervezeti egységeinek biztonsági szintjét megállapítsa, a hatósági adatszolgáltatást előkészítse, és a Kancellár számára előterjessze.

(8) Az Egyetem és szervezeti egységei által használt informatikai rendszerek biztonsági osztályba sorolásait, az Egyetem vagy szervezeti egység biztonsági szintbe sorolását, az IBF javaslata alapján a Kancellár hagyja jóvá.

(9) Az elektronikus információs rendszerek biztonságáért felelős személy gondoskodik az adatszolgáltatás teljesítéséről a Hatóság (Nemzeti Kibervédelmi Intézet Nemzeti Elektronikus Információbiztonsági Hatóság) által előírt módon (feltöltés a NEIH hivatali kapujára vagy tömörített, titkosított/jelszóval védett állomány elküldése).

(10) A 2013. évi L. törvénynek és a 41/2015. (VII. 15.) BM rendelet való megfelelés vizsgálatának eredményeként a Debreceni Egyetem elektronikus információs rendszereket üzemeltető szervezeti egységeinek **biztonsági szintje a 4. biztonsági szintbe**, míg az Egyetem többi szervezete **3-as szintű elvárásnak** kell, hogy megfeleljen.

(11) Az Egyetem Klinikai Központja a 246/2015. (IX. 8.) Kormányrendelet szerint besorolás alapján, Nemzeti létfontosságú rendszerelem (alapvető szolgáltatást nyújtó szereplő), így **legalább 4.-es biztonsági szintbe és osztályba** sorolandó.

III.1.2. Cselekvési terv készítése

(1) Cselekvési tervet kell készíteni, ha egy elektronikus információs rendszer vonatkozásában biztonsági osztály meghatározásánál hiányosság állapítható meg.

(2) A cselekvési terv dokumentálja a megállapított hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeket.

(3) A meglévő cselekvési tervet az Egyetem által meghatározott gyakorisággal a biztonsági értékelések, biztonsági hatáselemzések és a folyamatos felügyelet eredményei alapján kell frissíteni.

III.2. Informatikai biztonsági kockázatelemzés

(1) A nem megfelelően kezelt informatikai és információbiztonsági kockázatok kárt okozhatnak a szervezetnek, ezért gondoskodni kell a biztonsági kockázatok felméréséről és megfelelő kezeléséről. A megfelelő kezelés érdekében az Egyetem felső vezetésének meg kell határoznia az elfogadható kockázat mértékét. A kockázatkezelés célja a kockázatok feltárása, dokumentálása, és ahol lehet, elfogadható szintre csökkentése.

(2) A kockázatelemzés szorosan kapcsolódik a biztonsági osztályba és biztonsági szintbe soroláshoz.

(3) Az információbiztonsági és informatikai kockázatokkal az azonosított kockázatok kezelésével kapcsolatos tevékenység az „Egyetem Belső Kontroll Szabályzatában" foglaltakkal összhangban az Integrált Kockázatkezelési Rendszer részeként, de az „Információbiztonsági kockázatok kezelésének eljárásrendje" dokumentumban szabályozott módon kerül végrehajtásra.

(4) Az információbiztonsági kockázatok kezelésének eljárásrendje kidolgozásáért - a GDPR Központ vezetője és az IT területek vezetőinek közreműködésével - az Informatikai Biztonsági Központ vezetője (IBF) a felelős, és egyben felel annak alkalmazásáért is.

(5) Az Egyetem az eljárásrendben rögzített szabályok szerint:

a) Végrehajtja a biztonsági kockázatelemzéseket;
b) Rögzíti a kockázatelemzések eredményét kockázatelemzési jelentésben;
c) Felülvizsgálja a kockázatelemzések eredményét;
d) Megismerteti a kockázatelemzés eredményét az érintettekkel;
e) Gondoskodik arról, hogy a kockázatelemzési eredmények a jogosulatlanok számára ne legyenek megismerhetők;
f) Olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát (új fenyegetések és sebezhetőségek megjelenése), ismételt kockázatelemzést hajt végre;

(6) A kockázatmenedzsmenti tevékenység átláthatósága, támogatása és teljes körű dokumentáltsága tekintetében szoftveres keretrendszert (ISMS) használ az Egyetem.

III.3 Informatikai biztonsági ellenőrzés

(1) Az informatikai biztonsági ellenőrzések alapvető célja, hogy a kockázat csökkentése és a rendkívüli események elkerülése érdekében, objektív információkat szolgáltasson a szervezet vezetői számára az informatikai biztonság helyzetéről.

(2) Potenciális vagy a valódi biztonsági eseményekkel és biztonsággal kapcsolatos információk, vagy riasztások alapján tesztelési eljárást vagy biztonsági ellenőrzést kell végezni.

(3) Az informatikai rendszereket rendszeres időközönként ellenőrizni kell, vizsgálva azt, hogy az informatikai rendszerek műszaki paraméterei teljesítik-e a feléjük támasztott biztonsági elvárásokat. A rendszer biztonsági ellenőrzésének követelményeit, valamint az ellenőrzést is magában foglaló tevékenységeket (ideértve az automatizált sebezhetőség-vizsgálatokat) gondosan meg kell tervezni, és az érintettekkel egyeztetni szükséges annak érdekében, hogy minimalizálni lehessen a szervezeti folyamatok megszakadásának a kockázatát.

(4) Az informatikai rendszer biztonsági ellenőrzésére az IT területek vezetőinek tájékoztatása mellett, a velük egyeztetett időszakban kerülhet sor. Szervezeti rendszerek biztonsági ellenőrzése előtt az adott rendszer szakmai adatgazdájával történő egyeztetés is szükséges.

(5) A biztonsági ellenőrzések és megfelelések dokumentált elvégzése az IBF feladata.

(6) A megállapított követelményeket, - beleértve a tesztelés típusával és gyakoriságával kapcsolatos követelményeket is - dokumentálni kell, az ellenőrzés alá vont szervezeti egység vezetőjével jóvá kell hagyatni és be kell vezetni.

IV. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

(1) Az ebben a fejezetben leírt adminisztratív védelmi intézkedéseket egységesen kell valamennyi elektronikus információs rendszerre vonatkozóan megvalósítani.

IV.1 Az elektronikus információs rendszerekkel kapcsolatos engedélyezés (3.3.6.2.2. [4])

(1) Az Egyetem informatikai rendszereinek használata előzetes engedélyhez kötött. Az informatikai rendszerek jogosultságkezelését, - ami a hozzáférési jogosultságok megállapítására, kiosztására, módosítására és visszavonására vonatkozik, - a szervezeti elvárásoknak és a biztonsági alapelveknek megfelelően kell kialakítani, és szükség szerint módosítani. Az Egyetem informatikai rendszereihez történő hozzáférési jogosultságok dokumentált szabályozásának („*Engedélyezési és jogosultságkezelési eljárásrend"*) kidolgozásáért az IBF és az informatikai rendszerek üzemeltetését és szolgáltatását nyújtó egyetemi vagy azon kívüli szervezetek vezetői (továbbiakban: IT területek vezetői), annak alkalmazásáért az IT területek vezetői felelnek.

(2) Az információs rendszerekhez való hozzáférési jogosultságok kiadására, módosítására, visszavonására az arra vonatkozó indok megjelölésével kerülhet sor, amelyet dokumentálni szükséges. A kiosztott jogosultságokat „felhasználói jogosultság mátrix" forma szerint, vagy jogosultságkezelő rendszerben nyilván kell tartani.

(3) A jogosultságkezelés alanyainak kell lenni azoknak a külsős szerződött partnerek munkatársainak is, akiknek szolgáltatás biztosításához hozzáférést kell biztosítani.

(4) A jogosultságok kiosztásánál követni kell a „Need-to-know", vagy „Least privilege" elvet. A felhasználó csak olyan funkciót, rendszerelemet, alkalmazást és annyi adatot, információt érhessen el, ami a munkavégzéshez, a feladatának, munkaköri kötelmének ellátásához feltétlenül szükséges. Ennek az elvnek a szoftver rendszerek használatára vonatkozó betartásán túl kiterjed a munkaállomás tartományvezérelt (Active Directory) eléréséhez szükséges házirend kialakítására is.

(5) A hozzáférési jogosultságokat az IBF koordinációjával rendszeres időközönként felül kell vizsgálni. A hozzáférési jogosultságok személyi kötődésének összhangban kell lenni az Egyetem munkaügyi rendszerében lévő foglalkozási státusz adatokkal, illetve külsős, jogosultsággal rendelkező szolgáltató munkatársak esetében a szerződés nyilvántartással.

IV. 1.1. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás (3.1.1.5. [1])

(1) Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás kiterjed minden, az Egyetem hatókörébe tartozó:
   a) emberi, fizikai és logikai erőforrásra,
   b) eljárási és védelmi követelményszintre és folyamatra.

(2) A fizikai és logikai jogosultságok engedélyezése az alábbiakat foglalja magába:
   a) melyek a jogosultsággal rendelkező személyek felelősségei, velük szembeni szabályok,követelmények,
   b) hogyan történik az elektronikus információs rendszerhez való hozzáférés engedélyezése, jogosultság adás,
   c) melyek a rendszer jogosultsági szintjei (biztonsági zónák védelme, minimum jogosultság,privilegizált, stb.),
   d) mit tartalmaznak az egyes jogosultsági szintek,

e) melyek a legkisebb jogosultság elve alapján, a jogosultsági körök,
f) kik az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek és milyen jogosultságaik vannak,
g) kik rendelkeznek, illetve rendelkezhetnek privilegizált jogosultsággal,
h) melyek azok a tevékenységek, amelyek az elektronikus információs rendszer használata során engedélyezettek, illetve tiltottak,
i) hogyan történik a jogosultsággal rendelkező személyek nyilatkoztatása (biztonsági szabályok és kötelezettségek megismerése),
j) hogyan történik a jogosultság visszavonás.

IV. 1.2. Engedélyek visszavonása/felfüggesztése (3.1.1.5. (1)

(1) A munkaviszony megszűnése, továbbá a munkakör megváltozása esetén gondoskodni kell arról, hogy az érintettek a változást követően csak azon rendszerekhez és az abban kezelt adatokhoz férhessenek hozzá, amelyek megismerésére, kezelésére a változást követően jogosultak.

(2) Kilépő dolgozók esetén legkésőbb az utolsó munkában töltött napon a következő teendők szükségesek biztonsági szempontból:
   a) Minden alábbi jogosultság megvonása:
      - LDAP
      - elektronikus levelezési fiók elérése
      - használt rendszerek rendszergazdai, felhasználói jogosultságok tiltása
      - Active Directory jogosultság visszavonása
      - munkavégzéshez használt eszköz (asztali munkaállomás, hordozható eszközök, telefon) jelszavának megváltoztatása

(3) A felhasználói hozzáféréseket felfüggesztett (inaktív) státuszba kell állítani, amennyiben:
   a) 5 egymást követő sikertelen bejelentkezési kísérlet történt,
   b) 6 hónapig nem történik aktív bejelentkezése,
   c) munkahelyi vezetője kérésére,
   d) illetéktelen adattartalom letöltése, nyomtatása esetén,
   e) log, napló bejegyzés szerinti rendszergazdai jelzésre,
   f) bizonyítottan más személynek átadott hozzáférési jogosultság alkalmával.

(4) A humánbiztonsággal kapcsolatos részletes feladatok a „Személybiztonsági eljárásrendben” kerülnek meghatározásra. Az eljárásrendet az Informatikai Biztonsági Központ vezetője, a HR Igazgató bevonásával dolgozza ki. Az eljárásrend betartásáért az összes szervezeti egység vezetője felel.

IV. 1.3. Felhasználók jogai

(1) Az Egyetem munkavállalóit jogviszonyuk szerint, informatikai eszköz használata tekintetében alap felhasználói jogosultságok illetik meg.

(2) Az alap felhasználói jogosultsággal biztosított használat:
   - egyetemi levelezési cím használata
   - internet használat
   - Office365 fiók által biztosított Microsoft alkalmazások használata

(3) A felhasználókat megillető egyéb jogosultságokat, a munkakör ellátásához elengedhetetlenül szükséges mértékben az adatgazdák határozzák meg.

IV. 1.4. Felhasználók kötelességei

a) Az Egyetem által kezelt információk biztonságos kezelése, az érzékeny adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megóvása, a jogosulatlan megismerés, módosítás és megsemmisülés elleni védelme minden munkatársnak és valamennyi, az Egyetemmel szerződéses kapcsolatban álló külső cégnek és munkatársainak feladata és kötelessége.
b) Az Egyetem minden munkavállalójának, valamint jogállástól függetlenül az Egyetem informatikai rendszerei valamennyi felhasználójának kötelessége a hatályos biztonsági szabályozások megismerése és betartása. Egyes informatikai rendszerekre külön is vonatkozhatnak szolgáltatás- és informatikai rendszer-specifikus biztonsági előírások, amelyeket az adott rendszerek felhasználóinak kötelességük időben megismerni és betartani.
c) Az Egyetem minden dolgozója személyes felelősséggel tartozik munkaeszközeiért, így a felhasználói munkaállomások, illetve a rajtuk tárolt vagy rajtuk keresztül elérhető adatok, a felhasznált információk védelméért, illetve az ezekkel kapcsolatos biztonsági és egyéb követelmények betartásáért.
d) Minden munkavállaló köteles haladéktalanul jelenteni az Informatikai Biztonsági Központ vezetőjének, ha olyan jelenséget vagy tevékenységet észlel, amely a hatályos biztonsági szabályokat sérti, vagy egyéb okból felmerül annak gyanúja, hogy az az Egyetem munkavállalóira, a kezelt adatok bizalmasságára, sértetlenségére, illetve rendelkezésre állására, vagy az Egyetem vagyontárgyaira és/vagy informatikai rendszereire nézve veszélyt jelenthet.
e) A bejelentést az **ibk@unideb.hu** elektronikus levelezési címen kell megtenni.

IV. 1.5. Felhasználók azonosítása

(1) Az Egyetem saját adatai, információi védelmében valamennyi informatikai eszköze, rendszere esetében azonosítási hitelesítő mechanizmust használ, így azok csak felhasználói azonosítást követően vehetők birtokba.

(2) A hitelesítés módszere a felhasználói azonosítóhoz tartozó jelszó ellenőrzése.

(3) Az Egyetem minden informatikai autentikációs felületén be kell vezetni a legalább kétfaktoros beléptetés kontrollt.

IV. 1.6. Felhasználók számára tiltott tevékenységek

(1) Tiltott minden olyan tevékenység, ami a hatályos jogszabályokba ütközik, különös tekintettel az alábbiakra:
   a) mások személyiségi jogainak megsértése;
   b) tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték);
   c) a szerzői jogok megsértése;
   d) szoftver szándékos és tudatos illegális terjesztése;
   e) profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése;

f) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, módosítása, megrongálása, megsemmisítésére irányuló tevékenység;
g) a hálózat biztonságos működését zavaró vagy veszélyeztető információk, programok terjesztése (pl. vírusok, trójai programok, hacker eszközök, férgek);
h) az internetről a legálisan hozzáférhető – nem ingyenes - programok letöltése, kivéve, ha arra vezetői engedély vonatkozik;
i) tilos a nem jogtiszta, „kalózszoftverek" letöltése és használata
j) a szolgáltatások blokkolását, lassítását célzó támadás, az azonosítási, illetve biztonsági intézkedések megsértésére irányuló kísérlet, valamint az egyéb azonosítóhoz, számítógéphez vagy hálózathoz történő illetéktelen hozzáférési kísérlet;
k) 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;

Mindezt a Debreceni Egyetem egyrészt az informatikai infrastruktúra üzemeltetés részéről úgynevezett „Black List" nemkívánatos, munkatevékenységhez nem köthető, nem támogató oldalak tiltásával, másrészt az egyetemi polgárok részére „Biztonsági öntudatosságra" történő oktatással és figyelem felhívással előzheti meg.

IV.2 Az elektronikus információs rendszerek nyilvántartása (3.1.1.4. [1])

(1) Az Egyetem összes informatikai vagyontárgyát eszközleltár keretében azonosítani- és nyilvántartásban kell rögzíteni.

(2) A nyilvántartás kötelező konfigurációs adatai:
   a) hardver elemek
      - szerver
      - kliens
      - hálózati eszköz
      - adattárolók (storage, streamer, NAS, SAN)
   b) szoftver elemek
      - operációs rendszer
      - alkalmazás
      - fejlesztői környezet
      - információs elemek
      - adatbázis kezelők
      - adatállomány
   c) szolgáltatási elemek
      - erősáram ellátás
      - aggregátoros betáplálás
      - légkondicionálás
   d) dokumentációs elemek
      - felhasználói leírás
      - rendszergazdai üzemeltető kézikönyv
      - rendszerleírás
      - fejlesztési dokumentáció (belső fejlesztés)

(3) A nyilvántartásnak minden rendszerre nézve tartalmaznia kell még az alábbiakat:
   a) annak alapfeladatait;
   b) a rendszerek által biztosítandó szolgáltatásokat;
   c) az érintett rendszerekhez tartozó licenc számot;
   d) a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;
   e) a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

(4) A leltár felvételével és karbantartásával kapcsolatos utasításokat az Egyetem „Az Eszközök és a Források Leltározási és Leltárkészítési Szabályzata” tartalmazza.

(5) El kell készíteni a szoftver adatvagyon leltárt, ami egyrészt alapja a 41/2015. (VII. 15.) BM rendelet bevallási kötelmének, másrészt információbiztonsági sérülékenységek, biztonsági rések feltárását, azok kezelését, kockázatkezelés kidolgozását teszik lehetővé.

(6) A szoftver adatvagyon felmérés, nyilvántartás és a bevallott adatok feldolgozása az Informatikai Biztonsági Központ feladata.

(7) Szoftver adatvagyon bevallásra minden olyan munkaszervezeti egység kötelezett, aki saját fejlesztésű, egyetemi fejlesztésű vagy vásárolt szoftver termék támogatásával végzi tevékenységét. A bevallásnak nem célterülete, az operációs rendszer, office termékek, média lejátszók, képfeldolgozó programok.

(8) Az Egyetem elektronikus információs rendszereinek nyilvántartása az **Információbiztonsági Irányítási Rendszer (IBIR) SeCube GRC keretrendszer „inventory” moduljában történik.**

(9) A SeCube konfigurációs adatbázisában, az „inventory”-ban az Egyetem szervezeti felépítését, telephelyi struktúráját, leltári elemeit, adatvagyonát, üzleti folyamatait és azok bizonyos tulajdonságait, illetve összefüggéseit tartja nyilván és ábrázolja. Az Inventory ezáltal lefedi a információs vagyonelem leltár követelményét.

(10) A tárolható konfigurációs elemek fő csoportjai:
- Szervezeti felépítés és Humán erőforrások
- Telephelyi struktúra
- Eszközök, erőforrások (fizikai és logikai erőforrások)
- Adatvagyon
- Szolgáltatások és Rendszerek
- Adatkezelési tevékenységek (GDPR)
- Üzleti vagy termelési folyamatok
- Védelmi intézkedések

Az Inventory szükséges alapot szolgáltat, a SeCube további moduljaiban implementált munkafolyamatokhoz.

IV.3 Kockázatkezelés, kockázatelemzés (3.1.2. [1])

(1) A nem megfelelően kezelt informatikai és információbiztonsági kockázatok kárt okozhatnak a szervezetnek, ezért gondoskodni kell a biztonsági kockázatok felméréséről és megfelelő kezeléséről. A kockázatkezelés célja a kockázatok feltárása, hatásának minimalizálása, dokumentálása, és ahol lehet, elfogadható szintre csökkentése.

(2) Az információbiztonsági és informatikai kockázatokkal az azonosított kockázatok kezelésével kapcsolatos tevékenység az **„Egyetem Belső Kontroll Szabályzatában”** foglaltakkal összhangban az Integrált Kockázatkezelési Rendszer részeként az „**Információbiztonsági kockázatok kezelésének eljárásrendje**” dokumentumban szabályozott módon kerül végrehajtásra.

(3) A kockázatok elemzésének ki kell térni az informatikai rendszerek tervezése, beszerzése, üzemeltetése, fejlesztése és ellenőrzése területére. A kockázatelemzést szükség szerint, de legalább évente felül kell vizsgálni.

(4) Kockázatelemzés lépései
   a) A vagyontárgyak azonosítása és értékelése;
   b) a fenyegetések felmérése;
   c) a sebezhetőségek felmérése;
   d) a kockázatok felmérése, értékelése;
   e) elfogadható kockázati szint meghatározása, a kockázatokhoz kapcsolódó lehetséges reakciók azonosítása;
   f) a kockázatokra adható válaszok mérlegelése.

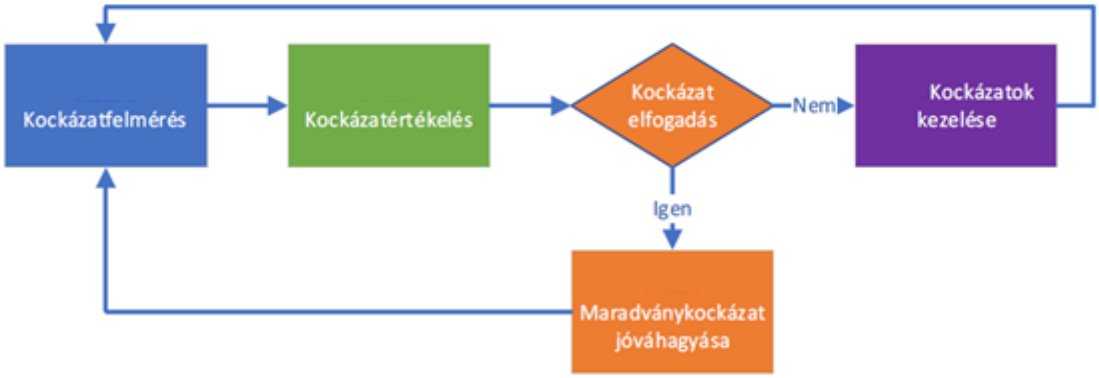
(5) Soron kívüli kockázatelemzésre van szükség a következő esetekben:
   a) jelentős információbiztonsági esemény következik be,
   b) új, kritikus informatikai rendszer és alkalmazás bevezetése vagy egy már meglévő jelentős módosítása történik,
   c) új, kritikus folyamat, adatkör kerül bevezetésre,
   d) új, kritikus modul kerül integrálásra egy már meglévő rendszerbe.

(6) Az informatikai és információbiztonsági kockázatkezelés koordinálását az IBF végzi, a kockázatok kezelése az alábbi feladatok végzését jelenti:
   a) a kockázatok azonosítása,
   b) a kockázatok értékelése és besorolása,
   c) a kockázatok kezelése,
   d) a kockázatok figyelemmel kísérése és jelentése,
   e) a kockázatok dokumentálása és nyilvántartása.

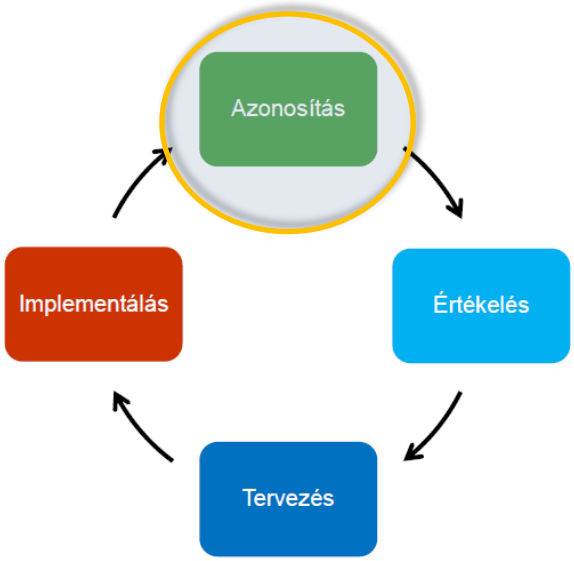
(7) Az információbiztonsági kockázatok kezelésének eljárásrendje kidolgozásáért - a GDPR Központ vezetője és az IT területek vezetőinek közreműködésével - az Informatikai Biztonsági Központ vezetője (IBF) a felelős, és egyben felel annak alkalmazásáért is.

(8) A kockázatmenedzsmenti tevékenység átláthatósága, támogatása és teljes körű dokumentáltsága tekintetében, szoftveres keretrendszer (ISMS) használatát kell alkalmazni. Az ISMS keretrendszer beszerzése, bevezetése, üzemeltetése az az Informatikai Biztonsági Központ vezetőjének (IBF) feladata és hatásköre.

Folyamat



IV. 3.1. A kockázat azonosítása



(1) Az Egyetem információit és információ-feldolgozó eszközeit fenyegető kockázatokat azonosítani kell.

(2) A kockázatok azonosításának kritikus pontja a kockázatok megfelelő megfogalmazása. A kockázatot úgy kell megfogalmazni, hogy tartalmazza:

- az esemény kiváltó okát;
- az esemény hatását;
- és azt, hogy mely szervezeti célra van hatással az adott esemény.

(3) A kockázatokat úgy kell megfogalmazni, hogy:

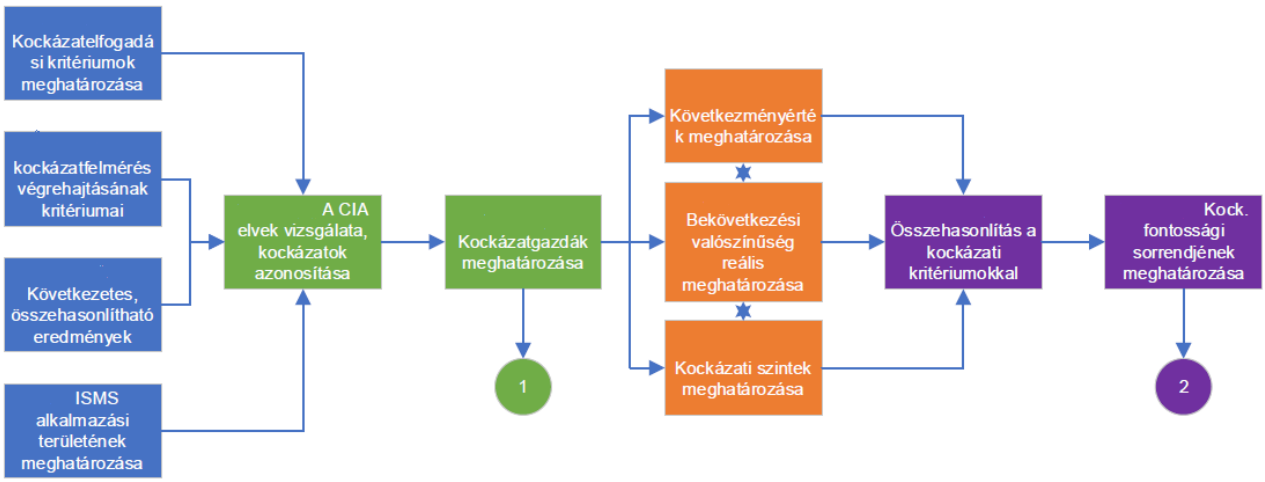
a) az mások számára értelmezhető legyen;
b) vissza lehessen vezetni a kockázati tényezőket;
c) hatékony kezelést eredményezzen;
d) meg lehessen előzni az újabb kialakulást.

(4) A pontos kockázatazonosítást követően fel kell venni a kockázati leltárt, amely tartalmazza:

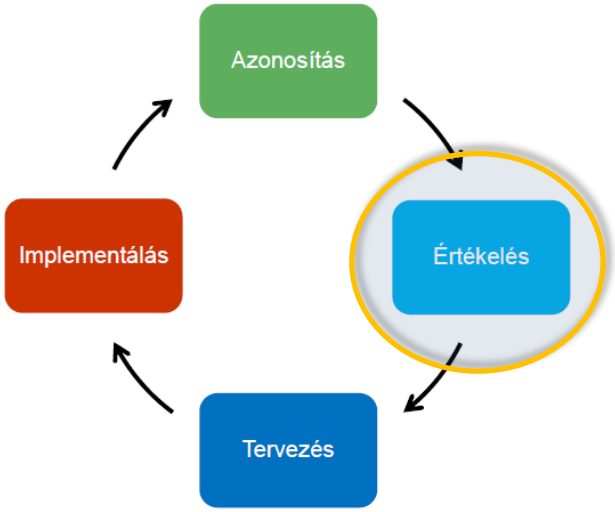
a) a kockázati eseményt,

b) a vonatkozó kockázati tényezőket,
c) a veszélyeztetett szervezeti célkitűzéseket,
d) az érintett folyamatokat,
e) a folyamatgazdát,
f) hogy integrált kockázatot vagy korrupciós kockázatot hordoz-e,
g) a kockázatkezelési intézkedést.

A kockázatfelmérés folyamata



IV. 3.2. A kockázat értékelése



(1) A kockázatok azonosítását követően el kell végezni azok elemzését, a kockázatoknak a kockázati tényezőkre való visszavezetését, a kockázati tényezők közötti összefüggések feltárását.

(2) Az azonosított kockázatok alapján a kockázati tényezőket meg kell határozni, majd a kockázati tényezők alapján el kell készíteni a kockázati kritérium mátrixot, ami a kockázatok kiértékelése.

(3) Az Egyetemen az azonosított kockázatok értékelése a kockázatként azonosított esemény bekövetkezésének a **valószínűsége** és a bekövetkezett esemény **hatásának** együttes értelmezésével történik.

(4) Az értéket a valószínűség és a hatás szorzataként kell megállapítani.

(5) A hatásskála a kockázatok bekövetkezése esetén az ötfokozatú skálán a hatás mértékét becsüli meg.

(6) Minden egyes kockázati szemponthoz 1-től 5-ig terjedő hatásmérőszámot kell rendelni a súlyosságnak megfelelően („1” a legalacsonyabb, „5” a legsúlyosabb).

1. 0-20 % között jelentéktelen
2. 21-40 % között alacsony
3. 41-60 % között közepes
4. 61-80 % között jelentős
5. 80 % felett meghatározó

(7) Minden egyes kockázati szemponthoz 1-től 5-ig terjedő valószínűségi mérőszámot is hozzá kell rendelni a súlyosságnak megfelelően.

1. 1-20 % közötti valószínűség, pl.: valószínűtlen - legalacsonyabb
2. 21-40 % közötti valószínűség, pl.: ritka
3. 41-60 % közötti valószínűség, pl.: lehetséges
4. 61-80 % közötti valószínűség, pl.: valószínű
5. 81-99 % közötti valószínűség, pl.: majdnem biztos - legsúlyosabb

A kockázati érték a hatás és a valószínűség értékek szorzata.

(8) A kockázatokat a kockázati érték szerint az alábbi 3 kategóriába kell sorolni:

- 1-9 kockázati érték: „A”-lacsony
- 10-19 kockázati érték: „K”-özepes
- 20-25 kockázati érték: „M”-agas

(9) A kockázatokat értékelést követően rangsorolni kell, annak érdekében, hogy az erőforrásokat a kulcskockázatokhoz koncentrálják és hatékonyan használják fel**.**

(10) Szükséges tűréshatárt meghatározni.

(11) Azokat a kockázatokat, amik a skálán a kockázati tűréshatár közelében, és afelett vannak, figyelni kell. Ezekhez a kockázatokhoz a kockázatkezelés során olyan folyamatokat kell definiálni, ami a kockázat felmerülése, megjelenése során azonnali kezelést tesz lehetővé.

(12) Minden kockázat esetén meg kell határozni egy válaszstratégiát, majd ennek megfelelően kell elkészíteni az integrált kockázatkezelési intézkedési tervet.

(13) A válaszstratégia kidolgozása során a kockázattal érintett rendszerek (dominó elv) helyreállítási, védelmi feladatait is számba kell venni.

IV.3.2.1. A kockázat bekövetkezéséből adódó lehetséges kár értékelése

(1) A kockázat bekövetkezte által okozott kár lehet,

a) közvetlen anyagi kár
b) közvetett anyagi kár
c) nincs bizalomvesztés a probléma a szervezeten belül marad
d) testi épség jelentéktelen sérülése
e) adat bizalmassága és hitelessége sérül

(2) Felmerült direkt költségek

a) Túlóraköltség

b) Vizsgálati, tesztelési költségek
c) Hibaelemzések költségei
d) Fejlesztési költségek
e) Dokumentációs költségek
f) Elveszett hasznon
g) Adat-helyreállítási költség
h) Adatelérés hiányából adódó plusz termelési költségek

(3) Felmerült indirekt költségek
a) Bírság (pl. NAIH)
b) Cégről kialakított kép helyreállítása
c) Termékről kiszivárgott adatok, új termék kifejlesztése
d) Elmaradt haszon
e) Személyi konzekvenciák költségei (HR költség)
f) Hosszú távú piacvesztés
g) Tréningköltségek

IV.3.2.2. A kockázati események bekövetkezésének valószínűsége

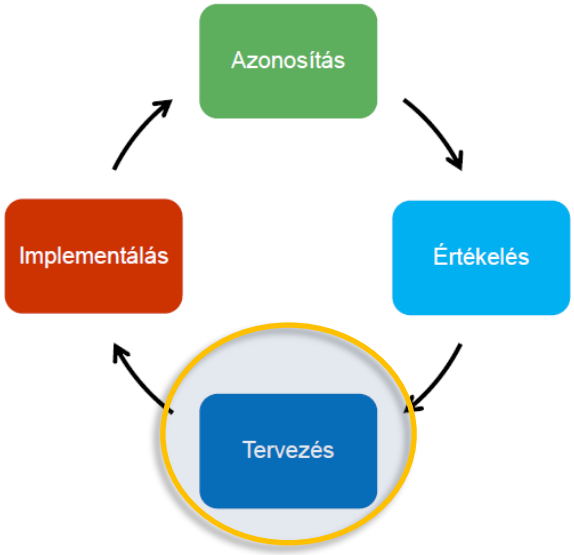
(1) A feltárt kockázati tényezők által generált események bekövetkezési valószínűségét csak megbecsülni lehet. A kockázat bekövetkezésének valószínűsége a körülmények mérlegelésével becsülhető.

IV.3.2.3. A kockázatok besorolása kockázati faktor szerint

(1) A kockázatok bekövetkezési valószínűségét tapasztalatok alapján lehet prognosztizálni. Azt, hogy a feltárt kockázatok milyen valószínűséggel fognak bekövetkezni, százalékosan be kell sorolni.

(2) A besorolás az egyes kockázati szemponthoz 1-től 5-ig terjedő valószínűségi mérőszámot rendel a megítélt súlyosságnak megfelelően:
- 1-20 % közötti valószínűség, valószínűtlen (legalacsonyabb)
- 21-40 % közötti valószínűség, ritka
- 41-60 % közötti valószínűség, lehetséges
- 61-80 % közötti valószínűség, valószínű
- 81-99 % közötti valószínűség, majdnem biztos (legsúlyosabb)

IV. 3.3. Az intézkedési terv és mérföldkövei (3.1.1.3. [2])



(1) A kockázatok kezelésére intézkedési tervet kell készíteni, amiben a kockázatkezelési stratégia és a kockázatokra adott válasz tevékenységek prioritása alapján mérföldköveket kell meghatározni.

(2) Az intézkedési tervet az IBF készíti elő közösen az IT területek vezetőivel, melyet a Kancellár hagy jóvá.

(3) Az intézkedési tervet legalább évente felül kell vizsgálni, a vizsgálat eredményétől függően karbantartani, indokoltság esetén módosítani szükséges.

(4) A válasz tevékenységek priorizálása alapján, a magastól az alacsonyabb prioritási sorrend szerint kell a mérföldköveket meghatározni.

IV. 3.3.1. Az intézkedési terv tartalma

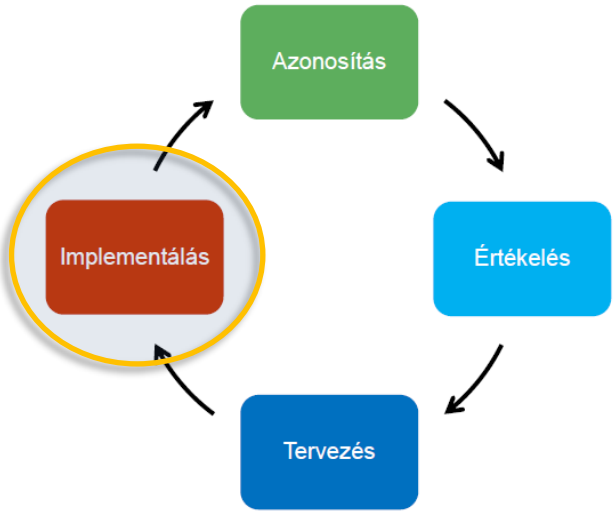
(1) Az intézkedési tervnek az alábbiakat szükséges tartalmaznia:

- tervezett intézkedés
- tervezett határidő
- megvalósítás dátuma
- intézkedés eredménye
- felelős
- ellenőrzésre jogosult
- fejlesztési célok
- prevenciós tevékenységek

IV. 3.3.2. Az intézkedési terv elkészítésének határidői

(1) Az elérendő biztonsági szint eléréséhez, a kockázatkezelési stratégia és a kockázatokra adott válasz tevékenység prioritása alapján, az Egyetem, intézkedési tervet készít, amiben meghatározza a mérföldköveket és tevékenységeket és azok megvalósításához határidőt rendel.

IV. 3.3.3. Kockázatkezelő intézkedések végrehajtása



(1) Az implementálás célja:
   a) A kockázatkezelési tervek végre legyenek hajtva;
   b) Az eredményességük le legyen ellenőrizve;
   c) Ahol szükséges, hozzuk meg a javító intézkedéseket;

(2) Az implementálás feladatai:
   1) Végrehajt
   2) Monitoroz
   3) Kontrollál
   4) Kockázati regiszter frissítése
   5) EWI-k finomhangolása
   6) Kockázatok lezárása
   7) Riportolás

IV. 3.4. A végrehajtás ellenőrzése, felülvizsgálat

(1) Az információvédelmet érintő mindennapi kihívások szükségessé teszik, hogy az informatikához kapcsolódó kockázatok kezelése kulcsfontosságú részévé váljon az irányítási és ellenőrzési folyamatoknak.

(2) Ellenőrzési területek:
   - kockázatcsökkentő intézkedések végrehajtásának ellenőrzése;
   - kockázatkezelő intézkedési tervek végrehajtásának ellenőrzése;
   - kockázatkezelési folyamat eredményességének és hatékonyságának ellenőrzése (monitoring).

(3) Folyamatos felülvizsgálat szükséges a kockázatkezelési tervek és intézkedések aktualitásának fenntartásához. A kockázatok kárkövetkezményeire vagy bekövetkezési valószínűségeire hatással lévő változások befolyásolhatják a kockázatkezelési intézkedések megfelelőségét és költségvonzatait. Ezért szükséges a kockázatkezelési folyamat rendszeres időközönként történő végrehajtása. A felülvizsgálatnak integráns részét kell képeznie a kockázatkezelési terveknek.

(4) Felülvizsgálat indokolt:

- ha az Egyetem egy adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, a hiányosság megszüntetése érdekében;
- ha a meghatározott biztonsági szint alacsonyabb, mint az Egyetemre érvényes szint, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, az előírt biztonsági szint elérése érdekében.

(5) Az ellenőrzési és felülvizsgálati dokumentumoknak a következőket kell tartalmazniuk:
- a kockázatfelmérés és a teljes kockázatkezelési folyamat ellenőrzésének módját és gyakoriságát;
- az ellenőrzési, felülvizsgálati és egyéb monitoring tevékenységek eredményeit;
- ellenőrzési, felülvizsgálati jelentésben foglalt következtetések és javaslatok alapján végrehajtott intézkedések részleteit;

(6) Az ellenőrzési és felülvizsgálati dokumentumok elkészítése és folyamatos naprakészen tartása az IBF feladata és felelőssége.

IV. 3.4.1. A kockázatkezelési feladatok nyomon követése (monitoring)

(1) A nyomon követés és felülvizsgálat célja a folyamat tervezésének, megvalósításának és eredményeinek minőségének és hatékonyságának biztosítása és javítása. A figyelemmel kísérésnek és a felülvizsgálatnak a folyamat minden szakaszában meg kell történnie. A monitoring magában foglalja a tervezést, az információk összegyűjtését és elemzését, az eredmények rögzítését és a visszajelzések gyűjtését.

(2) A kockázatkezelési folyamatot és annak eredményeit megfelelő mechanizmusokon keresztül kell dokumentálni és riportálni, melynek célja:
a) kommunikálja a kockázatkezelési tevékenységeket és eredményeket a szervezeten belül;
b) tájékoztatást nyújt a döntéshozatalhoz;
c) javítja a kockázatkezelési tevékenységek minőségét;
d) elősegíti az érdekelt felekkel való kapcsolattartást;
e) beleértve azokat is, akik felelősek és elszámoltathatók a kockázatkezelési tevékenységekért.

(3) A riportok:
a) a szervezet irányításának szerves részét képezik;
b) javítaniuk kell az érdekelt felekkel folytatott párbeszéd minőségét;
c) támogatniuk kell a felső vezetést és a felügyeleti szerveket.

(4) A riportkészítés során figyelembe veendő tényezők:
a) az érdekelt felek specifikus információs igényei és követelményei;
b) a jelentések előállítási költsége, gyakorisága és időszerűsége;
c) a jelentéstétel módja;
d) az információk relevanciája a szervezeti célok és a döntéshozatal szempontjából.

(5) A rendszeresen felügyelet információt ad arról, hogy:
- a kockázatkezeléssel kapcsolatos tevékenységek naprakészek-e;
- kerültek-e újabbak a látókörünkbe;
- az ellenintézkedések megvalósultak-e;
- a preventív intézkedések hatékonyan működnek-e

IV. 3.4.2. Eszkaláció (problémakezelés kiterjesztés)

(1) Amennyiben a kockázatkezelés során nem megoldható tevékenység jelentkezik, vagy a kockázat az Egyetem kockázat tűrési, kockázati tolerancia, kockázat kitettségi (hatás vagy előfordulási valószínűség) küszöbérték fölötti, a problémát az illetékes vezető és az IT üzemeltetés szakmai vezetői felé eszkalálni (felterjeszteni, továbbítani) kell.

(2) Az eszkalációs folyamat kezdeményezője az IBF.

IV. 3.5. A Kockázatkezelés lezárása

(1) A kockázatkezelés lezárása során elemezni kell:
   a) a kockázatkezelés sikerességét;
   b) keletkezett járulékos kockázatot;
   c) létrejött új kockázatot;
   d) minden érdekelt fél részt vett-e;
   e) minden dokumentáció, jelentés elkészült-e.

IV.4 Biztonsági osztályba sorolás (3.1.2.2. [1]

IV. 4.1. Adatbesorolás

(1) Az adat, információ bizalmassága és a védelemmel szemben támasztott követelmények alapján az Egyetem négy kategóriát különböztethet meg, melyek a következők:
   - **Nyilvános:** ebbe a kategóriába tartoznak az Egyetem azon adatai, amelyek az Egyetemen kívül is szabadon terjeszthetők.
   - **Belső használatra**: ebbe a kategóriába tartoznak az Egyetem azon adatai, amelyekhez az Egyetem munkatársai szabadon hozzáférhetnek, de harmadik félnek engedély nélkül nem adhatók át.
   - **Bizalmas:** ebbe a kategóriába tartoznak az Egyetem azon adatai, amelyekhez az Egyetemen belül sem férhet hozzá mindenki.
   - **Szigorúan bizalmas:** ebbe a kategóriába tartoznak az Egyetem azon adatai, amelyek az Egyetemen belül is csak szűk körben hozzáférhetők.

IV.4.1.1 Az adatok osztályozása bizalmasság szerint

(1) Bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

(2) Bizalmassági besorolás:
   a) Titkos
   b) Bizalmas
   c) Korlátozott terjesztésű

IV.4.1.2 Az adatok osztályozása sértetlenség és rendelkezésre állás szerint

a) **Sértetlenség**: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség) és a származás megtörténtének bizonyosságát (letagadhatatlanság) is, illetve a rendszerelem tulajdonsága, amely arra vonatkozik, hogy a rendszerelem rendeltetésének megfelelően használható;
b) **Rendelkezésre állás**: az adat, illetve az informatikai rendszer elemeinek tulajdonsága, amely arra vonatkozik, hogy az arra jogosultak által a szükséges időben és időtartamra használható;

IV. 4.2. A rendszerrel kapcsolatos biztonsági kockázatelemzés

(1) Végre kell hajtani a biztonsági kockázatelemzést, aminek eredményét rögzíteni szükséges az alábbi dokumentumok egyikében:
   a) az informatikai biztonsági szabályzatban;
   b) a kockázatelemzési jelentésben, vagy
   c) a kockázatelemzési eljárásrendben előírt dokumentumban.

(2) Az IBF a kockázatelemzések eredményét:
   a) felülvizsgálja;
   b) megismerteti az érintettekkel;
   c) gondoskodik, hogy az jogosulatlanok számára ne legyenek megismerhetők.

(3) Amikor változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát, ismételt kockázatelemzést kell végrehajtani.

IV. 4.3. A rendszer tényleges biztonsági osztályának meghatározása

(1) A biztonsági osztályba sorolás olyan értékelési tevékenység, amely során a kockázat mértékét az adatok értékét, az adatok kezelésének módját, körülményeit, a védelem eszközeit figyelembe véve meghatározzák a védelmi szintet.

(2) A biztonsági osztályba sorolás során meghatározásra kerül, hogy milyen kategóriába (pl. alacsony, fokozott, kiemelt) kerül bizalmasság, sértetlenség, és rendelkezésre állás szempontjából az információs rendszer. A szempontok aggregálása során a legszigorúbb kategóriát kapja maga az információs rendszer.

(3) Az informatikai vagyon minden elemét be kell sorolni, annak megfelelően, hogy rendelkezésre állásának megszűnése, milyen mértékbe, és hogyan hat az Egyetem egészének funkcionalitására.

(4) A nyilvántartott informatikai rendszereket osztályba, az információs rendszerekben érintett szervezeti egységeket biztonsági szintbe kell sorolni.

(5) Gondoskodni szükséges az információk biztonsági osztályba sorolásáról annak érdekében, hogy az Egyetem által kezelt összes információ, adat számára a megfelelő védelem biztosítható legyen. Az információk osztályozása során figyelembe kell venni az alábbiakat:
   - az általuk képviselt érték,

- jogszabályi elvárások,
- érzékenység,
- kritikusság a szervezet számára.

(6) A 41/2015 (VII. 15.) BM rendelet ide vonatkozó kivonatát jelen szabályzat 2. számú melléklete tartalmazza.

(7) Az osztályba sorolást az IBF koordinációja és szakmai iránymutatása alapján az egyes elektronikus információs rendszerek adatgazdái és az üzemeltetéséért felelős szervezeti egység végzi, az erről szóló bevallás benyújtása a hatóság részére az IBF felelőssége és feladata.

IV. 4.4. A biztonsági osztálybesorolás eredményének rögzítése a rendszer nyilvántartásába

(1) A 41/2015. (VII. 15.) BM rendelet utasítása szerint az elektronikus információs rendszerek osztályba és szintbe sorolásának bevallásához szükséges adattáblák:
- „Osztályba sorolás és védelmi intézkedés (OVI)" űrlap
- „Szintbe sorolás és védelmi intézkedés (SZVI)" űrlap

(2) Az elektronikus információs rendszerek besorolásait az Egyetem szoftver adatvagyon nyilvántartásában, változáskezelő módon kell rögzíteni.

(3) Az Egyetem szintbe és osztályba soroló jelentésének hatósági beküldése az IBF feladata és kötelessége.

IV. 4.5. A biztonsági osztályba sorolás felülvizsgálata

(1) A biztonsági osztályba és biztonsági szintbe sorolást legalább háromévenként vagy szükség esetén, soron kívül, dokumentált módon felül kell vizsgálni.

(2) A soron kívüli biztonsági osztályba és szintbe sorolást az elektronikus információs rendszer biztonságát érintő jogszabályban meghatározott változás vagy új elektronikus információs rendszer bevezetése esetén, ill. a szervezet státuszában, szervezetében, ill. az általa kezelt vagy feldolgozott adatok vonatkozásában bekövetkezett változás esetén szükséges elvégezni.

IV.5 Az informatikai rendszerek biztonsági követelményei

IV. 5.1. A biztonsági követelmények elemzése és meghatározása

(1) Egy informatikai rendszer, alkalmazás beszerzését megelőzően, illetve fejlesztés esetén a tervezés lépéseként a beszerzést, illetve tervezést végző szervezeti egység vezetője köteles gondoskodni az Informatikai Biztonsági Központ bevonásáról.

(2) A szervezeti egység vezetőjének írásos megkeresése alapján a biztonsági követelmények meghatározását az Informatikai Biztonsági Központ és személyes adat érintettsége esetén a GDPR Központ végzik. A biztonsággal kapcsolatos követelményeket írásba kell foglalni.

(3) Csak olyan informatikai eszközök szerezhetők be, amelyeket az ISZK információbiztonsági, karbantartási, jogtisztasági és üzemeltetési szempontból bevizsgált és jóváhagyott.

IV. 5.2. Biztonság az alkalmazási rendszerekben

(1) Az Egyetem területén és kezelésében működő alkalmazási rendszerek tervezésére, bevezetésére, üzemeltetésére és ellenőrzésére vonatkozó feladatokat úgy kell elvégezni, hogy a rendszerek védelme a jogszabályi előírásoknak eleget tegyen, valamint a védelem hiányából eredő kockázatokkal legyen arányos.

(2) Az informatikai rendszereket az adatok bizalmasságára, sértetlenségére és rendelkezésre állására vonatkozó elvárásnak megfelelően kell üzemeltetni.

(3) Az adatokra vonatkozóan olyan védelmi eljárásokat kell alkalmazni, amelyek ellenőrizhetővé teszik a feladatvégzést, az illetéktelen cselekedetek felderítését.

(4) Az adatot, információt és egyéb szellemi tulajdont az Egyetem számára jelentkező értékével arányosan kell védeni az illetéktelen betekintéstől, módosítástól, megsemmisítéstől, nyilvánosságra kerüléstől. A védelemnek biztosítania kell az informatikai rendszer megbízható üzemét fenyegető káresemények elhárítását, hatásuk minimalizálását.

(5) Az alkalmazási rendszer biztonsági követelményei:
   a) ellenőrzött (többfaktoros) beléptetés
   b) inaktivitási kényszerített kiléptetés (képernyőzár),
   c) tevékenység naplózás
   d) többszintű jogosultság kezelés
   e) kényszerített jelszóváltoztatás
   f) jelszó megfelelés ellenőrzés
   g) erőforrás hozzáférés védelem

IV. 5.3. A bemeneti adatok ellenőrzése

(1) Az Egyetem tulajdonában, használatában lévő valamennyi informatikai eszközön tárolt adathoz, információhoz a hozzáférés csak az Egyetem és a felhasználó közötti jogviszony létrejötte után és a jogosultság ellenőrzését követően lehetséges, megvédve az informatikai rendszerekben tárolt adatok, információk jogosulatlan hozzáférésből adódó bizalmasságának, sértetlenségének és rendelkezésre állásának sérelmétől.

(2) Az elektronikus információs rendszereknek ellenőrizni kell az információ belépési pontok érvényességét (hozzáférési kontroll), az adatok, információk bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése érdekében.

IV. 5.4. Az adatfeldolgozás ellenőrzése

(1) A rendszerekhez és információkhoz kizárólag illetékes személyek (felhasználó, user) férhetnek hozzá.

(2) A kritérium betartása, betartatása az adatfeldolgozó felelőssége az Adatkezelő irányításával, felügyeletével.

(3) Az adatfeldolgozó megfelelő biztonsági intézkedéseket köteles alkalmazni az adatok, információk illetéktelen vagy jogellenes feldolgozásából, elvesztéséből, megsemmisüléséből, sérüléséből, megváltoztatásából vagy nyilvánosságra kerüléséből származó esetleges károk megelőzése érdekében.

(4) Ennek érdekében az adatkezeléshez kapcsolódó feladatok részét kell képeznie:
   a) a feldolgozást kezdeményező felhasználó (ide értve a technikai felhasználói is), adathozzáférési jogosultságának ellenőrzése;
   b) a felhasználói időfaktoros eseménynaplózása;
   c) a rendszer működési, hozzáférési logolása.

IV. 5.4.1. A sértetlenség biztosítása

(1) Az elektronikus információbiztonság az elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint a rendszer elemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítását jelenti.

(2) A védelem alapvető tárgya az adat, de az adatot kezelő rendszer elemeit is védeni kell, hiszen annak megfelelő állapota feltétele az adat védelmének.

(3) Az Egyetem maga üzemelteti az elektronikus információs rendszerit, ezért írásba foglalja és kihirdeti a „*Rendszer és információsértetlenségre*" vonatkozó eljárásrendjét és ellenőrzések megvalósítását segítő folyamatokat, azokat meghatározott időközönként frissíti.

IV. 5.4.2. Vezérlő és ellenőrző eljárások

(1) Az adatok, információk bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása érdekében az azokhoz való hozzáférést csak felhasználói hozzáférés kontrollja alatt lehet engedélyezni.

(2) Az elektronikus információs rendszerekben történő adat elérése a hozzáférésvezérlő mátrix-ból (felhasználói jogosultság cross reference tábla) kinyert jogosultság szerint engedélyezhető, a felhasználói azonosító és a valid jelszó autentikációt követően.

IV. 5.5. Az üzenetek hitelesítése, védelme

(1) Az elektronikus üzenetekben foglalt adatokat, információkat:
   a) védeni kell a jogosulatlan hozzáféréstől, módosítástól;
   b) biztosítani kell a célba juttatásukat;
   c) biztosítani kell a megbízhatóságukat elektronikus aláírások használatával.

IV. 5.6. A kimenő adatok ellenőrzése

(1) Az elektronikus információs rendszer adatfeldolgozás rendszerében ellenőrizni kell a kimenő adatokat.

(2) A kimenő adatok biztonsága érdekében, a következő védelmi eljárásokat kell alkalmazni:
   a) integritás ellenőrzése;
   b) adattartalom meglétének értékének ellenőrzése;
   c) megfelelő minősítés meglétének ellenőrzése (nem publikus adat, ne jelenjen meg publikus helyen);
   d) a kimenő adatok értékelésében és ellenőrzésében részvevők feladatainak és felelősségeinek meghatározása.

IV.6 Rendszer és Szolgáltatás beszerzés eljárásrendje (3.1.3.1. [3])

(1) Egy informatikai rendszer, alkalmazás beszerzését megelőzően, illetve fejlesztés esetén a tervezés lépéseként a beszerzést, illetve tervezést végző szervezeti egység vezetője köteles gondoskodni az Informatikai Biztonsági Központ bevonásáról.

(2) A szervezeti egység vezetőjének írásos megkeresése alapján a biztonsági követelmények meghatározását az Informatikai Biztonsági Központ és személyes adatok érintettsége estén a GDPR Központ végzik. A biztonsággal kapcsolatos követelményeket írásba kell foglalni.

(3) Csak olyan informatikai eszközök szerezhetők be, amelyeket az ISZK információbiztonsági, karbantartási, jogtisztasági és üzemeltetési szempontból bevizsgált és jóváhagyott.

(4) Az Egyetem beszerzéssel foglakozó szervezetének felelőssége:
   - a beszerzendő IT eszközök (hardver és szoftver) beszerzés előtti véleményeztetése az Informatikai Szolgáltató Központtal informatikai és információbiztonsági szempontból,
   - IT eszközök (hardver, szoftver, licencköteles termékek), informatikai szolgáltatások beszerzése csak az Informatikai Szolgáltató Központ jóváhagyását követően történhet.
   - A beszerzett IT eszközök csak az Informatikai Szolgáltató Központ tudtával kerülhetnek átadásra, kihelyezésre mivel az eszközök telepítése (Operációs rendszer, Active Directory, vírusvédelmi rendszer,…) esetében az informatikai biztonsági szabályok betartásához szükséges szakmai kompetenciával a szervezeti egység munkatársai rendelkeznek.

IV. 6.1. Erőforrás igény felmérés (3.1.3.2. [3])

(1) Az Egyetem elektronikus információs rendszereinek beszerzésére előzetes, hatékony és biztonságos üzemeltetésére folyamatos erőforrás igény felmérést kell végezni. Az erőforrás igénynek ki kell terjedni az Egyetemen üzemelő központi erőforrásokra és alkalmazásokra, a hálózatra, a munkaállomásokra, valamint ezek fizikai és személyi környezetére.

(2) Az erőforrás igény felmérés szereplői:
- működtető informatika
- kiszervezett IT szolgáltatás esetén szolgáltató
- információbiztonsági terület szervezete
- beszerzési terület szervezete

IV. 6.2. Szerződéses körülmények meghatározása a beszerzés során (3.1.3.3.2. [4])

(1) Információbiztonság szempontjából érintett beszerzések:
- **Hardver:** Hardver infrastruktúra beszerzése során, amennyiben a hardver gyártói szoftvert használnak a működéséhez, a szerződésben deklarálni kell az adat, információ védelmére irányuló Egyetemi elvárásokat. Amennyiben a szállítónak a szoftverhez távfelügyeletet is kell biztosítani, titoktartási nyilatkozatokat is kell tennie
- **Szoftver:** szoftver rendszer beszerzés során külön elvárásokat kell megfogalmazni az Egyetem saját infrastruktúrájára telepített rendszer és külön felhőbe telepített szoftver szolgáltatás esetén.
- **Szolgáltatás:** Az Informatikai Biztonsági Központ (GDPR Központ bevonásával) által meghatározott biztonsági követelmények szerződésekbe, megállapodásokba történő befoglalása a szerződés vagy megállapodás jogi ellenjegyzőjének - vagy mintaszerződés alkalmazása esetén a mintaszerződés kidolgozójának - a feladata, felelőssége. A megfelelő kontroll érdekében az érintett szerződésekben ellenjegyzőként az információbiztonság megteremtésének felülvizsgálata és elfogadása miatt az Informatikai Biztonsági Központ vezetőjét (mint Egyetemi IBF) is fel kell tüntetni

(2) Felelősök:

a) Informatikai Biztonsági Központ központvezető, Adatvédelmi Tisztviselő

- A szerződésekben szerepeltetendő általános információbiztonsági rendelkezések kidolgozása az GDPR központ vezetővel és szükség szerinti aktualizálása.

b) Jogi Igazgatóság

- A szerződésekben szerepelendő általános titoktartási rendelkezések kidolgozása és szükség szerinti aktualizálása
- Titoktartással és információbiztonsággal kapcsolatos szerződéses rendelkezések beillesztése a releváns vállalkozási és szolgáltatási szerződésekbe,
- A vállalkozási és szolgáltatási szerződésekhez kapcsolódó titoktartási és információbiztonsági nyilatkozatok aláíratása.

IV. 6.3. A rendszerre vonatkozó dokumentáció

IV. 6.3.1. A védelmi intézkedések terv-, és megvalósítási dokumentációi (3.1.3.3.3. [4])

(1) A **védelmi intézkedési terv** fő fejezetei

a) Adminisztratív védelmi intézkedések
b) Fizikai védelmi intézkedések
c) Logikai védelmi intézkedések

(2) A **megvalósítás dokumentációi**

a) Adathordozók védelmére vonatkozó eljárásrend
b) Azonosítási és hitelesítési eljárásrend
c) Biztonságelemzési eljárásrend
d) Biztonságértékelési eljárásrend
e) Biztonsági eseménykezelési eljárásrend
f) Biztonságos fejlesztési követelmények eljárásrend
g) Biztonságtervezési eljárásrend
h) Engedélyezési és jogosultságkezelési eljárásrend
i) Fizikai védelmi intézkedések eljárásrendje
j) Hozzáférés ellenőrzési eljárásrend
k) Információbiztonsági kockázatok kezelésének eljárásrendje
l) Informatikai beszerzési eljárásrend
m) Internet használati eljárásrend
n) Katasztrófa elhárítási eljárásrend
o) Kockázatelemzési és kockázatkezelési eljárásrend
p) Konfigurációkezelési eljárásrend
q) Kriptográfiai eljárásrend
r) Mentési és archiválási eljárásrend
s) Mobil eszközök használatának eljárásrend
t) Naplózási és naplóelemzési eljárásrend
u) Rendszer- és információsértetlenségre vonatkozó eljárásrend
v) Rendszer- és kommunikációvédelmi eljárásrend
w) Rendszer karbantartási eljárásrend
x) Személybiztonsági eljárásrend
y) Távoli hozzáférés engedélyezési, használati eljárásrend
z) Tesztelési, felügyeleti és képzési eljárásrend
aa) Üzletmenet-folytonosságra vonatkozó eljárásrend
bb) Vírusvédelmi eljárásrend

IV. 6.3.2. Biztonságtervezési elvek (3.1.3.5. [4])

(1) Az Egyetemnek biztonságtervezési elveket kell kidolgozni a bevezetendő elektronikus információs rendszereihez.

(2) A hatékony és biztonságos üzemeltetéshez ezeket az elveket előzetesen meg kell határozni, ahhoz hogy a megoldást szállító - belső vagy külső szolgáltató - azokat a tervezés (korai fázisában) során be tudja építeni a fejlesztési menetbe.

(3) Az alábbi biztonságtervezési technikák kiválasztását a célfeladat határozza meg:
   a) Minimise (a lehető legkevesebb, de elégséges adat gyűjtése);
   b) Hide (az adat és kapcsolatainak elrejtése);
   c) Separate (az adat elosztott módon, külön tárolóegységen tárolva);
   d) Aggregate (az adat a legmagasabb aggregálási szinten van kezelve, amelynek részletei elégségesek a feldolgozáshoz);
   e) Inform (transzperancia elv, avagy az érintettek tájékoztatása);
   f) Control (az érintetteknek kontroll lehetőséget kell biztosítani);
   g) Enforce (követni kell a jogi követelmények érvényesülésének elvét);
   h) Demonstrate (bizonyítható irányelvi és jogszabályi teljesülés).

(4) A biztonságtervezési elveknek tartalmaznia kell az alábbiakat:
   a) a kommunikáció formája,
   b) titkosítás,
   c) tárolók biztonsága,
   d) adatbázisok biztonsága,
   e) felhasználó kezelés,
   f) működési védelmek (inaktivitás kezelés),
   g) lekérdezési információk kezelése,
   h) maradványinformációk védelme,
   i) a kommunikáció formája,
   j) titkosítás.

IV. 6.3.3. Külső elektronikus információs rendszerek szolgáltatásai (3.1.3.6. [2])

(1) Annak érdekében, hogy a külső elektronikus információs rendszerek szolgáltatásai biztonságosan működjenek, az Egyetem megköveteli és a szállítóval kötött szerződésben határozza meg, hogy a nyújtott szolgáltatás megfeleljen a szervezet elektronikus információbiztonsági (IBSZ) követelményeinek.

(2) A külső szolgáltatást használó felhasználók kötelezettségeit külön dokumentumban szükséges rögzíteni, ahol rögzítésre kerül hogy milyen szerepkörű munkavállalók kapnak jogosultságot a használatra, és mi a velük szemben elvárt biztonsági szabály (jelszavak tárolása, kötelező időszaki cseréje).

IV. 6.4. Független értékelők (3.1.3.7. [4])

(1) Az Egyetem elektronikus információs rendszereit érintő védelmi intézkedéseinek folyamatos ellenőrzésére, független véleményt megfogalmazó külső értékelőket vagy értékelő csoportokat alkalmazhat.

IV. 6.4.1. Folyamatos ellenőrzés (3.1.3.8. [3])

(1) A védelmi intézkedések egyes területei folyamatos ellenőrzésre szorulnak, ennek érdekében az Egyetemnek meg kell határoznia, hogy mely területeket milyen gyakorisággal és milyen értékeléssel szükséges ellenőrizni.

IV. 6.4.2. Folyamatos független értékelés (3.1.3.8.2. [4])

(1) A védelmi intézkedések folyamatos ellenőrzésére felkért harmadik fél részéről várható el elfogulatlan és független véleménynyilvánítás.

IV. 6.5. Külső információs rendszerek szolgáltatásai (3.2.3.6 [2])

(1) Külső információs rendszereknek minősülnek az olyan információs rendszerek vagy azok egyes alkotóelemei, amelyek az Egyetemen kívül állnak, így az Egyetemnek nincs közvetlen felügyelete és felhatalmazása a szükséges biztonsági kontrollok ellenőrzésére.

(2) Külső elektronikus információ rendszerek a személyes tulajdonban lévő mobiltelefonok, laptopok, magántulajdonban lévő kommunikációs eszközök, továbbá azok a rendszerek, amelyek az Egyetem adatainak feldolgozását, tárolását, továbbítását végzik, úgymint felhőszolgáltató alkalmazás.

(3) A felhőszolgáltatással kapcsolatos - Egyetem érdekében elvárt - biztonsági elvárások és a használatra vonatkozó irányelvek az IBSZ-ben kerülnek rögzítésre.

IV. 6.6. A beszerzések folyamatos ellenőrzése (3.1.3.8.1. [3])

(1) Az Egyetem elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben meghatározza a biztonsággal kapcsolatban elvárt követelményeit, amelyek a következők:
   a) Funkcionális biztonsági követelmény
   b) Garanciális biztonsági követelmény
   c) Biztonsággal kapcsolatos dokumentáció követelmény
   d) Biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelmények
   e) Elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó elvárások
   f) Alkalmazandó védelmi intézkedések funkcionális tulajdonságok leírása

IV. 6.6.1. Ellenőrzési terv készítése

(1) A rendszeres ellenőrzést be kell építeni a folyamatokba, és annak kivitelezéséhez tervet kell készíteni, ami magába foglalja az alábbiakat:
   a) az ellenőrzés alá vont területeket;
   b) ellenőrzés gyakoriságát;
   c) folyamatos biztonsági értékelést;
   d) mérőszámok megfelelőségét;
   e) biztonsággal kapcsolatos adatok összehasonlító elemzését;
   f) a szervezet reagálását a biztonsággal kapcsolatos adatok elemzésének eredményére;

g) meghatározza, hogy milyen gyakran kell az érintett szereplőkkel megismertetni az elemzési adatokat.

IV. 6.6.2. A védelem szempontjainak érvényesítése a beszerzés során (3.1.3.3.2. [4])

(1) Az Egyetem védi az elektronikus információs rendszereit, rendszerelemeit vagy rendszerszolgáltatásait a beszerzés, vagy a beszerzett eszköz beillesztéséből adódó kockázatok ellen.

(2) Az Egyetem szerződéses követelményként határozza meg a fejlesztő, szállító számára, hogy dolgozza ki és bocsássa rendelkezésére a rendszerében alkalmazandó védelmi intézkedések funkcionális tulajdonságainak leírását:
   a) szerver használat
   b) adatbázis hozzáférés
   c) tevékenység naplózás (időbélyeggel)
   d) logolás
   e) hozzáférés kezelés
   f) felhasználó kezelés
   g) bizalmas információ kezelés
   h) kényszerített felhasználói biztonsági intézkedések (erős jelszó, kötelező jelszóváltás, inaktivitás kezelés)
   i) maradványinformációk
   j) erőforrás kezelés (adat tárolók, nyomtatók)

IV. 6.6.3. Elvárt dokumentáció

(1) A fejlesztő, szállító bocsássa rendelkezésére az alkalmazandó védelmi intézkedések terv- és megvalósítási dokumentációit, köztük a biztonsággal kapcsolatos külső rendszer interfészek leírását, a magas és alacsony szintű biztonsági tervet, - ha azzal a szállító rendelkezik - a forráskódot és futtatókörnyezetet.

IV. 6.6.4. Az ellenőrzés végrehajtása

(1) Az Egyetem külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

IV. 6.6.5. Az ellenőrzés eredményének értékelése

(1) Az értékelések és az ellenőrzések által generált biztonsággal kapcsolatos adatok összehasonlító elemzése.

IV. 6.6.6. Reagálás az ellenőrzés eredményének értékelésére

(1) A biztonsággal kapcsolatos adatok elemzésének eredményét egyeztetni kell a fejlesztővel, szállítóval.

(2) Amennyiben eltérés, nem megfelelés mutatkozik az Egyetemi biztonsági előírásoktól, elvárástól úgy annak hiánypótlását kell írásban kezdeményezni.

IV.7 Üzletmenet (Ügymenet) folytonosság tervezés (3.1.4. [2], 3.1.4.2. [2])

(1) Az üzletmenet-folytonossági (Business Continuity Plan – BCP) tervezés feladata olyan cselekvési terv meghatározása, ami biztosítja az Egyetem üzleti funkcióinak fenntartását, visszaállítását azok megzavarásakor.

(2) Az üzletmenet folytonossági tervezés az alábbi területekre tér ki:

a) a biztosítandó szolgáltatások és funkciók, illetve a hozzájuk kapcsolódó vészhelyzeti követelmények,
b) helyreállítási feladatok és prioritások,
c) vészhelyzet szerepkörök, felelősségek, kapcsolattartók,
d) a szervezet alapszolgáltatásainak fenntartása,
e) helyreállítási terv.

IV. 7.1. A folyamatos működésre felkészítő képzés (3.1.4.3. [3])

(1) Az elektronikus információs rendszer folyamatos működésére felkészítő képzést kell tartani a felhasználóknak az alábbiak szerint:

a) szerepkörüknek és felelősségüknek megfelelően;
b) a felelősségbe kerülésüket követő meghatározott időn belül;
c) meghatározott gyakorisággal;
d) vagy amikor az elektronikus információs rendszer változásai ezt szükségessé teszik.

IV. 7.2. Az üzletmenet-folytonossági terv tesztelése (3.1.4.4. [4])

(1) Annak érdekében, hogy az üzletmenet folytonossági terv valóban megvalósítható legyen, tesztelni szükséges meghatározott gyakorisággal.

(2) A tesztet évente érdemes elvégezni, hogy kiderüljön mely pontjai nem megfelelőek. A tesztelés során a következő pontokra szükséges figyelni:
- az üzletmenet folytonossági terv megállja-e a helyét, szükség van-e módosításra;
- volt-e az érintettek körében változás: személyi, felelősségi, feladatköri;
- korábbi esetleges valós incidens során miket tapasztaltunk;
- audit során milyen megállapítások, jobbító javaslatok érkeztek.

(3) Amennyiben a teszt eredményei nem megfelelőek, akkor a terven hangolni, javítani kell.

IV. 7.3. Tartalék feldolgozási helyszín (3.1.4.6. [4])

(1) Ki kell jelölni egy tartalék feldolgozási helyszínt azért, hogy ha az elsődleges feldolgozási képesség nem áll rendelkezésére, az elektronikus információs rendszer előre meghatározott műveleteit, előre meghatározott időn belül a tartalék helyszínen újra lehessen kezdeni, vagy folytatni.

(2) A tartalék feldolgozási helyszínt és az ott kialakított infrastruktúrát egy harmadik fél is szolgáltathatja. Ebben az esetben a tartalék feldolgozási helyszínnel szembeni elvárásokat szerződésben szükséges rögzíteni.

(3) Az Egyetemnek úgy kell felkészíteni a tartalék feldolgozási helyszínt, hogy az meghatározott időn belül készen álljon az alapfunkciók működésének támogatására.

IV. 7.4. Infokommunikációs szolgáltatások

(1) Az Egyetemnek tartalék infokommunikációs szolgáltatásokat kell létesítenie. Erre vonatkozóan olyan megállapodásokat kell kötnie, amelyek lehetővé teszik az elektronikus információs rendszer alapfunkciói, vagy meghatározott műveletek számára azok meghatározott időtartamon belüli újrakezdését, ha az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszínen.

IV.7.4.1 Tartalék Infokommunikációs szolgáltatások (3.1.4.7. [4], 3.1.4.7.3. [4])

(1) Olyan tartalék infokommunikációs szolgáltatást kell igénybe venni, ami csökkenti az elsődlegessel közös hibalehetőségek valószínűségét.

IV.7.4.2 Szolgáltatások prioritása (3.1.4.7.2. [4])

(1) A tartalék feldolgozási helyszínen olyan intézkedéseket kell bevezetni, amik támogatják a kialakított szolgáltatás-prioritási rendelkezéseket.

IV. 7.5. Az elektronikus információs rendszer mentései (3.1.4.8. [3])

(1) Az információ és az információ-feldolgozó eszközök sértetlenségének és rendelkezésre állásának biztosítása érdekében gondoskodni kell azok - biztonsági besorolásukkal arányos, ennek hiányában, az IT területek vezetői által meghatározott - rendszeres szakszerű mentéséről.

(2) Az elektronikus információs rendszerek adatgazdáival egyeztetve meg kell állapodni és írásban rögzíteni a mentések megőrzésére, valamint a visszaállításra vállalt helyreállítási időket (RTO) és a legkorábbi visszaállítási pontokat (RPO). Az üzleti területek által definiált időket az adatok biztonsági besorolásával arányban kell meghatározni.

(3) Gondoskodni kell az elkészült mentéseknek a mentett adat előfordulásától távoli helyszínen történő (diszlokáció) szakszerű tárolásáról (környezeti feltételek, bejutás, tevékenység regisztrálás, adathordozók struktúrálása, stb.).

(4) A központilag tárolt adatok mentési és archiválási eljárásainak rendjét (erőforrás, ütemezés) felelősségi viszonyait, idejét, módját, módszertanát, (duplikálás, növekményes, teljes, stb.) technológiai részletezéssel (merevlemez, NAS, SAN, szalag) és a mentésbe bevont erőforrások felsorolásával kell részletesen szabályozni, és az abban leírtaknak megfelelően dokumentálni.

(5) Incidens, üzemzavar, upgrade hiba, fizikai meghibásodást követő helyreállíthatóság érdekében mentés szükséges:
   a) a felhasználói szintű információkról;
   b) rendszerszintű információkról;
   c) rendszer dokumentációjáról, beleértve a biztonságra vonatkozókat is.

(6) A mentések biztonsági kontrolljai (hozzáférések, fizikai biztonság stb.) ugyanolyan szintűek kellenek, hogy legyenek, mint az elsődleges adatoké. A mentéseket a helyreállítási időre és helyreállítási pontokra figyelembe véve kell elvégezni. A mentéseknek meg kell védenie a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását az elsődleges és a másodlagos tárolási helyszínen is.

IV.7.5.1 Mentési eszközök

(1) Adattárolási modellek:
   a) Merev lemez
   b) Storage szerver
   c) Mágnesszalag
   d) Optikai tárolás
   e) Szilárd állapotú tárolás
   f) Felhő szolgáltatás

IV.7.5.2 A mentett adatok tárolása

(1) Az adatok mentése az Egyetem belső hálózatán, külső szolgáltató infrastruktúráján vagy felhő tárhelyen történhet.

(2) Felhő, vagy külső szolgáltató tárhelyén történő mentési infrastruktúra biztonsági kontrolljára, annak ellenőrzésére az Egyetemnek nincs közvetlen felügyelete és felhatalmazása, így ennek érvényesítése részletes biztonsági elvárást deklaráló szerződés keretében történik.

IV.7.5.3 Biztonsági tárolási helyszín (3.1.4.5. [4])

(1) A biztonsági tárolási helyszínt úgy kell kialakítani, hogy az elősegítse a helyreállítási tevékenységeket, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

(2) A biztonsági tárolási helyszínen a mentett adatoknak mindig rendelkezésre kell állnia, ahhoz hogy az Egyetem üzletmenet folytonossága a legkisebb mértékű kárértékkel helyre tudjon állni.

(3) Az első példányt abban a helyiségben kell tárolni, ahol a mentés történik, és abban a létesítményben, ahol a mentés visszatöltése elvégezhető. A második példányt (redundáns) az adott rendszer tartalék központjában, annak hiányában az Egyetem erre kijelölt, az első példány tárolási helyétől eltérő földrajzi távolságban lévő helyiségében (disz lokáció).

IV.7.5.4 Visszatöltési eljárások

(1) A visszatöltési eljárások, a mentések visszatöltését, a visszatöltés megfelelőségének ellenőrzését végzik.

IV.7.5.5 Mentési feladatok

1. Biztonsági (nem archiválás) mentés:
   a) a felhasználói szintű információkról,
   b) rendszerszintű információkról,
   c) rendszer dokumentációjáról, beleértve a biztonságra vonatkozókat is;
2. Mentési folyamat naplózása;
3. Hibás mentésről elektronikus értesítés küldése az illetékes rendszergazdának.

IV.7.5.6 Mentési naplók

(1) A mentési folyamat napló állományának/állományainak létrehozása a mentési job aktiválási helyszínén, tárolása a redundáns naplószerveren történik.

(2) A naplószerveren úgy kerül tárolásra, hogy az:
   a) sérülésmentes
   b) egyértelmű leíró névvel ellátott (pl. létrehozás dátuma, ideje)
   c) letárolását követően nem módosul
   d) illetéktelenek nem férnek hozzá
   e) hozzáférésük logolva van

(3) A naplóállományok törlési idejét, kezelését részletesen a „Naplózási és naplóelemzési eljárásrend" tartalmazza.

IV.7.5.7 Megbízhatósági és sértetlenségi teszt (3.1.4.8.2. [4])

(1) Az adathordozók megbízhatóságának és az információk sértetlenségének garantálása érdekében meghatározott gyakorisággal tesztelni kell a mentett információkat.

(2) Az Egyetem meghatározott időközönként helyreállítási tesztet végez, ahol:
   a) tervezetten, körültekintően eljárva teszteli, hogy a mentett adatokat vissza tudja-e állítani, azok nem sérültek-e, nincs-e váratlan technikai probléma;
   b) a tesztet dokumentálja, jegyzőkönyvezi.

IV. 7.6. Minősített adatok, elektronikus dokumentumok tárolása

(1) Amennyiben az Egyetem „minősített adat" besorolás alá eső adatot kezel, úgy a minősített adat védelméről szóló 2009. évi CLV. törvény és a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III.26.) Korm. rendelet szerinti követelményeket kell betartania és érvényesíteni az IBF közreműködésével.

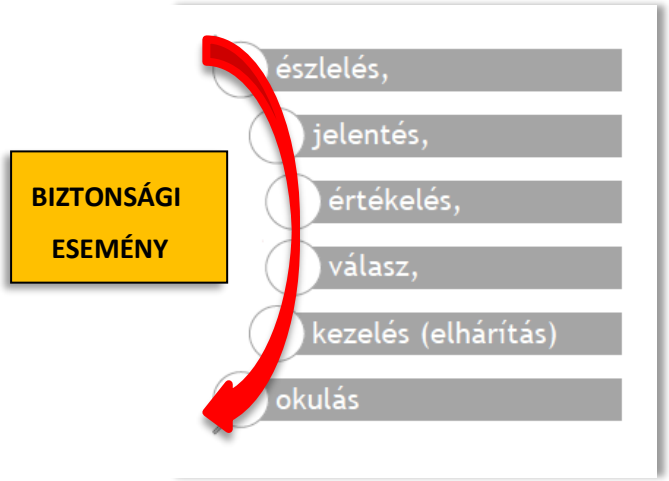
IV.8 Biztonsági események figyelése és kezelése (3.1.5.)

(1) Az információbiztonság a megelőzés, korai figyelmeztetés, észlelés, reagálás és a biztonsági események kezelése feladatainak folyamatosan végzendő tevékenységein keresztül valósul meg.

(2) A biztonsági események, olyan nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat bekövetkeztének azonnali észlelése, amely az elektronikus információs rendszerben kedvezőtlen változást vagy ismeretlen helyzetet idéz elő, aminek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.

(3) Biztonsági eseménynek kell tekinteni minden olyan eseményt, amely ténylegesen kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára.

IV. 8.1. Biztonsági események figyelése (3.1.5.4. [3], 3.1.7.1. [3])



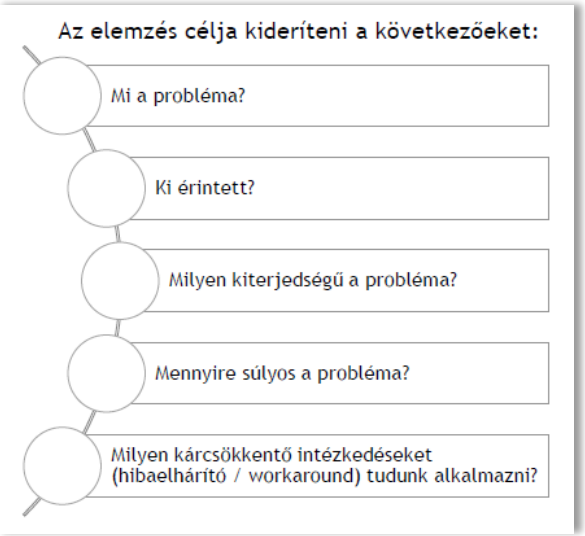
(1) Az Egyetem nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági eseményeit.

(2) Az események nyomon követése, elemzése a informatikai infrastruktúra elemek működésének, használatának tevékenység naplózása által történik.

(3) Az egyetem a naplózás átfogó, központosított és hatékony feldolgozás támogatására **SIEM (Security Incident and Event Management)** rendszert használ, ami biztonsági incidensek, események azonosítását, megfigyelését, rögzítését támogatja.

(4) Minden biztonsági eseményhez köthető naplózási bejegyzést automatikus információbiztonsági elemzésre kell továbbítani a kockázatmenedzsmenti keretrendszerbe.

IV. 8.2. Biztonsági események priorizálása, reagálás a biztonsági eseményekre



(1) A biztonsági események prioritás besorolása az Egyetem üzletmenet folytonosságának sérülékenysége alapján történik. A kockázat mértéke határozza meg a cselekvési tervet. Az esemény besorolás;

a) nem incidens (nem igényel cselekvést, de elemezni kell);

b) incidens (azonnali intézkedést igényel);
c) katasztrófa (azonnali intézkedést igényel);

(2) Amennyiben a kiesett erőforrás visszaállítási ideje meghaladja az általa támogatott folyamat, szolgáltatás maximálisan megengedhető kiesési idejét, úgy az állapot vészhelyzetnek kell minősíteni. A besorolás szerinti cselekvés lépései:
a) vezetők értesítése
b) havaria team felállítása
c) külső partner értesítése (ha érintett és indokolt)
d) információ, adatgyűjtés az elhárítási feladathoz
e) elhárítási tevékenység megkezdése

IV. 8.3. A biztonsági események kezelése (3.1.5)

(1) Az Egyetemnek biztonsági eseményekre vonatkozó eseménykezelési eljárást kell definiálnia, annak érdekében, hogyha bekövetkezik, akkor egységesen és hatékonyan lehessen kezelni. Az eljárásrendnek összhangban kell lennie az üzletmenet folytonossági tervvel. Az eseménykezelési tevékenységből levont tanulságokat be kell építenie az eljárásaiba.

(2) A biztonsági események kezelésére az Egyetem „Biztonságkezelési eseménykezelési eljárásrend”-jének tartalmi követelményei alapján kerül sor. Az eseménykezelési eljárásrend leírja:
a) előkészületek lépéseit
b) események észlelésének folyamatát, lépéseit
c) események kategorizálását/besorolását
d) esemény kivizsgálásának folyamatát
e) esemény elszigetelésének folyamatát
f) esemény megszüntetésének lépései
g) helyreállítás lépéseit
h) felelősségi köröket (pl. RACI mátrix segítségével)
i) hatóságokkal való kapcsolattartásra, bejelentési kötelezettségekre (pl. NAIH)
j) tanulságok levonásának folyamatára

IV.8.3.1 Általános alapelvek

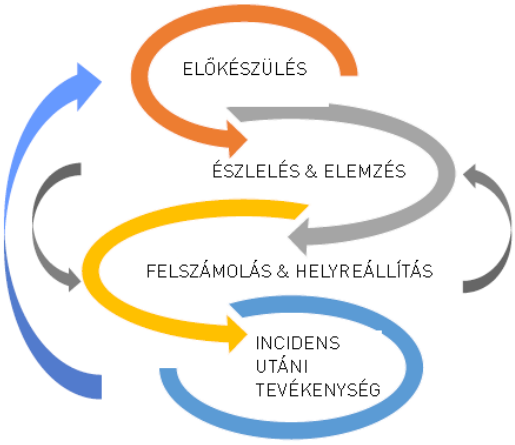
(1) Információbiztonsági eseménynek tekintendő minden olyan tevékenység, illetve esemény, amely az Egyetem által kezelt, tárolt vagy továbbított információk biztonságát (bizalmasságát, sértetlenségét és/vagy rendelkezésre állását), illetve az Egyetem informatikai rendszereinek funkcionális integritását vagy rendelkezésre állását veszélyeztetve kárt okoz, vagy annak veszélyét idézi elő. Ide értendő különösen:

a) a hardver- és szoftverkonfiguráció illetéktelen megváltoztatása;
b) a jogosulatlan hardver- és szoftvertelepítés és használat;
c) a hardvereszköz jogosulatlan megbontása,
d) az Egyetem informatikai rendszerének jogosulatlan használata, a hozzáférési rendszer kijátszása;
e) a saját jogosultsággal való visszaélés;
f) más személy felhasználói azonosítójának használata;
g) a telepített szoftver biztonsági beállításainak engedély nélküli, önkényes megváltoztatása;
h) az adatok jogosulatlan törlése, módosítása;
i) károkozó számítógépes program létrehozása, telepítése, tárolása, terjesztése, futtatása;
j) kalóz, hackelt szoftvertermék telepítése lokális vagy hordozható (hazavihető) eszközre;
k) üzenet meghamisítása;
l) adatátviteli csatorna engedély nélküli lehallgatása;
m) jogosulatlan erőforrás-használat, erőforrások túlterhelése;
n) a hálózati eszközök működésének engedély nélküli befolyásolása, módosítása;
o) az informatikai biztonsági kontrollok kijátszása, a hálózati határvédelmi rendszer megkerülése;
p) az informatikai biztonság veszélyeztetésére alkalmas felhívást, közlést hordozó üzenetek terjesztése;
q) vírusfertőzés;
r) bizalmas adatot tároló adathordozó elveszítése, eltűnése.

(2) Információbiztonsági esemény kezelésekor az „Katasztrófa elhárítási eljárásrend” alapján kell eljárni.

(3) Abban az esetben, ha az incidens érintett személyes adatokat is, minden esetben értesíteni kell az Egyetem Adatvédelmi tisztviselőjét, és az incidens kezelését és kivizsgálását közösen kell végrehajtani.

IV.8.3.2 Az incidenskezelés folyamata (3.1.5.1 [3])



Ciklikus végrehajtás

(1) Az incidenskezelés célja a normál szolgáltatási körülmény visszaállítása a legminimálisabb időintervallumon belül, minimalizálva az üzleti tevékenységre gyakorolt káros hatását. Az incidenskezelési folyamat szakaszai:

a) Tervezés és előkészítés
b) Észlelés és jelentés
c) Vizsgálat és döntés
d) Válasz az incidensre, elhárítás
e) Elszigetelés és vizsgálat
f) Megszüntetés
g) Helyreállítás
h) Incidens elhárítás utáni feladatok

IV. 8.4. Képzés a biztonsági események kezelésére (3.1.5.9. [3])

(1) Az Egyetem az elektronikus információs rendszerei felhasználóinak biztonsági eseménykezelési oktatást tart szerepkörüknek megfelelően.

(2) Minden, az Egyetem által kezelt információhoz hozzáférő munkatársat, az egyetem hallgatóit, illetve az Egyetemmel szerződésben álló külső partnerek egyetemi informatikai rendszerekhez hozzáférő alkalmazottjait évenkénti ismétlődési gyakorisággal, dokumentáltan megfelelő általános, valamint szükség szerint a munkavégzési területükhöz kapcsolódó specifikus információbiztonsági (biztonságtudatossági) tájékoztatásban kell részesíteni, amely tartalmazza a jelen szabályzat rájuk vonatkozó előírásainak ismertetését is.

(3) Az oktatás megszervezése és dokumentált lebonyolítása az IBF feladata és felelőssége. Az oktatások elektronikus formában, informatikai biztonsági képzési keretrendszer alkalmazásával valósulnak meg, amely a dokumentáltságot is biztosítja.

(4) A biztonság-tudatossági oktatáson túlmenően rendszeres időközönként fel kell hívni a fenti személyek figyelmét a hatályos biztonsági szabályzatokban és eljárásokban bekövetkező változásokra, amely szintén az IBF feladata és felelőssége.

IV. 8.5. A biztonsági események kezelésének tesztelése (3.1.5.9.4. [4])

(1) Az Egyetem meghatározott gyakorisággal teszteli az elektronikus információs rendszerre vonatkozó biztonsági eseménykezelési képességeket, előre kidolgozott tesztek felhasználásával, annak érdekében, hogy meghatározza a biztonsági eseménykezelés hatékonyságát, és dokumentálja az eredményeket.

(2) A biztonsági események kezelésének folyamatát "table-top" jelleggel kell tesztelni, ahol az érintett szereplők összegyűlnek és feltételezett incidens példákon keresztül végig mennek az incidenskezelési lépéseken, azonosítva a feladatokat, azok végrehajtóit, felelőseit.

(3) A biztonsági incidensek során gyűjtött tanulságokat a tesztelésbe kell integrálni.

(4) A szimulációhoz hasonlóan, a tipikusan várható vagy generált incidensekkel történő tesztelés is alkalmas a kidolgozott eljárások végrehajtási hatékonyságágának visszamérésére.

IV. 8.6. Informatikai incidensek nyilvántartásba vétele (segítségnyújtás a biztonsági események kezeléséhez (3.1.5.7. [3])

(1) Az Egyetem tanácsadást és támogatást nyújt az elektronikus információs rendszer felhasználóinak a biztonsági események kezeléséhez és jelentéséhez. Ennek érdekében a belső hálózatból online elérhető dokumentumot tesz közzé, amiben a biztonsági események bejelentésének lépéseit írja le. (Egyetemi honlap) Ez a dokumentum az új belépők képzésébe, illetve a rendszeres IT biztonsági tudatosság oktatási anyagába is beépítésre kerül.

IV. 9. Emberi tényezőket figyelembe vevő – személy – biztonság (3.1.6., 3.3.1.4. [2])

(1) Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed az Egyetem teljes személyi állományára, valamint minden olyan természetes személyre, aki az Egyetem elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet.

(2) Az elektronikus információs rendszerekben kezelt adatokat és információkat, az azokat kezelő dolgozók „Személybiztonsági eljárásrend” szabályai is védik. A Személybiztonsági eljárásrend szabályozza a következőket:

- Titoktartási kötelezettségek, titoktartási nyilatkozatok,
- Szabályzatok, eljárásrendek megismertetésének módja, formája ,
- Szabályozza a belépés és kilépés személybiztonsági vonatkozásait, vagy hivatkozik más szabályzatokra (pl. jogosultság menedzsment, HR szabályzat, stb.)

(3) A „Személybiztonsági eljárásrend” az Egyetem munkavállalóin túl, a szerződéses partnerek esetében is rendelkezik a folyamatokról.

IV. 9.1. Munkakörök, feladatkörök biztonsági alapú besorolása (3.1.6.2. [3])

(1) Az Egyetem minden Egyetemi munkakört, vagy Egyetemhez kapcsolódó feladatot biztonsági szempontból besorol, kiemelten kezelve a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat.

(2) Az Egyetem HR szervezete az IBF-fel közösen a munkaköröket kategóriákba sorolja biztonsági szempontból. A besorolás alapját képezi, hogy az egyes munkakörökhöz milyen ellenőrzés szükséges. Pl.: erkölcsi bizonyítvány meglétének ellenőrzése, nemzetbiztonsági ellenőrzés stb.

(3) A besorolást évente frissíti egyeztetve az egyes osztályokkal, illetve jogi elvárásokkal összhangban. A kategóriák megjelennek a munkaköri leírásokban, amit a munkavállalónak formálisan is (pl. emailes visszajelzés, aláírás) is tudomásul kell vennie.

IV. 9.2. Személyi biztonság a munkaerő felvételnél

(1) Az Egyetem HR szervezete és az IBF által kialakított munkakör biztonsági szempontrendszer figyelembe vétele szükséges a munkakör betöltéséhez, mint;
   a) érvényes erkölcsi bizonyítvány megléte
   b) előző munkahelyek
   c) ajánlólevelek
   d) biztonságtudatossági teszt eredménye

IV. 9.3. Adatvagyon kezelése, hozzáférése

(1) Az Egyetem elektronikus információs rendszereihez a hozzáférés, kezelés:
   a) csak a jogviszony létrejöttét követően létesülhet;
   b) csak a jogviszony fennállása alatt lehetséges;
   c) csak a munkakör betöltéséhez elengedhetetlenül szükséges jogokkal biztosított;
   d) csak a munkavállaló részére kiadott jogosultsággal engedélyezett.

IV. 9.4. Jogosult felhasználók

(1) Az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint:
   a) érhetik el;
   b) ismerhetik meg;
   c) használhatják fel;
   d) kezelhetik (új bevitel, lekérdezés, módosítás, törlés);
   e) rendelkezhetnek annak felhasználásáról.

(2) Az Egyetemen a felhasználók elektronikus információs rendszerekhez rendelt jogosultságai felhasználói jogosultság nyilvántartásban (jogosultsági mátrix) vannak tárolva, ahol követve van a munkavállaló érvényes és feltétlen indokolt jogosultság kiosztása. (pl. egy munkakörváltás más jogosultságot követel meg, munkakör megszűnése, munkaviszony megszűnés).

(3) A nyilvántartás kezelői az IT üzemeltetési szervezetek.

(4) Kiemelt jelentőséggel kell eljárni a rendszergazdák, admin - és kiemelt felhasználók munkaviszonyának megszűnése alkalmával. Ezekben az esetekben a kilépő munkavállaló kezelésében volt területeken, eszközökön, felhasználói szoftverekben, rendszer szoftverekben, adatbázis kezelő rendszerekben, az admin, root, rendszergazdai jelszavakat a kilépés napján azonnal meg kell változtatni, a változtatást dokumentálni, a jelszavakat hivatalosan lezárt borítékban, páncélszekrényben elhelyezni.

IV. 9.5. Informatikai biztonság a munkaköri leírásokban

(1) A munkaköri leírásnak tartalmaznia kell a munkaterületre vonatkozó informatikai biztonsággal kapcsolatos elvárt követelményeket és az egyértelműen megfogalmazott és számon kérhető felelősségeket.

(2) Az információbiztonságot érintő területekkel foglakozó munkatársak (infrastruktúra- és alkalmazás-üzemeltetés) végzendő feladatai a munkaköri leírásában illeszkedjenek az egyes rendszerek technológiai leírásában található tevékenységekhez. Ezek az információbiztonságot érintő területek a következők:
   a) felhasználói jogosultság kezelés;
   b) alkalmazásüzemeltetés;
   c) mentés;
   d) napló és log elemzés;
   e) vírusvédelem;
   f) határvédelem (tűzfal, hálózati eszköz, VPN, DMZ);

(3) A munkaköri leírásnak tartalmaznia kell továbbá, hogy a munkavállaló a foglalkoztatása alatt tudomására jutott nem publikus információkat sem a munkavégzése során, sem munkaviszonyának megszűnését követően harmadik fél tudomására nem hozhatja. Ennek megszegése jogi következményeket von maga után.

(4) Informatikai biztonság szempontjából elengedhetetlen a humánerőforrási, az informatikai üzemeltetési és az információ biztonsági szakterületek folyamatos együttműködése.

IV. 9.6. Személyi biztonság a jogviszony alatt (3.1.6.1. [3])

Az Egyetem „Személybiztonsági eljárásrend” irányelveinek követése.

IV. 9.7. Viselkedési szabályok az interneten (3.1.6.9. [1])

(1) Az Egyetem „Internet használati eljárásrend” című dokumentumában foglalt irányelveinek követése minden munkavállaló számára kötelező.

(2) Az internethasználat főbb elvárásai a következők:
   Az Egyetem:
   a) tiltja és számon kéri a szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét;
   b) tiltja a belső szabályzatában meghatározott, interneten megvalósuló tevékenységet (chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták, privát levelezési fiók munkaköri használata),
   c) elvárja az üzleti partnerek, ügyfelek bizalmasságának megőrzését,
   d) elvárja, hogy a munkavállaló a közösségi médiában tiszteletben tartsa az Egyetem reputációját, megítélését, ne tegyen olyan cselekedetet, ami sértheti azt,
   e) elvárja a szerzői jogokra, licencekre, szabadalmakra és egyéb szellemi tulajdonra vonatkozó szabályok betartását,
   f) csak a munkakörének feladatellátásához feltétlen szükséges képek és videók letöltését engedélyezi,
   g) tiltja szórakoztató és játék alkalmazások használatát.

(3) Az Mt. 6. § (2) bekezdése szerint a jóhiszeműség és tisztesség elve értelmében a munkaviszony alanyai kötelesek tekintettel lenni a másik fél érdekeire, és nem tanúsíthatnak olyan magatartást, amely a másik fél jogát vagy jogos érdekét sérti, valamint kötelesek jogaikkal a másik fél érdekeit figyelembe véve úgy élni, hogy azzal indokolatlanul hátrányt ne okozzanak.

(4) A munkavállaló munkaviszonyból fakadó kötelezettségeit az Mt. 52. § (1) bekezdése sorolja fel, ezek közül jelen szabályozás szempontjából kiemelendő, hogy a munkáját az általában elvárható

szakértelemmel és gondossággal, a munkájára vonatkozó szabályok, előírások, utasítások és szokások szerint kell elvégeznie; valamint a munkavállaló a munkakörének ellátásához szükséges bizalomnak megfelelő magatartást köteles tanúsítani.

IV. 9.8. E-mail használat

(1) Minden munkavállaló egyedi egyetemi elektronikus levelezési cím használatára jogosult, ami részére a jogviszonyának kezdetét követően a bekörözősi ponton kerül megigénylésre.

(2) Az elektronikus levelezés használata során az alábbi szabályoknak kell betartani:
   a) az Egyetem elektronikus levelező rendszere elsődlegesen belső- és külső kommunikációt szolgálja, a belső folyamatok támogatását szolgálja;
   b) az elektronikus levelezés használata során az Egyetem fenntartja a jogot arra, hogy - kizárólag indokolt esetben a munkavállaló előzetes tájékoztatása mellett - betekintsen az elektronikus levelekbe ellenőrzés céljából, továbbá hogy a felhasználók levelezési forgalmát figyelje, naplózza. A betekintés során a munkáltató kizárólag a munkavégzéssel összefüggő levelezések tartalmát ismerheti meg, az esetleges magáncélú levelek tartalmába nem tekinthet be. A postafiókban a magáncélú leveleket elkülönített módon kell tárolnia a munkavállalónak. A felhasználók tudomásul veszik, hogy az általuk küldött és fogadott elektronikus küldeményeket az Egyetem ilyen módon kezeli;
   c) szükség esetén az elektronikus üzenetek bizalmasságának, illetve hitelességének, 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, illetve 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;

(3) Az elektronikus levelezéshez kapcsolódóan tilos:
   a) a hivatalosan támogatott elektronikus levelező szolgáltatáson (szerveren) kívül más elektronikus levelező szolgáltatást hivatalos levelezésre használni;
   b) a hivatalosan támogatott levelező szoftveren kívül más programot használni;
   c) az elektronikus leveleket úgy titkosítani, hogy a visszafejtésre használható kulcs nincs, vagy nem kerülhet az Egyetem birtokába;
   d) az Egyetem hálózatát vagy szervereit nagy terjedelmű vagy nagy mennyiségű levél, illetve kéretlen kereskedelmi üzenetek küldésére használni (ha ilyenre van szükség, akkor azt az Informatikai Szolgáltató Központ bevonásával, más technológia alkalmazásával kell teljesíteni);
   e) a levelezőrendszert reklám célra, pártpolitikai célra, mások munkájának hátráltatására, illetve az internet veszélyeztetésére használni;
   f) az Egyetem hálózatát vagy szervereit kéretlen, nagy mennyiségű, illetve kereskedelmi elektronikus levelekre való válaszok begyűjtésére használni;
   g) feliratkozni nem szakmai jellegű illetve nem az ügyviteli vagy oktatási munkát segítő hírlevél küldő szolgáltatásra;

h) indokolatlanul nagyméretű üzeneteket vagy fájlokat küldeni;
i) láncleveleket vagy hasonló üzeneteket küldeni, illetve ”hólabda” levelezést továbbítani (chain letters, olyan üzenet mely tartalmazza azt, hogy a címzettje azt küldje tovább ismerősöknek);
j) vírusos levelek szándékos küldése;
k) ügyviteli szempontból titkos, bizalmas, illetve belső információk jogosulatlan nyilvánosságra hozatala;
l) válaszolni olyan levelekre, amelyek arra szólítanak fel, hogy az Egyetem biztonsági rendszeréről, vagy a felhasználó saját hozzáférési adatairól (felhasználónév, jelszó) adjon tájékoztatást;
m) az e-mailben csatolt futtatható állományok megnyitása/letöltése a munkaállomásokra;
n) ismeretlen feladótól származó levelekben található csatolmány megnyitása;
o) valótlan információt hordozó levelek tudatos továbbítása;
p) az elküldött levél járulékos adatainak (például feladó e-mail címe, küldés időpontja) meghamisítása;
q) a munkatársak e-mail címeinek másik félhez történő, jogosulatlan továbbítása;
r) az Egyetemi e-mail címről magáncélú regisztrációt végrehajtani. Ennek megfelelően nem engedélyezett az üzleti célú levelezési listákra, fórumokra, hírcsoportokra feliratkozás egyetemi e-mail címmel;
s) privát postafiók tartalom automatikus továbbítás az Egyetemi e-mail címre;
t) az Egyetem elektronikus levelezési címjegyzékének kiadása harmadik fél számára.

IV. 9.9. A felhasználó feladatai a munkahely elhagyásakor (3.1.6.4. [1])

(1) A felhasználó feladata, hogy ha elhagyja, eltávolodik munkahelyétől mindig szabályosan lépjen ki a rendszerből, hogy aktív belépésével visszaélve, arra nem jogosult, nem illetékes illetve megtévesztő (social engineering) személy ne tudjon tevékenykedni.

(2) A felhasználó akkor is felelősségre vonható, ha a szándékosan átadott vagy gondatlanságból nyilvánosságra jutott azonosítójával történik illetéktelen szabálytalan, akár jogszerűtlen használat, visszaélés.

IV. 9.10. Tiszta asztal, tiszta képernyő szabályok a munkavégzés közben

(1) Az információvédelem az íróasztalon kezdődik. A rendezett íróasztal (clear desk) az információvédelem előszobája. A napi munkavégzés során:
a) a monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő függöny használatával)
b) a felhasználó a számítógépét zárolni köteles (a Ctrl +Alt +Del billentyűk, majd a Zárolás gomb lenyomásával), ha azt rövidebb időre őrizetlenül hagyja
c) hosszabb idejű távollét esetén a számítógépből ki kell jelentkezni, illetve ki kell azt kapcsolni (amennyiben lehetősége van, áramot is lekapcsolni – pl. kapcsolható elosztó);
d) a munkafázis végeztével ki kell jelentkezni az alkalmazásokból, majd leállítani a számítógépet;
e) munkavégzés után minden érzékeny információt tartalmazó anyagot (papír alapú anyagokat, valamint elektronikus adathordozókat) el kell tenni az asztalokról, és zárható irodabútorban kell tárolni;

f) gondoskodni kell arról, hogy a nyomtatókból, faxokból, fénymásolóból kijövő dokumentumokhoz illetéktelenek ne férjenek hozzá;
g) érzékeny információt tartalmazó dokumentum ne maradjon a fénymásolóban;
h) illetéktelen személy nem tartózkodhat felügyelet nélkül az irodában;
i) az iroda elhagyásakor az irodaajtót kulccsal kell zárni (tartósabb távollét esetében is);
j) a szemetes kosárban érzékeny adatot tartalmazó piszkozatot sem lehet kidobni, csak iratmegsemmisített változatban.

IV. 9.11. A vezetők felelőssége

(1) Az egyetemi szervezeti egységek vezetőinek felelőssége, hogy az Egyetem információbiztonsági politikáját a munkavállalókkal megismertesse, betartassa, számon kérje, a szabálytalanságokat szankcionálja.

IV. 9.12. Személyi biztonság a jogviszony megszűnésekor, megszüntetésekor, vagy kinevezés módosítása esetén (3.1.6.4. [1]; 3.1.6.5. [3])

(1) A jogviszony megszűnése, megszüntetése a felhasználói hozzáférés jogainak teljes visszavonását követeli meg az Egyetem elektronikus információs rendszereiben.
(2) Kilépő dolgozók esetén, legkésőbb az utolsó munkában töltött napon kötelező - biztonsági szempontból – az alább felsorolt, minden jogosultság megvonása:
    a) LDAP
    b) elektronikus levelezési fiók elérése
    c) használt rendszerek rendszergazdai, felhasználói jogosultságok tiltása
    d) Active Directory jogosultság visszavonása
    e) munkavégzéshez használt eszköz (PC, hordozhatók, telefon) jelszavának megváltoztatása

(3) Használatba adott mobil eszközök (notebook, tablet, telefon) visszavétele, használhatóság ellenőrzése (jelszóvédelem feloldás a kilépő dolgozó részéről, jelszómódosítás az IT üzemeltetés részéről).

(4) Kinevezés módosítása, munkakör megváltozása esetén gondoskodni kell arról, hogy az érintett a változást követően csak azon rendszerekhez és az abban kezelt adatokhoz férhessen hozzá, amelyek megismerésére, kezelésére a változást követően jogosultak.

(5) Az IT üzemeltetési szervezet megadja a hozzáférést az áthelyezés után használandó rendszerhez, illetve a már nem szükséges hozzáféréseket módosítja, elveszi.

(6) A változásokat (hozzáférés törlések, hozzáférés módosítások) át kell vezetni a felhasználói jogosultság kezelő rendszerben.

(7) A jogviszony megszűnés külső szolgáltató esetében történő szerződés felmondás, megszűnés esetére is értendő, így a biztosított hozzáférések kezelésére is az ide vonatkozó irányelvek betartása szükséges.

IV. 9.13. A jogviszony megszűnésének, megszüntetésének biztonsági kérdései (3.1.6.4. [1])

(1) Jogviszony megszűnésekor, a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartásának megelőzése a cél.

IV. 9.14. Az eszközök visszaadása

(1) Jogviszony megszűnésekor a jogviszonyt megszüntető személytől minden rendelkezésére bocsájtott informatikai eszközt vissza kell venni. A visszavétel alapja a leltári személyi karton. Visszavétel tárgyát az alábbiak képezik:
   a) laptop,
   b) notebook,
   c) tablet,
   d) külső merevlemez,
   e) pendrive,
   f) telefon,
   g) belépő kártya,
   h) egyéb személyi azonosítást biztosító eszköz.

(2) Amennyiben home office munkavégzéshez asztali számítógépes környezet is biztosítva lett, a visszavétel tárgyát képezi.

(3) A visszavett eszközökön magán célú adatok nem maradhatnak. Erre a jogviszonyt megszüntető személy figyelmét fel kell hívni, az arról való másolatkészítés, törlés lehetőségét biztosítani. Amennyiben az eszközök jelszavas védelemmel voltak ellátva, amit csak a jogviszonyt megszüntető személy tudott, azt el kell kérni és tesztelni azok megfelelősségét.

(4) A jelszavakat az IT üzemeltetésnek meg kell változtatni, az erről szóló írásos dokumentációt az üzemeltetési vezetőnek át kell adni. A dokumentáció tartalma:
   a) eszköz típusa
   b) eszköz gyári száma
   c) leltári azonosító
   d) új jelszó
   e) jelszó változtatás dátuma
   f) régi tulajdonos neve, beosztása
   g) IT munkatárs neve
   h) dokumentáció átadás dátuma

(5) Kivételt képeznek a fentiek alól azok az esetek, amikor a munkavállaló a korábban rendelkezésére bocsátott valamely eszközt Kancellári engedéllyel saját részre megvásárolja. Ebben az esetben az összes munkavégzésével összefüggő adatot törölni szükséges legkésőbb az utolsó munkában töltött napon, az ISZK munkatársának jelenlétében és közreműködésével.

IV. 9.15. A hozzáférési jogok visszavonása

(1) Jogviszony megszűnésekor, a jogviszonyt megszüntető személy minden elektronikus információs rendszerhez, elektronikus levelezési fiókhoz, helység belépéshez kiadott jogosultságát vissza kell vonni, hatályon kívül kell helyezni. A visszavétel, megszüntetés alapja a felhasználói jogosultság nyilvántartó rendszer.

IV. 9.16. Az informatikai biztonsági oktatás és képzés (3.1.7.)

(1) Információbiztonsági tudatosság növelése érdekében, és ahhoz, hogy az Egyetem munkavállalói naprakész tudással rendelkezzenek a fenyegetésekről, sebezhetőségekről, humán kockázatokról,

biztonsági eseményekről és felkészülhessenek a lehetséges belső fenyegetések felismerésére, folyamatos oktatásban, képzésben kell részesüljenek.

(2) A felhasználók biztonságtudatossági oktatását évente, tudás és ismeret ellenőrzéssel kell végrehajtani.

(3) Az Egyetem elektronikus informatikai rendszer felhasználóinak, az általuk használt informatikai rendszer használata előtt, annak változásakor illetve új információbiztonsági kockázatok megjelenésekor oktatást kell biztosítani.

(4) Az oktatás során átadott biztonsági ismeret betartásának, alkalmazásának hatékonyságát fokozva, az Egyetem olyan informatikai biztonsági képzési és szimulációs keretrendszert alkalmaz, ami szimulált (nem kártékony) támadásokkal méri fel a felhasználók biztonságtudatos viselkedését. Így a rendszer által előállított statisztika, lehetőséget biztosít célzott ismeretanyag terjesztésére, általánosan vagy személyre szabottan.

(5) Az információbiztonsági oktatás megszervezése az Informatikai Biztonsági Központ vezetőjének, a felhasználói szoftverek biztonságtudatos kezelésének oktatása a szoftver üzemeltetéséért felelős szervezet feladata és felelőssége.

IV. 9.17. Belső fenyegetés (3.1.7.4. [4])

(1) Az Egyetem számára jelentős károkat okozhat, ha a munkavállaló véletlenül vagy rossz szándékkal adatokat szivárogtat ki, vagy rosszindulatú támadót enged be az Egyetem rendszereibe. Fontos a belső fenyegetések felismerése, hogy a fenyegetés minél hamarabb felismerhető legyen. Ennek érdekében az informatikai biztonsági tananyag részét kell képeznie a fenyegetések lehetséges eseteinek bemutatása, valamint a jelentési kötelezettség folyamatának leírása.

(2) Az oktatást évente meg kell ismételni, hogy az újonnan megjelenő fenyegetéseket megismerjék a munkavállalók.

(3) Új munkavállalók esetében szükséges a képzés megtartása, ami elmagyarázza a fenyegetés fogalmát, következményeit és tudatosítja a jelentési kötelezettségüket.

IV. 9.18. A biztonsági képzésre vonatkozó dokumentációk (3.1.7.6. [3])

(1) A biztonságtudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzések megtörténtét dokumentálni kell, amely lehet elektronikus és fizikai is.

(2) A képzésen történő részvétel elismerése, a tananyag egészének megtekintése és az ellenőrző kérdések elfogadható mértékű helyes megválaszolását követően elektronikusan történik.

IV. 9.19. Fegyelmi eljárás (3.1.6.7. [1])

(1) Az információ biztonsági szabályok betartása minden munkavállalóra nézve kötelező. Azon munkavállalók esetében, akik a biztonsági szabályokat súlyosan megsértik, a Munka Törvénykönyve által meghatározott, a vétkes kötelezettségszegésre vonatkozó hátrányos jogkövetkezmények alkalmazhatók.

(2) Az Egyetem fegyelmi eljárást kezdeményez az információbiztonsági szabályokat és hozzá kapcsolódó eljárásrendeket megsértő érintettekkel szemben.

IV. 9.20. Külső szervezetre vonatkozó követelmények (3.1.6.6. [3])

(1) Az Egyetem az alábbi személybiztonsági követelményeket fogalmazza meg a külső (szerződéses jogviszonyban álló) szervezetekkel szemben:
   a) a külső szervezettel kötött megállapodásban, szerződésben megköveteli, hogy a külső szervezet határozza meg az érintett szervezettel kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is;
   b) megköveteli, hogy a szerződő fél feleljen meg az érintett szervezet által meghatározott személybiztonsági követelményeknek;
   c) megköveteli, hogy dokumentálja a személybiztonsági követelményeket;
   d) előírja, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az érintett szervezet elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az érintett szervezetnek;
   e) folyamatosan ellenőrzi a szerződő féltől személybiztonsági követelményeknek való megfelelését.

V. FIZIKAI VÉDELEMI INTÉZKEDÉSEK ELJÁRÁSRENDJE (3.2.1.2 [2])

V.1 Fizikai belépési engedélyek (3.2.1.3. [2])

(1) Az Egyetem elektronikus információs rendszerek szempontjából érintett és azoknak helyt adó épületeibe és helyiségeibe, az ott tárolt, kezelt adatokhoz történő illetéktelen fizikai hozzáférés, az esetleges károkozások, illetve zavar keltésének megakadályozása érdekében korlátozza a belépésre jogosultak körét.

(2) Az Egyetemen nyilvántartást (rendszeresen felülvizsgált és karbantartott) kell készíteni azokról, akik az elektronikus információs rendszereknek helyt adó épületekbe beléphetnek. Külön információs rendszerben kell kezelni a belépésre jogosultak körét.

(3) A birtoklás alapú (kártya) belépést csak annak engedélyezi a rendszer, aki a nyilvántartásban szerepel és a státusza aktív engedéllyel rendelkező.

(4) Amennyiben nincs lehetőség kártyás beléptető rendszer kiépítésére, vagy az épület mérete és látogatottsága nem indokolja, akkor a belépés a portaszolgálat felügyelete mellett történik.

(5) Olyan jellemzően kisebb épületekben, ahol nem indokolt a portaszolgálat, szükséges megakadályozni, hogy bárki engedély és ellenőrzés nélkül beléphessen az épület egyes részeibe, vagy ha megoldható magába az épületbe és onnan esetleg bizalmas információkat szerezzen meg. Ehhez elengedhetetlen legalább azon termek, irodák ajtajának kulcsra zárása, ahol szerverek, hálózati eszközök, dolgozói munkaállomások, bizalmas információk találhatók. A kulcsot a terem, iroda felelősének kell elraknia olyan helyre, ahol illetéktelen nem férhet hozzá.

(6) Mivel a birtoklás alapú jogosultság ellenőrzéshez használt kártya elveszhet, a visszaélés elkerülése érdekében azt azonnal jelenteni kell a beléptető rendszer rendszergazdájának, aki a belépési engedélyt a kártyához azonnal visszavonja.

V.2 A fizikai belépés ellenőrzése (3.2.1.4. [2])

(1) Az Egyetem a fizikai belépést ellenőrzi és kontrollálja az alábbiak szerint:

a) naplózza a fizikai belépéseket (erre szolgáló informatikai rendszerben vagy papír alapon). Amennyiben rendszert használ, azt nyilvántartja (praktikusan az eszköz menedzsment folyamat részeként);
b) ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;
c) szabályozza a látogatók fogadását, ennek rendjét;
d) megóvja a kulcsokat, hozzáférési kódokat;
e) manuálisan (pl. biztonsági őr segítségével) vagy informatikai rendszer segítségével ellenőrzi a bejutást és annak jogosságát;
f) nyilvántartást vezet a fizikai belépést ellenőrző eszközről;
g) meghatározott rendszerességgel változtatja meg a hozzáférési kódokat és kulcsokat, vagy azonnal, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az adott személy elveszti a belépési jogosultságát bizonyító kártyáját;
h) az egyéni belépési engedélyeket a belépési pontokon ellenőrzi;
i) a kijelölt pontokon való átjutást felügyeli a szervezet által meghatározott fizikai belépést ellenőrző rendszerrel vagy eszközzel;
j) felhívja a szervezet tagjainak figyelmét a rendellenességek jelentésére.

V.3 Hozzáférés az adatátviteli eszközökhöz és csatornákhoz (3.2.1.5. [4])

(1) Az Egyetem védi az elektronikus információs rendszer adatátviteli eszközeinek és kapcsolódási pontjainak helyt adó helyiségekbe történő fizikai belépést is.

(2) Az Egyetem mérete indokolja a zónavédelmet, ahol a beléptetés folyamata a benne található informatikai eszközöktől és az elektronikus információs rendszertől függően működik.

1. **szintű biztonsági zóna:**
   Nyilvános helyiségek, amelyek bárki által szabadon látogathatók vagy igénybe vehetők
2. **szintű biztonsági zóna:**
   Olyan helyiségek, irodák, amelyek minden munkavállaló számára elérhetőek, de külsősök számára csak kísérettel;
3. **szintű biztonsági zóna:**
   Korlátozott zóna - A munkavállalók korlátozott köre férhet hozzá. Pl. hálózati eszközöket tartalmazó helységek, informatikai raktárak, védett folyosók;
4. **szintű biztonsági zóna:**
   Különösen korlátozott zóna. Egyedileg adható hozzáférés. (Pl. szerverterem, konfigurálható hálózati eszközöket tartalmazó helységek, különösen védendő tárgyaló.) A belépésre jogosult csak informatikai üzemeltetési munkakörrel rendelkező munkavállaló vagy szerződéses partner lehet. Egyéb munkavállaló (műszaki szolgáltató, takarító személyzet) csak felügyelettel léphet be és tartózkodhat ezekben a helyiségekben, amennyiben jelenléte feltétlenül indokolt.

V.4 A kimeneti eszközök hozzáférés ellenőrzése (3.2.1.6. [4])

(1) Az Egyetem ellenőrzi az elektronikus információs rendszer kimeneti eszközeihez való fizikai hozzáférést annak érdekében, hogy jogosulatlan személyek ne férjenek hozzá azokhoz.

(2) A kimeneti eszközöket, mint nyomtatók, fénymásolók olyan folyosón vagy helyiségben kell elhelyezni, ahol nem férhet hozzá bárki. Az eszközök felett kifüggesztett helyes használati útmutató (ne hagyd a fénymásolóban a dokumentumot, használd az iratmegsemmisítőt stb.) elősegíti az információbiztonság szempontjából követendő helyes gyakorlatot.

(3) A secure printing bevezetése segít megőrizni az adatok és dokumentumok biztonságát. Például a secure printing beállításával csak az azonosított felhasználók nyomtathatnak, ezzel megelőzhető, hogy jogosulatlan személy nyomtasson ki és vigyen el bizalmas információkat.

(4) Kimeneti eszközök hozzáférés engedélyezése a tartományvezérelt (Active Directory) erőforrás kezelés, illetve a teljes körű nyomtatásfelügyeleti megoldás bevezetése javasolt (pl. SafeQ), ami átfogó központosított felügyeletet és magas szintű biztonság elérést teszi lehetővé.

V.5 A fizikai hozzáférések felügyelete (3.2.1.7 [3])

(1) Az Egyetem kártyás beléptető rendszer és élőerős őrzés segítségével biztosítja a fizikai hozzáférés ellenőrzését.

(2) Annak érdekében, hogy az Egyetem tudomására jusson az elektronikus információs rendszereinek helyt adó létesítménybe és helyiségbe történő illetéktelen belépés, ahhoz hogy észlelje a fizikai biztonsági eseményt és reagáljon arra, átvizsgálja a fizikai hozzáférések naplóit.

(3) Amennyiben a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak, azonnal átvizsgálja a fizikai hozzáférésekről készült naplókat, összehangolja a biztonsági események kezelését, valamint a napló átvizsgálások eredményét.

V.6 Behatolás riasztás, felügyeleti berendezések (3.2.1.7.2. [4])

(1) Az Egyetem felügyeli a fizikai behatolás riasztásokat és a felügyeleti berendezéseket.

(2) A kiemelt létesítmények, épületek, helyiségek riasztóval védettek, amik távfelügyeletre is bekötésre kerültek.

(3) A riasztások az incidenskezelési folyamat részét képezik.

V.7 A látogatók ellenőrzése (3.2.1.8 [3])

(1) Az elektronikus információs rendszereknek helyt adó létesítményekbe való látogatói belépésekről szóló információkat az Egyetem megőrzi. Amennyiben jogosulatlan belépés jelei mutatkoznak, azonnal átvizsgálja azokat (felvételek).

V.8 Áramellátó berendezések és kábelezés (3.2.1.9. [4])

(1) Az elektromos hálózatot és az adattovábbításra, illetve informatikai szolgáltatások nyújtására használt telekommunikációs kábelezést védeni kell a jogosulatlan lehallgatástól és rongálástól. Ennek érdekében a hálózati elemeket és eszközöket zárható szekrényben kell elhelyezni, a strukturált kábelezés (a fali végponttól az informatikai eszközig tartó szakasz kivételével) az álmennyezet fölött, vagy az álpadló alatt, a falazatban, illetve, ott ahol ez nem megoldható, akkor zárt kábelcsatornában kiépíteni.

(2) Az áramellátás kábeleit az informatikai adatkábelektől szeparáltan kell elhelyezni, megelőzve ezzel az interferenciát. A kábelezés nyomvonalát és típusát kábelezési rajzokon és nyilvántartásokban kell rögzíteni, úgy, hogy az létesítményeken belüli pontos futásvonal és elhelyezés leolvasható legyen.

(3) A kábelezés biztonságos kialakítása az ISZK feladata és felelőssége.

V.9 Tartalék áramellátás (3.2.1.9.1. [4])

(1) Az informatikai eszközöket és az elektronikus információs rendszereket védeni kell az áramkimaradások hatásaitól, valamint minden olyan nem kívánt hatástól, amelyet a különféle közművek (pl. áram, klíma) kimaradása okozhat.

(2) Az Egyetem elsődleges áramforrás kiesése esetére, a tevékenységhez méretezett, rövid ideig működőképes szünetmentes áramellátást biztosít az elektronikus információs rendszer szabályos leállításához vagy a hosszú távú tartalék áramellátásra történő átkapcsoláshoz.

(3) A hosszú távú tartalék áramellátás az elektronikus információs rendszer minimálisan elvárt működési képességének és előre definiált minimálisan elvárt működési idejének fenntartására áll rendelkezésre.

(4) A szerverek, storage adattárolók fokozott védelme érdekében valamint az egészségügyi szolgáltatások fokozottan kiemelt területein (pl. intenzív ellátás, műtők, diagnosztikai-, és képalkotó eszközök) redundáns tápellátások biztosítása mellet aggregátoros erősáram betáplálás is szükséges.

(5) Kiemelt figyelmet kell fordítani a szünetmentes eszközök (UPS) rendszeres felülvizsgálatára, akkumulátorainak cseréjére.

(6) A közművek kiesése elleni védekezés megtervezése és fenntartása a műszaki szolgáltatás biztosításáért felelős szervezeti egység és az ISZK vezetőjének a felelőssége, ennek ellenőrzését pedig az Informatikai Biztonsági Központ vezető végzi.

V.10 Vészkikapcsolás (3.2.1.10 [4])

(1) Az Egyetem lehetőséget biztosít az elektronikus információs rendszer vagy egyedi rendszerelemek áramellátásának kikapcsolására vészhelyzetben.

(2) Vészhelyzet: külső és környezeti fenyegetések, mint tűz, csőtörés, árvíz, földrengés, robbanás, zavargások, egyéb természeti csapások és ember által előidézett károsító hatások.

(3) A vészkikapcsoló berendezések biztonságos és könnyű megközelíthetőségét biztosítani kell. Olyan vészkikapcsoló panelt kell kiépíteni, amely az áramellátás azonnali megszakítását teszi lehetővé. A kikapcsolást jogosulatlan személy nem végezheti el.

V.11 Vészvilágítás (3.2.1.11. [3])

(1) Az Egyetem automatikus vészvilágítási rendszert alkalmaz és tart karban. A rendszer áramszünet esetén aktiválódik és biztosítja a vészkijáratokat és a menekülési útvonalakat.

(2) A folyosókon és a helyiségek kijáratainál zöld paneleket kiépíteni, amelyek áramszünet esetén világítanak és mutatják a vészkijáratokat, illetve a menekülési útvonalakat.

V.12 Tűzvédelem (3.2.1.12. [3])

(1) Az Egyetem az elektronikus információs rendszerek számára független áramellátással támogatott észlelő (tűz érzékelő, jelző) rendszert, az informatikai eszközökhöz, megfelelő tűzelfojtó berendezéseket alkalmaz, és tart karban.

(2) A tűzjelző és automatikus tűzoltó berendezések létesítése, üzemeltetése, karbantartása és állapotuk rendszeres dokumentált felülvizsgálata a műszaki szolgáltató terület feladata.

V.13 Automatikus tűzelfojtás (3.2.1.12.2. [4])

(1) Azokban az elektronikus információs rendszereket is tartalmazó helyiségekben, amelyekben nincs mindennapos bejárás, munkavégzés, vagy egyéb élőerős felügyelet, olyan automatikus tűzelfojtási berendezést kell alkalmazni, ami nem igényel emberi indítást. A szervereket, informatikai eszközöket tároló helyiségekbe a berendezést úgy kell megválasztani, hogy alkalmas legyen elfojtani az elektromos berendezések körül keletkezett tüzet - a vízzel oltás ilyen esetben nem megfelelő megoldás.

(2) A szerver helyiségekben található berendezési tárgyakat (asztalok, polcok, szekrények stb.) úgy kell megválasztani, hogy "nem éghető" anyagokból készüljenek (fém, üveg stb.). A szerverszobában fa bútorok használata, illetve papír tárolása nem javasolt, ezek könnyen és gyorsan égnek. Amennyiben mégis szükséges papírt tárolni a szerverszobában (pl. különböző dokumentumok vagy kartondoboz), azt zárt fém lemezszekrényben, tűzbiztosan ajánlott tárolni.

(3) A szerverszobában található folyamatosan áram alatt lévő aktív hálózati elemek (switch-ek, routerek, NAS-ok, stb.) és az azokat tároló rack szekrények tűzbiztonságát a szerverszobákkal azonos módon kell kialakítani. Közvetlen közelükben tárolhaóak fém polcon a használaton kívüli informatikai eszközök rendezett formában.

V.14 Hőmérséklet és páratartalom ellenőrzés (3.1.2.13. [3])

(1) Az Egyetem azokban a helyiségekben, ahol informatikai erőforrások koncentráltan találhatóak, az erőforrások biztonságos működése érdekében szinten tartja a hőmérsékletet és a páratartalmat, illetve figyeli azok szintjét.

(2) Ha az értékek eltérőek a normál szinttől, akkor lépéseket (pl. klímaberendezésen állít) tesz annak érdekében, hogy újra normál állapot álljon vissza.

(3) Teljesen automatizált és biztonságos hőmérséklet felügyeleti rendszer használata ajánlott, ami biztosítja az azonnali riasztást, és visszakövethető digitális dokumentációban tárolja (naplózás) az eseményeket.

(4) Távfelügyeleti és riasztási rendszer (pl. NAGIOS) használatával lehetőség van mind az erőforrások (pl. szerver, storage hőmérséklet) mind a tároló helyiség felügyeletére. Beállított határérték túllépés esetén képes többlépcsős figyelmeztetésre, sms, email riasztás küldésre az illetékes rendszergazdáknak, rendszerüzemeltetőknek a gyors és hatékony beavatkozás megkezdéséhez.

V.15 Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem (3.1.2.14. [3])

(1) Az Egyetem védi az elektronikus információs rendszereit a víz-, és más, csővezetéken szállított anyag okozta kár ellen. Biztosítja, hogy a főelzárószelepek hozzáférhetőek legyenek és megfelelően működjenek, valamint a kulcsszemélyek számára ismertek legyenek. A szervezet az informatikai erőforrásokat koncentráltan tartalmazó helyiségek tervezése során biztosítja, hogy a víz-, és más hasonló kártól védett legyen, akár csővezetékek kiváltásával, áthelyezésével.

V.16 Be- és kiszállítás (3.2.1.15 [3])

(1) Az Egyetem nyomon követi az információs rendszerelemek teljes életútját, ezekről nyilvántartást (inventory-t) vezet, naprakészen tartja.

(2) Az Egyetem engedélyezi, vagy tiltja, továbbá figyeli és ellenőrzi a létesítménybe bevitt, onnan kivitt információs rendszerelemeket, és nyilvántartást vezet ezekről.

(3) Különös figyelmet fordít a rendszerelemek elszállítására, csak olyanok elszállítását teszi lehetővé amelyek már nem tartalmaznak bizalmas információt.

(4) A kiadott/bevitt eszközökről nyilvántartást kell készíteni, amely tartalmazza az eszköz megnevezését, modellszámát, kinek lett kiadva/ki hozta be, mikor történt.

V.17 Az elektronikus információs rendszer elemeinek elhelyezése (3.2.1.16. [4])

(1) Az Egyetem úgy helyezi el az elektronikus információs rendszer elemeit, hogy a legkisebb mértékre csökkentse a szervezet által meghatározott fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét.

(2) Az elektronikus információs rendszer elemeit külön helyiségben kell elhelyezni, aminek zárható az ajtaja és megfelelő védelemmel van ellátva (az ablakon rácsok vannak, tűz ellen megfelelően védett, klimatizált, beléptető rendszer, kamera).

V.18 Karbantartók (3.2.1.19 [3])

(1) Az Egyetem nyilvántartást vezet a karbantartó szervezetekről és személyekről.

(2) A szolgáltatás megkezdése előtt ellenőrizni kell, hogy a karbantartás elvégzésére megjelent személy a szerződés karbantartói listáján szerepel.

(3) A karbantartók számára ismertetni kell az Egyetem, szolgáltatásra vonatkozó információbiztonsági előírásait.

(4) Az információbiztonsági előírások be nem tartására vonatkozó következményeket, szerződésben kell rögzíteni.

(5) Amennyiben a szolgáltatásnyújtás megkívánja, az Egyetem elektronikus információs rendszerihez való hozzáférést, a munkavégzéshez elengedhetetlen minimális felhasználói jogosultságot kell paraméterezni.

(6) Távoli hozzáféréssel biztosított karbantartás esetében (szerverek, orvostechnikai eszközök) csak annak a hálózati szegmensnek, vagy csak egy eszköznek a hálózati elérés engedélyezése adható, ami elégséges a szolgáltatásnyújtás végzéséhez.

V.19 Időben történő javítás (3.2.1.19.3 [4])

(1) Az Egyetem elektronikus információs rendszerinek és az azt kiszolgáló infrastruktúrának, az Egyetem elvárt szintű üzletmenet folytonosságának biztosításához magas rendelkezésre állással kell üzemelniük. Ennek érdekében az Egyetem karbantartási szerződésben, belső folyamatleírásban rögzíti:

a) A karbantartási időszakokat, minimum követelményeket, valamint
b) SLA-kat határoz meg a karbantartással kapcsolatban, amit szerződésbe foglal

VI. LOGIKAI VÉDELMI INTÉZKEDÉSEK

VI.1 Általános védelmi intézkedések (3.3.1.1. [2])

(1) Az Egyetem:
   a) megfogalmazza, és az Egyetemre érvényes követelmények szerint dokumentálja, valamint az Egyetemen belül kihirdeti az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési eljárási folyamatokat;
   b) felügyeli az elektronikus információs rendszer és környezet biztonsági állapotát;
   c) meghatározza az információbiztonsággal összefüggő szerepköröket és felelősségi köröket, kijelöli az ezeket betöltő személyeket;
   d) integrálja az elektronikus információbiztonsági engedélyezési folyamatokat a szervezeti szintű kockázatkezelési eljárásba, összhangban az informatikai biztonsági szabályzattal.

VI. 1.1. Az elektronikus információs rendszer kapcsolódásai (3.3.1.3. [3])

(1) Az egyes elektronikus információs rendszerek más rendszerekkel való kapcsolatai, valamint az azokon keresztül zajló információ típusa, szabályozottan és dokumentáltan történik.

(2) Az Egyetem dokumentálja és naprakészen tartja:
   a) informatikai rendszereit és kapcsolatait leíró architektúra ábrát,
   b) interfész kapcsolódási ábrát, amely leírja mely rendszerek mely interfészeken keresztül kapcsolódnak, ott milyen adatkapcsolatok vannak és az egyes interfészek biztonsági beállításait,
   c) tűzfal, proxy, portok kapcsolódási szabályait, előírásait dokumentálja,
   d) új interfész bevezetését engedélyhez köti, ennek folyamatát a megfelelő Szabályzatban leírja,
   e) engedélyhez köti és dokumentálja a külső rendszerhez való kapcsolódás folyamatát.

VI.1.1.1 Belső rendszerkapcsolatok (3.3.1.3.2. [3])

(1) Az Egyetem belső engedélyhez köti az elektronikus információs rendszereinek egymáshoz kapcsolódását, összekapcsolását.

VI.1.1.2 Külső kapcsolódásokra vonatkozó korlátozások (3.3.1.3.3. [3])

(1) A külső rendszerekkel való kapcsolódás szigorú szabályozással működik.

(2) Az Egyetem a külső elektronikus információs rendszerekhez való kapcsolódásokhoz az informatikai biztonsági szabályzatában szabályrendszert állít fel és alkalmaz, amelynek eredménye lehet:
   a) az összes kapcsolat engedélyezése vagy tiltása,
   b) meghatározott kapcsolatok engedélyezése,
   c) meghatározott kapcsolatok tiltása,
   d) meghatározott protokollok engedélyezése vagy tiltása,
   e) meghatározott kommunikációs csatornák engedélyezése vagy tiltása,
   f) kapcsolat létesítésére egyes tűzfal portok tiltása.

VI.2 Tervezés (3.3.2.)

(1) Az Egyetem megfogalmazza, az Egyetemre érvényes követelmények szerint dokumentálja, és a munka- és feladatkörük miatt érintettek számára kihirdeti a biztonságtervezési eljárásrendet, amely tartalmazza a biztonságtervezési eljárás folyamatait, valamint biztosítja annak ellenőrzését.

(2) A biztonságtervezési eljárásrendet az abban meghatározott gyakorisággal felülvizsgálja és frissíti.

VI. 2.1. Felmérés

(1) Az Egyetem meghatározza, a munka- és feladatkörük miatt érintettek számára kihirdeti a biztonságtervezési szabályzat felmérés, adat és információgyűjtésre vonatkozó elvárásait.

VI. 2.2. Az elvárt biztonsági osztály meghatározása

(1) Az osztályba és szintbe sorolás részletes szabályait az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet tartalmazza.

(2) A rendszer biztonsági osztályba sorolását kockázatelemzés alapján kell végrehajtani.

(3) Az Egyetem minden elektronikus információs rendszerének osztályba sorolását külön-külön kell elvégezni.

(4) A rendszerek osztályba sorolása két részből áll, az első fázisban azt kell megállapítani, hogy az adott elektronikus információs rendszer a kockázatelemzés alapján melyik biztonsági osztályba tartozik (elvárt/tervezett biztonsági osztály). A biztonsági osztályok megállapítása a káresemények szempontjából a rendszer által kezelt adatok sérülésének és az ebből fakadó következmények, a szervezettel szembeni bizalomvesztés, illetve a közvetlen- és közvetett anyagi kár mértékének szintezésével történik. A jogszabályban megadott elvek szerinti besorolás alkalmazása nem kötelező, de más módszer használatánál is fel kell tüntetni az értékelési szempontokat.

(5) Az osztályba sorolás második lépéseként azt kell megvizsgálni, hogy az elvárt osztályhoz előírt védelmi intézkedések hogyan teljesülnek az adott rendszer tekintetében, ez lesz a rendszer teljesített biztonsági osztálya.

VI. 2.3. Követelményrendszer kidolgozása

(1) A rendszerek biztonsági osztályba sorolása kockázatelemzés alapján történik.

(2) Az elfogadható kockázatok és az elfogadható kockázatok szintjének meghatározásához egy követelményrendszer szükséges.

(3) Az Egyetem ezeket a követelményeket az „Információbiztonsági kockázatok kezelésének eljárásrendje” dokumentumban fektette le.

VI. 2.4. Biztonságtervezési szabályzat (3.3.2.1. [4])

(1) Az Egyetem magának a biztonságnak (annak elérésére tett törekvéseknek) a tervezési folyamatát „Biztonságtervezési eljárásrendben” rögzíti, amit az abban meghatározott időközönként felülvizsgál és frissít.

(2) Folyamatot szabályozó dokumentum, tartalmazza az egyes rendszerelemek teljes életciklusában megvalósítani kívánt, a szervezet biztonságpolitikai céljainak megfelelő követelményeket.

(3) Az eljárásrend kitér az alábbiakra:
   a) cél, hatókör, szerepek, felelősségek, a vezetői elkötelezettség, a szervezeti egységek közötti koordináció
   b) meghatározza az elektronikus információs rendszer alapfunkcióit (pl. levelezőrendszer, számlázási rendszer stb.), működési koncepcióját és üzleti folyamatait
   c) a kockázatelemzéssel összhangban rögzíti a rendszer biztonsági osztályát,
   d) valamint a rendszer által kezelt adatok biztonsági osztályát,
   e) meghatározza az EIR adatkapcsolatait, interfész kapcsolatait más rendszerekkel (kitérve az adatok integritását és bizalmasságát megvédő technikai megoldásokra),
   f) meghatározza, mely szabályzatok vonatkoznak a rendszerre (pl. IBSZ),
   g) átfogó képet ad a rendszerre vonatkozó biztonsággal kapcsolatos elvárásokról,
   h) részletezi a biztonságtervezés alapelveit (bizalmasság, sértetlenség, rendelkezésre állás "háromszög"),
   i) leírja a cselekvési terv folyamatának lépéseit.

VI. 2.5. Rendszerbiztonsági terv készítése (3.3.2.2. [2])

(1) A Rendszerbiztonsági terv egy összefoglaló dokumentum, amely leírja és összegzi mely biztonsági intézkedésekkel éri el az Egyetem az adott elektronikus információs rendszer biztonságának megtartását.

(2) A rendszerbiztonsági terv tartalma:
   a) leírja az adott elektronikus információs rendszer minden, információbiztonsággal kapcsolatos szabályzatát, kontrollpontját,
   b) hivatkozza a meglévő szabályzatokat (pl. változáskezelés, IBSZ, jogosultságmenedzsment, stb.)

(3) Rendszerbiztonsági terv készítése saját fejlesztésre, vásárolt szoftveres megoldásra-, dobozos termékekre nem vonatkozik.

VI. 2.6. A rendszerbiztonsági terv audit

(1) Az audit célja, hogy megállapítást nyerjen, hogy a terv biztonsági intézkedései:
   a) elegendőek a veszély elhárítására,
   b) elegendőek a biztonság fenntartására,
   c) mi az az intézkedés, ami változtatást igényel,
   d) költséghatékony-e az intézkedés,
   e) milyen új intézkedés javasolt.

(2) A rendszerbiztonsági tervet évente, vagy biztonsági esemény bekövetkezte után felül kell vizsgálni, a biztonsági eseménykezelés „okulás” tapasztalataival finom hangolni.

VI. 2.7. A rendszerbiztonsági terv megismertetése

(1) Az Egyetem gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is).

VI. 2.8. A rendszerbiztonsági terv felülvizsgálata

(1) A tervet rendszeres időközönként, évente egyszer felül kell vizsgálni. A tervet soron kívül felül kell vizsgálni minden olyan változás esetén, amelyek a rendszerbiztonsági tervben foglaltak

alkalmazhatóságát, megfelelőségét vagy hatékonyságát érintik illetve, ha olyan információbiztonsági incidens történik, amit jelen terv környezet az eset egyedisége, ismeretlensége miatt nem érint, nem érinthet.

VI.2.8.1 Időszaki felülvizsgálat

(1) A rendszerbiztonsági tervnek, tervezett éves felülvizsgálatán kívüli, időszaki vizsgálatát kell elvégezni, ha a tervben hivatkozott egyéb egyetemi szabályzatokban változás következik be.

VI.2.8.2 Rendkívüli felülvizsgálat

(1) A rendszerbiztonsági terv rendkívüli felülvizsgálata indokolt, amennyiben olyan események következnek be, amik felülvizsgálatot, hatékonyságelemzést, változtatást, módosítást generálnak a dokumentumban.

VI.2.8.3 A rendszerbiztonsági terv frissítése

(1) Az Egyetem frissíti a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén.

VI.2.8.4 Belső egyeztetések

(1) Az Egyetem belső egyeztetéseket kezdeményez a rendszerbiztonsági terv elkészítése, véleményezése, módosítása, auditálása témaköreiben.

VI. 2.9. A biztonságtervezés auditja (3.3.2.1. [4])

(1) Biztonságtervezés auditra célszerű független szakértőt felkérni. Független külső auditot, felülvizsgálatot az Informatikai Biztonsági Központ vezetője, a GDPR Központ vezetője, az ISZK vezetője kezdeményezhet a Kancellár előzetes jóváhagyásával.

VI. 2.10. Cselekvési terv (3.3.2.3. [2])

(1) Amennyiben az adott elektronikus információs rendszer biztonsági osztályához előírtak alapján hiányosság tapasztalható, akkor annak elhárítására pontos terv szükséges, amely tartalmazza a javítás és felülvizsgálat főbb elemeit.

(2) Az Egyetem a cselekvési tervben dokumentálja a megállapított hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeit.

VI.2.10.1 Cselekvési terv készítése

(1) A cselekvési tervnek, reálisnak, tarthatónak és számon kérhetőnek kell lennie. A cselekvési terv meghatározza a következőket:
   a) Az elvégzendő feladatok, akciók pontos leírását;
   b) Felelősöket;
   c) Határidőket;
   d) Akciók, projektek végrehajtásának pénzügyi hatásait, feltételeit:

(2) A cselekvési terv egy projektterv a következő szint eléréséhez.

VI.2.10.2 Cselekvési terv frissítése

(1) Az Egyetem frissíti a cselekvési tervét az Egyetem által meghatározott gyakorisággal a biztonsági értékelések, biztonsági hatáselemzések és a folyamatos felügyelet eredményei alapján.

VI. 2.11. Személyi biztonság (3.3.2.4. [2])

(1) Az Egyetem, írásba foglalja azokkal a személyekkel szembeni elvárásait, akik hozzáférést igényelnek az elektronikus információs rendszereihez.

(2) Az elvárásokat jelen szabályzatban és az ehhez kapcsolódó eljárásrendekben rögzíti, azokat megismerteti és elérhetővé teszi a munkavállalói számára.

(3) A dokumentumokat meghatározott időközönként frissíti, az új verziókat is elérhetővé teszi azt az érintettek számára

(4) Az információbiztonsággal kapcsolatos szabályzatokat, eljárásrendeket, titoktartási kötelezettségeket, szerződéses partnereivel is elfogadtatja.

VI.2.11.1 A felhasználókkal szemben támasztott elvárások megfogalmazása

(1) Az Egyetem az elektronikus információs rendszereiben tárolt adatai, információi, bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása, megőrzése érdekében az azokat kezelő felhasználókkal szemben viselkedési, eljárási normákat fogalmaz meg.

(2) Az Egyetem elektronikus információs rendszereihez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja.

VI.2.11.2 A rendszer használattal kapcsolatos információk biztosítása

(1) Az Egyetem egyes elektronikus információs rendszerei vonatkozásában - az informatikai biztonsági és az informatikai feladatellátásáért felelős szervezeti egység által - megfogalmazott, az elektronikus információs rendszerek informatikai biztonsági szabályoknak megfelelő használatára vonatkozó elvárások a felhasználókkal a használatbavétel előtt (a hozzáférési jogosultság aktiválása előtt) kerülnek átadásra, aminek tudomásulvételét aláírásukkal ellenjegyzik.

VI.2.11.3 A felhasználókkal szemben támasztott elvárások felülvizsgálata

(1) A felhasználókkal szemben támasztott elvárások évente, illetve biztonsági esemény, incidens bekövetkezése esetén azonnal felülvizsgálatra kerülnek.

(2) Amennyiben a felülvizsgálat az elvárások és szabályok változását vonja maga után, erről az érintett felhasználók tájékoztatása megtörténik, aminek tudomásulvételét írásos formában vagy elektronikus válasszal (email) igazolnak.

VI. 2.12. Információbiztonsági architektúra leírás (3.3.2.5. [4])

(1) Az információbiztonsági architektúra leírás:
   a) összegzi az elektronikus információs rendszer bizalmasságának, sértetlenségének és rendelkezésre állásának védelmét szolgáló filozófiát, követelményeket és megközelítést,
   b) megfogalmazza, hogy az információbiztonsági architektúra miként illeszkedik a szervezet általános architektúrájába, és hogyan támogatja azt,
   c) leírja a külső szolgáltatásokkal kapcsolatos információbiztonsági feltételezéseket és függőségeket,
   d) tartalmazza, hogy melyek:
      - az elektronikus információs rendszerek Rendszerbiztonsági tervei,
      - az elektronikus információs rendszerek egyéb tervei, üzemeltetési leírásai,
      - az Egyetem infrastruktúrájára vonatkozó tűzfal és hálózati architektúrák,
      - az Informatikai Biztonsági Irányítási Rendszer dokumentumai.

VI.3 Rendszer és szolgáltatás beszerzés (3.3.3. [2])

(1) Az Egyetem az informatikai beszerzések során az informatikai biztonsági követelményeket már az életciklus tervezési, fejlesztési, beszerzési szakaszában figyelembe veszi és folyamatosan nyomon követi.

(2) Az IBF által meghatározott információbiztonsági elvárásokat, mint beszerzési követelményeket már a beszerzés kezdetén érvényesíti.

(3) Az Egyetem az általa kialakítandó beszerzési eljárásban a biztonsági osztályoknak megfelelően a szállítók számára is meghatározza az Ibtv. szerinti követelményeket.

(4) A rendszer és szolgáltatás beszerzésekre, valamint a fejlesztésekre vonatkozó részletes informatikai biztonsági követelményeket és szabályokat az „Informatikai beszerzési eljárásrend” és a „Biztonságos fejlesztési követelmények eljárásrend” tartalmazza.

VI. 3.1. A rendszer fejlesztési életciklusa (3.3.3.2. [2])

(1) Az Egyetem az elektronikus információs rendszereit minden életciklusában (követelmény felmerülésétől egészen a használatból való kivonásig) információbiztonsági szempontból gondozza, nyomon követi. A rendszerekre vonatkozóan meghatározza az információbiztonsági feladatokat és felelősségeket, valamint gondoskodik azok elvégzéséről. A rendszer életciklus szakaszai a következők:
   a) követelmény meghatározás,
   b) fejlesztés vagy beszerzés,
   c) megvalósítás vagy értékelés,
   d) üzemeltetés és fenntartás,
   e) kivonás (archiválás, megsemmisítés).

VI. 3.2. Funkciók, portok, protokollok, szolgáltatások (3.3.3.3. [3])

(1) Az Egyetem megköveteli, hogy a szolgáltató meghatározza a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat.

(2) Csak olyan szolgáltatótól vesz igénybe szolgáltatást, aki ezeket előre átadja, azért hogy a szolgáltatás beszerzése előtt el tudja dönteni, hogy az elvárt feltételek összhangban vannak-e a saját elvárásaival.

VI. 3.3. Fejlesztői követelmények (3.3.3.4. [4], 3.3.3.5. [4])

(1) Az Egyetem megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:
   a) vezesse végig a változtatásokat az elektronikus információs rendszer, rendszerelem vagy rendszer szolgáltatás tervezése, fejlesztése, megvalósítása, üzemeltetése során;
   b) dokumentálja, kezelje, és ellenőrizze a változtatásokat, biztosítsa ezek sértetlenségét;
   c) csak a jóváhagyott változtatásokat hajtsa végre az elektronikus információs rendszeren, rendszerelemen vagy rendszerszolgáltatáson;
   d) csak hibátlan, tesztelt új verziót adhat át;
   e) dokumentálja a jóváhagyott változtatásokat és ezek lehetséges biztonsági hatásait;
   f) kövesse nyomon az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás biztonsági hibáit és azok javításait;
   g) jelentse észrevételeit az Egyetem által meghatározott személyeknek.

(2) Az Egyetem elvárásainak az alábbiak szerint kell megfelelni:
   a) Az egyes rendszereket fejlesztőknek kötelességük a változások pontos dokumentálása, biztonsági hibák feltárása és a szervezettel való előzetes egyeztetés, valamint a biztonsági hibajavítás nyomon követesé így biztosítva a fejlesztés bár mikori folytatását az azt végző személyektől függetlenül;
   b) Minden fejlesztés átadása előtt biztonsági tesztelést és annak kiértékelését kell elvégeznie a rendszer fejlesztőjének az előre elkészített és jóváhagyott biztonságértékelési terv alapján, amely folyamatot dokumentálnia szükséges;
   c) A fejlesztőnek kötelessége dokumentált fejlesztési folyamat elvégzése és a szervezet biztonsági előírásainak való megfelelés meghatározott időnként való ellenőrzése;

d) A fejlesztő által - az általa fejlesztett rendszer tekintetében - tartandó kötelező oktatás a fejlesztett rendszer szempontjából illetékes adminisztrátorok, biztonsági felelősök számára, hogy a lehető legrészletesebb képet kapjanak első kézből az új fejlesztés biztonsági aspektusait illetően;
e) Az új funkció, rendszerelem, rendszer teljes körű bemutatása, kiemelve a beépített biztonsági kontrollokat, az azokhoz használt technikákat, megoldásokat, technológiákat, felhívva a figyelmet a lehetséges megkerülésükre;
f) A fejlesztőnek kötelessége olyan biztonsági fejlesztési dokumentumot előállítania, amely illeszkedik az Egyetem meglévő felépítésébe, részletezi a beépített biztonsági kontrollpontokat, és bemutatja, hogy azok milyen módon, hogyan erősítik egymást és ezáltal az Egyetem teljes biztonságát;
g) A fejlesztés tervezési fázisában készítendő, a biztonsági funkciókat tartalmazó strukturált dokumentum. Ennek összhangban kell, hogy legyen az Egyetem többi szabályzatával és eljárásrendjével, különösen az üzemeltetési, naplózási, jogosultság- és változásmenedzsment szabályzatával;

VI.4 Biztonsági elemzés (3.3.4.)

(1) Az Egyetem megfogalmazza, dokumentálja, kihirdeti a biztonságértékelési eljárásrendet, amely a biztonságértékelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. Ehhez biztonságértékelési tervet készít.

(2) A biztonságértékelési terv magában foglalja az elektronikus információs rendszerek fenyegetési környezetét, a védelmi intézkedések hatékonyságát, az ellenőrzés módját és kivitelezésének egyéb jellemzőit, valamint az eredmények értékelését és érintettekkel való megosztásának folyamatát.

VI. 4.1. Biztonsági teljesítmény mérése (3.3.4.4. [3], 3.3.5.2. [3])

(1) A biztonsági teljesítmény mérése dokumentált mérési módszertannal történik, amely kiterjed a biztonsági események utáni feltáró vizsgálatok eredményeire és az elvégzett sérülékenység vizsgálatok által feltárt kritikus megállapítások értékelésére.

(2) A biztonsági teljesítményt a biztonsági események elemzésével és az elvégzett sérülékenység vizsgálatok kritikus megállapításaival kell értékelni.

(3) Az Egyetem dokumentálja, hogy milyen eszközökkel (pl. biztonsági audit, sérülékenység vizsgálat) milyen rendszerességgel, belső vagy külső erőforrást felhasználva méri, ellenőrzi saját biztonsági szintjét.

(4) Megfogalmazza az elvárt metrikákat, KPI-okat, amik lehetnek:
   a) sérülékenységek száma vs "célszám";
   b) hány rendszert kell tesztelni vs. az összes rendszer száma;
   c) átlagos idő a tesztek között;
   d) a kritikus sérülékenységek hány %-át patchelte az Egyetem meghatározott SLA-n belül;
   e) a bejelentett biztonsági események száma és súlyossága;
   f) az elvégzett tesztek száma.

VI.4.1.1 Biztonsági teljesítmény értékelés (3.3.4.2. [3])

(1) A biztonsági teljesítmény értékelésében figyelembe vett tényezők:
   a) Határvédelmi incidensek, és hálózati illegális tevékenység;
   b) Vírusvédelmi incidensek;
   c) Jogosultság kezelési incidensek;
   d) Mentési feladatok sikeres/sikertelen végrehajtása;
   e) Külső felhasználók tevékenységei, távoli elérések naplózása;
   f) Privilegizált felhasználók tevékenységei;
   g) Biztonsági riasztórendszerek naplózása (pl.: UPS, Tűzvédelem stb.);
   h) Kritikus adatok törlése, másolása. (pl.: rendszerfájlok, naplók, magas védelmet igénylő adatok);
   i) SLA sértés;
   j) levelezési rendszerbe bejutó támadási potenciálok;
   k) Social engineering.

VI.4.1.2 Speciális értékelés (3.3.4.3. [4])

(1) A biztonsági teljesítmény értékelésére az Egyetem rosszindulatú külső-belső támadást szimulál, így próbálja felderíteni a biztonsági architektúrában létező esetleges gyenge, sebezhető pontokat.

(2) Az Egyetem speciális értékeléseket végez, amely magában foglalja:
   a) bejelentés nélküli sérülékenység vizsgálat. Jellemzően külső fél, úgynevezett "etikus hacker" által végzett teszt, amely rosszindulatú támadást szimulál;
   b) meghatározza a különböző fajta (ún. black, white, gray box) sérülékenység vizsgálatok rendszerességét;
   c) a sérülékenység vizsgálat eredményeit értékeli, a hiányosságok javítására akciótervet dolgoz ki;

VI.5 Tesztelés, képzés és felügyelet (3.3.5.)

(1) Az Egyetem kidolgozza, írásba foglalja és az érintettek számára elérhetővé teszi az elektronikus információs rendszereire vonatkozó tesztelési, felügyeleti és képzési eljárásrendet.

(2) A dokumentum kitér az alábbiakra:
   a) Felelősségi körök;
   b) Kivételkezelés;
   c) Részletezi a rendszeres tesztek folyamatát;
   d) Részletezi az ad-hoc tesztelés folyamatát;
   e) Leírja a lehetséges módszertanokat;
   f) Kialakítja a hiányosságok és teszteredmények riportálási folyamatát, eszkalációs láncot;
   g) Megfogalmazza az elvárt metrikákat, KPI-okat;
   h) A különböző tesztelések tapasztalt hiányosságokat figyelembe veszi a kockázatelemzés során.

VI. 5.1. Tesztelési, képzési és felügyeleti eljárások (3.3.5.1.1. [3])

(1) Az Egyetem megfogalmazza, dokumentálja, kihirdeti az elektronikus információs rendszer tesztelésével, képzésével és felügyeletével kapcsolatos eljárásokat, amelyek támogatják a tesztelési, képzési és felügyeleti tevékenységek;
   a) fejlesztését és fenntartását,
   b) folyamatos időbeni végrehajtását,
   c) felülvizsgálja a tesztelési, képzési és ellenőrzési terveket a kockázatkezelési stratégia és a lehetséges, vagy bekövetkezett biztonsági események súlya alapján.

VI.5.1.1 Teszttervezés

(1) Az Egyetem az elektronikus információs rendszerei és alkalmazásai tekintetében biztonsági tesztet végez, ha azt az elektronikus információs rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik.

(2) A tesztelés történhet meghatározott gyakorisággal, véletlenszerűen, valamint olyan esetben, amikor új lehetséges sérülékenység merül fel az elektronikus információs rendszerrel vagy alkalmazásaival kapcsolatban.

VI.5.1.2 Teszt analízis és Design

(1) Az Egyetem a biztonsági tesztet sérülékenység vizsgálati eszközök és technikák alkalmazásával, vagy külső szervezet bevonásával hajtja végre.

VI.5.1.3 Végrehajtás

(1) A tesztelés kivitelezője (belső erőforrás, külső szervezet):
   a) végrehajtja az ellenőrzési listákat és tesztelési eljárásokat;
   b) felméri a sérülékenység lehetséges hatásait;
   c) kimutatást készít a feltárt hibákról, valamint a nem megfelelő konfigurációs beállításokról.

VI.5.1.4 Értékelés, beszámolás, kilépés

(1) A tesztelés kivitelezője (belső erőforrás, külső szervezet):
   a) elemzi a sérülékenység teszt eredményét;
   b) megosztja a sérülékenység teszt eredményét az Egyetem által meghatározott személyekkel és szerepkörökkel.

VI. 5.2. A tesztelés típusai

(1) A tesztelés folyamata lehet;
   a) rendszeres,
   b) ad-hoc.

(2) Folyamatosan frissített adatbázisból dolgozó sérülékenység felderítő eszköz használata. A frissítés mind az új rendszerelemek bevezetése, mind a meglévő elemek új, időközben ismertté vált sérülékenységei szempontjából jelentős.

(3) Rendszeres, automatizált felderítés (scan) a jó gyakorlat, a feltárt sérülékenységekről készült riport feldolgozásával folytatva.

(4) Az Egyetem a sérülékeny verziókat frissíti, frissítés hiányában egyéb mitigáló (enyhítő) lépéseket tesz.

VI. 5.3. Tesztelési kategóriák

(1) Igénybevett erőforrás tekintetében:
   a) belső;
   b) külső.

VI. 5.4. Teszttervezési technikák

(1) Lehetséges módszertanok;
   a) white box (A vizsgálat elvégzése előtt a tesztelők megismerik a teljes infrastruktúrát, a hálózati diagramokat, forráskódot, az IP cím információkat.)
   b) gray box (A vizsgálat feltételezi a vizsgált infrastruktúra részleges ismeretét.)
   c) black box (a vizsgálat az infrastruktúra előzetes ismerete nélkül történik)

(2) A szimulált támadás során az Egyetem azonosítja azon információkat, amelyeket a lehetséges támadó elérhet, majd megkísérli elhárítani a jövőbeni potenciális támadásokat

VI. 5.5. Sérülékenység teszt (3.3.5.3. [3])

(1) Az Egyetem az elektronikus információs rendszerei és alkalmazásai tekintetében sérülékenység tesztet végez, ha azt az elektronikus információs rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik.

(2) Amikor új lehetséges sérülékenység merül fel az elektronikus információs rendszerrel vagy alkalmazásaival kapcsolatban, a preventív cselekvési terv kidolgozása érdekében azonnal megismétli a sérülékenység tesztet.

(3) A sérülékenység tesztek kitérnek arra is, hogy egy esetleges rosszindulatú támadó, különösen internet felől elérhető rendszerek esetében milyen ismert és általánosan alkalmazott felderítési technikák alkalmazásával megszerezhető információkhoz férnek hozzá.

A sérülékenységvizsgálat életciklusa

VI.6 Konfigurációkezelés (3.3.6.)

(1) A konfigurációkezelés célja az informatikai infrastruktúra adatainak kézben tartása, az egyes komponensek beazonosítása, figyelemmel követése és karbantartása. A szolgáltatásokról, a szoftver és hardver konfigurációkról és azok dokumentációjáról központilag tárol információkat így segíti az incidensfelügyeletet, problémakezelést, változáskezelést és a verziókövetést.

(2) Az Egyetem megfogalmazza, dokumentálja, valamint szervezeten belül kihirdeti a konfigurációkezelési eljárásrendet, mely a konfigurációkezelési folyamatát és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

VI.6.1. Konfigurációs eljárásrend és nyilvántartások (3.3.6.1. [2])

(1) Az Egyetem konfigurációkezelési eljárásrendje kitér az alábbiakra;
   a) konfigurációmenedzsment felelőseire, alapvető folyamatára;
   b) gondoskodik arról, hogy a konfigurációs elemeket nyilvántartsa, és naprakészen elérhetővé tegye;
   c) meghatározza a konfigurációmenedzsment hatókörét (alapvetően az elektronikus információs rendszereihez kapcsolódó konfigurációs elemek);
   d) rendelkezik a konfigurációmenedzsmenthez használt szoftver használatáról.

VI.6.2. Alkalmazási rendszerek konfigurációinak nyilvántartása

(1) Az alkalmazási rendszerek konfiguráció nyilvántartásának célja az informatikai infrastruktúra adatainak kézben tartása, a szoftver és hardver konfigurációk dokumentációjának, figyelemmel követése és karbantartása.

VI.6.3. Alapkonfiguráció (3.3.6.2. [2])

(1) Az Egyetem az elektronikus információs rendszereihez egy-egy alapkonfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges elemeit. A dokumentációt a releváns szereplők számára elérhetővé teszi.

(2) Az alapkonfigurációt úgy kell kialakítani, karbantartani és változatlan állapotban megőrizni, hogy szükség esetén vissza lehessen térni rá, ezzel biztosítva, hogy egy működőképes verzió álljon rendelkezésre (pl. egy szoftver új verziójának bevezetése sikertelen).

VI.6.4. Áttekintések és frissítések (3.3.6.2.2. [4])

(1) Az alapkonfiguráció frissítését az elektronikus információs rendszerelemek telepítésének és frissítéseinek szerves részeként kell elvégezni.

VI.6.5. Korábbi konfigurációk megőrzése (3.3.6.2.3. [4])

(1) Változatlan állapotban meg kell őrizni az elektronikus információs rendszer alapkonfigurációját és annak további verzióit, hogy szükség esetén lehetővé váljon az erre való visszatérés.

(2) A korábbi konfigurációkra történő visszaállás lehetőségének biztosítása érdekében változatlan formában meg kell őrizni az alapkonfiguráció leírását is, amely alapján vissza lehet állni.

(3) A konfigurációs leírás megfelelő megőrzése mellett szoftveres megoldást kell alkalmazni a konfigurációmenedzsment kezelésére.

VI.6.6. Magas kockázatú területek konfigurálása (3.3.6.2.4. [4])

(1) Biztonsági szempontokból meghatározott módon konfigurált elektronikus információs rendszerelemeket vagy eszközöket kell biztosítani azon személyek számára, akik az elektronikus információs rendszert külső helyszínen használják.

(2) Külső helyszínről is használható eszközök magasabb biztonsági kockázati besorolása miatt, biztonságosabb konfiguráció kialakítása igényelt. Például:
   a) Notebook konfiguráció:
   b) USB portok tiltása,
   c) full disk encryption,
   d) erős jelszó kikényszerítése illetve
   e) biometrikus második faktor használata,

(3) Saját eszközről végzett otthoni munkavégzés (amennyiben ez engedélyezett) esetében a konfiguráció gyengeségeit (több személy, gyenge vírusvédelem – ha van, rendszergazdai jogosultság,..) a munkahelyi hálózathoz való csatlakozás keretében kell lekezelni, súlyos esetben a használatot nem engedélyezni.

VI.6.7. A konfigurációváltozások felügyelete (változáskezelés) (3.3.6.3. [3])

(1) Az Egyetem:
   a) meghatározza a változáskezelési felügyelet alá eső változástípusokat;
   b) meghatározza az egyes változástípusok esetén a változáskezelési vizsgálat kötelező és nem kötelező elemeit, előfeltételeit (csatolt dokumentációk, teszt jegyzőkönyvek, stb.);
   c) meghatározza a változtatásokat, majd kockázatelemzés alapján jóváhagyja vagy elutasítja azokat;
   d) dokumentálja az elektronikus információs rendszerben történt változtatásokra vonatkozó döntéseket;
   e) megvalósítja a jóváhagyott változtatásokat az elektronikus információs rendszerben;

f) visszakereshetően megőrzi az elektronikus információs rendszerben megvalósított változtatások dokumentumait, részletes leírását (pl.: jegykezelőrendszer segítségével);
g) auditálja és felülvizsgálja a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket;
h) beépíti a folyamatba a megfelelő jóváhagyási folyamatot (üzleti, technikai jóváhagyás, információbiztonsági jóváhagyás).

VI.6.7.1 Előzetes tesztelés és megerősítés (3.3.6.3.2. [4])

(1) A konfiguráció megváltoztatása előtt az új verziót tesztelni kell, ezután dönteni kell annak megfelelőségéről, továbbá dokumentálni kell az elektronikus információs rendszer változtatásait az éles rendszerben történő megvalósítása előtt. A tesztelés a konfiguráció- és változásmenedzsment egyik alapja.

(2) Az Egyetem előírja és betartatja a különböző teszt típusokat (IT, felhasználói, regressziós stb.). Pontos és részletes dokumentációs követelményeket állít fel a teszteléssel kapcsolatban. A teszteredményeket és azok jóváhagyását visszakereshetően dokumentáltatja (pl. jegykezelőben vagy más repository-ban)

VI.6.7.2 Változáskezelés alapvető szabályai

(1) A változástatások dokumentálás, visszakereshetősége.

(2) Automatikus megoldások használata a változások dokumentálására, jogosultak értesítésére, végrehajtott változások teljes dokumentálására.

(3) Az Egyetem workflow alapú szoftveres megoldást használ (jegykezelő rendszer) a tesztelés és a változáskezelés támogatásához.

VI.6.8. Biztonsági hatásvizsgálat (3.3.6.4. [3])

(1) Az Egyetem megvizsgálja az elektronikus információs rendszerben tervezett változtatásoknak az információbiztonságra való hatását, még a változtatások megvalósítása előtt.

(2) Az Egyetem a változtatásokat éles rendszerben történő megvalósításuk előtt egy elkülönített tesztkörnyezetben vizsgálja, hibákat, sebezhetőségeket, kompatibilitási problémákat és szándékos károkozásra utaló jeleket keresve.

(3) Az Egyetem a változáskezelés folyamatába építi az információbiztonsági ellenőrzést az alábbi módon:
a) a tervezés során meghatározza mely esetekben kell bevonni információbiztonsági szakértőt, (aki lehet az IBF vagy a delegáltja);
b) biztosítani kell a hatásvizsgálat szekértő módon történő elvégzését.

VI.6.9. A változtatásokra vonatkozó hozzáférés korlátozások (3.3.6.5. [4])

(1) Az Egyetem elektronikus információs rendszerei bármely elemének változtatása csak arra jogosult felhasználó - adminisztrátor, rendszergazda - által elvégezhető.

(2) Az Egyetem az elektronikus információs rendszerre vonatkozóan, szabályozásban meghatározza a változtatásokhoz való hozzáférési jogosultságot, dokumentálja a hozzáférési jogosultságokat,

jóváhagyja azokat, fizikai és logikai hozzáférés korlátozásokat alkalmaz az elektronikus információs rendszer változtatásaival kapcsolatban.

(3) Az Egyetem változásmenedzsment szoftvert alkalmaz, amely kezeli a verzióváltás folyamatát. A változásmenedzsment szoftver időben korlátozza és jóváhagyáshoz, kiemelt jogosultsághoz köti a változásokat.

(4) Az elektronikus információs rendszer automatikus mechanizmust, dokumentálást lehetővé tevő megoldást alkalmaz a hozzáférés menedzsmentben történő változások pontos nyomon követesére és adminisztrálására.

VI.6.10. Új konfiguráció éles üzembeállása

(1) Új konfigurációt csak elkülönített teszt környezetben történő sikeresnek minősített teszt után lehet éles üzembe állítani. A tesztet és éles üzembeállítást dokumentálni szükséges, verziószám, teszt dátum, tesztelő/minősítő neve, éles üzembeállítás dátuma, üzembeállító neve adattartalommal.

VI.6.11. A működő rendszer konfiguráció figyelése

(1) Az Egyetem meghatározott gyakorisággal átvizsgálja az elektronikus információs rendszert, meghatározza és kizárja, vagy letiltja a szükségtelen vagy nem biztonságos funkciókat, portokat, protokollokat és szolgáltatásokat.
(2) A jogosulatlan hardver-, szoftver- és firmware elemek észlelését automatizált mechanizmusok biztosítják.

VI.6.12. Konfigurációs beállítások (3.3.6.6. [3])

(1) Az Egyetem figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait, az Egyetem belső szabályzataival és eljárásaival összhangban.

(2) Az Egyetem dokumentálja a működési követelményeknek még megfelelő, de biztonsági szempontból a lehető leginkább korlátozott módon az IT eszközökre a kötelező konfigurációs beállításokat és azokat naprakészen tartja.

VI.6.13. Legszűkebb funkcionalitás (3.3.6.7. [3])

(1) Az Egyetem meghatározza a működési követelményeknek még megfelelő, de biztonsági szempontból a lehető leginkább korlátozott módon - a „szükséges minimum” elv alapján - az elektronikus információs rendszerben használt információtechnológiai termékekre kötelező konfigurációs beállítást, és ezt ellenőrzési listaként dokumentálja:
    a) kizárólag az előre engedélyezett alkalmazások futásának biztosítása;
    b) nem feltétlenül szükséges USB és egyéb külső adatbeviteli pontok és portok tiltása;
    c) kommunikációs csatorna tatalmára vonatkozó szűrés beállítása;
    d) Az eszközök, rendszerek konfigurációja csak a szükséges szolgáltatások nyújtására legyen elegendő, minden ezekhez nem szükséges funkció tiltva legyen.

(2) Az elektronikus információs rendszerekben az egyes ügyintézői szinteken csak az általa végzett tevékenységhez nélkülözhetetlen funkciók legyenek engedélyezve, csak az engedélyezett menüpontok jelenjenek meg a képernyőjén.

VI.6.20.1 Rendszeres felülvizsgálat (3.3.6.7.2. [4])

(1) Az Egyetem meghatározott gyakorisággal átvizsgálja az elektronikus információs rendszert, meghatározza és kizárja, vagy letiltja a szükségtelen vagy nem biztonságos funkciókat, portokat, protokollokat és szolgáltatásokat.

(2) Az Egyetem irodai hálózati végponton futó szoftvereket, nyitott portokat, USB portokat és egyéb hardveres vagy szoftveres kommunikációs pontokat ellenőrzi, hiba esetén a szükséges lépéseket (zárás, tiltás) megteszi.

(3) Az elektronikus információs rendszerek egyes ügyintézői szinteken elérhető funkcióit is rendszeresen felülvizsgálja.

VI.6.20.2 Nem futtatható szoftverek (3.3.6.7.3. [4])

(1) Az Egyetem meghatározza, rendszeresen felülvizsgálja és frissíti az elektronikus információs rendszerben nem futtatható (tiltott, úgynevezett feketelistás) szoftverek listáját, és megtiltja ezek futtatását.

(2) A beállítások alapján előre tiltásra került elemek pl.: torrent kliensek, freeware szoftverek, gyanúsnak és veszélyesnek ítélt egyéb alkalmazások adatbázisának folyamatos felülvizsgálata és frissítése.

(3) Az explicit tiltott szoftverek listája, rendszeresen frissítve van.

VI.6.14. Elektronikus információs rendszerelem leltár (3.3.6.8. [2], 3.3.6.8.2. [4])

(1) Az Egyetem leltárt készít az elektronikus információs rendszer elemeiről, meghatározott gyakorisággal felülvizsgálja és frissíti azt.

(2) Gondoskodik arról, hogy a leltár:
   a) pontosan tükrözze az elektronikus információs rendszer aktuális állapotát;
   b) az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmazza;
   c) legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez.

(3) A rendszerelem leltárban az összes hardver és szoftver komponens szerepel. A leltár formáját tekintve egy Excel fájl is megfelelő, amelyben szerepeltethető a frissítés, követhető módon a meghatározott gyakorisággal elvégezve.

VI.6.15. Konfigurációkezelési terv (3.3.6.9. [4])

(1) Az Egyetem:
   a) kialakít, dokumentál és végrehajt egy, az elektronikus információs rendszerre vonatkozó konfigurációkezelési tervet, mely figyelembe veszi a szerepköröket, felelősségeket, konfigurációkezelési folyamatokat és eljárásokat;
   b) Meghatározza az elektronikus információs rendszer konfigurációelemeit, és a konfigurációelemeket a konfigurációkezelés alá helyezi;
   c) Védi a konfigurációkezelési tervet a jogosulatlan felfedéssel és módosítással szemben.

(2) A konfigurációkezelési terv elkészítésének, karbantartásának felelőseit az Egyetem úgy választja ki, hogy a felelősök ne legyen közvetlenül a rendszer fejlesztésében is érintettek, ezáltal biztosítva hogy az Egyetem megfelelő szintű függetlenséget tartson fenn az elektronikus információs rendszer

fejlesztési és integrációs, valamint konfigurációkezelési folyamatai között. Ezáltal megfelelő minőségellenőrzés és hatékony felügyelet valósulhat meg az adott rendszerre.

VI.6.16. A szoftverhasználat korlátozásai (3.3.6.10. [2])

(1) Az Egyetem kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a rájuk vonatkozó szerződés béli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak.

(2) A másolatok, megosztások nyomon követésével megakadályozza, hogy a szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására kerüljön.

(3) Az Egyetem olyan szoftvereket és dokumentációkat használ, amelyek megfelelnek a rájuk vonatkozó szerződésben foglalt elvárásoknak, szerzői jogi vagy más jogszabályoknak.

(4) A telepítések végrehajtása adminisztráció köteles (végpont, felhasználó, felhasznált licencek), ezzel biztosítva a mennyiségi licencekkel védett szoftverek nyomon követését.

VI.7 Karbantartás (3.3.7.)

(1) Az Egyetem megfogalmazza, és az Egyetemre érvényes követelmények szerint dokumentálja, valamint az Egyetemen belül kihirdeti a ***„rendszer karbantartási eljárásrendet”***, mely tartalmazza a rendszer karbantartási kezelés folyamatát és elősegíti az ahhoz kapcsolódó ellenőrzések megvalósítását.

VI.7.1. Távoli karbantartás (3.3.7.4. [4])

(1) Távoli karbantartás esetén az Egyetem a folyamat minden szakaszában ellenőrzi és dokumentálja a tevékenységet, jóváhagyja a használt eszközöket, amennyiben azok megfelelnek az IBSZ-bem előírtaknak. Az egyes munkaszakaszoknál szoftveres hitelesítést alkalmaz, valamint a tevékenység befejezése után lezárja az adott hálózati kapcsolatot így megszüntetve a külső bejárhatóságot.

(2) A távoli karbantartási feladatokhoz dedikált virtuális végpont (jump host) valamint karbantartási folyamatot láthatóvá és rögzíthetővé tevő szoftveres naplózó - lehetőség szerint vizuális rögzítést is végző - alkalmazást, valamint erős hitelesítés alkalmazást használ (pl. kétfaktoros autentikáció használata: jelszó és SMS kód, authentikator által generált belépési kód).

VI.7.2. Karbantartók (3.2.1.19. [3])

(1) Az Egyetem ellenőrzi, hogy a karbantartást csak a szerződésben meghatározott karbantartói listán szereplő személyek végezhessék el. A karbantartók számára az Egyetem ismerteti az információbiztonsági előírásokat, azok be nem tartására vonatkozó következményeket a szerződésben rögzíti.

VI.8 Adathordozók védelme (3.3.8. [4])

(1) Az adathordozókon tárolt adatokat egyaránt védeni kell a jogosulatlan megismeréstől, módosítástól és megsemmisüléstől. Az adatok védelmét az adathordozók megfelelően biztonságos kezelésével, a szükséges technikai kontrollok és eljárások kialakításával kell biztosítani.

(2) Az Egyetem megfogalmazza, dokumentálja, kihirdeti az ***„adathordozók védelmére vonatkozó eljárásrendet”***, mely az adathordozókra vonatkozó védelmi szabályok és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő.

(3) A ***„Mobil eszközök használatának eljárásrendje”*** szabályozza az alábbiakat:
a) tartalmazza a felelősöket, jóváhagyókat,
b) megfogalmazza az adathordozókkal kapcsolatos elvárásait, mint:
- azok nyilvántartását,
- igénylésének,
- titkosításának,
- szállításának,
- selejtezésének,
- törlésének folyamatát

c) kitér a felhő alapú adattárolásra (tiltja a nem jóváhagyott felhő alapú tárolást)
d) szabályozza a fizikai és elektronikus címkézési szabályokat.

(4) Cserélhető adathordozónak tekintendő jelen szabályzat szempontjából valamennyi, az asztali számítógépbe, szerverbe, hálózati eszközbe, irodatechnikai eszközbe rögzítetten beépített adathordozókon kívüli adathordozó. (pl. flash disk, USB pendrive, memóriakártya, hordozható HDD és SSD)

(5) Az Egyetem által kezelt adatok tárolására és szállítására csak az Egyetem tulajdonában vagy kizárólagos használatában álló, és nyilvántartásában szereplő cserélhető adathordozók használhatóak. Az Egyetem adathordozóin csak a munkavégzéshez szükséges adatokat lehet tárolni.

(6) A felhasználók saját tulajdonú adathordozóikat, amennyiben az a munkakörhöz kapcsolatosan indokolt, az informatikai hálózatra csak vírus ellenőrzés külső adathordozóra lefuttatása után csatlakoztathatják.

(7) A munkaasztalokon csak a munkavégzéshez használatos adathordozók lehetnek, amit minden munkavállaló köteles rendeltetésszerűen, csak a munkakörével kapcsolatos adattartalom tárolására és körültekintő védelem mellett használni.

(8) Cserélhető adathordozón jogszabály által védeni rendelt adat, kizárólag titkosítást követően lehet tárolva.

(9) Tilos az adathordozó használatával a védendő adatokat otthoni munkavégzés céljából otthoni számítógépre vagy egyéb, nem az Egyetem tulajdonát képező számítógépekre vagy egyéb eszközökre engedély nélkül felmásolni, az adathordozó tartalmáról másolatot készíteni.

VI.8.1. Hozzáférés az adathordozókhoz (3.3.8.2. [2], 3.3.8.7. [2])

(1) Az Egyetem meghatározza, az egyes adathordozó típusokat és meghatározza az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, jogosítványuk tartalmát.

(2) Az Egyetem meghatározza, hogy az adathordozókat (mind digitális: hordozható merevlemez, pendrive, memóriakártya, CD stb., mind analóg: papír) csak az használhat, akinek a feladatköre megkívánja és azt írásban jóváhagyták neki (praktikusan a felettese, IT vezető).

(3) Az Egyetem kialakít egy mátrixot, ami tartalmazza, hogy az egyes adathordozó típusokat mely munkakörben használhatják.

VI.8.2. Adathordozók címkézése (3.3.8.3. [4])

(1) A használatba vett adathordozókat fel kell címkézni annak érdekében, hogy annak esetleges nyilvánosságra hozatali módja, kezelésének módszertana, esetleges biztonsági besorolása azonosítható legyen, oly módon, hogy az összhangban legyen a klasszifikációval (pl. bizalmas, publikus feliratokkal).

(2) Az Egyetem megjelöli az elektronikus információs rendszer adathordozóit, jelezve az információra vonatkozó terjesztési korlátozásokat, kezelési figyelmeztetéseket és a megfelelő biztonsági jelzéseket, ha ezek rendelkezésre állnak.

VI.8.3. Az adathordozók tárolása (3.3.8.4. [4])

(1) Az Egyetem fizikailag ellenőrzi és biztonságosan tárolja az adathordozókat, az arra engedélyezett vagy kijelölt helyen.

(2) Védi az elektronikus információs rendszer adathordozóit mindaddig, amíg az adathordozókat jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy nem törlik.

(3) A munkavállaló a használt adathordozót munkanap végén elzárja a szekrényébe, nem hagyja elől.

(4) A rendszergazda az adathordozókat egy zárható szekrényben tárolja, amihez csak a szükséges személyeknek van kulcsa rajta kívül (pl. információbiztonságért felelős személy). A szekrényben elkülönítve kerülnek tárolásra a még nyilvántartásba nem vett új eszközök, a nyilvántartásban lévő eszközök és a törlendő tartalmú eszközök.

VI.8.4. Adathordozók szállítása (3.3.8.5. [4], 3.3.8.5.2. [4])

(1) Az Egyetem meghatározott biztonsági óvintézkedésekkel védi és ellenőrzi az elektronikus információs rendszer adathordozóit az ellenőrzött területeken kívüli szállítás folyamán. Az adathordozók szállítása közben:
   a) biztonsági óvintézkedéssel védik azokat,
   b) nyilvántartással segítik az elszámolhatóságot (induláskor és érkezéskor),
   c) dokumentáció készül a szállítás pontjairól,
   d) csak arra kijelölt személyek szállíthatják az adathordozókat.

(2) Az ellenőrzött területeken kívüli szállítás folyamán, kriptográfiai mechanizmusokat kell alkalmazni a digitális adathordozókon tárolt információk bizalmasságának és sértetlenségének a védelmére.

VI.8.5. Adathordozók törlése (3.3.8.6. [2])

(1) Az Egyetem a helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törli az elektronikus információs rendszer meghatározott adathordozóit a leselejtezés, a szervezeti ellenőrzés megszűnte, vagy újrafelhasználásra való kibocsátás előtt.

(2) A törlési mechanizmusokat az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően alkalmazza.

(3) Az Egyetem felülvizsgálja, jóváhagyja, nyomon követi, dokumentálja, és ellenőrzi az adathordozók törlésével és megsemmisítésével kapcsolatos tevékenységeket.

(4) A törlésre alkalmazott eszközök és eljárások meghatározott gyakorisággal tesztelésre kerülnek.

(5) Az adathordozók törlésére olyan szoftver használt az Egyetem, amely nemzetközileg elismert „Common Criteria” (informatikai termékek és rendszerek biztonsági értékelésének módszertana/követelményrendszere) tanúsítvánnyal rendelkezik. Ez biztosítja, hogy az adattörlő szoftvert egy független fél megvizsgálta és képesnek nyilvánította az adatok végleges törlésére. A törlésre használt szoftvert az Információbiztonsági felelős jelöli ki.

(6) Azokat az adathordozókat, amelyeket nem lehet biztonságosan törölni, tilos újrafelhasználni, azokat meg kell semmisíteni.

VI.8.6. Ismeretlen tulajdonos (3.3.8.7.2. [4])

(1) Az Egyetem megtiltja olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható. Ennek érdekében pl. az Egyetem letilthatja a munkavállalók laptopjain a külső adathordozók használatát (pl. külső merevlemezt nem tudnak csatlakoztatni).

(2) A munkavállalók számára az információbiztonsági oktatóanyagban részletezni kell, hogy a "talált", gazdátlan, nem beazonosítható tulajdonosú pendrive-okat ne használják, hanem azonnal adják le a rendszergazda vagy az ISZK számára.

VI.8.7. Adathordozók újrahasznosítása

(1) Az adathordozók újrafelhasználásra való kibocsátás előtt a helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törlésre kerülnek, így védve az adatok bizalmasságát. A biztonságos törlés eredményessége minden esetben ellenőrzésre kerül.

VI.8.8. Az adathordozók selejtezése (3.3.8.6.4. [5])

(1) Adathordozók selejtezése, az Egyetem használatából történő kivonása kizárólag biztonságos adatmentesítést követően történhet, amely képes biztosítani az adatok helyreállíthatatlan törlését oly módon, hogy az adathordozón korábban tárolt adatokat, részinformációkat, töredékadatokat illetéktelenek ne ismerhessék meg.

(2) Az adatmentesítést (jegyzőkönyv formájában) dokumentálni szükséges, ami megfelelő szoftver alkalmazásával elektronikus formában is előállhat.

(3) Az Egyetem fizikai helyszíneiről a selejtezés/tovább értékesítés során kizárólag olyan adathordozó kerülhet ki, amely adatokat nem tartalmaz. Fontos, hogy megfelelő dokumentációval utólag is bizonyíthatónak kell lennie annak, hogy amikor az érintett adathordozó elhagyta az Egyetem területét, adatokat már nem tartalmazott.

(4) Az adatmentesítésben az ISZK legalább két munkatársának kell részt vennie, egyik magát a törlést, a másik annak ellenőrzését végzi (4 szem elve). Az adatmentesítés elvégzéséről, eredményéről az ISZK felveszi a jegyzőkönyvet, és tájékoztatja az IBF-et.

VI.8.9. Adathordozók megsemmisítése (3.3.8.1. [2])

(1) Az adathordozók fizikai roncsolással kerülnek megsemmisítésre, amelyet követően azok további felhasználása már nem lehetséges.

(2) Nagyteljesítményű adathordozók esetében figyelemmel kell lenni a technológia szerinti sűrű felületi írásra, mert amennyiben az „átfúrásos" módszert alkalmazzuk, ebben az esetben az alkalmazott egy „átfúrásos" alkalmatlanná tétel nem bizonyul elégségesnek, mivel így még az információk nagy hányada visszanyerhető.

(3) Információvédelmi szempontokat figyelembe véve hatékonynak tekinthető a több „átfúrásos" módszer és a zárt láncú megsemmisítési folyamat.

VI.9 Azonosítás és hitelesítés (3.3.9.)

(1) Az Egyetem elektronikus információs rendszerei egyedileg azonosítják és hitelesítik az Egyetem jogosult felhasználóit, a felhasználók által végzett tevékenységet.

(2) Az Egyetem ehhez megfogalmazza, dokumentálja, kihirdeti az ***„azonosítási és hitelesítési eljárásrendet"***, mely az azonosítási és hitelesítési folyamat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. Az azonosítás és hitelesítés eljárásrend magába foglalja:

a) Felhasználói fiókok létrehozása, kezelése,
b) Hozzáférés ellenőrzése,
c) Azonosítási elvárások (jelszavak, multifaktoros autentikáció, kriptográfia),
d) Hitelesítési eljárások,
e) Privilegizált felhasználókra vonatkozó szabályok,
f) Helyi-, hálózati-, távoli hozzáférések szabályozása.

(3) Az Egyetem az eljárásrendet elérhetővé teszi a munkavállalói számára. Új belépőkkel már az elektronikus információs rendszer használatbavétele előtt megismerteti annak tartalmát. Az eljárásrend kétévente kerül felülvizsgálatra, kritikus rendszerek esetében, évente, biztonsági esemény, incidens bekövetkezése esetében, azonnali eljárással.

VI. 9.1. A felhasználók azonosítása (3.3.9.2. [2])

(1) Az Egyetem elektronikus információs rendszerei egyedileg azonosítja és hitelesíti a felhasználót.

VI.9.1.1 Felhasználói azonosítókkal szemben támasztott követelmények

(1) Minden felhasználóhoz egyedi azonosítót (felhasználónevet) kell rendelni. A felhasználónak egyedi felhasználónévvel és jelszóval kell rendelkeznie a központi hálózati és operációs rendszerekhez, felhasználói szoftverekhez és adatbázisokhoz.

(2) A névre szóló azonosítót másnak átadni tilos. Minden személy, aki az Egyetem informatikai rendszereiben azonosítóval rendelkezik, felelősséggel tartozik és felel valamennyi, az érintett azonosítóval végzett tevékenységért, függetlenül attól, hogy azzal ténylegesen ki végzett műveletet.

VI.9.1.2 A felhasználói azonosítók képzésének és kezelésének szabályai

(1) Felhasználói azonosító képzés:
   a) felhasználó név (Szabálya: a felhasználó neve, ponttal/pontokkal elválasztva. Amennyiben már van ilyen nevű felhasználó a rendszerben, sorszámmal, munkaszervezeti egység rövid logikai nevével van kiegészítve)
   b) alap jelszó (ami eleget tesz az Egyetemi jelszóerősség kritériumnak és az első bejelentkezéskor kötelező megváltoztatni)

A felhasználói azonosítók visszavonásig, lejáratig vagy újrahitelesítésig érvényesek.

VI.9.1.3 Felhasználói azonosítók nyilvántartása

(1) A felhasználói jogosultságok kiadása, módosítása és visszavonása dokumentált eljárások alapján történik.

(2) A kiosztott felhasználói azonosító és jogosultság, felhasználói jogosultságkezelő rendszerben (felhasználói jogosultság mátrix) van nyilvántartva, aktuálisan kezelve. Kezelő szervezet: ISZK, koordináció: IBF.

VI. 9.2. Felhasználók hitelesítése (3.3.9.2. [2])

(1) Az Egyetem elektronikus információs rendszerei tudás alapú (jelszó) hitelesítést használnak a felhasználók azonosítására. A hitelesítési adat forrásai:
   a) LDAP (címtár alapú felhasználó hitelesítés)
   b) Active Directory (tartomány (domain) vezérelt felhasználó kezelés)
   c) szoftver rendszer adatbázisa (ORACLE, SQL)
   d) Active Directory LDAP azonosítással

(2) A fizikai védelmi megoldások (beléptetés) birtoklásalapú (kártya) hitelesítéssel üzemelnek.

VI. 9.2.1. A hitelesítők képzéseinek és használatuknak szabályai

(1) A felhasználói jelszavak képzésére a következő szabályokat kell alkalmazni:
   a) A felhasználónak kötelezően alá kell írnia egy nyilatkozatot, melyben felelősséget vállal jelszavai bizalmas kezelésére.
   b) Belépéskor megkapott ideiglenes jelszó átadása csak biztonságos csatornán történhet, a felhasználó előzetes azonosítása után. Az ideiglenes jelszavak véletlenszerűen generáltak, csak 1 napig lehetnek érvényesek, megváltoztatásuk kötelező.

c) Technikai felhasználók, valamint beépített (privilegizált) felhasználók jelszavait oly módon kell tárolni, hogy csak arra felhatalmazottak férhessenek hozzá, illetve a hozzáférések naplózottak legyenek.
d) Amennyiben egy technikai felhasználói fiókhoz többen is hozzáférnek és a hozzáféréshez jogosultak listája változik, a csoport felhasználói fiókokhoz tartozó hitelesítő eszközöket vagy adatokat újra ki kell bocsátani.
e) Jelszó alapú hitelesítő rendszer használata esetén a jelszavakat cserélni kell minden esetben, ha kompromittálódnak, vagy illetéktelen személy birtokába jutnak.

VI. 9.2.2. A hitelesítés kezelése az informatikai rendszerekben (3.3.9.5.2 [4])

(1) Az Egyetem elektronikus információs rendszereibe csak a felhasználó hitelesítésére használt belépési adatok (felhasználó név és jelszó páros) teljes azonosságát követően lehet belépni.

(2) A belépett felhasználó rendszer hozzáférési szintjei, erőforrások használata a rendszerben beállított jogosultsági szint szerint érvényesül.

(3) A rendszerek meghatározott időszakonként kötelező jelszóváltoztatást kényszerítenek ki.

VI. 9.2.3. Felhasználói tanúsítványhordozó eszközök nyilvántartása

(1) Az Egyetemen használt tanúsítványhordozó eszközök, mint az UNIPASS egyetemi kártya az UNIPASS Kártyamenedzsment Központ és az elektronikus aláírást hitelesítő kártya naprakész nyilvántartása az Informatikai Biztonsági Központ gondozásában történik.

(2) Felhasználói tanúsítványhordozó eszközöknek kell tekinteni az EESZT (Elektronikus Egészségügyi Szolgáltatási Tér) információs portál felület elérését támogató elektronikus személyi igazolványt (e-SZIG) is.

(3) A nyilvántartás ebben az esetben az e-Személyi olvasók vonatkozásában releváns, amik leltári tárgyként a munkaszervezet leltári nyilvántartásában, összesítve központilag digitális formában, a használati terület, hely, iroda, rendelő feltüntetésével, az ISZK felelős vezetőjénél vannak.

VI. 9.2.4. Hitelesítésre szolgáló eszközök kezelése (3.3.9.5.3. [4])

(1) A hitelesítésre szolgáló eszközök a jogviszony fennállása alatt használhatók, azokat munkaviszony megszűnését követően az eszközhöz hozzárendelt jogosultság megszüntetésével vissza kell venni.

VI. 9.2.5. Speciális felhasználókhoz tartozó jelszavak kezelése

(1) Speciális felhasználó a kiemelt hozzáférési jogot birtokló felhasználó.

(2) Kiemelt hozzáférési jogok alatt a rendszergazdai hozzáférést kell érteni.

(3) Az operációs rendszerek, adatbázisok és alkalmazások adminisztrátori hozzáférését - az üzletmenet folytonosság fenntartásának figyelembe vételével - a lehető legkevesebb személyhez kell hozzárendelni.
(4) A kiemelt hozzáférési jogkörökkel rendelkező munkavállalókról az IT területek vezetőinek nyilvántartást szükséges készíteni, és azt rendszeresen felül kell vizsgálniuk.

(5) Informatikai biztonsági kockázatot jelent a „Kiemelt hozzáférési joggal” rendelkező dolgozó munkaviszonyának megszűnése.

(6) A rendszergazda hozzáférések (rendszer- és adatbázis hozzáférési jelszavak) „tudása” illetve „átruházása” komoly informatikai incidensveszélyt hordoz magában, így ilyen esetekben azt meg kell változtatni, melynek felelőse az informatikai üzemeltetési szervezetek vezetői.

(7) A nyilvántartás meglétének, aktualizáltságának időszakonkénti ellenőrzése az IBF feladata.

(8) A kiemelt hozzáférések jelszavát vezetői pecséttel ellátott borítékban, és olyan zárt helyen kell tárolni, aminek kulcsa csak illetékes vezető birtokában van.

(9) Beépített adminisztrátori fiókok, technikai felhasználók jelszavait olyan jelszókezelő alkalmazásban kell tárolni, ami a hozzáféréseket naplózza.

VI. 9.2.6. Jelszó (tudás) alapú hitelesítés (3.3.9.5.2. [4])

(1) Az Egyetem a jelszavak erősségére elvárásokat fogalmaz meg, amit minden olyan ponton érvényesíteni kell, ahol a felhasználó új jelszavának vizsgálata történik (0. jelszóra is vonatkozó elvárás).

(2) Az Egyetem a jelszóra elvárásokat alakít ki a következők figyelembevételével:
   a) kis- és nagybetűk megkülönböztetése;
   b) a karakterek számának meghatározása;
   c) a kisbetűk, nagybetűk, számok és speciális karakterek, és
   d) minimális jelszóhosszúság;
   e) új jelszó létrehozásánál a felhasználótól megköveteli, hogy bizonyos karakterszámmal különbözzön az előző jelszótól az új jelszava;
   f) nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hasító érték tárolást), vagy továbbítja a jelszavakat;
   g) a jelszavak élettartamát meghatározza;
   h) megtiltja a jelszavak ismételt felhasználását meghatározott számú új jelszóig;
   i) rendszerbe első belépés során az ideiglenes jelszót kötelezően lecseréltteti.

(3) Speciális felhasználók (rendszergazdák) jelszó követelménye szigorúbb feltételek alá tartozik, így:
   a) a rendszergazdák jelszavát rendszeresen cserélni kell;
   b) a rendszergazda jelszavak minimum 12 karakterből álljanak;
   c) rendszergazda esetében 3 próbálkozás után zárolja az azonosítót;
   d) rendszergazda munkaviszonyának megszűnése esetén azonnali jelszóváltoztatás szükséges;
   e) technikai felhasználói jelszavak gyakori felülvizsgálata.

VI. 9.2.7. Birtoklás alapú hitelesítés (3.3.9.5.3. [4])

(1) Az Egyetem, birtoklás alapú hitelesítést alkalmazhat, amikor is a felhasználó egy hitelesítésre használható eszköz (token, PKI -Public Key Infrastructure- chip kártya) használatával kap jogosultságot.

VI. 9.2.8. Tulajdonság alapú hitelesítés (3.3.9.5.4. [4])

(1) Az Egyetem tulajdonság alapú hitelesítést is alkalmazhat, ami a felhasználó valamilyen egyedi, csak rá jellemző tulajdonsággal azonosítja magát. Ilyen azonosítási eszköz a biometrikus azonosító, pl.

ujjlenyomat, írisz szkenner, arcfelismerés stb., illetve ezek kombinációja. Pl.: A munkavállaló laptopjára az ujjlenyomat olvasó segítségével jelentkezik be.

VI. 9.3. Felhasználói fiókok kezelése (3.3.10.2. [2])

(1) Annak érdekében, hogy átlátható legyen az egyes rendszerekhez ki és milyen jogosultsággal fér hozzá, az Egyetem:

a) meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait és ezek típusait;
b) kijelöli a felhasználói fiókok fiókkezelőit;
c) kialakítja a csoport- és szerepkör tagsági feltételeket;
d) meghatározza az elektronikus információs rendszer jogosult felhasználóit, a csoport- és szerepkör tagságot és a hozzáférési jogosultságokat, valamint (szükség esetén) az egyes felhasználói fiókok további jellemzőit;
e) létrehozza, engedélyezi, módosítja, letiltja, és eltávolítja a felhasználói fiókokat a meghatározott eljárásokkal vagy feltételekkel összhangban;
f) ellenőrzi a felhasználói fiókok használatát;
g) értesíti a fiókkezelőket, ha:
   - a felhasználói fiókokra már nincsen szükség,
   - a felhasználók kiléptek vagy áthelyezésre kerültek,
   - az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak;
h) feljogosít az elektronikus információs rendszerhez való hozzáférésre:
   - az érvényes hozzáférési engedély,
   - a tervezett rendszerhasználat,
   - az alapfeladatok és funkcióik alapján;
i) meghatározott gyakorisággal felülvizsgálja a felhasználói fiókokat, a fiókkezelési követelményekkel való összhangot;
j) kialakít egy folyamatot a megosztott vagy csoport felhasználói fiókokhoz tartozó hitelesítő eszközök vagy adatok újra kibocsátására (ha ilyet alkalmaznak), a csoport tagjainak változása esetére.

VI.9.3.1 Személyes vagy megbízható harmadik fél általi regisztráció (3.3.9.5.5. [4])

(1) Az Egyetem meghatározott hitelesítő eszköz átvételéhez megkövetel egy olyan regisztrációs eljárást, melyet meghatározott regisztrációs szervezet folytat le az Egyetem által meghatározott személyek vagy szerepkörök jóváhagyása mellett.

(2) Hitelesítésre szolgáló eszközt az Egyetem csak megfelelő jóváhagyás után ad ki.

VI.9.3.2 Sikertelen bejelentkezési kísérletek (3.3.10.7. [3])

(1) Az elektronikus információs rendszer az Egyetem által meghatározott esetszám korlátot alkalmaz, a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire.

(2) Ha a sikertelen bejelentkezési kísérletekre meghatározott esetszám korlátot a felhasználó túllépi, automatikusan zárolja a felhasználói fiókot, vagy csomópontot meghatározott időtartamig, vagy meghatározott módon késlelteti a következő bejelentkezési kísérletet.

(3) A sikertelen kísérletek szubjektív (fáradság, figyelmetlenség –pl. CapsLock billentyű aktív-) tényezőkön túl utalhatnak illetéktelen kísérletekre is, ezért a naplóállományok manuálisan, de célravezetőbb módon automatikus vizsgálattal, nagyobb gyakorisággal vizsgálni szükséges, a prevenció érdekében.

VI. 9.4. Hálózati hozzáférés

(1) Az Egyetem elektronikus információs rendszeri számára, adatai, információi bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése céljából, megbízható és kellő gondossággal védett belső hálózati kapcsolatokat fenntartani, biztosítani.

(2) E tekintetben az információvédelem szempontjából csak a belső hálózat minősíthető megbízható hálózatnak, minden egyéb kapcsolatot, külső hálózat elérést úgy kell értékelni, és kezelni, hogy az potenciális biztonsági veszélyforrás lehet.

(3) A védelem legmagasabb prioritású pontja az Egyetem tűzfala.

(4) A tűzfal konfigurációja során gondoskodni kell arról, hogy csak az engedélyezett kapcsolati lehetőségek, protokollok, portok legyenek elérhetők. Az engedélyezett kapcsolati lehetőségek listáját ACL-ek (Access Control List) formájában kell nyilvántartani.

(5) Minden „külvilági” kapcsolat (adatcsere, adatátvitel, adatfeltöltés) csak az Egyetem tűzfalán keresztül kommunikálhat.

(6) Az elektronikus információs rendszerek elérésére, használatára csak megbízható hálózati működést biztosító számítógépek, mobil eszközök használhatók.

(7) Megbízható eszköznek, csak az Egyetem illetékes informatikai szakemberei által konfigurált eszköz minősíthető, ami az Egyetemi egyik hálózati tartományába (VLAN) van konfigurálva, lehetőleg tartományvezérelt (Active Directory) felhasználó kezelést biztosít és naprakész vírusvédelmi megoldás van telepítve.

VI.9.4.1 Hálózati hozzáférés privilegizált fiókokhoz (3.3.9.2.2. [3])

(1) A privilegizált fiókok feltörése az üzleti tevékenységet működtető érzékeny információkhoz adnak hozzáférést. Jelszavas védelmük kiemelt figyelmet érdemel.

(2) Az Egyetem multi faktoros (több lépcsős) autentikációt használ a privilegizált (rendszergazda, adminisztrátor) fiókok hozzáféréséhez.

(3) Az Egyetemen belül minden privilegizált fiókot ismerni (ha szükséges, felderíteni) kell, mert azok védelem nélkül nem maradhatnak, biztonsági kockázat hordozói.

VI.9.4.2 Hálózati hozzáférés nem privilegizált fiókokhoz (3.3.9.2.3. [4])

(1) Az Egyetem multi faktoros (több lépcsős) autentikációt használ a nem privilegizált fiókok hozzáféréséhez.

VI. 9.5. Helyi hozzáférés

(1) Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a fiókok helyi hozzáféréshez.

VI. 9.5. 1. Helyi hozzáférés privilegizált fiókokhoz (3.3.9.2.4. [4])

(1) Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a privilegizált felhasználói fiókokhoz való helyi hozzáféréshez.

VI. 9.6. Ellenőrzés

(1) Az Egyetem legalább évente, biztonsági esemény vagy incidens esetén azonnal felülvizsgálja a privilegizált fiókok hozzáférését.

(2) A felülvizsgálat részét kell képeznie a VPN kapcsolatok hozzáféréseinek is.

VI. 9.7. A hitelesítésre szolgáló eszköz visszacsatolása (3.3.9.6. [2])

(1) Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a felhasználói fiókokhoz való távoli hozzáféréshez, és az egyik hozzáférést megelőző tényező egy, az elektronikus információs rendszertől elkülönülő olyan eszköz, amelyen a meghatározott biztonsági követelmények teljesülnek.

(2) Hitelesítés során az elektronikus információs rendszer fedett visszacsatolást biztosít, hogy megvédje a hitelesítés során továbbított információkat az esetleges felfedéstől.

(3) A elektronikus információs rendszer és a hitelesítő eszköz biztosítja a bizalmasságot:
   a) nem látszódhatnak jelszavak a képernyőkön (pl. csak * a jelszó helyett);
   b) amennyiben sikertelen a bejelentkezés, limitált információt oszt meg a sikertelenség miértjéről (nem informál arról, hogy miért hibás a jelszó, csak annyit hogy "sikertelen belépés", illetve nem ad információ arról, hogy a felhasználónév vagy a jelszó nem megfelelő-e).

VI. 9.8. Hitelesítés kriptográfiai modul esetén (3.3.9.7. [3])

(1) Az elektronikus információs rendszer egy adott kriptográfiai (információnak illetéktelenek előli elrejtése) modulhoz való hitelesítésre olyan mechanizmusokat használ, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának.

(2) A HSM eszközön tárolt kulcsok csak a gyártói kézikönyve által előírt hitelesítési mechanizmus által hozzáférhetőek.

VI. 9.9. Azonosítás és hitelesítés (Egyetem kívüli felhasználók) (3.3.9.8. [2])

(1) Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti az Egyetemen kívüli felhasználókat és tevékenységüket.

(2) Az Egyetemen kívüli felhasználók egyedi felhasználónevet és jelszót kapnak az elektronikus információs rendszerekhez.

VI. 9.10. Hitelesítés szolgáltatók tanúsítványának elfogadása (3.3.9.8.2. [2])

(1) Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság (NMHH) elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat fogadhatja el az Egyetemen kívüli felhasználók hitelesítéséhez.

(2) Az Egyetem az Egyetemen kívüli felhasználókat csak olyan módszerekkel azonosítja és hitelesíti, ami az NMHH elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatótól származik.

VI.10 Hozzáférés az informatikai rendszerekhez (3.3.10., 3.3.10.1. [2])

(1) Az Egyetem megfogalmazza, dokumentálja, valamint kihirdeti a „***hozzáférés ellenőrzési eljárásrendet”***, mely a hozzáférés ellenőrzési eljárás és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

(2) Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

VI. 10.1. Általános alapelvek

(1) Annak érdekében, hogy átlátható legyen az egyes rendszerekhez ki és milyen jogosultsággal fér hozzá, az Egyetemnek ki kell alakítania az elektronikus információs rendszer felhasználói fiókjait és típusait, valamint az ellenőrzésre vonatkozó lépéseket.

(2) Az Egyetem ezért meghatározza az alábbiakat:
   a) meghatározza / felméri az elektronikus információs rendszer felhasználói típusait, fiókjait;
   b) dokumentálja az adott rendszerekhez milyen típusú felhasználói fiókok elérhetőek és azok milyen jogosultságot jelentenek;
   c) folyamatosan ellenőrzi az egyes felhasználói fiókok használatát, valamint értesíti a felhasználói fiók kezeléséért felelős személyt a fiókváltozásokról;
   d) meghatározza, hogy mely szerepkörök férhetnek hozzá mely fiókokhoz;
   e) rögzíti a hozzáférés megadásának módját;
   f) érvényesíti legalább a "4-szem elvét";
   g) meghatározza a jogosultság elvételének folyamatát;
   h) kidolgozza a folyamatot a felhasználó Egyetemen belüli pozíció/munkakör váltására;
   i) rendszeresen felülvizsgálja az adott elektronikus információs rendszer felhasználói fiókjait, felhasználóit.

VI. 10.2. Hozzáférés ellenőrzés eljárásrend (3.3.10. [2])

(1) Az Egyetem megfogalmazza, az érvényes követelmények szerint dokumentálja, valamint kihirdeti a hozzáférés ellenőrzési eljárásrendet, mely a hozzáférés ellenőrzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

VI.10.2.1 Ellenőrzés informatikai rendszerekben

(1) A hozzáférési jogosultság ellenőrzése (access control) nem felhasználó azonosítás, hanem valamilyen védett objektum (számítógép, számítógép-hálózat) biztonságát szolgáló különböző védelmi eljárások összessége.

(2) A hozzáférési jogosultság feladata a számítógép erőforrásainak vagy magának a számítógépes hálózatnak illetéktelen felhasználástól való védelme.

(3) A hozzáférési jogosultság dönti el, hogy egy személynek, vagy egy a számítógépen futó eljárásnak van-e lehetősége valamilyen objektum elérésére.

(4) Az Egyetem elektronikus információs rendszereit kiszolgáló infrastruktúra tartományvezérelt formában (Active Directory) történő üzemeltetése a legjobb megoldás a felhasználóhoz rendelt erőforrás primer kiosztásához, míg az elektronikus információs rendszerben történő hozzárendelés már csak finomhangolási megoldás.

VI.10.2.2 Az operációs rendszerhez való hozzáférés ellenőrzése

(1) A munkavégzéshez elengedhetetlen, minimális felhasználói hozzáférést kell paraméterezni.

(2) Az operációs rendszerhez a felhasználó csak felhasználói fiók felügyeleti módban férhet hozzá, korlátozva ezzel olyan erőforrás eléréseket, használatot, amik nem tartoznak illetékességi körébe (pl, admin, rendszergazdai jog), munkaköri kötelmébe.

VI.10.2.3 Privilegizált fiókok (3.3.10.6.4. [4])

(1) Az Egyetem az elektronikus információs rendszer privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza.

(2) Az Egyetemen a privilegizált felhasználói fiókok, admin, karbantartói és rendszergazdai műveletekhez, tevékenységekhez használtak.

VI.10.2.4 Nem privilegizált hozzáférés a biztonsági funkciókhoz (3.3.10.6.3. [4])

(1) Az Egyetem kötelezővé teszi, hogy a szervezet meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező felhasználói a nem biztonsági funkciók használatához nem a különleges jogosultsághoz kötött – úgynevezett privilegizált - fiókjukat vagy szerepkörüket használják:
   a) egy IT adminnak vagy rendszergazdának van nem privilegizált fiókja is, amelyet nem biztonsági funkciókhoz használ;
   b) a privilegizált hozzáférést külön fiókon keresztül kapja meg a felhasználó, alapesetben nem azzal dolgozik.

VI.10.2.5 Privilegizált funkciók tiltása nem privilegizált felhasználóknak (3.3.10.6.6. [4])

(1) Az elektronikus információs rendszer megakadályozza, hogy a nem privilegizált felhasználók privilegizált funkciókat hajtsanak végre, ideértve a biztonsági ellenintézkedések kikapcsolását, megkerülését, vagy megváltoztatását. A privilegizált funkciókat csak privilegizált felhasználók érhetik el.

VI.10.2.6 Jogosult hozzáférés a biztonsági funkciókhoz (3.3.10.6.2. [4])

(1) Az Egyetem hozzáférési jogosultságokat biztosít a meghatározott biztonsági funkciókhoz és biztonságkritikus információkhoz.

(2) Az IT admin vagy Rendszergazda hozzáfér és privilegizált felhasználói fiókot kap az elektronikus információs rendszerhez.

VI.10.2.7 Legkisebb jogosultság elve (3.3.10.6.1. [4])

(1) Az elektronikus információs rendszer a legkisebb jogosultság elvét alkalmazza, azaz a felhasználók - vagy a felhasználók tevékenysége -számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi.

(2) Az Egyetem a legkisebb jogosultság elvét alkalmazza a jogosultságok kiosztásánál. A "legkisebb" ebben az esetben a "munkájához, feladatához minimálisan szükséges" jogosultságot jelenti. A felhasználónak a feladata elvégzéséhet szükséges hozzáférés van megadva. Például, ha a munkavállalónak az elektronikus információs rendszerben riportokat kell lekérnie, akkor csak olvasási jogosultsággal rendelkező felhasználót kap, nem pedig olyat, amelyikkel módosítani is tud a rendszeren, hiszen az nem szükséges a feladatához.

VI.10.2.8 A felelősségek szétválasztása (3.3.10.5. [4])

(1) Az Egyetem:
   a) szétválasztja az egyéni felelősségeket,
   b) dokumentálja az egyéni felelősségek szétválasztását,
   c) meghatározza az elektronikus információs rendszer hozzáférés jogosultságait az egyéni felelősségek szétválasztása érdekében.

(2) Az Egyetem a dokumentált, szétválasztott egyéni felelősségek alapján határozza meg az elektronikus információs rendszer hozzáférés jogosultságait.

(3) Az Egyetem készít egy összeférhetőségi mátrixot a feladatkörökről és felhasználói fiókokról, minden elektronikus információs rendszerre külön-külön.

(4) A jogosultság megadás folyamatánál figyelembe veszi, hogy "ütköző" felhasználói fiókokat ne kapjon meg ugyanazon felhasználó. Nem csak IT, hanem üzleti szempontokat is figyelembe vesz a felelősségek szétválasztásánál.

(5) Fontos kritérium hogy:
   a) a felelősségek szétválasztása során mindenképp figyelni kell arra, hogy az elektronikus információs rendszer fejlesztői ne férjenek hozzá az éles rendszerhez, csak a fejlesztésre, tesztelésre kialakított környezethez,
   b) a privilegizált jogok kiosztásánál azok, akik IT admin, admin jogosultsággal rendelkeznek, ne rendelkezzenek üzleti hozzáférési jogosultsággal.

VI. 10.3. Hálózati hozzáférés

(1) A meghatározott privilegizált parancsok hálózaton keresztüli elérését csak meghatározott üzemeltetési szükséghelyzetben lehet engedélyezni, és az ilyen hozzáférések indoklását dokumentálni kell a rendszerbiztonsági tervben.

(2) Privilegizált parancsok csak meghatározott munkaállomásokról, terminálokról, szegmensekről és IP címekről adhatóak ki, mely munkaállomások/terminálok helyiségei fizikai hozzáférés szempontjából a normáltól eltérő szintű besorolást kapnak.

(3) Az Egyetem korlátozza a privilegizált parancsokhoz való hálózati hozzáférést, és dokumentálja a korlátozásra vonatkozó elvárásokat az elektronikus információs rendszer biztonsági tervében. Az elektronikus információs rendszerhez hálózati hozzáférésnek számít minden olyan kapcsolat, ami esetében nem helyi hozzáférés történik, azaz a felhasználó nincs fizikailag jelen. Például, a router admin felületét csak a szerverteremben lévő konfigurációra használt rendszergazdai laptopról lehet elérni és csak a rendszergazda felhasználói fiókjából lehet módosító parancsokat kiadni.

VI.10.3.1 Távoli hozzáférés (3.3.10.13. [3])

(1) Az Egyetem:
   a) kidolgozza és dokumentálja minden engedélyezett távoli hozzáférés típusra a felhasználásra vonatkozó korlátozásokat, a konfigurálási vagy a kapcsolódási követelményeket és a megvalósítási útmutatókat;
   b) engedélyezési eljárást folytat le az elektronikus információs rendszerhez történő távoli hozzáférés feltételeként.

(2) IPSec (IKEv2) használata a VPN kiépítésekor, certificate alapú azonosítás és csatlakozás előtt állapot ellenőrzés (posture), (pl. operációs rendszer frissítések megléte, végpontvédelem állapota, stb.). A posture vizsgálat eredményeként a végpont vagy belépést kap a hálózatba, vagy egy karantén hálózatba kerül ahol a hiányosságok kiküszöböléséhez szükséges telepítések, módosítások elvégezhetők.

VI.10.3.2 Privilegizált parancsok elérése (3.3.10.13.5. [4])

(1) Az Egyetem a privilegizált parancsok végrehajtásához és biztonságkritikus információk eléréséhez távoli hozzáférést csak meghatározott és elfogadott igény esetén engedélyez. A hozzáférési engedélyeket indok feltüntetésével dokumentálja.

VI.10.3.3 Visszajátszás-védelem (3.3.9.2.5. [4])

(1) Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

(2) Az Egyetem olyan autentikációs protokollokat alkalmaz, amely biztosítja a visszajátszás elleni védelmet, vagyis a hitelesítési folyamat nem játszható ki a korábbi hitelesítési üzenetek rögzítésével/visszajátszásával. A visszajátszásnak ellen állnak például a TLS (Transport Layer Security), Kerberos és időszinkron alapú protokollok.

VI.10.3.4 Távoli hozzáférés - külön eszköz (3.3.9.2.6. [4])

(1) Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a felhasználói fiókokhoz való távoli hozzáféréshez, és az egyik hozzáférést megelőző tényező egy, az elektronikus információs rendszertől elkülönülő olyan eszköz, amelyen a meghatározott biztonsági követelmények teljesülnek.

(2) A többfaktoros hitelesítés során a számítógépen kívül, amin az elektronikus információs rendszerre történik a bejelentkezés,
   a) egy külön eszközre érkezik az egyszer használatos jelszó, pl. mobiltelefonra, fizikai tokenre;
   b) külső eszközön biometrikus azonosítót kell használni, pl. mobiltelefonon ujjlenyomat olvasó vagy arcfelismerő használata hitelesítésként.

VI. 10.4. Biztonságos hitelesítő, bejelentkező eljárások (3.3.13.16. [3])

(1) Az Egyetem elektronikus információs rendszeriben kezelt adatainak védelmében folyamatosan bevezeti és kiterjeszti a többfaktoros hitelesítő eljárást.

(2) A következő három azonosító közül, legalább kettő párhuzamos használata javasolt:
1) Valamit, amit tud (például egy jelszó)
2) Valamit amit birtokol (például egy személyi igazolvány vagy egy kriptográfiai hardverkulcs)
3) Valamit amivel csak Ön rendelkezik (például ujjlenyomat vagy más biometrikus adat)

VI.10.4.1 Munkaállomások automatikus azonosítása, hitelesítése

(1) A munkaállomások automatikus azonosítása, hitelesítése érdekében az Egyetemen egységes munkaállomás névhasználatot kell alkalmazni.

(2) A munkaállomás automatikus azonosítása kötelező, ha egy feladat végrehajtás-, tranzakció kezdeményezése adat és információvédelem érdekében csak egy eszközről végezhető.

(3) Az Egyetem elektronikus információs rendszerei védelme érdekében elvárható, hogy csak az Egyetemen bejegyzett eszközök férhessenek hozzá a rendszerhez, hálózathoz.

(4) Ehhez technikailag biztosítani kell, hogy csak a központilag nyilvántartott munkaállomásokról, címekről lehessen a rendszerekbe belépni.

VI.10.4.2 Biztonságos bejelentkezési eljárások

(1) Az Egyetem elektronikus információs rendszerekbe történő a belépési eljárást úgy kell kialakítani, hogy a jogosulatlan hozzáférés esélye a minimálisra csökkenjen.

(2) A beléptető eljárásnak a rendszerről csak a lehető legkevesebb információt szabad mutatnia, megjelenítenie.

(3) Sikertelen belépés esetén a rendszer nem jelölheti meg, hogy az autentikációhoz megadott adok melyik része bizonyult az ellenőrzési fázisban hibásnak.

(4) A belépésnél limitálni kell a sikertelen belépések számát, korlátozni kell a belépésre fordítható időintervallumot, és az újra belépés idejét:
a) 3 sikertelennek minősített bejelentkezést követően a felhasználói fiók tiltásra kerül;
b) 3 percen belül érvényes belépést kell végrehajtani;
c) hibás bejelentkezések miatt letiltott felhasználó csak 60 perc múlva ismételheti meg a belépést.

(5) Időkorláttal letiltott felhasználó bejelentkezési lehetőségét a rendszergazda feloldhatja, amennyiben a felhasználó az OTRS rendszerbe (helpdesk) bejelentve kérelmét, magát egyértelműen azonosítani tudja.

VI.10.4.3 Eszközök azonosítása és hitelesítése (3.3.9.3. [4])

(1) Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a meghatározott eszközöket, vagy eszköz típusokat mielőtt helyi vagy távoli hálózati kapcsolatot létesítene velük.

(2) Mielőtt az elektronikus információs rendszer engedélyezné a távoli hozzáférést, megnézi hogy a csatlakozandó eszköz MAC címe szerepel-e az engedélyezhető eszközök listáján. Ha ismeretlen MAC címmel rendelkezik az eszköz, akkor nem engedi csatlakozni. Az elektronikus információs rendszer naplózza a hozzáférés kéréseket, és ha a rendszer képes rá, akkor e-mailben értesíti a rendszergazdát a hozzáférés kezdeményezéséről.

VI. 10.5. A rendszerhasználat jelzése (3.3.10.8. [3])

(1) Az Egyetem az elektronikus információs rendszer felhasználásával az Egyetem által meghatározott rendszer használatra vonatkozó figyelmeztető üzenetet vagy jelzést küld a felhasználó számára a rendszerhez való hozzáférés engedélyezése előtt, mely jelzi, hogy:
   a) a felhasználó az Egyetem elektronikus információs rendszerét használja;
   b) a rendszer használatot figyelhetik, rögzíthetik, naplózhatják;
   c) a rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással jár;
   d) a rendszer használata egyben a felhasználó előbbiekbe történő beleegyezését is jelenti.

(2) Egy "felugró ablakban" vagy kezdőképernyőn jelennek meg a fentebbi információk.

VI. 10.6. Mobil eszközök hozzáférés ellenőrzése (3.3.10.15. [3])

(1) Az Egyetem belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre.

(2) Az Egyetem engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

VI. 10.7. Vezeték nélküli hozzáférés (3.3.10.14. [3])

(1) Az Egyetem belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán valamint definiálja az engedélyezési eljárást.

VI. 10.8. Külső elektronikus információs rendszerek használata (3.3.10.16. [2])

(1) Az Egyetem meghatározza, hogy milyen feltételek és szabályok betartása mellett jogosult a felhasználó egy külső rendszerből hozzáférni az elektronikus információs rendszerhez, meghatározza, hogy külső elektronikus információs rendszerek segítségével hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani az Egyetem által ellenőrzött információkat.

(2) Külső információs rendszereknek számítanak az olyan információs rendszerek vagy információs rendszerek alkotóelemei, amelyek az Egyetemen kívül állnak (az Egyetemnek nincs közvetlen felügyelete és felhatalmazása a szükséges biztonsági kontrollok ellenőrzésére). Külső elektronikus információ rendszerek lehetnek például a személyes tulajdonban lévő mobiltelefonok, laptopok, magántulajdonban lévő kommunikációs eszközök (pl. hotelben, vasútállomáson találhatók). Továbbá azok a rendszerek, amelyek az Egyetem információinak, adatainak feldolgozását, tárolását, továbbítását végzik, pl. felhőszolgáltató alkalmazása.

VI.10.8.1 Korlátozott használat (3.3.10.16.2. [4])

(1) Az Egyetem csak abban az esetben engedélyezi jogosult felhasználóknak egy külső elektronikus információs rendszer felhasználását az elektronikus információs rendszerhez való hozzáférésre, az által ellenőrzött információk feldolgozására, tárolására vagy továbbítására, ha:
   a) előzetesen ellenőrzi a szükséges biztonsági intézkedések meglétét a külső rendszeren saját szabályzóinak megfelelő módon vagy;
   b) jóváhagyott kapcsolat van az elektronikus információs rendszerek között; vagy
   c) megállapodás született a külső elektronikus információs rendszert befogadó szervezettel.

VI.10.8.2 Hordozható adattároló eszközök (3.3.10.16.3. [4])

(1) A Egyetem tiltja vagy korlátozza az adathordozók használatát azok számára, akik külső elektronikus információs rendszer hozzáféréssel rendelkeznek.

VI. 10.9. Információáramlás ellenőrzés érvényesítése (3.3.10.4. [4])

(1) Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információáramlás ellenőrzéséhez az Egyetem által meghatározott információáramlás ellenőrzési szabályoknak megfelelően.

(2) Az információáramlás megakadályozása történhet a hozzáférések kontrollálásával, pl. File serveren, végponton vagy akár felhőben tárolt adatok, információk megosztásánál megbizonyosodni, hogy minden felhasználó, aki jogot kapott a megosztáshoz valóban jogosult a hozzáféréshez. Pl. csoportnak adott jog esetén ellenőrizni, hogy a csoport minden tagja valóban kell, hogy hozzáférjen, illetve ha a csoport része egy másik csoportnak, akkor értelemszerűen felfelé ugyanez a feladat. Szintén kritikus web/ftp szerveren elhelyezett információkhoz való hozzáférés explicit szabályozása, "directory traversal" tiltása.

(3) Az engedély nélküli információáramlást az elektronikus információs rendszer megakadályozza megosztott erőforrásokon keresztül, amikor az információfeldolgozási szintekben váltás történik, pl. amikor az információk periodikus feldolgozása különböző biztonsági kategóriákban történik.

VI. 10.10. Lezárással járó inaktivitás (3.3.10.11. [4], 3.3.10.10.2. [4], 3.3.10.10. [4])

(1) Az elektronikus információs rendszer automatikusan lezárja a munkaszakaszt az Egyetem által meghatározott feltételek vagy munkaszakasz szétkapcsolást igénylő események megtörténte után.

(2) A felhasználó által indított logikai munkamenetet (helyi, hálózati és távoli hozzáférés) 3 perc inaktivitás után szükséges leállítani (az ilyen munkamenetek a hálózati munkamenet leállítása nélkül is megszüntethetők). A logikai munkamenet megbüntetése az összes kapcsolódó folyamatot leállítja, kivéve azokat amelyeket a felhasználó a felhasználó hozott létre (pl. ő a folyamat tulajdonosa).

(3) Az elektronikus információs rendszer automatikus lezárását követően a munkaasztal utolsó tevékenységének képernyőképe törlődik, elhalványul, olvashatatlan formát ölt.

(4) A lezárt munkamenet újranyitása, csak ismételt autentikációval történhet.

(5) Amennyiben a felületre nem a kijelentkeztetett felhasználó lép be, az új felhasználó nem kaphatja vissza az előző munkamenetét, csak a hozzáférés jogosultsági szintjének megfelelő kezdőlapot.

VI. 10.11. Információ megosztás (3.3.10.17. [4])

(1) Az Egyetem elősegíti az információ megosztást azzal, hogy engedélyezi a jogosult felhasználóknak eldönteni, hogy a megosztásban résztvevő partnerhez rendelt jogosultságok megfelelnek-e az információra vonatkozó hozzáférési korlátozásoknak, olyan meghatározott információ megosztási körülmények esetén, amikor felhasználói megítélés szóba jöhet.

(2) Az Egyetem a munkavállalók számára elektronikus tájékoztatást nyújt, amiben leírja, hogy a minősített információkra (pl. orvosi végdokumentumok, szerződések érzékeny információi, tulajdonlással kapcsolatos információk, minősített információk) milyen megosztással kapcsolatos elvárások vannak (kivel oszthatóak meg és milyen feltételekkel).

VI. 10.12. Nyilvánosan elérhető tartalom (3.3.10.18. [2])

(1) Az Egyetem kijelöli, és rendszeres oktatásban részesíti azokat a személyeket, akik jogosultak a nyilvánosan hozzáférhető elektronikus információs rendszeren az Egyetemmel kapcsolatos bármely információ közzétételére.

(2) A közzétett tartalmat közzététel előtt átvizsgálja, valamint közzétételt követően meghatározott gyakorisággal felülvizsgálja.

VI.11 Rendszer és információsértetlenség (3.3.11., 3.3.11.2. [2])

(1) Az Egyetem maga üzemelteti az elektronikus információs rendszereit, ezért írásba foglalja és kihirdeti az IBSZ-ben korábban megfogalmazott rendszer és információsértetlenségre vonatkozó szabályzat és ellenőrzések megvalósítását segítő folyamatokat és azokat meghatározott időközönként frissíti.

(2) Rendszer- és információsértetlenségre vonatkozó eljárásrendet készít.

(3) Az eljárásrend, folyamatleírást tartalmazó dokumentum, amely a szervezeten belül nyilvánosságra hozott és rendszeresen frissített.

(4) Az eljárásrend elvárásait, üzemeltetési szerződés részeként, szerződéses kötelemként kell érvényesíteni.

VI. 11.1. Hibajavítás (3.3.11.3. [2])

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

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

(3) A biztonságkritikus szoftvereket a frissítésük kiadását követő meghatározott időtartamon belül telepíti vagy telepítteti, beépíti a hibajavítást a konfigurációkezelési folyamatba.

(4) A teljes hibajavítási eljárás a konfigurációkezelési folyamatba kerül integrálásra.

VI.11.1.1 Automatizált hibajavítási állapot (3.3.11.3.2. [4])

(1) Az Egyetem automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer elemei hibajavítási állapotának meghatározására.

(2) Az automata sérülékenység kereső szoftver folyamatosan frissülő - sérülékenységeket tartalmazó - adatbázis alapján ellenőrzi az elektronikus információs rendszer elemeit. Rendszeres, a találatokat tartalmazó riport feldolgozásával, az érintett rendszer, felelős rendszergazdái elvégzik a szükséges frissítések, hibajavítások telepítését, konfigurációmódosításokat.

VI. 11.2. Kártékony kódok elleni védelem (3.3.11.4. [2])

(1) Az Egyetem az elektronikus információs rendszerét annak belépési és kilépési pontjain:
   a) védi a kártékony kódok ellen;
   b) felderíti és megsemmisíti azokat;
   c) frissíti a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg;
   d) konfigurálja a kártékony kódok elleni védelmi mechanizmusokat úgy, hogy a védelem eszköze:
      - rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren és hajtsa végre a külső forrásokból származó fájlok valós idejű ellenőrzését a végpontokon, a hálózati belépési vagy kilépési pontokon, a

biztonsági szabályzatnak megfelelően, amikor a fájlokat letöltik, megnyitják, vagy elindítják,
- a kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt, és riassza a rendszeradminisztrátort és az érintett szervezet által meghatározott további személyeket,
- ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az elektronikus információs rendszer rendelkezésre állására.

(2) Az Egyetem a munkaállomásokon, laptopokon olyan beállításokat alkalmaz, amely nem engedi a felhasználónak a vírusírtó automatikus frissítésének kikapcsolását, a vírusirtó ideiglenes kikapcsolását, annak uninstallálását.

VI. 11. 2.1. Központi kezelés (3.3.11.4.2. [4])

(1) Az elektronikus információs rendszer központilag kezeli a kártékony kódok elleni védelmi mechanizmusokat.

(2) A vírusirtó kezelése központilag irányított, központilag kezelt.

(3) Az Egyetem hatókörébe tartozó informatikai eszközökre automatikusan telepíti a vírusirtó szoftvert, amely az eszközökön automatikusan és központilag frissül (a frissítéseket a szerver tölti le a vírusirtó honlapjáról, a kliensekre innen történik az adatbázis upgrade).

VI. 11. 2.2. Automatikus frissítés (3.3.11.4.3. [4])

(1) Az elektronikus információs rendszer automatikusan frissíti a kártékony kódok elleni védelmi mechanizmusokat.

(2) Önműködő technológia alkalmazása a kártékony kódok elleni védelem frissítése során (Malware elleni szoftver esetében is).

VI. 11. 2.3. Vírustámadás elleni védekezés

(1) Az Egyetem az elektronikus információs rendszereiben tárolt adatait, információit a vírustámadás ellen a külvilági első kapcsolati pontjától, ami az Egyetem tűzfala, a szerverek, számítógépek, hordozható eszközök vírusvédelmi megoldásokon keresztül védi.

(2) A védelem csak akkor teljes, ha az kiegészítésre kerül a felhasználók biztonságtudatos viselkedésével, enélkül „csak” részleges védelmi megoldásról beszélhetünk.

(3) A vírustámadás elleni védekezés részletes szabályait az IBSZ ***„Vírusvédelmi eljárásrend”*** c. dokumentum tartalmazza.

VI. 11. 2.4. Vírusvédelmi szoftverek használata

(1) Az Egyetem szervereinek, számítógépeinek, hordozható eszközeinek védelmére korszerű, biztonságos, központilag menedzselhető vírusvédelmi rendszert alkalmaz.

VI. 11.3. Szoftver- és információsértetlenség (3.3.11.8. [4])

(1) Az Egyetem sértetlenség ellenőrző eszközt alkalmaz a szoftverek és információk jogosulatlan módosításának észlelésére, és automatizált eszközöket a meghatározott személyek vagy szerepkörök értesítésére, ha a sértetlenség ellenőrzés rendellenességet tár fel.

(2) Az elektronikus információs rendszer;
   a) sértetlenség ellenőrzést hajt végre a meghatározott szoftverekre és információkra, a rendszer újraindításakor, vagy biztonsági esemény bekövetkezését követően, vagy meghatározott gyakorisággal;
   b) automatikusan leállítja vagy újraindítja a rendszert, vagy egyéb intézkedést valósít meg, ha a sértetlenség ellenőrzés rendellenességet tár fel;
   c) megtiltja az olyan bináris vagy gépi kód használatát, amely nem ellenőrzött forrásból származik, vagy amelynek forráskódjával nem rendelkezik.

VI. 11.4. Kéretlen üzenetek elleni védelem (3.3.11.9. [S4)

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

(2) Ennek megvalósításához:
   a) új verziók elérhetővé válásakor frissíti a levélszemét elleni védelmi mechanizmusokat, összhangban a konfigurációkezelési szabályzattal és eljárásrenddel;
   b) központi beállításokkal irányítja a levélszemét elleni védelmet;
   c) automatikusan frissíti a levélszemét elleni védelmi mechanizmusokat azok újabb verzióival.

VI. 11.5. Bemeneti információ ellenőrzés (3.3.11.10. [S4])

(1) Az elektronikus információs rendszer folyamatosan ellenőrzi a meghatározott információ belépési pontok érvényességét.

(2) Publikusan elérhető rendszerek inputjainak védelmében - a biztonságos fejlesztésen túl - web application firewall (WAF) használata a bemeneti információk vizsgálatára, támadó kódok kiszűrésére.

(3) Dokumentum feltöltési lehetőség esetén a feltöltött dokumentumok karantén zónába helyezése, és csak sandboxban (tesztelést lehetővé tevő kontrollált, elkülönített fizikai vagy virtuális környezet) elemzése és/vagy szanitációs konverzió (tisztítási átalakítás) után áthelyezése a védett rendszerbe.

VI. 11.6. Hibakezelés (3.3.11.11. [S4])

(1) Az elektronikus információs rendszer hibajelzéseket generál a hibajavításhoz szükséges információkat biztosítva, ugyanakkor nem nyújt semmi olyan információt, amelyet a támadók kihasználhatnak.

(2) A hibajelzéseket kizárólag a meghatározott személyek vagy szerepkörök számára teszi elérhetővé.

VI. 11.7. Az elektronikus információs rendszer felügyelete (3.3.11.5. [2])

(1) Az Egyetem felügyeli az elektronikus információs rendszert:
   a) hogy észlelje a kiber támadásokat, vagy a kiber támadások jeleit a meghatározott figyelési céloknak megfelelően;

b) feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat;
c) azonosítja az elektronikus információs rendszer jogosulatlan használatát;
d) felügyeleti eszközöket alkalmaz a meghatározott alapvető információk gyűjtésére, és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére;
e) védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;
f) erősíti az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel;
g) meghatározott gyakorisággal biztosítja az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek;
h) Automatizált eszközöket alkalmaz az események közel valós idejű vizsgálatának támogatására.

(2) Az elektronikus információs rendszerek:
a) felügyelik a beérkező és kimenő adatforgalmat a szokatlan vagy jogosulatlan tevékenységekre vagy körülményre tekintettel;
b) riasztják az érintett szervezet illetékes személyeit, csoportjait, amikor veszélyeztetés vagy lehetséges veszélyeztetés előre meghatározott jeleit észleli.

(3) Az elektronikus információs rendszerek felügyelete többféle eszközzel megoldható például:
a) behatolás-észlelő rendszerek;
b) behatolás-megelőző rendszerek;
c) rosszindulatú kód elleni szoftverek;
d) naplóbejegyzéseket felügyelő eszközök;
e) naplózást nyilvántartó eszközök;
f) hálózati felügyeleti eszközök;
g) a rendszer által generált riasztások.

VI. 11.8. Biztonsági riasztások és tájékoztatások (3.3.11.6. [3])

(1) Az Egyetem:
a) folyamatosan figyeli a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;
b) folyamatosan figyelemmel kíséri a Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező értesítéseket;
c) szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki;
d) a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez;
e) kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, és kapcsolatot tart az érintett, külön jogszabályban meghatározott szervekkel;
f) megfelelő ellenintézkedéseket és válaszlépéseket tesz.

VI. 11.9. Memóriavédelem (3.3.11.13. [4])

(1) Az elektronikus információs rendszerben biztonsági beállításokat kell alkalmaznia azért, hogy védje a memóriát a jogosulatlan kódok végrehajtásától. Azon támadások kivédésére, ahol a támadó a memória azon részén futtat le kódot, amelyen nem lehetne, az Egyetem különböző védelmi megoldásokat vezet be (pl. Data Execution Prevention (DEP) bekapcsolása, megfelelő konfigurálása a Windows-ban).

VI. 11.10. A kimeneti információ kezelése és megőrzése (3.3.11.12. [2])

(1) Az Egyetem az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg. (Például a személyes adatok az Általános adatvédelmi rendeletet (GDPR) figyelembe véve kezeli és megőrzi.)

VI. 11.11. Használatból történő kivonás

(1) Az Egyetemen az elektronikus információs rendszer vonatkozásában a használatból történő kivonás esetei:
   a) felhasználói szoftver,
   b) adattároló eszköz (számítógép-, hordozható eszköz HDD, storage, külső HDD, pendrive).

(2) Felhasználói szoftver adatbázisát, annak biztonsági mentéseit a tartalomtól függő jogszabályi követelmények szerinti ideig kell megőrizni.

(3) Adattáró eszköz (működőképes) újrahasznosítása, végleges kivonása előtt a tartalmat speciális szoftverrel visszaállíthatatlan módon törölni kell.

(4) Selejtezendő adattároló eszközöket olyan roncsolási technikával kell használhatatlanná tenni, hogy arról még töredék információt se lehessen visszanyerni.

VI.12 Naplózás és elszámoltathatóság (3.3.12., 3.3.12.1. [2])

(1) Az Egyetem megfogalmazza, az érvényes követelmények szerint dokumentálja, valamint a szervezeten belül a szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a ***„naplózási és naplóelemzési eljárásrendet”***, mely a naplózásra és elszámoltathatóságra vonatkozó ellenőrzések megvalósítását segíti elő.

(2) A Naplózási és naplóelemzési eljárásrend szabályozza az alábbiakat:
   a) Naplózandó rendszerelemek meghatározásának módja;
   b) Naplózandó események köre;
   c) Naplók felülvizsgálatának módja (ad-hoc vagy rendszeres, automatikus);
   d) Naplók biztonságos tárolása, védelme.

(3) A naplózásban érintett rendszerek (beleértve a szoftvereket és az eszközöket), események és automatikus riasztások egy előzetes kockázatértékelés alapján kerül meghatározásra.

VI.12.1. Biztonsági események naplózása

(1) A naplózandó eseményeket úgy kell kiválasztani, hogy azok egy esetleges incidens során megfelelő információt adjanak annak kivizsgálására.

VI.12.1.1 Naplózandó események (3.3.12.2. [2])

(1) Az Egyetem:
   a) meghatározza a naplózható és naplózandó eseményeket, és
   b) felkészíti erre az elektronikus információs rendszerét;

c) egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő szervezeti egységgel, hogy növelje a kölcsönös támogatást, és hogy iránymutatással segítse a naplózható események kiválasztását;
d) megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

(2) A naplózási eljárásrendben meg kell határozni, hogy milyen események naplózása történjen, milyen rendszerekre, milyen formátumban.

(3) Minimális naplózandó események:
a) felhasználói tevékenységek (belépés, kilépés, módosítás);
b) távoli belépések, belépési kísérletek;
c) admin, privilegizált felhasználók tevékenysége (részletesen, nem csak a rendszerhasználat ténye);
d) hozzáférések módosításával kapcsolatos tevékenységek;
e) jogosulatlan hozzáférési próbálkozások;
f) biztonsági eszközök (határvédelem, végpontvédelem) eseményei;
g) szerverek operációs rendszer szintű eseményei.

VI.12.1.2 A napló adattartalma (3.3.12.3. [2], 3.3.12.3.2 [4])

(1) Az elektronikus információs rendszer a naplóbejegyzésekben gyűjtsön be elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

(2) Az elektronikus információs rendszerek esetében a naplózási szabályokat úgy kell kialakítani, hogy az eseményekről tárolt naplóinformációk segítsék a biztonsági események, incidensek feltárását.

(3) Minimális tartalom:
a) esemény birtokosa (ki? - felhasználó, rendszer folyamat, szolgáltatás/service)
b) időbélyeg (mikor?)
c) esemény (mit?)
d) forrásrendszer (hol?)
e) esemény státusza / sikeressége

VI.12.1.3 Alapvető naplózási követelmények

(1) A felhasználói műveletekről, hibajelenségekről és az információ biztonságával kapcsolatos eseményekről a rendszereknek naplóbejegyzést kell generálni.

(2) A naplókat az előírásoknak megfelelő ideig kell megőrizni az utólagos visszakereshetőség és a hozzáférések felülvizsgálata érdekében.

(3) 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) automatizált megoldások, naplóelemző rendszerek támogassák a különböző naplóállományok összefésülését, feldolgozását és elemzését;
d) 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.

VI.12.2. Automatikus naplózás (3.3.10.2.5. [BR4])

(1) Az elektronikus információs rendszer automatikusan naplózza a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket, és értesíti ezekről a meghatározott szerepkörű személyeket.

(2) A rendszer minden felhasználókkal, fiókokkal kapcsolatos eseményt naplóz, esetleges biztonsági incidensek felderítése illetve auditok miatt is.

(3) A napló módosítása nem lehetséges.

VI.12.3. Privilegizált funkciók használatának naplózása (3.3.10.6.5. [4])

(1) Az elektronikus információs rendszer kiemelt prioritással és részletesebben naplózza a privilegizált funkciók végrehajtását (tény, idő, tevékenység).

VI.12.4. Ideiglenes naplózás

(1) A naplózandó esemény, a naplózás időtartamának és céljának pontos megjelölésével, arra felhatalmazással rendelkezők által ideiglenesen naplózás történhet.

(2) A naplózást elrendelheti: kancellár, adatgazda szervezeti egység vezető, ISZK Igazgató, IBK központvezető, GDPR központvezető.

(3) A cél lehet teszt, felhasználói tevékenység biztonsági vizsgálata, folyamatvizsgálat, működési hatékonyságvizsgálat, statisztikai.

(4) Az ideiglenes naplózást csak az igényelt időtartam ideje alatt kell fenntartani, ezt követően fenntartási igény generálás hiányában meg kell szüntetni.

(5) Az ideiglenes naplózási igényt írásos formában az ISZK Igazgatónak kell benyújtásra.

VI.12.5. A rendszer használat megfigyelése

(1) A rendszerhasználat folyamatának megfigyelése naplózással történik. A naplóállományok vizsgálata a rendszergazdák általi rendszeres elemzésével és naplóelemző rendszer használatával történik.

VI.12.6. Kockázati tényezők

(1) A naplóelemzéssel olyan kockázati tényezők kerülhetnek napvilágra, amik biztonsági kockázatot, biztonsági rést jelentenek. Ezek a megállapítások olyan preventív intézkedéseket generálnak, amik lehetőséget adnak a biztonság növelésére.

(2) Az automatikus, mesterséges intelligenciával támogatott naplóelemzők nélkülözik a szubjektív ítélet, megállapítás hibáját, gyorsabb és hatékonyabb észlelést tesznek lehetővé.

VI.12.7. Naplózási információk védelme (3.3.12.9. [2])

(1) Az elektronikus információs rendszer megvédi a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

(2) A naplófunkciók kezelésére csak az Egyetem által meghatározott, privilegizált felhasználók jogosultak.

(3) Az elektronikus információs rendszer a naplóbejegyzéseket meghatározott gyakorisággal elmenti, egy a keletkezési helyétől fizikailag elkülönülő rendszerre vagy rendszerelemre.

(4) Kriptográfiai mechanizmusokat kell alkalmazni a naplóinformáció és a naplókezelő eszköz sértetlenségének védelmére.

(5) A hozzáférések, jogosultságok megfelelő beállításával védhetők a jogosulatlan hozzáféréstől. A naplófájlokat tartalmazó meghajtóhoz, illetve a központi menedzsment rendszerhez való hozzáférés a legkisebb jogosultság elve alapján való kiosztása követendő, szorítkozva az azokkal feladatokat végző adminisztrátorokra.

(6) A naplófájlokat nem módosíthatja senki, még admin / privilegizált felhasználói fiókokkal sem.

(7) A naplófájlok fizikai védelmét is biztosítani kell, a tárolóeszköz és a környezetének megfelelő védelmi intézkedéseivel.

VI.12.8. Naplóinformációk figyelése, reagálás a napló információkra (3.3.12.6. [3])

(1) Az Egyetem:
   a) rendszeresen felülvizsgálja és elemezi a naplóbejegyzéseket nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából, jelenti ezeket a meghatározott szerepkörű személyeknek;
   b) automatikus mechanizmusokat használ a naplóbejegyzések vizsgálatának, elemzésének és jelentésének átfogó folyamattá integrálására, amely a veszélyes vagy tiltott tevékenységekre és történésekre reagál;
   c) megvizsgálja és összefüggésbe hozza a különböző adattárakban található naplóbejegyzéseket, a teljes Egyetemre kiterjedő helyzetfelmérés érdekében;
   d) egyesíti a naplóbejegyzések vizsgálatát a sebezhetőség ellenőrzési információkkal, a teljesítmény adatokkal, az elektronikus információs rendszer felügyeletéből származó információkkal, vagy egyéb forrásokból begyűjtött adatokkal vagy információkkal;
   e) összefüggésbe hozza a naplóbejegyzésekből származó információkat a fizikai hozzáférés felügyeletéből nyert információkkal.

VI.12.9. Rendszer órajel szinkronizáció (3.3.12.8. [2])

(1) Az elektronikus információs rendszer:
   a) belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához;
   b) időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz - úgynevezett UTC - vagy a Greenwichi középidőhöz – úgynevezett GMT - rendelhető módon, megfelelve az Egyetem által meghatározott időmérési pontosságnak;
   c) meghatározott gyakorisággal összehasonlítja a belső rendszerórákat egy hiteles külső időforrással, és ha az időeltérés nagyobb, mint a meghatározott időtartam, szinkronizálja a belső rendszerórákat a hiteles külső időforrással.

(2) A belső rendszerórák folyamatosan pontos időhöz igazításához külső, publikus NTP (Network Time Protocol, Időszinkronos szolgáltatás) szolgáltatást kell igénybe venni.

VI.12.10. A naplóbejegyzések megőrzése (3.3.12.11. [2])

(1) Az Egyetem a naplóbejegyzéseket meghatározott - a jogszabályi és az Egyetemen belüli információ megőrzési követelményeknek megfelelő - időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.
(2) A megőrzési idő a rendszerek osztályba sorolása szerint:
   - 1.-3.szint – 3 hónap
   - 4.szint – 6 hónap

VI.12.10. 1. Naplózás mentése

(1) A naplóesemények napló állományait az előállításuk lokális helyéről, paraméterezéssel, script megoldással a napló szerverre kell másolni.

(2) A másolás minden nap, minden héten, minden hónapban, méretkorlát elérése szerint történhet.

(3) Az Adatbázis kezelők bináris naplóállományokat hoznak létre. A bináris naplófájlok szolgáltatják a szükséges információt ahhoz, hogy megismételhesse az adatbázisban azokat változtatásokat, amelyek azon időpontot követően lettek megtéve, miután végrehajtott egy biztonsági mentést.

(4) A naplóbejegyzéseket valós időben kell továbbítani az Egyetem központi naplóelemző rendszerébe, így intézkedésre okot adó esemény bekövetkezése esetén időben megtörténhet a reagálás, elhárítás, és az érintett rendszer védelme érdekében.

VI.12.10. 2. Naplóállomány külön mentése

(1) A naplóállományokat redundáns, biztonsági mentett állapotban is őrizni szükséges. A megőrzési idő lejáratakor, a primer állomány törlésével egy időben, gondoskodni kell ezek törléséről is.

VI.12.10. 3. Naplóállományok rendszeres mentéseinek felülvizsgálata

(1) Naplók mentésének felülvizsgálata ad-hoc, rendszeres vagy automatikus módon történhet. Az Egyetem automatikus megoldásokat alkalmaz naplóállományok mentésére.

VI.12.10. 4. Biztonsági naplók archiválása

(1) A biztonsági események utólagos kivizsgálása érdekében a biztonsági naplók redundáns, elkülönített, módosíthatatlan, illetéktelen hozzáférés, megtekintés ellen védett megőrzését kell biztosítani.

VI.12.11. Hozzáférés a naplóállományokhoz (3.3.12.9.2. [4])

(1) A naplózás funkcióinak eléréséhez kizárólag a privilegizált, többlet jogkörrel rendelkező felhasználók engedélyezettek.

(2) A naplófájlokat tartalmazó meghajtóhoz, illetve a központi menedzsment rendszerhez való hozzáférés a legkisebb jogosultság elve alapján való kiosztása követendő, szorítkozva az azokkal feladatokat végző adminisztrátorokra. A tároló rendszerekhez hozzáférést csak adminisztrátori (menedzsment) hálózati zónából lehet biztosítani.

(3) A naplófájlokat nem módosíthatja senki, még admin / privilegizált felhasználói fiókokkal sem. Olvasási jogot is csak privilegizált felhasználóknak adni.

VI.12.11.1 Naplóállományok írása

(1) Időbélyeggel ellátott esemény azonnali bejegyzése történik:
   a) a felhasználói műveletekről
   b) hibajelenségekről
   c) információ biztonságával kapcsolatos eseményekről
   d) hálózati adatforgalomról
   e) rendszergazdai és rendszerüzemeltető tevékenységről.

VI.12.11.2 Lekérdezés a naplóállományokból

(1) A naplóállományokból csak illetékességgel és jogosultsággal rendelkező rendszergazdák, informatikai biztonsági munkatársak kérdezhetnek le.

VI.12.11.3 Naplóinformációk kiadása külső szervezetek számára

(1) Külső szervezet számára csak szerződésben foglalt kötelezettség, és biztonsági esemény, incidens bekövetkezése esetén adható ki naplóinformáció.

VI.12.11.4 Naplóállományból lekérdezési jogosultság dokumentálása

(1) A naplóállomány lekérdezési jogosultságát részleteiben a „Naplózási és naplóelemzési eljárásrend" tartalmazza.

VI.12.12. Naplózó rendszer beállításainak módosítása

(1) A naplózó rendszer beállítását csak illetékes rendszergazda, és csak utasításra változtathatja meg. Beállítás módosítás kezdeményező:
   a) ISZK Igazgató,
   b) IBK központvezető,
   c) GDPR Központ vezető / Adatvédelmi tisztviselő.

VI.12.13. Naplózási beállításokról nyilvántartás vezetése

(1) A naplózó rendszer beállításairól nyilvántartás készítése, aktualizálása az illetékes rendszergazda feladata.

(2) A nyilvántartást rendszeres időközönként felettes vezetőjének kell ellenőrizni.

(3) A beállítás módosításának bejegyzésénél fel kell tüntetni, a kezdeményező nevét, engedélyező nevét, kezdeményezés okát, időpontját, a módosítás végrehajtásának idejét, annak végrehajtóját.

VI.12.14. Hozzáférés korlátozása (3.3.12.9.2. [4])

(1) A naplózás funkcióinak eléréséhez kizárólag a privilegizált, többlet jogkörrel rendelkező felhasználók engedélyezettek.

VI.12.14.1. Kiegészítő információk (3.3.12.3.2. [4])

(1) Az elektronikus információs rendszer a naplóbejegyzésekben további, az Egyetem által meghatározott kiegészítő, részletesebb információkat is rögzít.

(2) A naplózási szabályok kialakításakor figyelembe kell venni, hogy mik azok az információk, ami letárolása mindenképp szükséges naplózás formájában. A szabályok kialakításakor viszont figyelembe kell venni azt is, hogy felesleges, később nem felhasználható információk ne kerüljenek naplózásra, ugyanis az növeli a naplófájlok méretet, nehezíti a mozgatásukat, feldolgozásukat, a rendelkezésre álló tárhelyet idő előtt megtelítik.

(3) A személyes adatok és érzékeny információk naplózására külön figyelmet kell fordítani, csak azon személyes adatokat lehet naplózni, amelyek további tárolására megfelelő jogalap áll rendelkezésre.

(4) Külön figyelmet kell fordítani a belső fejlesztésű, vagy egyedi megrendelésre készült szoftverek, eszközök esetén, hogy az eseményekről keletkezzenek (megfelelő részletességgel) naplóbejegyzések, akár saját adatbázisban, ahonnan napló begyűjtő (log collector, agent) segítségével kinyerhető.

(5) A kiegészítő információk során figyelembe kell venni, hogy mik azok az információk, amiket az Egyetem számára szükséges lehet későbbi ellenőrzés céljából, pl. privilegizált felhasználó által kiadott parancsok vagy a csoportos felhasználók által végzett tevékenységek. Ezen információk közül

mindenképp csak a szükségesek naplózásával elkerülhető, hogy például egy incidens nyomozása során az értékes információ elvesszen a nagymennyiségű letárolt adat között.

VI.12.14.2. Naplózási beállítások felülvizsgálata

(1) A naplózási beállításokat, paraméterezést akkor kell felülvizsgálna, ha a naplóállomány adattartalma, elemzés során nem nyújt kellő vagy nem releváns információt ad a feldolgozó számára.

VI.12.14.3. A naplózás vizsgálata

(1) Illetékes rendszergazdai feladattal rendszeres időszakonként, központi naplóelemző rendszerrel legalább hetente szükséges mélyebb vizsgálat, elemzés.

VI.12.14.4. Naplózási hiba kezelése (3.3.12.5. [3])

(1) Az elektronikus információs rendszer naplózási hiba esetén riasztást küld a meghatározott szerepkörű személyeknek, akik elvégzik a meghatározott végrehajtandó tevékenységeket, így például a rendszer leállítását, a legrégebbi naplóbejegyzések felülírását, a naplózási folyamat leállítását.

(2) Olyan naplógyűjtő rendszer használatát kell bevezetni, amely a naplózás sikertelensége esetén (pl. megtelt a tárhely vagy nem érkezik teljes naplóbejegyzés a forrásrendszertől) riasztást küld a felelősnek, illetve a beállítások alapján automatikusan végrehajt előre definiált utasításokat a hiba megszűntetése illetve a károk enyhítése céljából (pl. régi, alacsony prioritású naplóbejegyzéseket felülírja, ha nincs elég tárhely a kritikus rendszerektől érkező bejegyzéseknek).

(3) A naplózási hiba keletkezését követően eldönthető hogy az a folyamat, amelyhez a naplózás tartozott, naplózási funkció működőképessége nélkül folytatható-e.

VI.12.14.5. Napló tárkapacitás figyelése (3.3.12.5.2. [5])

(1) Az elektronikus információs rendszer figyelmezteti a meghatározott személyeket és szerepkörű embereket, ha a lefoglalt naplózási tárhely eléri a beállított maximális naplózási tárhely előre meghatározott részét.

VI.12.15. Folyamatba illesztés (3.3.12.6.2. [4])

(1) Az Egyetem automatikus mechanizmusokat használ a naplóbejegyzések vizsgálatának, elemzésének és jelentésének átfogó folyamattá integrálására, amely a veszélyes vagy tiltott tevékenységekre és történésekre (incidens bekövetkezésére) reagál.

VI.12.15.1. Időbélyegek (3.3.12.8. [2])

(1) A naplózott eseményekről eltárolt információk között szerepelnie kell az időbélyegnek - forrása belső hiteles idő szolgáltató (NTP eszköz mely a pontos időt és a bélyeghez szükséges aláíró tanúsítványt is biztosítja) - annak érdekében, hogy bizonyítható legyen a bejegyzés időpontjának valódisága.

VI.12.15.2. Szinkronizálás (3.3.12.8.2. [4])

(1) Az elektronikus információs rendszer:
   a) belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához;
   b) időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz - úgynevezett UTC - vagy a Greenwichi középidőhöz – úgynevezett GMT - rendelhető módon, megfelelve az Egyetem által meghatározott időmérési pontosságnak;
   c) meghatározott gyakorisággal összehasonlítja a belső rendszerórákat egy hiteles külső időforrással, és ha az időeltérés nagyobb, mint a meghatározott időtartam, szinkronizálja a belső rendszerórákat a hiteles külső időforrással.

VI.12.15.3. Összegzés (3.3.12.6.3. [4])

(1) Az Egyetem megvizsgálja és összefüggésbe hozza a különböző adattárakban található naplóbejegyzéseket, a teljes Egyetemre kiterjedő helyzetfelmérés érdekében.

(2) A teljes szervezet elektronikus rendszereiben keletkező naplóállományok átfogó, kontextusban történő vizsgálata a rendszerekben történt események közti összefüggések, korrelációk feltárására.

(3) Különböző rendszerekből gyűjtött naplóbejegyzések egy helyen - egy rendszerben – történő feldolgozása, elemzése (SIEM).

VI.12.16. A naplók tartalmának elemzése, jelentéskészítés a naplózásról (3.3.12.6. [3])

(1) Az Egyetem rendszeresen felülvizsgálja és elemzi a naplóbejegyzéseket nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából, ezeket jelenti a meghatározott szerepkörű személyeknek.

(2) Eltérés elemzés céljából a naplóbejegyzések ellenőrzése és jelentés készítése.

(3) Az Egyetem naplóbejegyzéseket készít a biztonsággal kapcsolatos eseményekről (pl. konfigurációs beállítások változása, távoli hozzáférések, fizikai hozzáférések). A naplóbejegyzéseket elemzi és jelentéseket készít az eredményéről az érintett szervezeti egységek felé, pl. információbiztonsági csapat, incidenskezeléssel foglalkozó csapat.

VI.12.16.1. Automatikus feldolgozás (3.3.12.7.2. [4], 3.3.12.7. [4])

(1) Az elektronikus információs rendszer biztosítja, hogy a fontos naplóbejegyzéseket automatikusan fel lehessen dolgozni.

(2) SIEM rendszer használata a biztonsági naplóbejegyzések feldolgozására, értékelésére, és az azok közti korrelációk felfedésére.

VI.13 Rendszer és kommunikációvédelem (3.3.13., 3.3.13.1. [2])

(1) Az Egyetem megfogalmazza, az érvényes követelmények szerint dokumentálja, valamint a szervezeten belüli szabályozásában meghatározott személyek vagy szerepkörű emberek számára kihirdeti a ***„rendszer- és kommunikációvédelmi eljárásrendet”***, mely a rendszeres kommunikációvédelmi ellenőrzések megvalósítását segíti elő.

VI. 13.1. A határok védelme (3.3.13.6. [2], 3.3.13.6.2. [4], (3.3.13.5. [3])

(1) Az elektronikus információs rendszer:

a) felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt;
b) a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól;
c) csak az Egyetem biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

(2) Határvédelmi és felügyeleti eszközök - tűzfalak, web, email gateway eszközök használata-, DMZ (-k), illetve egyéb belső zónák (irodai, szolgáltatás, egészségügy, kutatás, oktatás, vendég wifi, adminisztrátori) kialakítása.

VI.13.1.1 Az adatátvitel sértetlensége (3.3.13.8. [4])

(1) Az elektronikus információs rendszer biztonsági kontroll alkalmazásával megvédi a külső vevő felé továbbított információk sértetlenségét. Az információ integritásának ellenőrzésére és védelmére szolgáló szoftver alkalmazást használ.

VI.13.1.2 A hálózati kapcsolat megszakítása (3.3.13.9. [4])

(1) Az elektronikus információs rendszer megszakítja a hálózati kapcsolatot egy munkaszakaszra épülő kétirányú adatcsere befejezésekor, meghatározott időtartamú inaktivitás után.
(2) Amennyiben az előre meghatározott időkeretben nem történik aktivitás, úgy a rendszer bontja a hálózati kapcsolatot. pl. FTP kapcsolatnál az utolsó befejezett tranzakciótól számított idő letelte után a kapcsolat egyoldalúan bontásre kerül.

VI.13.1.3 Biztonságos név/cím feloldó szolgáltatások (úgynevezett hiteles forrás) (3.3.13.16 [3])

(1) Az elektronikus információs rendszer a név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó kiegészítő adatokat is biztosít, és ha egy elosztott, hierarchikus névtár részeként működik, akkor jelzi utódtartományok biztonsági állapotát is, és (ha azok támogatják a biztonságos feloldási szolgáltatásokat) hitelesíti az utód- és elődtartományok közötti bizalmi láncot.

(2) DNSSEC (Domain Name System Security Extensions) használata a névfeloldás hitelességének biztosítására. A technológia tanúsítvány alapú, ezzel biztosítja a lekérdezések hitelességét.

VI.13.1.4 Biztonságos név/cím feloldó szolgáltatás (úgynevezett rekurzív vagy gyorsító tárat használó feloldás) (3.3.13.17 [3])

(1) Biztonságos név/cím feloldó szolgáltatás (úgynevezett rekurzív vagy gyorsító tárat használó feloldás) Az elektronikus információs rendszer eredethitelesítést és adatsértetlenség ellenőrzést kér, és hajt végre a hiteles forrásból származó név/cím feloldó válaszokra.

(2) DNSSEC (Domain Name System Security Extensions) használata a rekurzív névfeloldók hitelességének biztosítására. A technológia tanúsítvány alapú, ezzel biztosítja a lekérdezések hitelességét.

VI.13.1.5 Architektúra és tartalékok név/cím feloldási szolgáltatás esetén (3.3.13.18 [3])

(1) Azok az elektronikus információs rendszerek, amelyek együttesen biztosítanak név/cím feloldási szolgáltatást egy szervezet számára, hibatűrők és belső/külső szerepkör szétválasztást valósítanak meg.

(2) A névfeloldó rendszerek kritikusak a hálózat működése szempontjából, így biztosítani kell a magas rendelkezésre állást. Ezt a célt redundáns architektúrával érhetjük el. Fontos a belső illetve külső névkiszolgálás szétválasztása rendszerszinten.

(3) A külső és belső névfeloldás szétválasztása nem csak külön eszközön megvalósítást, de külön hálózat szegmensben elhelyezést is jelent: a külsőt DMZ szegmensbe, a belsőt pedig a belső hálózatba minden azt igénylő eszköz számára elérhetően kell elhelyezni.

(4) A magas rendelkezésre állás biztosítását aktív redundáns eszközökkel érjük el, ami az elsődleges kiszolgáló meghibásodása esetén automatikus átállás (billentés) a másodlagos eszközre.

VI.13.2. A hálózati szintű hozzáférések menedzsmentje

(1) A hálózati szolgáltatások rendelkezésre állását, az üzletmenet folyamatos fenntartása érdekében kell biztosítani. Ennek érdekében:
    a) Csak jogosult felhasználók férhetnek hozzá a hálózat szolgáltatásaihoz. Minden sikeres és sikertelen bejelentkezést, vagy annak kísérletét regisztrálni kell;

b) A nyitott hálózati portokat (tűzfal külső oldaláról jövő kérések), amelyek kívülről szolgáltatásként vannak jelen, nyilván kell tartani;
c) Az aktív hálózati eszközök skálázhatóak, bővíthetőek legyenek, valamint biztosítani kell a dinamikus teljesítmény-eloszlás megvalósulását;
d) Virtuális hálózati szeparáció, az áttekinthető és védett hálózat kezeléshez (hálózati eszközök managementje).

VI.13.2.1. Kötelező elérési útvonal

(1) Az Egyetem hálózatát, a hálózatba lépést csak egy ponton (tűzfal) lehet elérni kívülről és csak egy ponton lehet elhagyni kifelé.

VI.13.2.2. Hálózati részek elválasztása

(1) Az Egyetem informatikai hálózatán egymást befolyásoló tevékenységek is folyhatnak, amelyek kiszolgáló hálózatait virtuális belső hálózati (VLAN) részekre kell szeparálni (elválasztani), úgy mint:
a) oktatás,
b) kutatás,
c) hallgatók,
d) gazdasági,
e) egészségügyi,
f) pénzügyi,
g) campusok,
h) IT menedzsment.

(2) A virtuális belső hálózatokat tűzfalnak kell elválasztania a többi zónától.

(3) A virtuális hálózatok hozzáférését szabályozni, a felhasználók felkapcsolódási lehetőségeit korlátozni kell.

(4) A hálózati forgalom ellenőrzésére szolgálnak:
a) a tűzfalak naplói;
b) hálózat figyelő és IDS szoftverek (Intrusion Detection System: behatolás- érzékelő rendszer);
c) belső hálózat szervereinek naplói;
d) hálózati eszközök naplói;
e) hálózati menedzsment eszközök naplói.

VI.13.2.3. Hálózati eszközök, munkaállomások azonosítása és hitelesítése

(1) Az Egyetem elektronikus információs rendszereihez való összes csatlakozást azonosítani és hitelesíteni kell.

(2) Különösen érzékeny és biztonságilag aggályos, ha a csatlakozási kezdeményezés olyan hálózatból érkezik, ami kívül esik az Egyetem biztonsági követelmény hatókörén (home office, szolgáltatók).
Belső hálózat védelme érdekében:
   a) technikailag kell biztosítani, hogy csak a központilag nyilvántartott munkaállomásról lehessen a rendszerekbe belépni;
   b) egységes munkaállomás névhasználatot kell kialakítani, a hálózatban lévő munkaállomások pontos azonosítása érdekében;
   c) tartományvezérelt (Active Directory) felhasználói munkaállomás használat;
   d) kívülről csak biztonságos csatornán (VPN) keresztül történhet feladatvégzés.

VI.13.2.4. A hálózatra történő csatlakozás ellenőrzése

(1) Felhasználói munkaállomásokról (asztali és mobil), kizárólag csak biztonságos beléptetési folyamat után lehet elérni az Egyetem hálózati erőforrásait.

(2) Az Egyetem számítógép-hálózata kizárólag az Egyetem által meghatározott tartományos rendszer szerint működhet.

(3) Nem csatlakozhat olyan munkaállomás a hálózatra, ami:
   a) nem megbízható hálózati kapcsolattal rendelkezik;
   b) nem tagja a megfelelő egyetemi tartománynak;
   c) nem rendelkezik naprakész vírusvédelmi megoldással.

VI.13.2.5. A hálózati útvonal kiválasztások ellenőrzése

(1) A hálózatok alapvető rendeltetése, hogy biztosítsák az erőforrások megosztását és a rugalmas útvonal- kiválasztását, ezzel lehetővé téve az elektronikus információs rendszerek engedély nélküli elérését, vagy az informatikai eszközök engedély nélküli használatát.

(2) A felhasználói terminál (asztali, mobil) és a felhasználó által használható informatikai szolgáltatások közötti útvonalat korlátozó ellenőrző eszközök alkalmazása (kötelező útvonal kialakítása), csökkenti a lehetséges kockázatokat.

(3) A kötelezően előírt útvonal célja, hogy a szolgáltatás igénybevétele csak az engedélyben rögzített útvonalon vehető igénybe, úgy hogy az útvonal különböző pontjain ellenőrző eszközök vannak beiktatva, ahol előre meghatározott választási lehetőségekkel történik a korlátozás. Ezt az alkalmazói szoftverek, operációs rendszer és aktív hálózati eszközök beállításaival, paraméterezésével kell elvégezni.

VI.13.2.6. Használható hálózati protokollok

(1) Az Egyetem belső hálózata és külső hálózatok közötti kapcsolat során csak az engedélyezett kommunikációs protokollok továbbíthatók, minden egyéb továbbítása tilos. Az eszközökre feleslegesen felinstallált protokollok biztonsági rést jelentenek.

VI.13.2.7. Távoli készülékek csatornahasználata (3.3.13.6.5. [4], 3.3.13.7.1. [4])

(1) A távoli készülékkel kapcsolatban álló elektronikus információs rendszer meggátolja, hogy a készülék egyidejűleg helyi kapcsolatokat létesítsen a rendszerrel.

(2) Az elektronikus információs rendszerrel kapcsolatban lévő távoli eszközök párhuzamosan nem létesíthetnek helyi (lokális) vagy másik publikus kapcsolatot. Cél, a VPN csatornát kikerülő kommunikációk megakadályozása, azaz minden kommunikáció a VPN csatornába irányítása.

(3) A végpontokon a hálózati beállítások illetve VPN kliensek megfelelő beállítása (központilag, terminál oldalról kikényszerítve), beállítások végponton módosításának adminisztrátori jogosultsághoz kötése, illetve tiltása.

VI.13.3. Mobilkód korlátozása (3.3.13.14. [4])

(1) Az Egyetem:
   a) meghatározza az elfogadható és a nem elfogadható mobilkódokat és mobilkód technológiákat;
   b) használati korlátozásokat vezet be vagy megvalósítási útmutatót bocsát ki az elfogadható mobilkódokra és mobilkód technológiákra;
   c) engedélyezi, felügyeli és ellenőrzi a mobilkódok használatát az elektronikus információs rendszeren belül.

(2) Mobilkódok és mobilkód technológiák használhatóságára és engedélyezésére kidolgozott útmutatók a káros tartalmak hordozására alkalmas kódok kiszűrésére, tiltására, karanténba helyezésére.

(3) A mobilkódok- és technológiákra vonatkozó részletes útmutató dokumentum megléte és a releváns személyeknek történő közzététele. Tartalma szabályozza a mobilkódok lehetséges használatát. Pl. beérkező dokumentumokban makrók tiltása, PDF állományokban scriptek tiltása, email szövegtörzsben script nyelvek futtatásának tiltása, scripteket tartalmazó csatolmányok automatikusan karanténba helyezése, valamint monitorozásának folyamatát.

VI.13.4. Elektronikus információs rendszeren keresztüli hangátvitel (VoIP) (3.3.13.15. [4], 3.3.13.12. [2])

(1) Az Egyetem használati korlátozásokat vezet be vagy megvalósítási útmutatót ad a VoIP technológiákhoz, felmérve a rosszindulatú használat esetén az elektronikus információs rendszerben okozható károkat, illetve engedélyezi, felügyeli, és ellenőrzi a VoIP használatát az elektronikus információs rendszeren belül.

(2) Potenciális kockázatok felmérésén alapuló VoIP használhatóságra vonatkozó korlátozások valamint folyamatos ellenőrzés és felügyelet megvalósítása az elektonikus információs rendszerben, kivédendő ezen technológiák segítségével megvalósított károkozást.

(3) Ellenőrző és felügyelő rendszer alkalmazása VoIP eszközök tekintetében, valamint VoIP protokoll szűrése, monitorozása.

VI.13.5. Mobil informatikai tevékenység, távmunka (3.3.10.13. [3])

(1) Az Egyetem kidolgozza és dokumentálja minden engedélyezett távoli hozzáférés típusra a felhasználásra vonatkozó korlátozásokat, a konfigurálási vagy a kapcsolódási követelményeket és a megvalósítási útmutatókat, engedélyezési eljárást folytat le az elektronikus információs rendszerhez történő távoli hozzáférés feltételeként.

VI.13.5.1. Mobil informatikai tevékenység (3.3.10.15. [3])

(1) Az Egyetem belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre, és engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

VI.13.5.2. A távmunka (3.3.10.13. [3])

(1) Az elektronikus információs rendszer figyeli és ellenőrzi a távoli hozzáféréseket.

(2) A távoli hozzáférés során a kommunikáció a rendszer besorolásának megfelelő erősségű titkosított csatornán keresztül történik.
(3) Belső rendszerekhez nem közvetlenül, hanem felügyelt hoston - pl. terminál szerver által biztosított - keresztüli hozzáférés engedélyezett csak.

(4) IPSec (IKEv2) használata a VPN kiépítésekor, certificate alapú azonosítás és csatlakozás előtt állapot ellenőrzés (posture), pl. operációs rendszer frissítések megléte, végpontvédelem állapota, stb. A posture vizsgálat eredményeként a végpont vagy belépést kap a hálózatba, vagy egy karanténhálózatba kerül ahol a hiányosságok kiküszöböléséhez szükséges telepítések, módosítások elvégezhetők.

VI.13.6. Kriptográfiai eszközök (3.3.13.7.2. [4])

(1) Az elektronikus információs rendszer kriptográfiai mechanizmusokat alkalmaz az adatátvitel során az információk jogosulatlan felfedése ellen, kivéve, ha az átvitel más, az Egyetem által meghatározott alternatív fizikai ellenintézkedéssel védett.

(2) Kriptográfiai információvédelem alkalmazása nyílt csatornán történő kommunikáció esetében. A titkosításra használt protokollok, algoritmusok illetve az ezekhez szükséges kulcsok hosszának meghatározása nemzetközi szabványok (pl. NIST 800-53) alapján.

VI.13.6.1. Digitális aláírás

(1) Az Egyetem részéről, adatállományok, dokumentumok hitelességének, sértetlenségének megőrzése és biztosítására használt megoldás.

(2) Felhasználói azonosítás eszköze, ahol az akkreditálást a hitelesítés szolgáltató hitelesítő szervere hagy jóvá.

VI.13.6.2. Szolgáltatások a le nem tagadhatóságra

(1) A le nem tagadhatóság biztosítására automatikus, a felhasználó által nem befolyásolható rendszereket kell kialakítani.

VI.13.6.3. Nyilvános kulcsú infrastruktúra tanúsítványok (3.3.13.13. [4])

(1) Az Egyetem nyilvános kulcsú tanúsítványokat állít ki a belső hitelesítési rend szerint, vagy a nyilvános kulcsú tanúsítványokat beszerzi, a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatótól.

VI.13.6.4. Kriptográfiai védelem (3.3.13.11. [2])

(1) Az elektronikus információs rendszer szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg.

(2) Az Egyetem kizárólag biztos forrásból származó, szabvány vagy jogszabály alapján biztonságosnak ítélt mechanizmusokat megvalósító szoftvert alkalmaz.

VI.13.6.5. Kriptográfiai vagy egyéb védelem (3.3.13.8.2., 3.3.13.7.2. [4])

(1) Az elektronikus információs rendszer kriptográfiai mechanizmusokat (algoritmikus védelem –CRC-) alkalmaz az adatátvitel során az információk megváltozásának észlelésére, ha az átvitel nincsen más alternatív fizikai intézkedésekkel védve.

VI.13.7. Kulcsmenedzsment (3.3.13.10. [2])

(1) Az Egyetem előállítja és kezeli az elektronikus információs rendszerben alkalmazott kriptográfiához szükséges kriptográfiai kulcsokat a kulcsok előállítására, szétosztására, tárolására, hozzáférésére és megsemmisítésére vonatkozó belső szabályozásnak megfelelően.

(2) Dedikált szoftverrendszer alkalmazása a releváns és hatályos belső szabályzatainak megfelelően. Kulcs illetve tanúsítvány kiosztó rendszer mellé a HSM (Hardware Security Modul) eszköz, mint root tároló eszköz használata.

VI.13.7.1. A kriptográfiai kulcsok védelme

(1) A kriptográfiai kulcsok szabályozott használata érdekében az IBF-nek és az IT területek vezetőinek rendelkezniük kell a ***„Kriptográfiai eljárásrendben”*** a kulcsok használatáról, védelméről, életciklus kezeléséről.

VI.13.8. Folyamatok és maradványinformációk védelme (3.3.13.2. [4], 3.3.13.4. [4], 3.3.13.22. [2], 3.3.13.21. [4])

(1) Az elektronikus információs rendszer:
   a) elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az elektronikus információs rendszer irányítási funkcionalitásától;
   b) meggátolja a megosztott rendszererőforrások útján történő jogosulatlan vagy véletlen információáramlást;
   c) meghatározza a maradvány információk (pl.: átmeneti fájlok) bizalmasságát, sértetlenségét;
   d) elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.

(2) A háttér- és egyéb tárolók fizikai elvesztése, eltulajdonítása, jogosulatlanokhoz kerülése esetén, ahhoz hogy illetéktelenek ne juthassanak adathoz, információhoz, a háttértárakon full-disk-encryption megoldás kell alkalmazni (pl. BitLocker), egyéb tárolókon (szalagos mentések, egyéb backup tárolók) a teljes adatmennyiség titkosítása megfelelő erősségű titkosítással (pl AES).

(3) A végrehajtó folyamatok adatait, információit szeparálni kell annak érdekében, hogy egyik folyamat kompromittálódása esetén más folyamatok által kezelt információhoz ne lehessen hozzáférni.

VI.13.9. Külső kommunikációs szolgáltatások (3.3.13.6.3. [3], 3.3.13.19. [4])

(1) Az Egyetem:
   a) felügyelt interfészt (tűzfal, router) működtet minden külső infokommunikációs szolgáltatáshoz;
   b) minden felügyelt interfészhez forgalomáramlási szabályokat alakít ki;
   c) védi az összes interfésznél az átvitelre kerülő információk bizalmasságát és sértetlenségét;
   d) dokumentál minden kivételt a forgalomáramlási szabályok alól, a kivételt alátámasztó alapfeladattal és az igényelt kivétel időtartamával együtt;
   e) meghatározott gyakorisággal áttekinti a forgalomáramlási szabályok alóli kivételeket, és eltávolítja azokat a kivételeket, amelyeket közvetlen alapfeladat már nem indokol.

VII. INFORMATIKAI BIZTONSÁGI ELLENŐRZÉS

(1) Az Egyetem rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén biztosítja, hogy az elektronikus információs rendszereinek biztonsága megfeleljen a jogszabályoknak és a kockázatoknak.

(2) A biztonsági megfelelőség ellenőrzést legalább kétévente, új rendszer bevezetésekor biztonsági esemény incidens bekövetkezése esetén azonnal el kell végezni.

(3) Az időszakos vizsgálat módszertana:
   a) technikai szintű audit,
   b) működés-folytonossági és katasztrófa-elhárítási tesztek,
   c) informatikai rendszerek monitorozása,
   d) naplóelemzés.

(4) Az ellenőrzésnek ki kell terjedni:
   a) munkavállalók biztonsági ellenőrzésére,
   b) adminisztratív biztonságra,
   c) hardver-szoftver biztonságra,
   d) kommunikáció-biztonságra.

(5) Az ellenőrzés résztvevői:
   a) informatikai biztonsági felelős,
   b) adatvédelmi tisztviselő,
   c) informatikai üzemeltetés vezetői,
   d) IT üzemeltetést végző külső szolgáltató vezetői.

VIII. AZ IBSZ–HEZ FELHASZNÁLT JOGSZABÁLYOK, SZTENDERDEK, HAZAI AJÁNLÁSOK

Jogszabályok, sztenderdek:

1) 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)
2) 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv)
3) 2013. évi V. törvény a Polgári Törvénykönyvről (Ptk.)
4) 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
5) 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
6) 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
7) 246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
8) ISO/IEC MSZ 27001:2014 Informatika. Biztonságtechnika. Információbiztonsági irányítási rendszerek. Követelmények.
9) az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (a továbbiakban: GDPR).
10) Magyarország Alaptörvénye VI. cikk
11) 1997. évi XLVII törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről
12) 2011. évi CCIV törvény a nemzeti felsőoktatásról
13) 2012. évi I. törvény a munka törvénykönyvéről
14) 2011. évi CXC. törvény a nemzeti köznevelésről
15) 2009. évi CLV. törvény a minősített adat védelméről
16) 2012. évi C. törvény a Büntető Törvénykönyvről (magán titok 223. § és levéltitok 224. §, személyes adattal visszaélés 219. § és közérdekű adattal visszaélés 220. §)
17) 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről
18) Szabványok, ajánlások és egyéb kapcsolódó dokumentumok
19) Tanulmány anyagok (Euzert Kft., TÜV incidens menedzser képzés, TÜV RISK menedzser képzés)

Ajánlások, és egyéb kapcsolódó dokumentumok:

1) Magyar Informatikai Biztonsági Ajánlások (MIBA)
2) Magyar Informatikai Biztonsági Keretrendszer (MIBIK)
3) Informatikai Biztonság Irányítási Követelmények (IBIK)
4) Nemzeti Közszolgálati Egyetem, oktatási tematikák, tananyagok

IX. ZÁRÓ RENDELKEZÉSEK

(1) Jelen szabályzatban foglaltak megismerése annak személyi hatálya alá tartozó valamennyi személy (I/2. fejezet) számára kötelező. A szabályzat tudomásul vételét a dolgozó az információbiztonsági nyilatkozat aláírásával igazolja, vagy elektronikus oktatási rendszerben hitelt érdemlően rögzíti a tudomásul vételt.

(2) A jelen szabályzatban foglalt munkavállalói és felhasználói kötelezettségek a munkaviszonyból vagy szerződésből származó lényeges kötelezettségnek minősülnek, így amennyiben az Egyetem munkavállalója, partnere a jelen szabályzatban foglalt kötelezettségét szándékosan vagy súlyos gondatlansággal jelentős mértékben és bizonyíthatóan megszegi, az Egyetem jogosult a munkavállalóval szemben fegyelmi eljárást kezdeményezni illetőleg a szerződésben foglaltak szerinti kártérítésre jogosult.

(3) Azon kapcsolódó szabályzatok (eljárások), amelyekre jelen IBSZ hivatkozik (azonban nem képezik az IBSZ tartalmi részét), mellékletenként (függelékként) kapcsolódnak az IBSZ keretszabályzathoz. Az IBF feladata az elkészítésük, aktualizálásuk koordinálása a kötelező felülvizsgálatok alkalmával. Az eljárások státuszáról („készítés alatt”, „felülvizsgálandó”, „hatályos” stb.) az IBF-nek rendszeres időközönként tájékoztatnia kell a Kancellárt.

(4) A szabályzat megismerésére vonatkozó oktatás megszervezése és a dolgozók tudomásul vételének nyilvántartása az IBF feladata.

(5) Jelen szabályzatot a Debreceni Egyetem Szenátusa 2022. április 28-ai ülésén, a 24/2022 (IV. 28.) számú határozatával fogadta el. A szabályzat az elfogadását követő napon lép hatályba.

(6) Az elfogadást követő módosításokat lábjegyzetek jelzik.

Debrecen, 2022. április 28.

Dr. Bács Zoltán

kancellár

X. AZ IBSZ-HEZ TARTOZÓ DOKUMENTUMOK JEGYZÉKE

(1) IBSZ eljárásrendjei:

- Adathordozók védelmére vonatkozó eljárásrend
- Azonosítási és hitelesítési eljárásrend
- Biztonságelemzési eljárásrend
- Biztonságértékelési eljárásrend
- Biztonsági eseménykezelési eljárásrend
- Biztonságos fejlesztési követelmények eljárásrend
- Biztonságtervezési eljárásrend
- Engedélyezési és jogosultságkezelési eljárásrend
- Fizikai védelmi intézkedések eljárásrendje
- Hozzáférés ellenőrzési eljárásrend
- Információbiztonsági kockázatok kezelésének eljárásrendje
- Informatikai beszerzési eljárásrend
- Internet használati eljárásrend
- Katasztrófa elhárítási eljárásrend
- Kockázatelemzési és kockázatkezelési eljárásrend
- Konfigurációkezelési eljárásrend
- Kriptográfiai eljárásrend
- Mentési és archiválási eljárásrend
- Mobil eszközök használatának eljárásrend
- Naplózási és naplóelemzési eljárásrend
- Rendszer- és információsértetlenségre vonatkozó eljárásrend
- Rendszer- és kommunikációvédelmi eljárásrend
- Rendszer karbantartási eljárásrend
- Személybiztonsági eljárásrend
- Távoli hozzáférés engedélyezési, használati eljárásrend
- Tesztelési, felügyeleti és képzési eljárásrend
- Üzletmenet-folytonosságra vonatkozó eljárásrend
- Vírusvédelmi eljárásrend

MELLÉKLETEK

1. számú melléklet - Információbiztonsági Politika

2. számú melléklet a 41/2015. (VII. 15.) BM rendelethez
Az elektronikus információs rendszerrel rendelkező szervezetek vagy szervezeti egységek biztonsági szintbe sorolása.

1. számú melléklet - Információbiztonsági Politika

Az Egyetem vezetősége elkötelezett, hogy az Egyetem a működése és nyújtott szolgáltatásai területén a partnerei, ügyfelei és saját adatai védelmét, és az érdekelt felek információbiztonsági elvárásainak való folyamatos megfelelést meghatározó elemként kezeli. Az Egyetem által kezelt adatok és információk összessége kiemelt értéket képviselő vagyonelem, melyet védeni kell a különböző fenyegetések ellen, ezért az Egyetem törekszik, hogy e vagyonelemek tekintetében is időben állandóan megvalósuljon annak bizalmassága, sértetlensége, rendelkezésre állása.
Az Egyetem által nyújtott szolgáltatásokat magas színvonalon, modern és biztonságosan működő technológiával nyújtja, ahol felügyelt információbiztonsági folyamatokkal biztosítja a kezelt adatok, információk sértetlenségét, bizalmasságát és rendelkezésre állását.
Üzletmenet folytonosságának biztosítása és alapfeladatainak zavartalan ellátása érdekében minden szükséges információ- és adatvédelmi intézkedést megtesz, adatkezelési, információvédelmi folyamatait az adatvédelmi az információbiztonsági elvárásoknak megfelelően alakítja ki.
Az Egyetem működése és az általa nyújtott szolgáltatások teljesítése során elkötelezett a vonatkozó törvényi, valamint az irányadó szabványokban foglalt előírásoknak való maximális megfelelés iránt, így különösen az 41_2015. (VII. 15.) BM rendeletben meghatározott iránymutatásoknak való megfelelés iránt, azáltal, hogy magára nézve a hivatkozott törvényeket és szabványokat kötelezően alkalmazandónak ismeri el.
Az Egyetem vezetése az Információ Biztonsági Politikában (IBP) megfogalmazott elvek és követelmények teljesítését várja el az Egyetem összes munkatársától, beszállítóitól és minden egyéb érdekelt féltől. Az IBP hatálya kiterjed az Egyetem valamennyi folyamatára és szervezeti egységére, így különösen az Egyetem elektronikus információs rendszereire, mely magában foglalja az adathordozókat, alkalmazásokat, szoftvereket, hardver elemeket, a környezeti infrastruktúra elemeit és objektumait, a papír alapú dokumentumokat, továbbá minden eljárására, melyek hatással lehetnek az Egyetem adatvagyonára.
Az Egyetem információbiztonságának folyamatos magas színvonalú fenntartása érdekében az alábbi alapelvek figyelembe vételével információbiztonsági irányítási rendszert (IBIR) vezet be és üzemeltet.
Az IBIR célja, hogy biztosítsa az Egyetem kezelésében lévő adatvagyon bizalmasságát, sértetlenségét és rendelkezésre állását, valamint az elektronikus információs rendszerek elemeinek sértetlenségét és rendelkezésre állását veszélyeztető, mindenkori fenyegetések kockázataival arányos, zárt, teljes körű és folyamatos, a rendszerek telje életciklusára kiterjedő védelmét logikai, fizikai és adminisztratív védelmi intézkedések bevezetésével.

Az Egyetem az információ biztonság területén az alábbi alapelveket érvényesíti:

1. **Bizalmasság:** az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

2. **Sértetlenség:** a tárolt adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség), a származás ellenőrizhető, megállapítható (letagadhatatlanság), illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

3. **Rendelkezésre állás:** az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatók.

4. **A védelem teljes körűsége:** az erre vonatkozó alapelvet a fizikai, a logikai és az adminisztratív védelem területén a következő három dimenzióban kell érvényesíteni:
    a) az összes rendszerelemre;

b) a rendszerek architektúrájának összes rétegére mind az informatikai infrastruktúra, mind az alkalmazások szintjén;
c) a központi, illetve a végponti informatikai eszközökre és környezetükre.

5. **A védelem zártsága:** az összes valószínűsíthető fenyegetés elleni megelőző védelmi intézkedés végrehajtása megtörténik, és azok összességükben szabályozott és szerves egészet alkotnak.

6. **A védelem kockázatarányossága:** a védelem mértéke és költségei a felmért kockázatokkal arányosak. Cél a szükséges és elégséges védelmi költséggel elért maximális védelmi képesség.

7. **A védelem folyamatossága:** a kialakított védelmi intézkedések az időben állandóan változó biztonsági környezet és viszonyok mellett is megszakítás nélkül fennállnak a rendszer teljes életciklusa alatt.

Az Információbiztonsági politika (IBP) szerepe

Az információbiztonság az Egyetem életében az informatika nélkülözhetetlenné válásával egyre határozottabban jelenik meg. Ma már nem az a kérdés kell-e, hanem hogy miként lehet a leggazdaságosabban megvalósítani, a leghatékonyabban működtetni.
Ez csak úgy lehetséges, ha az Információbiztonsági Politika:

a) Az első számú vezető elkötelezettségét élvezi és támogatja minden érintett vezető,
b) Az Egyetem egyéb terveivel összhangban, a többi biztonsági területtel (Vagyonbiztonság, Üzembiztonság) szinergiában valósítják meg és működtetik,
c) Ha kellőképpen kommunikált, oktatott,
d) Beépül a szervezet mindennapi életébe, a működési folyamatokba,
e) Része a szervezeti kultúrának, a dolgozók tudatos viselkedésének,
f) A biztonsági intézkedések, funkciók működése ellenőrzött és visszacsatolt, a hiányosságok szankcionáltak,
g) A szervezetben megfelelően képviselik az információ biztonság kérdését, van kijelölt szerepkör, szervezeti egység a menedzselésére.

Az információbiztonsági politika célja

a) Az Egyetem informatikai rendszerei által kezelt információk hitelességének, sértetlenségének, rendelkezésre állásának, funkcionalitásának megőrzésére és fenntartására irányuló intézkedések bevezetése.
b) Az ügyfél, partneri, munkatársi, szerződéses, és egyéb üzleti információk bizalmasságának megőrzése, különös tekintettel az ügyfelek bizalmas adatainak biztonságos kezelésére.
c) Az ügyfeleknek biztosított szolgáltatások jól definiált és magas minőségű információbiztonságának folyamatos biztosítása.
d) Az alkalmazott támogató informatikai, illetve információtechnológiai rendszerek információbiztonságának, illetve információtechnológiai biztonságának fenntartása, beleértve a jogszabályi követelmények előírásainak megfelelő biztosítását is.
e) Az ügyfeleknek nyújtott szolgáltatások üzemeltetése és fejlesztése érdekében alkalmazott támogató folyamatokra, illetve információtechnológiai rendszerekre vonatkozó mindenkori jogszabályi és egyéb szabályozási követelményeknek való megfelelőség folyamatos biztosítása.

Az IBP célja, hogy irányelveket adjon a biztonságért felelős vezető részére a biztonsági politikánál alacsonyabb szintű szabályozások kialakításához, a jelen és jövőbeli informatikai biztonsági döntéseik meghozatalához, illetve a biztonsági rendszer működtetői és a felhasználók számára a napi rendeltetésszerű tevékenységük gyakorlásához.

Az Egyetem a célok eléréséhez és fenntartásához alapvető eszköznek tekinti;

a) A szervezeti, üzleti és szolgáltatás működés folyamatos fejlesztését, a korszerű technológiák bevezetését, és alkalmazását;
b) A szolgáltatások folyamatos fejlesztését a szabályozási követelmények, az ügyfelek és a piac igényei alapján;
c) Folyamatos továbbképzéssel a legmagasabb szakmai kompetencia vagy színvonal elérését;
d) A feladatok és megbízások elvégzéséhez szükséges erőforrások felmérését és biztosítását;
e) Megfelelő és megbízható beszállítók, alvállalkozók kiválasztását és alkalmazását, amelyek elfogadják és teljesítik az információbiztonsági követelményeket;
f) A munkavégzés során – törekvéseink ellenére is - bekövetkező hibák kijavítását;
g) A tevékenységekre vonatkozó szakmai, adat- és információvédelmi, és egyéb jogszabályi követelmények – és ezek változásainak – folyamatosan figyelemmel kísérését, és azok maradéktalan betartását;
h) A védendő ügyfél és saját információs-, illetve adatvagyon fenyegetettségének és azok biztonsági kockázatainak rendszeresen, legalább évente történő felülvizsgálatát és újraértékelését, majd ennek megfelelően az információvédelmi előírások és eljárások aktualizálását;
i) A szolgáltatások feltételeinek folyamatos biztosításához a következő – kiemelkedő kockázatúnak értékelt – incidens kategóriák elfogadhatatlannak tartását és legnagyobb veszélynek értékelését:
    - az ügyfelek adatainak beleegyezés nélküli nyilvánosságra kerülése;
    - adatvesztések, amelyek mentésekből nem állíthatók vissza;
    - hálózati betörés a támogató és szolgáltató informatikai, információtechnológiai rendszerekbe.

2. számú melléklet a 41/2015. (VII. 15.) BM rendelethez

Az elektronikus információs rendszerrel rendelkező szervezetek vagy szervezeti egységek biztonsági szintbe sorolása.

1. Az érintett szervezet biztonsági szintje 1.,

ha a szervezet nem üzemeltet és nem fejleszt elektronikus információs rendszert, és saját hatáskörben erre más szervezetet vagy szolgáltatót (ide nem értve a telekommunikációs szolgáltatót) sem vesz igénybe. Az adatfeldolgozás módját nem maga határozza meg, az adatkezelés tekintetében technikai vagy információtechnológiai döntést nem hoz, a használt elektronikus információs infrastruktúra kialakítása tekintetében döntési jogköre - ide nem értve a szervezet munkavégzését érintő informatikai rendszerelemek elhelyezését - nincs, egyedi adatokat és információkat kezel vagy dolgoz fel, és kritikus adatot nem kezel. A szervezet információbiztonsági tevékenysége elsődlegesen az elektronikus információs rendszerrel kapcsolatba kerülő személyek információbiztonsággal kapcsolatos kötelezettségeinek szabályozására, számonkérésére terjed ki, addig a mértékig, ameddig a szervezet vagy az egyes személyek tevékenysége az elektronikus információs rendszerre hatást tud gyakorolni.

1.1. Az 1. biztonsági szervezeti szint követelményei:

1.1.1. az érintett szervezet az érintett személyi kör részére biztosítja az 1.1.3. pont szerinti szervezeti vagy feladathoz rendelt működési terület hatályos információbiztonságot érintő munkautasítását, belső rendelkezését, szabályozását vagy más erre célra szolgáló dokumentumot (a továbbiakban együtt: szabályzat);

1.1.2. az informatikai biztonsági szabályzat része a folyamatos kockázatelemzési eljárás, amely tartalmazza a beépített ellenőrzési pontokat;

1.1.3. az informatikai biztonsági szabályzat vonatkozhat egész szervezetre és működési területére, vagy meghatározott vagyonelemre vagy szervezeti egységre;

1.1.4. a informatikai biztonsági szabályzatot a szervezetre érvényes rendelkezések szerint az erre jogosult vezetőnek kell jóváhagynia;

1.1.5. a informatikai biztonsági szabályzat tartalmazza az információbiztonság felügyeleti rendszerét, az információbiztonsággal kapcsolatos kötelezettségeket és felelősségeket;

1.1.6. az informatikai biztonsági szabályzat be nem tartása jogkövetkezményt von maga után.

2. Az érintett szervezet biztonsági szintje 2.,

ha a szervezet vagy szervezeti egység az 1. szinthez rendelt jellemzőkön túl olyan elektronikus információs rendszert használ, amely személyes adatokat kezel, és a szervezet jogszabály alapján kijelölt szolgáltatót vesz igénybe.

2.1. A 2. biztonsági szervezeti szint követelményei az 1. szinthez rendelt követelményeken túl:

2.1.1. az érintett szervezet biztonsági kontrollfolyamatai eljárásrendben szabályozottak;

2.1.2. a 2.1.1. pont szerinti eljárásrend tartalmazza a kontrollfolyamatok végrehajtásának menetét, módját, időpontját, végrehajtóját, tárgyát, eszközét;

2.1.3. az egyes folyamatok egyértelműen meghatározzák az információbiztonsági felelősségeket és a biztonságtudatos viselkedést az elektronikus információs rendszerrel kapcsolatba kerülő személyek, valamint az információbiztonságért felelős személyek és szervezeti egységek tekintetében;

2.1.4. az egyes folyamatokat szervezeti egységek vagy személyek felügyelete alá kell rendelni, akik az adott folyamat végrehajtása érdekében közvetlen kapcsolatban állnak a folyamatban érintett más személyekkel vagy szervezeti egységekkel;

2.1.5. a folyamatokat és végrehajtásukat úgy kell dokumentálni, hogy abból az elvégzett kontroll tevékenység - ideértve annak egyes jellemzőit, így különösen mélységét, érintett személyi és tárgyi körét - megállapítható legyen.

3. Az érintett szervezet biztonsági szintje 3.,

ha a szervezet vagy szervezeti egység a 2. szinthez rendelt jellemzőkön túl szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt. A szervezet kritikus adatot, nem minősített, de nem közérdekű, vagy közérdekből nyilvános adatot kezel, központi üzemeltetésű, és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszerek vagy zárt célú elektronikus információs rendszer felhasználója, illetve feladatai támogatására más külső szolgáltatót vesz igénybe.

3.1. A 3. biztonsági szervezeti szint követelményei a 2. szinthez rendelt követelményeken túl:

3.1.1. az érintett szervezet a biztonsági kontroll folyamataiba bevonja, és feladataikról, a velük szemben támasztott elvárásokról tájékoztatja a folyamatokban résztvevő személyeket;

3.1.2. a 3.1.1. pont szerinti folyamatokat az érintett szervezet vagy szervezeti egység tekintetében szabályozottan és ellenőrizhető módon kell bevezetni, az érintett személyek számára oktatás tárgyává tenni;

3.1.3. a 3.1.1. pont szerinti folyamatok nem alkalmazandók egyéni vagy eseti eljárásokra;

3.1.4. a 3.1.1. pont szerinti folyamatokat a szervezetre érvényes rendelkezések szerint erre jogosult vezetőnek kell jóváhagynia;

3.1.5. a 3.1.1. pont szerinti folyamatok előzetes tesztelésével biztosítani kell a folyamatok előre meghatározott követelmények szerinti működését;

3.1.6. a szervezetnek rendelkeznie kell információbiztonsági költség- és haszonelemzési módszertannal.

4. Az érintett szervezet biztonsági szintje 4.,

ha a szervezet vagy szervezeti egység a 3. szinthez rendelt jellemzőkön túl elektronikus információs rendszert vagy zárt célú elektronikus információs rendszert üzemeltet vagy fejleszt.

4.1. A 4. biztonsági szervezeti szint követelményei a 3. szinthez rendelt követelményeken túl:

4.1.1. az üzemeltetési vagy fejlesztési tevékenységbe épített rendszeres, előre meghatározott tesztekkel biztosítani kell az üzemeltetés vagy fejlesztés információbiztonsági intézkedéseinek hatékonyságát és megfelelőségét;

4.1.2. tesztelési eljárásban rögzítetten biztosítani kell minden szabályozási folyamat és kontroll működését az elvárt és előre meghatározott információbiztonsági követelmények szerint;

4.1.3. azonnali és eredményes, előre meghatározott biztonsági intézkedéseket kell bevezetni a feltárt vagy bekövetkezett biztonsági események kezelésére, beleértve az eseménykezelő központok, a beszállítók vagy egyéb megbízható forrás jelzése alapján lehetséges vagy bekövetkezett biztonsági esemény kezelését is;

4.1.4. folyamatba épített rendszeres belső értékelés alá kell vonni az egyes információ, rendszer vagy alkalmazás biztonsága érdekében bevezetett intézkedések megfelelőségét és hatékonyságát, mely belső értékelések részben, vagy egészben történhetnek alvállalkozók vagy más, erre feljogosított, vagy a szerv felett felügyelet gyakorló szerv bevonásával;

4.1.5. a szervezet folyamatba épített belső értékelései nem helyettesíthetőek;

4.1.6. a 4.1.3. pont szerinti forrásból származó, potenciális vagy a valódi biztonsági eseményekkel és biztonsággal kapcsolatos információk, vagy riasztások alapján tesztelési eljárást vagy biztonsági ellenőrzést kell végezni;

4.1.7. a tesztelés értékelése alapján megállapított követelményeket, - beleértve a tesztelés típusával és gyakoriságával kapcsolatos követelményeket is - dokumentálni kell, az arra jogosulttal jóvá kell hagyatni és be kell vezetni;

4.1.8. az egyedi kontroll eljárások tesztelésének gyakoriságát és mélységét ahhoz kell igazítani, hogy milyen biztonsági kockázattal jár a kontrollok nem megfelelő működése.

5. Az érintett szervezet biztonsági szintje 5.,

ha a szervezet vagy szervezeti egység a 4. szinthez rendelt jellemzőkön túl európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek elektronikus információs rendszereinek üzemeltetője, fejlesztője, illetve az információbiztonsági ellenőrzések, tesztelések végrehajtására jogosult szervezet vagy szervezeti egység.

5.1. Az 5. biztonsági szervezeti szint követelményei a 4. szinthez rendelt követelményeken túl:

5.1.1. biztosítani kell az információbiztonsági kontrollfolyamatoknak a szervezet alapfeladataiba történő beépítését;

5.1.2. biztosítani kell a szabályzatok, tesztelési eljárások, biztonsági folyamatok folyamatos felülvizsgálatát és továbbfejlesztését;

5.1.3. a szervezetnek rendelkeznie kell át fogó információbiztonsági programmal, amely szerves része a szervezet feladatellátásnak és biztosítja a személyi állomány biztonságtudatosságának növelését;

5.1.4. a szervezet személyi állományának rendelkeznie kell információbiztonsági operatív képességgel és a feladat elvégzéséhez szükséges szaktudással;

5.1.5. a biztonsági sérülékenységek felismerésének és kezelésének képességét a szervezet egésze tekintetében meg kell valósítani;

5.1.6. a fenyegetettségek folyamatos újraértékelésével, a kontrollfolyamatok felülvizsgálatával nyomon kell követni információbiztonsági környezet változását;

5.1.7. az információbiztonságot érintő külső vagy belső környezeti változásokra figyelemmel további információbiztonsági alternatívákat kell meghatározni;

5.1.8. a szervezetnek ki kell alakítania az információbiztonsági képesség- és állapotmérési és értékelési módszertanát, meg kell határozni annak mutatóit és az 5.1.7. pont szerinti esetben aktualizálnia kell azt.